ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS E INFORMÁTICA

AUTORES:

BASANTES SALAZAR, CÉSAR ANDRÉS

SANCHEZ HERRERA, KATHERINE ELIZABETH

TEMA: "ANÁLISIS FORENSE A SISTEMAS OPERATIVOS MEDIANTE LA UTILIZACIÓN DE HERRAMIENTAS OPEN SOURCE, CASO DE ESTUDIO WINDOWS 8"

DIRECTOR: ING. GERMÁN ÑACATO

martes, 19 de Abril de 2016

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

CERTIFICACIÓN

Certifico que el trabajo de titulación **"Análisis Forense a Sistemas Operativos mediante la utilización de herramientas Open Source, caso de estudio Windows 8"**, realizado por, Katherine Elizabeth Sánchez Herrera y César Andrés Basantes Salazar, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas por la Universidad de las Fuerzas Armadas ESPE, en el Reglamento de Estudiantes de la Universidad de las Fuerzas Armadas – ESPE. Debido a la originalidad del trabajo y su aplicabilidad, se recomienda su publicación.

Sangolquí, 18 de Abril del 2016

Ing. Germán Ñacato
DIRECTOR

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORÌA DE RESPONSABILIDAD

Nosotros, Katherine Elizabeth Sánchez Herrera con CI: 1721540860 y César Andrés Basantes Salazar con CI: 1721876215, declaramos que este trabajo de titulación **"Análisis Forense a Sistemas Operativos mediante la utilización de herramientas Open Source, caso de estudio Windows 8",** ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan el pie de las páginas correspondiente, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente declaramos que este trabajo es de nuestra autoría, en virtud a ello nos declaramos responsables del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 18 Abril del 2016

Katherine Elizabeth Sánchez Herrera
C.C. 1721540860

César Andrés Basantes Salazar
C.C. 1721876215

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORIZACIÓN

Nosotros, **KATHERINE ELIZABETH SÁNCHEZ HERRERA Y CÉSAR ANDRÉS BASANTES SALAZAR**, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación, **"ANÁLISIS FORENSE A SISTEMAS OPERATIVOS MEDIANTE LA UTILIZACIÓN DE HERRAMIENTAS OPEN SOURCE, CASO DE ESTUDIO WINDOWS 8",** cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, 18 de Abril 2016

Katherine Elizabeth Sánchez Herrera
C.C. 1721540860

César Andrés Basantes Salazar
C.C. 1721876215

Katherine Elizabeth Sánchez Herrera
C.C. 1721540860

César Andrés Basantes Salazar
C.C. 1721876215

AGRADECIMIENTO

A Dios quien me ha dado la fortaleza necesaria para continuar, guiándome por el camino correcto y ayudándome a aprender de mis errores.

A mi familia, por su amor y apoyo incondicional a lo largo de mi vida y mi carrera;

A todos mis profesores, especialmente al Ing. German Ñacato, quien en todo momento fue amigo e impulsor para la elaboración de este proyecto; y,

A mi compañero de trabajo de titulacion y mejor amigo por su dedicación, apoyo y conocimientos para la realización de este trabajo.

KATHERINE SANCHEZ H.

AGRADECIMIENTO

En primer lugar a mi familia, mi MADRE Martha Salazar, mi PADRE César E. Basantes, mi HERMANO Steven Basantes, quienes siempre me han dado la fuerza y apoyo incondicional lo cual me ha llevado donde estoy ahora;

A mi TÍA Alba Basantes quien con mucho esfuerzo me apoyó cuando más lo necesite económicamente para poder continuar mi carrera;

A todos mis profesores, especialmente al Ing. German Ñacato, quien me impulsó para elaborar este proyecto y me guió a lo largo de todo el proceso; y,

A mi compañera de trabajo de titulación y mejor amiga por su dedicación, apoyo y conocimientos que hicieron posible la realización de este trabajo.

CÉSAR BASANTES S.

DEDICATORIA

A mis padres, por su amor, apoyo y sacrificios en todos estos años, gracias a ustedes soy la persona que hoy en día soy y son ustedes quienes han dado razón a mi vida. Son los mejores padres.

A mis hermanas, por siempre estar a mi lado haciéndome reír en momentos duros y ayudándome cuando siempre lo necesite. Son mi pilar fundamental y un ejemplo a seguir.

A mis pequeñas Anaid y Aimee, por alegrar mi vida simplemente por existir, iluminan mi vida con su sola sonrisa. Son lo más lindo de mi vida.

A mi familia, tíos, tías, primos y primas que siempre estarán en mi corazón y agradezco cada consejo y apoyo en todo momento.

A mi mejor amigo César, quien durante años ha sido mi amigo, confidente, hermano y de gran apoyo mutuo en todo momento. Gracias por tantas experiencias vividas juntos.

Aquellas personas maravillosas que están en mi vida con el propósito de hacerme feliz.

KATHERINE SANCHEZ H.

DEDICATORIA

A mis padres, por su amor, apoyo, paciencia y sacrificios en todos estos años, lo cual me ha convertido en la persona que soy ahora.

A mi hermano Steven, por siempre haber estado a mi lado en las buenas y en las malas, por haberme dado la fortaleza de seguir adelante en los momentos más difíciles de nuestras vidas.

A mis pequeños hermanos Mishelle y Alan, a quienes espero servir de ejemplo y tener la oportunidad apoyarles siempre en sus vidas.

A mi novia Fernanda, por siempre estar ahí apoyándome e impulsándome para seguir adelante y lograr mis metas, gracias por todo este tiempo tu comprensión y gracias por ser mi amiga, mi compañera, mi gran amor, mi todo. Eres lo mejor que me ha pasado en la vida.

A mi gran amiga y casi hermana Kathy, por todos estos años de amistad y por tantas experiencias vividas juntos las cuales las llevo siempre presentes. Te agradezco por siempre estar ahí y sabes que cuentas conmigo siempre.

CÉSAR BASANTES S.

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

En la actualidad el mundo se encuentra en medio de una nueva Era Digital, la tecnología avanza tanto que ha llegado a formar parte de nuestro día a día en actividades como, ocio, educación, comunicación, salud, negocios, etc. Sin embargo conjuntamente con estos avances también la delincuencia ha buscado la forma de adaptarse al medio, y recientemente en la última década, la informática forense ha tomado gran importancia a nivel mundial, los gobiernos han implementado leyes que castiguen este tipo de delitos pero al igual que en cualquier delito se necesita pruebas, un análisis minucioso y a fondo que permita encontrar un culpable, como se llevó a cabo el delito y poder tomar acciones preventivas en base a estos casos. En el mercado se puede encontrar muchas herramientas válidas para este tipo de tareas sin embargo hablando de Windows 8 que es un sistema privativo, muchas de estas herramientas son privadas y para su uso se debe adquirir una licencia por un lapso de tiempo establecido. El presente trabajo de titulación desarrolla una propuesta para el uso de herramientas Open Source aplicando adecuadamente las fases de un análisis forense y basado teóricamente en las mejores prácticas de la informática forense.

Palabras Clave

INFORMÁTICA FORENSE

OPEN SOURCE

WINDOWS 8

CADENA DE CUSTODIA

CYBER-CRIMEN

ABSTRACT

Nowadays the world is in the middle of a new digital era, technology advances so much that has become part of our day to day activities such as entertainment, education, communication, health, business, etc. Nevertheless together with these advances also crime has found new ways to adapt to the environment, and recently in the last decade, computer forensics took importance globally, governments have implemented laws that punish such crimes but any crime needs evidence, and a meticulous and thoroughly analysis which help to find the guilty, how it was done and take corrective and preventive actions on the basis of these cases. In the market you can find many valid tools for these tasks however talking about Windows 8 which is a proprietary system, many of these tools are private and for use must acquire a license for a set time period. This thesis develops a proposal for the use of Open Source tools properly applying the phases of a forensic analysis and theoretical based on the best practices of computer forensics.

Key Words

COMPUTER FORENSICS

OPEN SOURCE

WINDOWS 8

CHAIN OF CUSTODY

CYBER-CRIME

CAPÍTULO 1

INTRODUCCIÓN

1.1. Antecedentes

Hoy en día la era digital, de la cual en el pasado se habló con mucho escepticismo ya es una realidad y parte del día a día de cada persona, los datos de las personas se encuentran almacenados digitalmente disponibles para diferentes plataformas y usos, desde el registro de una compra en un supermercado hasta la información de registro civil del gobierno. Además nuestra vida es guardada y utilizada digitalmente en nuestros computadores y dispositivos móviles, fotografías, archivos personales, agenda, contactos, videos, información confidencial e importante, todo esto con el fin de optimizar el almacenamiento y procesamiento de datos.

Pero qué pasa cuando esa información es vulnerada, y utilizada de forma perjudicial para nosotros o para terceros en delitos como: sustracción de información, clonación de tarjetas, fraude, hostigamiento, acoso sexual, terrorismo virtual entre otros.

Siguiendo el proceso más lógico y haciendo un símil a una situación parecida ¿qué hacer frente a un crimen común?, Se debe llevar a cabo una rigurosa investigación para determinar ¿qué es lo que pasó?, ¿cómo pasó? ¿Qué afectaciones o consecuencias tuvo este delito?, y ¿de qué forma se puede prevenir delitos similares a futuro?

La problemática antes mencionada hace que surja la necesidad de aplicar la informática forense, como herramienta y medio para resolver hechos delictivos,

mediante el análisis forense e identificar cuáles son las vulnerabilidades en nuestros sistemas y aplicar las estrategias necesarias para mitigar estos riesgos, haciendo uso de herramientas de software adecuadas.

Dentro del procedimiento para realizar un análisis forense, se debe contar con una infraestructura informática apta para tal análisis es decir el estudio de cualquier componente que tenga una memoria informática. Se parte de un estudio preliminar del caso que va a ser evaluado, se obtiene la información y los datos más relevantes para realizar el análisis del mismo, culminando con la elaboración del informe.

En este caso se propone el estudio puntual de la aplicación de software libre para el análisis forense sobre Windows 8.

1.2. Importancia y justificación

Los sistemas operativos evolucionan conforme pasa el tiempo, integrando poco a poco las funcionalidades y herramientas que han hecho más fácil el trabajo del ser humano, como: acceso a Internet, videoconferencias, cámara, capacidad de almacenamiento entre otros.

Sus ventajas son grandes, pero al mismo tiempo estas ventajas son utilizadas para cometer un sin número de actos delictivos como: fraudes, acoso, tráfico de drogas y otros. Toda la información que un sistema operativo guarda puede ser utilizada como evidencia para resolver un caso y aporta.

El objetivo principal de la informática forense es asegurar la integridad de la información y de los aplicativos, además de la generación de pruebas que van ayudar en un tribunal para resolver un caso. La ciencia forense es en realidad el proceso de

utilizar el conocimiento científico con el propósito de recolectar, analizar, y lo más importante presentar la evidencia en el tribunal de justicia. Esta nace debido a la preocupación por proteger la información, cuyo valor en estos últimos años ha aumentado, implementando estrategias y políticas de prevención, reacción y corrección a los problemas que pudiera presentarse y afectar a los sistemas informáticos.

Es necesario que cada uno de los países comiencen a reconocer el valor que tiene la información y con esto crear leyes que penalicen a las personas que hagan uso indebido y mal intencionado de la información, de esta manera vamos a garantizar que el análisis forense informático sea exitoso.

1.3. Planteamiento del problema

Los sistemas operativos evolucionan con el pasar del tiempo a tal punto que hoy en día son un medio necesario para procesar, almacenar y trasmitir datos, lo que los convierte en instrumentos de apoyo básicos en las actividades de las personas o es más objetivo decir en los instrumentos usuales como computadores personales, teléfonos inteligentes, cámaras digitales, tabletas, relojes táctiles, etc. Esto le permite al usuario: crear, actualizar y procesar gran cantidad de información electrónica de diversos tipos en tiempo real.

Hoy en día es común que la comunicación interpersonal sea por medios electrónicos y este intercambio de información puede ser muy beneficioso para varios propósitos, sin embargo es muy susceptible de caer en manos malintencionadas y causar daños de pequeña o gran proporción con consecuencias que afectan a nivel personal, económico y legal. Esto debido a la falta de conocimiento sobre el uso y

manejo seguro de la información personal. Un ejemplo común de esto, es la publicación de fotos en Internet, las cuales han sido tomadas furtivamente y sin permiso del dueño; o la modificación de algún documento importante.

Los daños producidos por los delitos efectuados usando las tecnologías de la información y comunicación, son frecuentemente de impacto considerable sobre los usuarios. Muchos son delitos ya catalogados como tales por la ley, pero con la cualidad de que un sistema operativo fue el "arma" utilizada para llevar a cabo de manera exitosa el delito. Bajo este escenario, y partiendo de la premisa de que el sistema operativo fue utilizado como instrumento activo, indudablemente existe una evidencia digital, que debe ser obtenida y analizada. Por ello, se requiere de profesionales que cuenten con la habilidad y los conocimientos para hacer frente a delitos que involucran el uso de la tecnología de información.

Ante este complejo escenario, se pueden puntualizar las siguientes interrogantes: ¿Cómo es posible obtener, manejar y analizar adecuadamente la evidencia digital almacenada en los sistemas operativos que han sido utilizados para cometer un delito? A partir de la evidencia analizada, ¿Es posible auxiliar a los sistemas legales en contra de estos delitos? ¿Existe alguna metodología para tratar la evidencia digital almacenada en los equipos? ¿Cuáles son las herramientas existentes para el manejo de evidencia almacenada en los dispositivos de almacenamiento? ¿Qué tan efectivas son las herramientas OPEN SOURCE para el análisis forense de un sistema privativo? ¿Qué correcciones se tomaron a comparación de las versiones anteriores de Windows 8 en cuanto a seguridad para hacer frente a los cyber-delitos?

1.4. Delimitación del tema

Windows 8 es una versión de Microsoft Windows, línea de sistemas operativos producida por Microsoft Corporation. Esta versión está diseñada para uso en PC, incluyendo equipos de escritorio en hogares y oficinas, equipos portátiles, tablet PC, notebooks y equipos media center.

El sistema operativo gestiona los recursos de hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes.

El alcance de este trabajo de titulación es realizar un análisis forense formal de los procesos que hacen referencia a la recuperación de la información, comprobación de hardware, análisis de procesos en ejecución y auditoria de inicio de sesión en sistemas operativos tomando como caso de estudio un ejemplo de desastre informático en Windows 8, con el fin de evaluar y revelar resultados aceptables que genere cada proceso de análisis con la ayuda de la utilización de varias herramientas Open Source.

Se abarcará los siguientes aspectos:

- Conocer y aplicar los conceptos de análisis de evidencia digital.
- Identificación de técnicas de recolección de evidencia digital.
- Manejo de herramientas de software libre para el óptimo análisis de evidencias.
- Realizar análisis informático forense sobre un caso práctico en Windows 8.

1.5. Objetivos

1.5.1. General

Realizar una guía metodológica que permita analizar y reconstruir la evidencia en sistemas operativos como Windows 8, con el uso de técnicas de análisis forense,

aplicando herramientas Open Source con el fin de entregar un informe formal, necesario para la ejecución de un proceso judicial.

1.5.2. Específicos

- Identificar las aplicaciones Open Source que se encuentran disponibles para realizar el análisis forense.
- Estudiar las metodologías de análisis forenses más aceptados en la actualidad para ser utilizados como guía principal para la elaboración de un informe forense formal.
- Estudiar las leyes que se encuentran vigentes en Ecuador, que nos permita identificar y analizar las evidencias que serán utilizadas como prueba judicial.
- Realizar un análisis informático forense tomando como caso práctico el sistema operativo Windows 8.

CAPÍTULO 2

MARCO LEGAL Y TEÓRICO

2.1. Marco legal

Desde que en 1999 en el Ecuador se puso en el tapete de la discusión el proyecto de ley de comercio electrónico, mensajes de datos y firmas electrónicas, desde ese tiempo se puso de moda el tema, se realizaron cursos, seminarios, encuentros. También se conformó comisiones para la discusión de la ley y para que formulen observaciones a la misma por parte de los organismos directamente interesados en el tema como el CONATEL, la Superintendencia de Bancos, las Cámaras de Comercio y otros. (Acurio Del Pino, 2012)

A partir de esto se tienen las siguientes leyes:

CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR – 2008

El Art. 66 determina en los numerales 19 y 20 que "reconoce y garantiza a las personas el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección" y "reconoce a los ciudadanos su derecho a la protección de sus datos, es decir nadie puede invadir la vida privada de los individuos". Al estar garantizado este derecho en la Carta Magna se convierte en deber primordial del Estado a través de los organismos competentes evitar cualquier tipo de delito informático y de ocurrir sancionarlo con la severidad del caso. (Constitucional, 2008)

Ley de comercio electrónico, firmas electrónicas y mensajes de datos

La ley de comercio electrónico, firmas digitales y mensaje de datos fue publicada en el Registro Oficial N° 557 del 17 de abril del 2002 en el que se dispone que los mensajes de datos tendrán, igual valor jurídico que los documentos escritos. La ley contiene los principios jurídicos que regirán las transmisiones de los mensajes de datos. Se le concede pleno valor y eficacia jurídica a los mensajes de datos, tanto a su información como a su contenido general; la interpretación de la ley y el ejercicio de la propiedad intelectual se rigen por la legislación ecuatoriana y por los tratados internacionales incorporados al cuerpo legal ecuatoriano. Se protege la confidencialidad de los mensajes de datos en sus diversas formas, señalando lo que se entenderá por tal concepto y su violación. Se equipara el documento escrito con el documento electrónico para el caso en que se requiera la presentación de un documento escrito, procediendo de igual manera con el documento original y la información contenida en él, siempre y cuando exista garantía de su conservación inalterable. (Constitucional, 2008)

Código orgánico integral penal (COIP)

Que fue publicado el lunes 10 de febrero de 2014 Registro Oficial Nº 180 cuerpo legal en el que se introdujeron ciertos delitos informáticos con su respectiva sanción estando estas contenidas en la SECCIÓN TERCERA Delitos contra la seguridad de los activos de los sistemas de información y comunicación esto a partir del artículo 229 hasta el artículo 235. (Constitucion, 2014)

- **El Artículo 229 determina acerca de la revelación ilegal de base de datos** sanciona el cometimiento de este delito con pena privativa de la libertad de uno a tres años sea que el cometimiento del mismo fuere realizado en provecho propio de quien lo comete o de un tercero realizando de una manera voluntaria e intencionada la violación del secreto contenido en una base de datos o cualquier otro medio semejante ya sea este electrónico o informático, endureciéndose la pena si el delito fuera cometido por un servidor público o por empleados bancarios que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años. (Constitucional, 2008)
- **El Artículo 230 que hace referencia a la interceptación ilegal de datos** establece la sanción con pena privativa de libertad de tres a cinco años: Las personas que sin orden judicial previa, intercepten, escuchen, desvíen, graben u observen, un dato informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. Las personas que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, Software malicioso que busque de tal manera inducir a una persona a ingresar a una dirección o sitio de web diferente a la que quiere acceder ya sea este un servicio financiero, pago electrónico o cualquier otro sitio personal o de confianza. De la misma manera es el numeral 3 del mismo artículo se establece la protección de la clonación de tarjetas que contengan cintas magnéticas de datos y a la vez el numeral 4 sanciona a la persona que facilite la comisión del delito contenido en el numeral 3. (Constitucional, 2008)

- **El Artículo 231 que se refiere a la transferencia electrónica de activo patrimonial** es importante para la presente investigación ya que por medio de la manipulación dentro del funcionamiento del programa, sistema informático o telemático que contenga los activos de una persona se configura otro delito que es la apropiación no consentida de un activo patrimonial mismo que será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial para sí mismo o para otra persona. (Constitucional, 2008)
- Así mismo el **Artículo 232 habla sobre el ataque a la integridad de sistemas informáticos** sancionando con pena privativa de la libertada de tres a cinco años a la persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de 22 información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, así mismo a quien desarrolle o comercialice, dispositivos o programas informáticos maliciosos destinados a causar los efectos antes indicados, si este acto se realizara a bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad. (Constitucional, 2008)
- En el **Artículo 233 se encuentra contenida la sanción para los delitos contra la información pública reservada legalmente** misma que será de tres a cinco años para la persona que destruya o inutilice información clasificada

de conformidad con la ley y de la misma forma será sancionado el servidor público que se apodere de esa información. (Constitucional, 2008)

- **El Artículo 234 hace referencia a el Acceso no consentido a un sistema informático, telemático o de telecomunicaciones** en el que manifiesta que, **"**La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o re direccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años". (Constitucional, 2008).

Ley orgánica de garantías jurisdiccionales y control constitucional.- Ley orgánica de garantías jurisdiccionales y control constitucional, fue publicada en el Registro Oficial N° 52 del 22 de Octubre del 2009. Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, en su Capítulo III Articulo 49, acción de habeas data establece que "la acción de habeas data tiene objeto garantizar judicialmente a toda persona el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informe que por sí misma, o sobre sus bienes, estén en poder de entidades públicas o de personas naturales o jurídicas privadas en soporte material o electrónico. Asimismo, toda persona tiene derecho a conocer el uso que se haga de dicha información, su finalidad, el origen y destino, y el tiempo de vigencia del archivo o banco de datos". En la Constitución Política del Ecuador vigente (2008), en su capítulo tercero de las Garantías Jurisdiccionales de su sección quinta Art. 92 sobre la acción

de Habeas Data, también se establece recurso jurídico de Habeas Data. De acuerdo a la especificación contemplada en la Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos, en su título quinto de las infracciones 24 informáticas, los delitos informáticos que se tipifican, mediante reformas al Código Penal hoy contenidas en el Código Orgánico Integral Penal. Se ha podido ver la definición de los delitos informáticos, su principal insumo que es la evidencia digital y las técnicas o mecanismos con los procedimientos existentes para su investigación, vale destacar, entonces que los profesionales dedicados a la persecución de actos ilícitos en los que se utilizan medios tecnológicos, se mantengan a la vanguardia de conocer los avances que se den de ésta índole, y de esta manera mantenerse preparados y reaccionar de manera adecuada ante los actos cometidos por la delincuencia informática. Ecuador ha dado sus primeros pasos con respecto a las leyes existentes, en las que se contemplan especificaciones de la información y la informática, lo que se considera un avance importante ante el desarrollo tecnológico que se ha tenido en los últimos años en el país, pero es evidente que aún falta mucho por legislar, para asegurar que no queden en la impunidad los actos que se comentan relacionados con las tecnologías. (Constitucional, 2008)

2.2. Marco conceptual

2.2.1. Sistemas operativos

2.2.1.1. Definición

El sistema operativo es el programa de mayor importancia que funciona en una computadora. El propósito de una computadora es tener un sistema operativo que soporte el funcionamiento de otros programas y aplicaciones.

Para (Tanenbaum, 2003) “un sistema de cómputo moderno consta de uno o varios procesadores, memoria principal, discos, impresoras, teclado, pantalla, interfaces de red y otros dispositivos de entrada y salida. Se trata de un sistema complejo cuya labor es administrar todos estos dispositivos y proporcionar a los programas de usuario una interfaz más sencilla para comunicarse con el hardware.”.

Los sistemas operativos tienen grandes responsabilidades y poderes, se los puede comparar con un policía del tráfico, este se asegura que los diferentes programas y usuarios que están corriendo al mismo tiempo no interfieran el uno con el otro. Estos deben ser diseñados de tal manera que sea muy fácil de utilizar y comprender por los usuarios, tal como se indica en la Figura 1. (Silberschatz, James, Galvin, Morales Peake, & García Escrivá, 1998)

Figura 1 Sistema operativo como intermediario

Fuente: (Sanchez Herrera & Basantes Salazar)

A un sistema operativo también se lo conoce como administrador de recursos, ya que es este decide a quién, cuándo y por cuánto tiempo se asignan todos estos recursos. Esto es necesario para el correcto funcionamiento de todo el sistema. (Flynn & Mclver, 2001)

2.2.1.2. Estructura interna de un sistema operativo

La estructura interna de los sistemas operativos pueden ser muy diferentes, debido a que los usuarios tienen metas distintas como: fácil de usar, rápido, confiable y las propias del sistema.

La capa externa es el sistema de ficheros que es la que se encuentra en contacto directo con el soporte físico de la máquina. La capa más interna es el núcleo que es aquella que permite agregar nuevas instrucciones especiales a la máquina. Sobre el núcleo esta la capa de gestión de memoria, que amplía la máquina virtual con operaciones de asignación, liberación y control de la memoria. Para que los procesos puedan comunicarse con los dispositivos de entrada y salida, existe una capa para la gestión de E/S a través de objetos denominados ficheros. Sobre todo esto el usuario interactuara con la maquina a través del intérprete de comandos (Martinez, 1997), como indica la Figura 2.

Figura 2 Estructura de capas de un SO

Fuente: MARTÍNEZ, P (1997). Sistemas Operativos Teoría y Práctica. España.

2.2.1.3. Tipos de sistemas operativos

Las grandes empresas como Microsoft, Macintosh, IBM y otros destacados han desarrollado distintas versiones de sistemas operativos acorde al momento tecnológico ; ya que es necesario que se adapte de manera correlacionada con el hardware existente y los nuevos programas que utiliza el usuario (Stallings, 1997). Los sistemas operativos más conocidos son:

- DOS: Es el más conocido y fue desarrollado por Microsoft. Su interfaz era líneas de comando modo texto o alfanumérico.
- Windows 3.1: Microsoft opto por tener un SO con una mejor interfaz gráfica (iconos) que sea amigable con el usuario.
- Windows NT: En esta versión de especializada en redes y servidores, en donde la comunicación entre dos computadores se realiza de forma más sencilla.
- OS/2: Fue elaborado por IBM, el cual posee una interfaz gráfica muy buena, su principal problema es que las aplicaciones no aprovechan al 100% las características del SO.
- MAC OS: Fue creado por Apple Computer Inc. Este es el sistema operativo que viene con las Macintosh, el cual tiene una interfaz muy amigable e intuitiva con el usuario.
- UNIX: Fue creado por Bell de AT&T. Es un sistema operativo robusto utilizado en computadores de escritorio, laptops, mainframes.

2.2.1.4. Windows 8

Windows 8 representa un cambio fundamental en la forma en la que Windows funciona, ya que está orientada para el uso en tabletas (touchscreen) como en las

computadoras tradicionales. Utiliza la tecnología Metro Design Language, lo cual facilita la interface touch como la que encontramos en los smartphone (teléfonos inteligentes) y tabletas. En la Figura 3 se observa la nueva interfaz de usuario que posee Windows 8. (Perez Marques, 2012)

Figura 3 Vista del menú inicio de Windows 8

Fuente: (Sanchez Herrera & Basantes Salazar)

Entre los principales cambios que Microsoft realizo es la eliminación del botón de Inicio, a pesar de que los usuarios pueden hacerlo aparecer haciendo click o tocando la parte izquierda de la pantalla. Además contiene la versión Metro de Internet Explorer 10 con aplicaciones para noticias, deportes, viajes, etc. (G. Arias, 2012)

Entre las principales características de este sistema operativos incluye son:

- Windows Store (descarga de aplicaciones)
- Sincronización con la cuenta Microsoft
- Windows Defender como antivirus.
- Soporta múltiples pantallas

- Acceso a documentos en OneDrive
- Se permite montar imágenes de disco

2.2.1.4.1. Requisitos de hardware

Para el funcionamiento del sistema operativo Windows 8 se requiere los siguientes requisitos mínimos, como se indica en la tabla 1

Tabla 1
Requisitos mínimos de hardware recomendados para Windows 8

ARQUITECTURA	32 bits	64 bits
Procesador	1 GHz o más rápido, compatible con PAE, NX y SSE2	
Memoria RAM	1 GB de RAM	2 GB de RAM
Tarjeta Grafica	Dispositivo de gráficos DirectX 9 con soporte de controladores WDDM 1.0	
Disco Duro	18 GB de espacio libre	22 GB de espacio libre
Pantalla	Entrada táctil y 1024x768 de tamaño.	

Fuente: (Zdnet, 2012)

2.2.1.4.2. Seguridades

Windows 8 hace que la comunicación con otros dispositivos a través del Internet sea más seguro y fácil que antes, teniendo lejos a los hacker y virus maliciosos. Entre algunas de las características que Windows 8 incorporo, se puede encontrar un Action Center (centro de acción) que brinda la posibilidad de administrar la seguridad del sistema, brindando un lugar sencillo para ver las alertas y tomar acción sobre la seguridad y los problemas de mantenimiento con el sistema. Con la incorporación de este nuevo centro de acción, es más fácil encontrar información sobre los últimos virus o amenazas a la seguridad, verificar el estado de las configuraciones, rápido soporte

por parte de Microsoft y acceso al Panel de Control, en el cual se encuentran otras configuraciones de seguridad y privacidad. (Portantier, 2013)

Otra característica de la que Windows 8 toma ventaja es que el computador necesita correr un nuevo sistema de arranque llamado Unified Extensible Firmware Interface (UEFI). Este sistema reemplazara el viejo BIOS, el cual añade nuevas características y gran velocidad al momento de iniciar los procesos. Esta posee una característica llamada Secure Boot, que ayuda a prevenir el uso no autorizado del sistema y que alguna amenaza se ejecute desde el arranque.

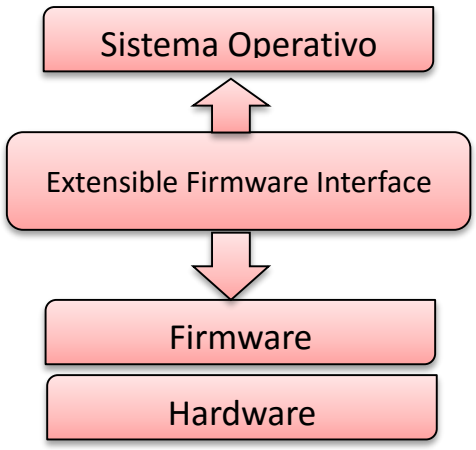


Figura 4 Posición de la Extensible Firmware Interface

Fuente: (Sanchez Herrera & Basantes Salazar)

Esto dificulta a ladrones de información el poder utilizar un disco de arranque o memorias para acceder a los documentos. Además permite mantener a salvo de rootkits (un tipo de malware que es muy difícil de detectar), para que este no infecte el computador durante el arranque del sistema. En la Figura 4 se puede ver en qué parte se encuentra la UEFI.

Por otro lado Microsoft incorporo el uso de contraseñas fuertes al momento de crear una cuenta en Windows 8, tratando de hacerlas más complejas con el uso de mayúsculas, minúsculas, números y caracteres especiales, dejando afuera todas aquellas palabras que se encuentro en el diccionario. Otra característica es un antivirus incorporado llamado Windows Defender, el cual puede ser desactivado si el usuario elige un antivirus de otro fabricante.

2.2.2. El crimen informático o cyber-crimen

Hoy en día se vive en una época en la que interactuar con otras personas alrededor del mundo se ha convertido en una parte integrante tanto a nivel personal como en los diferentes negocios. El Internet se ha vuelto el enlace necesario para llevar a cabo las comunicaciones, pero al mismo tiempo abre nuevas oportunidades para que los delincuentes sin escrúpulos lleven a cabo su cometido. (Más & Rosado)

Hace unos años muchos profesionales en la rama de la informática, redes, tecnología de información y el derecho, se interesaron por este nuevo modo de operación con respecto al cyber-crimen. Como usuarios finales siempre se harán preguntas como ¿Estaré utilizando Internet de forma segura? ¿Habrá algún problema si compro algún producto por Internet?

2.2.2.1. Definición

Cyber-crimen es un término utilizado para cualquier actividad ilegal que usa como medio de ejecución un computador, una red u otros medios telemáticos. Además, el cyber-crimen incluye también a los crímenes tradicionales llevados a cabo a través de Internet. Por ejemplo tele-mercadeo, fraude, suplantación de identidad, clonación

de tarjetas de crédito, entre otras son consideradas como cyber-crimen. (Contreras Clunes, 2003).

El cyber-crimen está creciendo muy rápidamente en el área de la delincuencia. Más y más criminales se aprovechan de la velocidad, conveniencia y anonimidad al momento de cometer los diversos tipos de actividades criminales que no conoce obstáculos ya sea física o virtual.

Estos crímenes pueden ser divididos en tres grandes áreas:

- Ataques a través del computador
- Crímenes financieros y corrupción
- Abuso

Nuevas mafias del cyber-crimen están emergiendo todo el tiempo, con un costo que de billones de dólares. En épocas anteriores, el cyber-crimen era ejecutado por individuos o grupos pequeños. Hoy en día se puede ver organizaciones criminales trabajando con profesionales en el ámbito de las TI que poseen una mentalidad criminal para cometer delitos informáticos, a menudo para financiar otras actividades ilegales. Estas organizaciones se encargan de reclutar varias personas en todo el mundo para cometer crímenes a escalas sin precedentes. (INEI, 2001)

Aquí los computadores pueden involucrarse de diferentes formas:

- El computador puede ser usado como herramienta para la ejecución del delito.
- El computador puede ser el objetivo.

- El computador puede ser utilizado por eventos incidentales como por ejemplo guardar archivos de venta de drogas, archivos de planificación de robos, etc.

2.2.2.2. Categorías del cyber-crimen

Este nuevo estilo de crimen tiene dos categorías en las que se podrán identificar los otros tipos de crímenes.

- Delitos sin violencia: Se puede nombrar el desfalco de fondos utilizando las TI.
- Delitos violentos: Este tipo de delitos son aquellos en lo que causan un daño físico a una o varias personas. Los principales son:
    - Sabotaje de sistemas informáticos de control aéreos que produzcan colisiones entre aviones,
    - Cyber-terrorismo
    - Asalto con amenazas
    - Uso de correo electrónico para distribuir información sobre actividades violentas
    - Acoso informático
    - Pornografía infantil, etc.

2.2.2.3. Perfiles del cyber-delincuente

El perfil criminológico es aquella técnica que tiene como objetivo descubrir las características socio demográfico, criminológico y psicológico de aquel individuo que haya cometido un delito y así determinar su identidad, con el propósito de ofrecer la información a la policía para su captura.

Para determinar un perfil de un delincuente, se deberá estudia la escena del crimen y analizar todas las evidencias, indicios, testigos y toda la información con la que se pueda establecer una hipótesis de aquella persona que cometió el delito. Todo esto ayudara a determinar la personalidad del delincuente. Hay que tomar en cuenta que los perfiles son solo una herramienta que se utilizara para la investigación y construcción de un caso criminal.

Existen dos métodos para crear un perfil, cada uno se basa en razonamiento concreto. Estos métodos son:

- Método Inductivo.- se basa en estadísticas y análisis comparativos para la creación de un perfil. Se revisa perfiles de los diferentes delitos que se han cometido y así buscar correlaciones con estos.
- Método Deductivo.- se basa en razonamiento deductivos de pruebas observables, es decir se analizan toda la información acerca del crimen para determinar características del criminal.

Existe un modelo que es utilizado como método deductivo al momento de realizar un perfil. Este modelo se llama SKRAM, el cual fue diseñado por Donn Parker. El significado de sus siglas está descritas en la Figura 5:

Figura 5 Siglas de modelo SKRAM

Fuente: (Sanchez Herrera & Basantes Salazar)

2.2.2.4. La mente del cyber-delincuente

Hablar de la mente de los cyber-delincuentes es referirse a las motivaciones, aquellos disparadores de acción y su manera de actuar para llegar hasta donde otros no se atreven. Adentrarse en la mente de los atacantes es avanzar en un terreno donde la imaginación es un factor mucho más importante que el conocimiento. No se puede comparar a un intruso, cuya motivación está más allá del reto y el reconocimiento de sus capacidades, con un hacker que presenta una manera de mostrar que nada está dicho y que solo se aprenderá con cada nueva experiencia y comportamiento inesperado del sistema.

Según Furnell (CFE, 2009), existen diferentes consideraciones para concebir o para clasificar a los atacantes, así como las motivaciones que los mueven a actuar en una situación particular, como se observa en la Tabla 2.

Tabla 2
Tipos de atacantes y sus motivaciones

MOTIVACIONES	Cyber-terroristas	Phreakers	Script Kiddies	Cracker	Desarrollo de Virus	Atacante Interno
Reto		X			X	X
Ego		X	X		X	
Espionaje				X	X	X
Ideología	X					
Dinero		X		X	X	X
Venganza	X		X		X	X

Fuente: (Furnell, 2002)

Furnell habla de atacantes con perfil de, entre otros términos, cyber-terroristas, phreakers, Script Kiddies, Crackers, desarrolladores de virus. Cada uno de ellos se mueve por motivos diferentes que llevan a una carga emocional que es importante analizar y no solamente, las consideraciones técnicas de sus acciones, que dicen del nivel de conocimiento del individuo. Además de los perfiles establecidos por Furnell, se agrega uno que muchas veces pasa inadvertido, como son los *empleados insatisfechos* o *atacantes internos.* Esos funcionarios o colaboradores, que no encuentran en su trabajo una motivación real para seguir creciendo, o que se llenan de resentimiento o sentimientos encontrados hacia personas específicas o hacia la organización y su directiva. Este perfil es un elemento fundamental para estudiar los cyber-delincuentes, pues con él se hace evidente que estos pueden ser tanto externos como internos, resultando estos últimos los de mayor nivel de riesgo dado las características que revisten dentro de la organización.

Adentrándose en este tipo de perfil, esta amenaza es una realidad en todas las empresas del mundo, los empleados son seres humanos que buscan en su lugar de trabajo un escenario para potenciar sus capacidades y avanzar en su desarrollo personal y profesional. Muchas pueden ser las razones por las que una persona se siente

insatisfecha por una organización, y por tanto, muchos pueden ser los escenarios para abordar el análisis de esta posible amenaza.

El atacante interno puede ser cualquier persona, solo requiere un disparador o detonante para transformarse en un potencial delincuente y quien encuentre en la organización y su infraestructura, la manera para demostrar que existe y que requiere atención a su situación. Situaciones de carácter personal, familiar, laboral o de celos profesionales pueden ser ocasión para que se desvíen las actividades de una persona hacia acciones que pueden impactar las infraestructuras de comunicaciones, o computación de una empresa. (Acurio, 2007)

Si adicionalmente esta persona insatisfecha posee la curiosidad técnica de un Script Kiddies y la perseverancia de un Hacker, se está en una ruta para gestar un incidente de seguridad informática de proporciones importantes, donde las acciones que se adelantaran se plantearan de manera cuidadosa, hábilmente mimetizadas y ejecutadas detalladamente, pues conocen los procedimientos internos y los alcances de los mismos cuando un evento anormal se presenta. Por lo general, se dice que el atacante se vincula a la investigación como parte de estrategia para ser descubierto o implicado.

Por lo tanto, las organizaciones deben desarrollar estrategias y mecanismos para avanzar en el desarrollo de índices de amenaza informática interna que permitan identificar, con el área de talento humano y tecnología de información, los referentes básicos para poner acciones preventivas que disminuyan esa amenaza y fortalecer las medidas de seguridad y control de acuerdo con la situación evidenciada.

2.2.3. Informática forense

Según Rodney McKemmish, 1999, la conocida informática forense, computación forense, análisis forense digital o examinación forense digital, es “el proceso de identificar, preservar, analizar y presentar evidencia digital de una manera que sea legalmente aceptable”.

Puede haber dos tipos de investigaciones en la informática forense. La primera es cuando un incidente ya ha ocurrido y la identidad del agresor no se conoce (por ejemplo, una intrusión remota). La segunda es aquella en donde ambos el agresor y la victima están identificados (por ejemplo, una investigación de pornografía infantil).

Esta ciencia es sistemática puesto que se basa en hechos premeditados para recolectar pruebas que luego serán sometidas a un proceso de análisis exhaustivo utilizando una serie de herramientas y técnicas forenses para extraer datos que sirvan como evidencia digital y asegurar la integridad; por ejemplo, la creación y verificación de la imagen, y la prevención de la modificación de la evidencia original. Se debe tener cuidado con la evidencia recolectada y guardada de tal forma que no sea alterada por la afectación accidental o intencional. (López, Amaya, & León)

En el caso de comprobarse que la evidencia digital no fue manejada adecuadamente, su validez puede ser totalmente cuestionada. (Matthew Meyers, 2004), describen un caso en donde la defensa cuestiona la calidad del manejo de la evidencia y termina reconociendo la eventualidad de perdida y manipulación de datos, pero la evidencia aun así fue reconocida, así como la prosecución posterior alegando que aunque es posible que existiera alguna perdida de datos el arreglo aleatorio de los datos para formar pornografía infantil era improbable. El escenario anterior muestra la

importancia de tener un manejo adecuado de la evidencia de manera que toda la evidencia sea fácilmente identificable y cuestiones como: ¿dónde?, ¿cuándo? y ¿Cómo fue descubierta? Deben quedar claras; por medio de una cadena de custodia totalmente garantizada durante todo el proceso. (Cano, 2006)

En la actualidad las organizaciones dependen cada vez más de las redes y sistemas de información y en el caso de que ocurriera algún incidente con estos puede llegar a comprometer a la organización entera a tal punto de detener la continuidad de las operaciones y del negocio. Hoy en día el incremento de los delitos y ataques informáticos ha llevado a que los gobiernos y las empresas incrementen su inversión en sistemas de protección y la implementación de las mejores prácticas en la gestión de la seguridad de la información incluyendo la definición de políticas de seguridad, el control de accesos, entre otras.

La computación forense tiene sus origines en el año 1984 cuando el FBI y otras agencias de los Estados Unidos tuvieron que empezar a desarrollar programas que permitan examinar la evidencia extraída de los computadores. Estas técnicas y herramientas fueron creadas con la intención de atender las necesidades específicas de la aplicación de la ley, para aprovechar al máximo esta nueva forma de evidencia.

Es una disciplina rigurosa en cuanto a sus procedimientos de investigación y las personas que lo realizan están altamente capacitadas en los puntos que caracteriza cualquier investigación de las ciencias forenses. Estas personas deben tener un alto grado de preparación técnica y científica para llevar una investigación de calidad. El tratamiento que debe tener la información en cualquiera de sus fases debe ser tan

importante y riguroso como a cualquier evidencia formal que se analice en las ciencias forenses.

2.2.3.1. Usos de la informática forense.

Existen varios usos de la informática forense, muchos de estos usos provienen de la vida diaria y no tienen que estar relacionados directamente con la informática forense: (Gutiérrez, 2006). En la Figura 6 se tiene uno de sus principales usos.

Figura 6 Usos de la informática forense

Fuente: (Sanchez Herrera & Basantes Salazar)

2.2.3.2. Requisitos de la investigación forense.

De poco servirían las herramientas y los métodos utilizados por el investigador si no pudieran acreditar una cierta solvencia y validez ante el tribunal. Para ello es necesario que cumplan determinados requisitos. No olvide que los resultados de su labor investigadora deberán ser puestos a disposición de autoridades judiciales y otras

instancias decisorias. Una herramienta forense, tanto si está homologada como si no, debe demostrar en su funcionamiento unos niveles de eficacia e integridad lo suficientemente altos para ganarse el respeto tanto de la comunidad profesional de investigadores como del personal que trabaja en la administración de justicia.

Lo mismo cabe decir de los métodos de trabajo y la forma de exponer resultados. Alexander Geschonneck, analista de departamento de informática forense de la sociedad de auditores de contabilidad KPMG AG WPG, Berlín autor de un libro clásico sobre la materia) Computerforensik, dpunkt.verlahg, Heielberg, 2008), establece seis requerimientos esenciales que toda investigación debe cumplir sin falta, que son los siguientes:

2.2.3.2.1. Aceptabilidad.

Las herramientas y métodos del investigador deberán ser conocidos y aceptados por los profesionales de su sector. La introducción de tecnologías innovadoras puede resultar problemática, porque no siempre el más moderno es también lo mejor. Lo ideal sería que otros investigadores hubieran trabajado previamente con esos procedimientos y existan informes positivos sobre la eficacia de los mismos.

2.2.3.2.2. Integridad.

Las pruebas no deben sufrir alteraciones de ningún tipo. Generalmente el medio – disco duro, pendrive o CD/DVD- se almacena adecuadamente después de haber obtenido tres copias cuyos hashes han de coincidir. Con una de ellas llevara a cabo su análisis el investigador. Otra se guardara como respaldo, y la tercera será

puesta a disposición de la parte contraria para que esta pueda realizar sus propias averiguaciones, manifestar su posición al respecto o elaborar un contra informe.

2.2.3.2.3. Credibilidad.

Todo lo que se haga debe ser demostrable. No basta con utilizar un software del cual nada se sabe, salvo que si se lo alimenta con determinados datos siempre brotan de él determinados resultados. El investigador debe acreditar un conocimiento adecuado a sus herramientas para poder explicar de manera plausible lo que consigue de ellas.

2.2.3.2.4. Relación causa-efecto.

Aunque no es cometido del investigador extraer conclusiones de ningún tipo sobre la culpabilidad o responsabilidades de las personas que intervienen en los hechos, los métodos empleados por aquel deben hacer posible una explicación de los acontecimientos en términos de causa y efecto.

2.2.3.2.5. Carácter repetible.

Este requisito se explica por sí mismo. Sean cuales fueren los métodos de trabajo empleados o la persona que realiza la investigación, los mismos datos de entrada deberán producir los mismos resultados.

2.2.3.2.6. Documentación.

Cada paso dado por el investigador deberá disponer de una descripción detallada y exacta, al objeto de que los informes no puedan ser impugnados por culpa de ambigüedades o negligencias de ningún tipo. Deberá tenerse especial cuidado a la hora de documentar la cadena de custodia que es la parta más sensible de todo el proceso y la que con más facilidad podrá atacar la parte contraria en caso de localizar la menor irregularidad. Para ello sería conveniente que el investigador elaborase sus

propias hojas de control de medios probatorios digitales, adjuntándolas debidamente al informe del caso.

2.2.3.3. Evidencia digital

Generalmente una evidencia se define de una manera amplia para describir cualquier registro generado o almacenado en un sistema computacional que puede ser utilizado como evidencia de un proceso legal. En el caso de la evidencia digital se habla de que está construida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales. (Mosquera, Certain Jaramillo, & Cano, 2005)

Algo que hace que la evidencia digital sea un total desafío para los investigadores es debido a que:

- Es volátil.
- Es anónima.
- Es duplicable.
- Es alterable.
- Es eliminable.

Sin embargo pese a lo anteriormente mencionado la evidencia digital también tiene características que permiten atacar este problema:

- Puede ser duplicada exactamente y una copia es perfectamente válida para una examinación tal cual si fuera la evidencia original.

- Generalmente es considerado una buena práctica la ejecución de análisis sobre copias de la evidencia y resguardar siempre la evidencia original para evitar perderla o alterarla.
- Con las herramientas adecuadas es fácil determinar su la evidencia ha sido modificada o tratada de forzar con una copia original.
- Es difícil de destruir. Aun cuando un fichero se suprime o se formatea ya que por medio de un mecanismo impulsor la evidencia puede ser recuperada.

En las figuras 7 y 8 se observa los tipos de pruebas y su clasificación respectivamente.

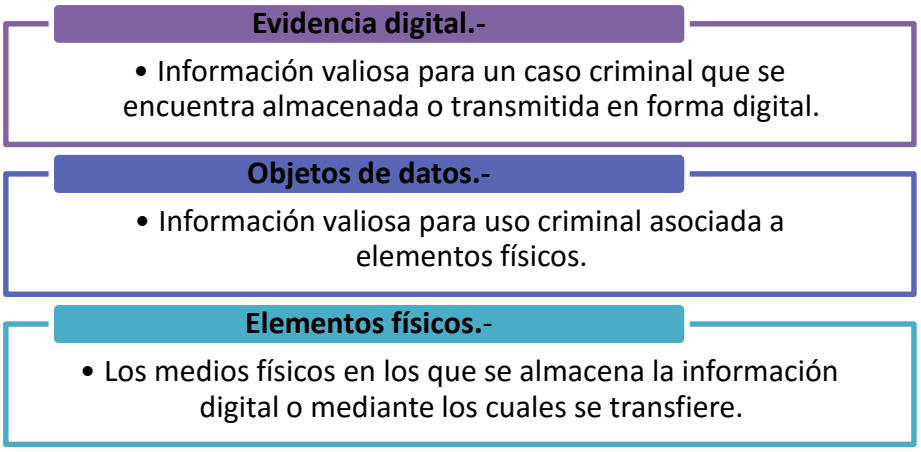


Figura 7 Tipos de pruebas o evidencias digitales.

Fuente: (Sanchez Herrera & Basantes Salazar)

Como reglas para el manejo de evidencia se tiene principalmente las siguientes:

- Manejar la evidencia original lo menos posible a fin de no alterarla o contaminarla e incluso perderla.

- Hacer uso estricto de software y hardware que garantice un proceso limpio.
- Examinar individualmente las evidencias procurando siempre mantener la integridad de su naturaleza.

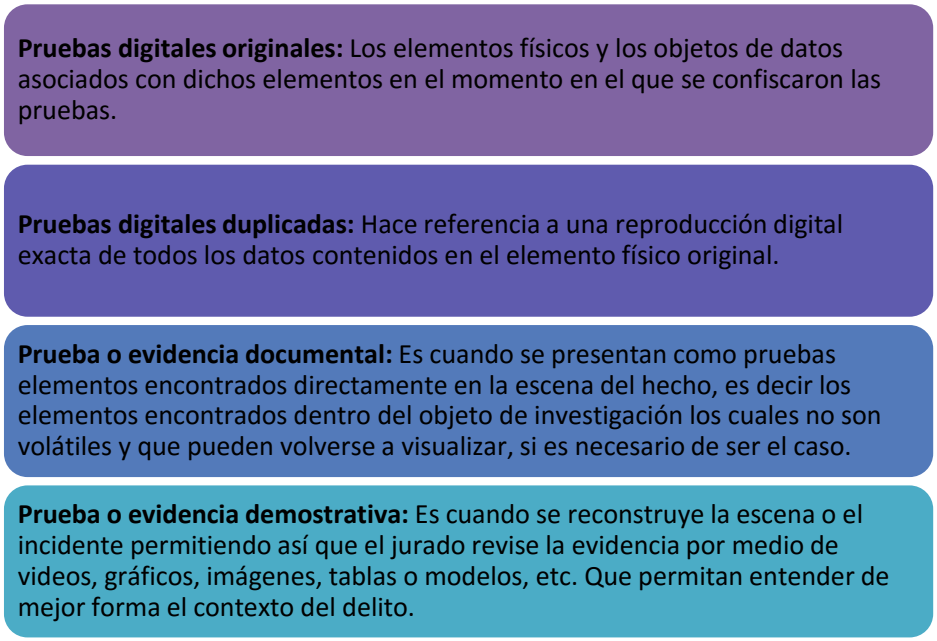


Figura 8 Clasificación de pruebas digitales.

Fuente: (Sanchez Herrera & Basantes Salazar)

La computación forense comprende cuatro elementos importantes en el tratamiento de la evidencia digital, como indica la Figura 9.

Figura 9 Pilares para el manejo de evidencia digital

Fuente: (Sanchez Herrera & Basantes Salazar)

2.2.3.4. Delitos informáticos.

El progreso tecnológico que ha experimentado la sociedad, supone una evolución en las formas de infringir la ley, dando lugar, tanto a las diversificaciones de los delitos tradicionales como la aparición de nuevos actos ilícitos. Esta situación ha motivado a un debate en torno a la necesidad de diferenciar o no los delitos informáticos del resto y de definir su tratamiento dentro del marco legal.

María de Luz Lima, (Lima, 1984). Indica que el delito electrónico en un sentido amplio "cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin", y que en su sentido estricto, el delito informático, es "cualquier acto ilícito penal que en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".

Julio Téllez Valdés, (Valdés, 1996) , conceptualiza el delito informático en forma típica y atípica entendiendo que en la forma típica son "Las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras para instrumento o fin"

y la forma atípica “actitudes ilícitas en que se tienen a las computadoras como instrumento o fin”.

En base a todo lo anteriormente mencionado por diferentes autores, se llega a la conclusión toda aquella conducta ilícita en la cual se utiliza como medio un computador se puede clasificar de inmediato como un delito informático o delito electrónico. Y con las definiciones anteriormente expuestas tampoco existe una sola definición para un delito informático por su gran diversidad pero todos se basan en un principio que se ha vuelto regla en la seguridad informática y todo al respecto del resguardo de información. Confidencialidad, integridad y disponibilidad. (Romero Echevarria, 2005)

La criminalidad informática organizada ha crecido de manera exponencial a la par que la misma sociedad lo ha hecho, según los varios informes de seguridad realizado por empresas como Red Iris, CERT, CSI (Computer Security Institute), FBI (Oficina Federal de Investigaciones), las vulnerabilidades reportadas y los altos costos que involucran para las empresas y los gobiernos, los mismos, que son aprovechados por intrusos cada vez más hábiles en su arte. Por todo esto es cada vez más fácil desaparecer la evidencia y confundir a los investigadores por lo cual es totalmente un reto para los afectados, legisladores judiciales, policiales e incluso hasta los mismos especialistas informáticos. En la Figura 10 se puede ver su clasificación

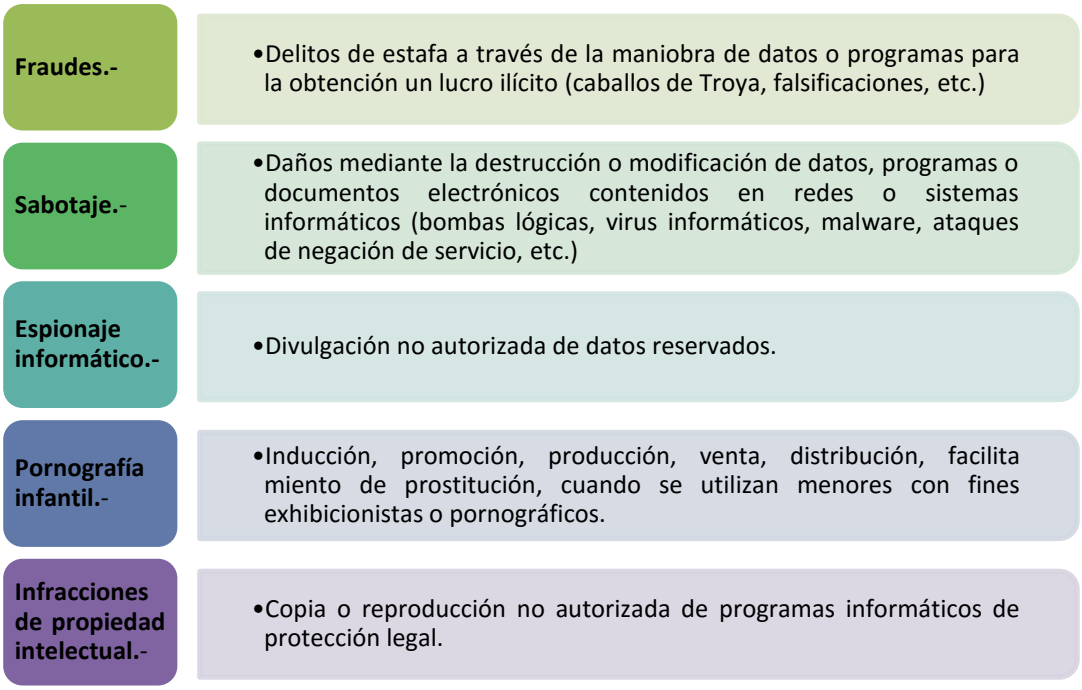


Figura 10. Clasificación de delitos informáticos.

Fuente: (Sanchez Herrera & Basantes Salazar)

En base a todo lo anteriormente indicado se podrá empezar una investigación tecnológica de vital importancia ya que mediante esta se llega a determinar la confirmación o desvirtuarían de lo que corresponde a la verdad. Es trascendental, tener en consideración la formalidad y claridad de los procedimientos o técnicas de análisis utilizados en un proceso de investigación, para brindar mayor claridad y precisión a las observaciones dentro del proceso, ante un hecho de delito informático.

A continuación se muestra un breve resumen del desarrollo histórico de los delitos informáticos, basado en estadísticas obtenidas de diversas fuentes que exponen ideas sobre la gravedad de los daños que se producen debido a los delitos informáticos en los que los bienes jurídicos vulnerado por ellos y dejan en evidencia la necesidad de dar una protección penal a los ciudadanos frente a esta nueva forma de criminalidad.

En los Estados Unidos, el Stanford Research Institute detecto la existencia de 10 delitos informáticos en el año de 1969, cifra que se disparó, ya que en 1977 esta cifra había aumentado a 85 delitos.

Pierini, Lorences y Tarnabene, en su libro titulado Hábeas Data, dan a conocer las estadísticas obtenidas del instituto de Seguridad para las Computadoras de los Estados Unidos, durante el año de 1997. De este informe se conoce que en año mencionado, los ataques a computadores se incrementaron en un 16%, siendo cada vez más sofisticados. En 2005 ya se reportaban 130 millones de dólares en pérdidas por este tipo de delitos de acuerdo a informes del FBI. Los crímenes más comunes estaban entre el acceso sin autorización a computadores por parte de empleados, ataques vía proveedores de servicios, robo de información o de software, fraudes financieros, sustracción de materiales, fraudes en las telecomunicaciones; entre otros.

Según (Palazzi, 2000) “en la década de los 80 hacen aparición los delitos de hacking, los virus informáticos y otras clases de programas destructivos. Este peligro se hizo evidente en 1989, cuando una investigación criminal en Alemania detecto varios hackers que usaban redes internacionales para acceder a información americana e inglesa y la vendían a los servicios de la KGB. En el mismo año, un virus escrito por un estudiante de informática en la Universidad de Cornell, Estados Unidos, infecto y dejo sin funcionamiento a más de 6000 ordenadores conectado a lo que en ese entonces era Internet”.

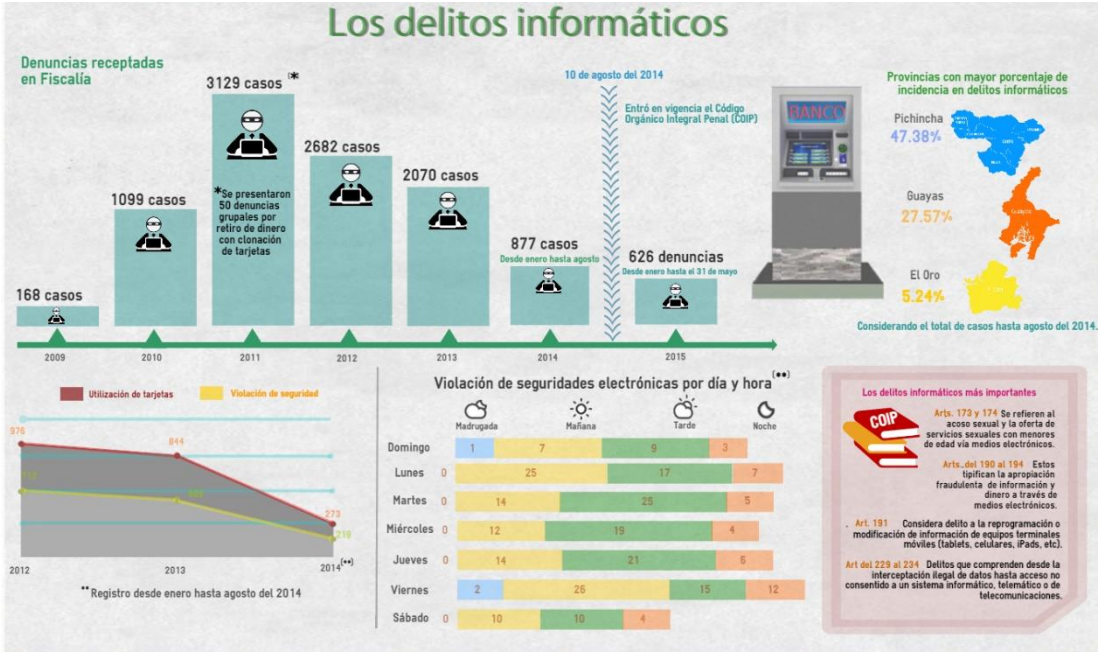


Figura 10 Estadísticas de los delitos informáticos en el Ecuador según la Fiscalía General de Gobierno

Fuente: (Sanchez Herrera & Basantes Salazar)

A fines de la década de los 80, surge la piratería informática, la cual constituye en la manipulación de cajeros informáticos y el abuso de las telecomunicaciones. Esta manipulación revelo la gran vulnerabilidad de los sistemas informáticos y la necesidad de prevenir y controlar esta nueva criminalidad; la que era propia de esta nueva sociedad de la información y la comunicación. En la Figura 10 se puede apreciar el aumento de los delitos entre el 2008 y 2014.

2.2.4. Normas y estándares relativos al análisis forense.

2.2.4.1. Norma ISO 17799-2000.

Esta norma está basada en la BS7799 (Publicada por el Instituto Británico de normas y Técnicas en 1995 y revisada y ampliada en una segunda versión en 1999).

Hoy en día es un estándar a seguir considerado dentro de las mejores prácticas en seguridad informática.

Propone 10 áreas de control conteniendo una serie de recomendaciones prácticas exitosas de seguridad que cualquier organización debería estar en la capacidad de poder aplicar independientemente de su tamaño o sector. En la Figura 11 se puede observar las áreas de control de esta norma.

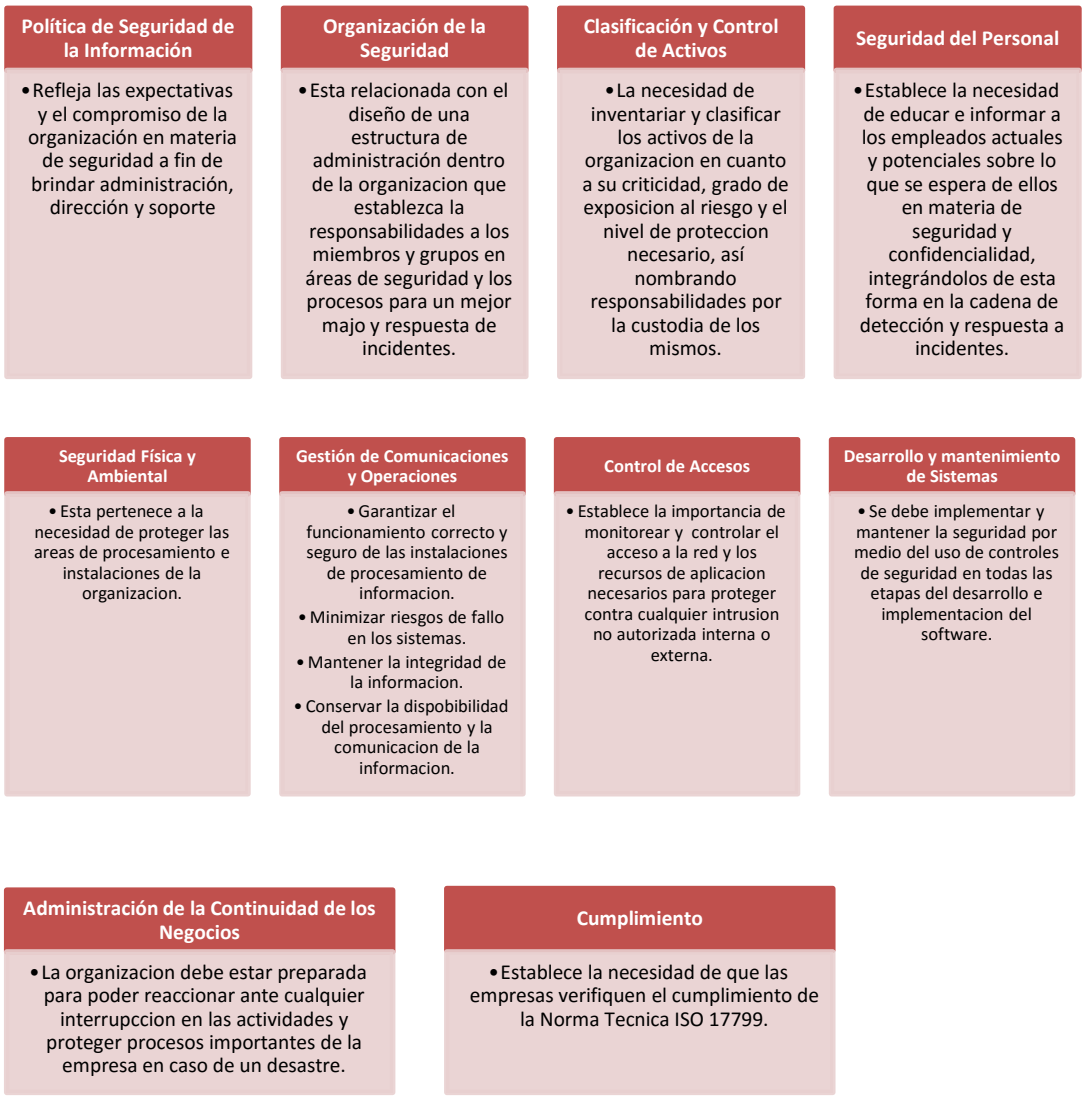


Figura 11 Áreas de control Norma ISO 17799-2000

Fuente: (Sanchez Herrera & Basantes Salazar)

2.2.4.2. Norma ISO/IEC 27037.

Otra de las normas considerada dentro de las mejores prácticas es la norma ISO/IEC 27037 conocida como la guía para la identificación, recolección, adquisición y preservación de evidencia digital, proveniente de la normativa de seguridad de la información ISO 27000.

Esta norma define los dispositivos y las funcionalidades que son incluidos en la misma por ejemplo: dispositivos de almacenamiento masivo. smartphone, GPS, sistemas de video vigilancia y CCTV, computadoras conectadas en red, dispositivos con conexión de red basadas en TCP/IP o cualquier otro protocolo, dejando así la puerta abierta a dispositivos con características y funcionalidades similares a los anteriormente mencionados.

Es importante recalcar dos términos sumamente básicos e importantes dentro del cómputo forense.

- DEFR Digital Evidence First Responder: Es el individuo autorizado, entrenado y calificado para actuar en primera instancia ante un delito y este deberá poseer la experticia para manipular, recolectar y adquirir evidencia digital.
- DES Digital Evidence Specialist.- Es la persona que posee el conocimiento especializado y la experiencia suficiente para resolver situaciones técnicas vinculadas el manejo de la evidencia digitar y hacer el análisis forense requerido.

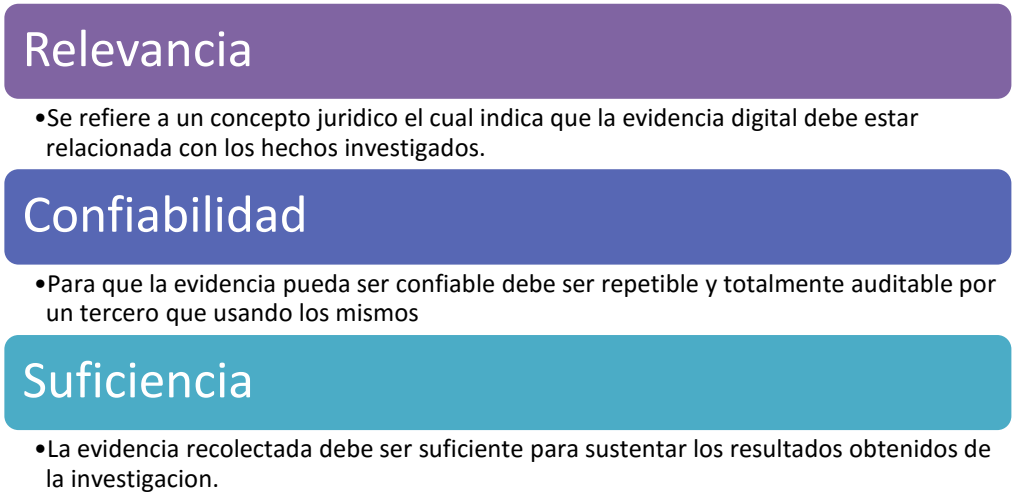


Figura 12 Características principales de la evidencia según Norma ISO/IEC 27037

Fuente: (Sanchez Herrera & Basantes Salazar)

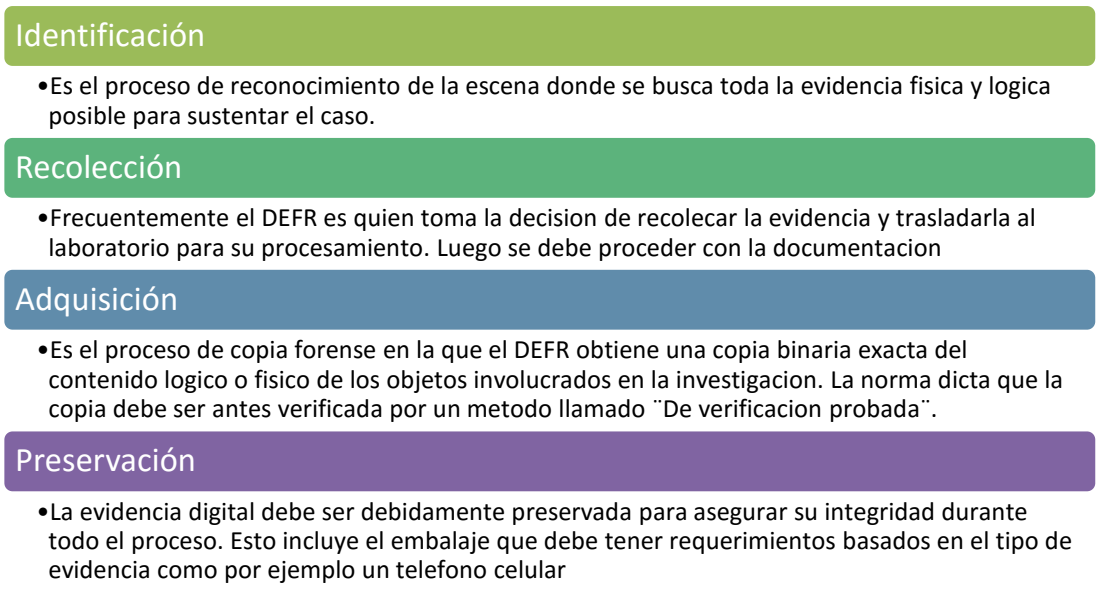


Figura 13 Proceso de obtención de evidencia según Norma ISO/IEC 27037

Fuente: (Sanchez Herrera & Basantes Salazar)

CAPÍTULO 3

GUÍA METODOLÓGICA DE ANÁLISIS FORENSE

La metodología que se plantea, se basa en el aplicar las buenas prácticas de la informática forense y la aplicación del método científico. Cuando se aplica el método científico se obtiene un nuevo conocimiento, mediante el uso de evidencia observable y medible, elaborando hipótesis que con el pasar del estudio, podrán ser corregidas y mejoradas conforme se obtiene más evidencias, aplicando las normas ISO/IEC 27037, que permite el manejo adecuado de la evidencia digital.

3.2. Metodología del análisis forense

Una vez revisadas las normas y estándares que existen con relación a la informática forense se puede determinar que en cada una de estas existen puntos que hay que tomar en cuenta como por ejemplo: preservar el escenario, el transporte y conservación de las evidencias, desarrollo de un informe. Dado estos puntos se determinan las fases que comprenderán la metodología para realizar un análisis forense que sea exitoso. (Ardita, 2007) Se analizaran estas fases como se observa en la Figura 14:

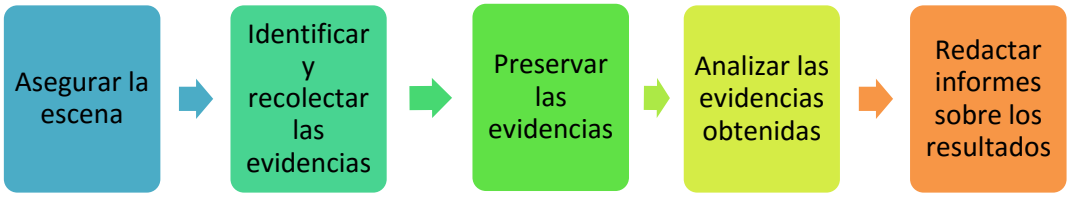


Figura 14 Fases de un análisis forense

Fuente: (Sanchez Herrera & Basantes Salazar)

- **Fase 1: Asegurar la escena**

El aspecto más importante de la recolección y preservación de la evidencias es proteger o asegurar la escena del crimen. Esto permite que las pruebas o evidencias no se contaminen hasta que se pueda ser grabado y recolectado. El enjuiciamiento de un caso puede depender del estado de la evidencia en el momento que esta es recolectada, por este motivo se tiene que tener en claro que todo acto que sea realizado por cualquier persona involucrada en la investigación puede afectar o no a los resultados.

Se recomienda realizar fotografías a la escena de crimen para tener evidencia del estado en el que se encontró esta. Además se deberá delimitar la escena y protegerla de accesos no autorizados a personas que no se encuentre dentro de la investigación. La protección de la escena de crimen será resguardada por unidades de policía e investigadores, quienes tendrán a su cargo el proteger las huellas dactilares dejadas en cualquiera de los equipos o cuerpos, para esto es recomendable el uso de guantes de látex.

Además se debe tomar en cuenta las siguientes opciones:

  - Se deberá anotar la hora y la fecha de todos los equipos. Si existe un desfase en esta información, se deberá documentar y tenerlo en cuenta posteriormente.
  - Si en las computadoras existe algún proceso corriéndose, hay que grabar lo que ocurre y verificar las entradas y salidas de los equipos.

- También se deberá documentarse que periféricos que encuentran en todos los equipos.
- Se tendrá que valorar si existe algún riesgo al momento que se interrumpa el fluido eléctrico, ya que la evidencia podría perderse.

- **Fase 2: Identificar y recolectar las evidencias**

Esta fase se dividirá en dos puntos que serán la identificación de las evidencias y recolección de las mismas:

- **Identificación de evidencias:** una vez llegado a este punto se debe identificar las evidencias más importantes y frágiles que están propensas a ser perdidos. Según la RFC 3227 la información será recolectada en orden de volatilidad de mayor a menor, como se muestra en la siguiente imagen. En la Figura 15 se muestra la volatilidad de la información.

  Una vez determinado cuales son las evidencias más volátiles, se tendrá un registro de los dispositivos dentro de la escena del crimen, sus características y los nombres de las personas encargadas de cada uno de estos equipos así como las contraseñas.

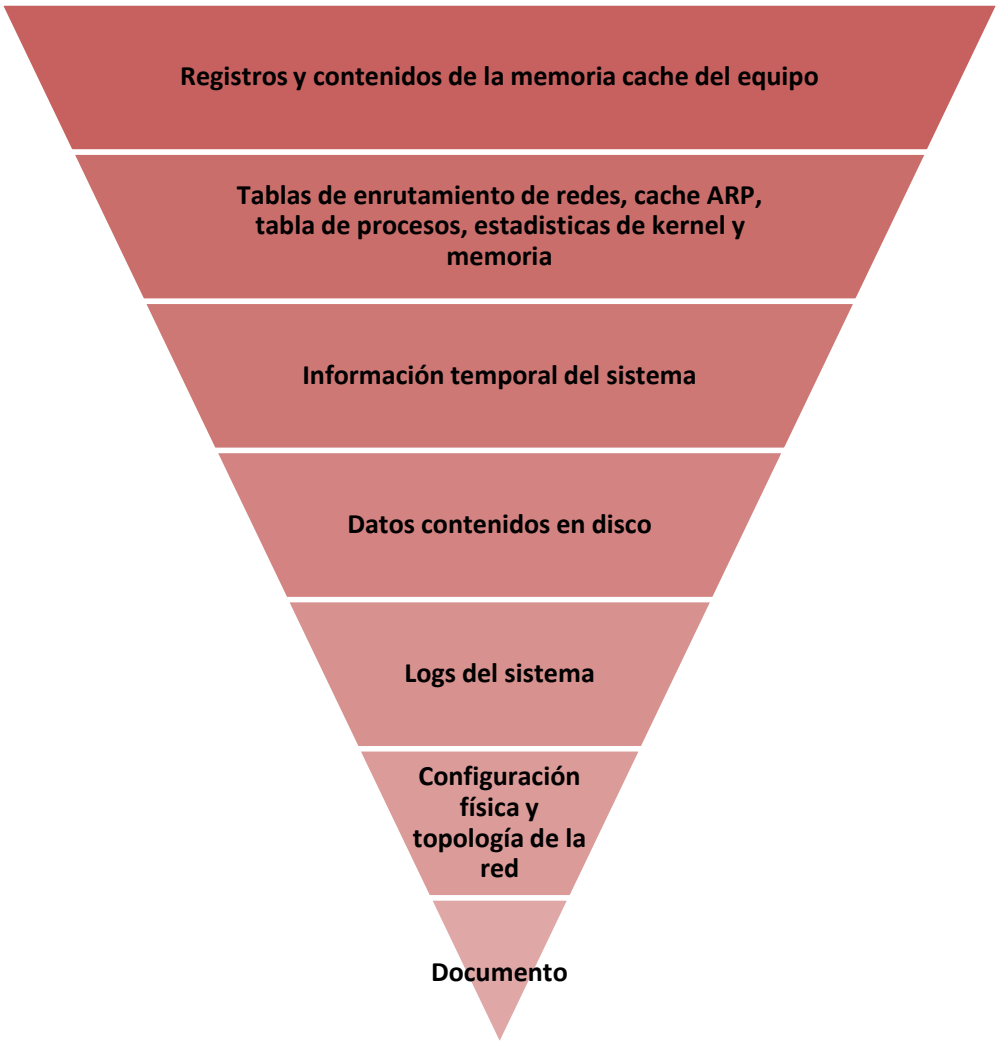


Figura 15 Orden de volatilidad según RFC 3227

Fuente: (Sanchez Herrera & Basantes Salazar)

También se realizará un diagrama topológico de la red, identificando los cables y puertos por lo que la computadora se conecta a la red. Es necesario identificar también los discos duros, su modelo, su capacidad de almacenamiento, su ubicación, entre otros.

Hay que tomar en cuenta las políticas que tiene la empresa en cuanto a la privacidad y tener en cuenta si es necesario tener una autorización para la recolección de evidencias.

- **Recolección de evidencias**

Según (Rivas, 2014) para recolectar evidencia se debe seguir los siguientes pasos:

"Copia bit a bit de los discos que se quieran analizar, es decir, se requiere una copia exacta del contenido de los discos incautados. Esto incluye todos los archivos del disco, por ejemplo los temporales, los ocultos, los de configuración, los eliminados y no sobrescritos y la información relativa a la parte del disco no asignada, es lo que se conoce como copia a bajo nivel. Esta copia se llevará a cabo sobre un soporte limpio mediante un borrado seguro de los datos que pudiera contener anteriormente para evitar así contaminaciones con otros casos.

Una vez realizada la copia se debe verificar la integridad de la misma. Para ello se calcula el hash o CRC de la copia, normalmente los equipos destinados al clonado de discos ya incorporan esa característica. Así con el hash del disco original y el de la copia se puede certificar que ambos son idénticos a todos los niveles y ante un juez, por ejemplo, quedará probado que no se ha manipulado de ningún modo. Con este procedimiento también se asegurara que no se han producido errores en la copia. Con la primera copia realizada y comprobada se procede a realizar una segunda copia sobre la primera. En este caso también se comprobará que el contenido es idéntico mediante el mismo proceso descrito anteriormente.

Teniendo ambas copias se entregara la primera al secretario judicial o notario responsable del caso y la segunda copia quedará en mano de

nosotros como investigadores para poder trabajar. La segunda copia será nuestra copia de respaldo en todo momento en el laboratorio y no será para trabajar directamente con ella en ningún caso. Para realizar el análisis se deberá realizar una tercera copia, comprobar su integridad y trabajar sobre ella, de tal modo que en caso de cualquier desastre o alteración de los datos siempre que se tenga la segunda copia exacta al original de donde poder volver a realizar otra copia para analizar."

- **Fase 3: Preservar las evidencias**

Esta fase es una de las más importantes por no decir la más importante, debido a que la mala preservación, el mal uso o la mala manipulación puede invalidar toda la investigación por lo cual este factor se repetirá durante toda la metodología.

Para preservar la evidencia adecuadamente esta debe tener una cadena de custodia la cual es el procedimiento controlado aplicado a las evidencias relacionadas con el delito, desde que son encontradas en la escena del crimen hasta su análisis en el laboratorio. El objetivo de la cadena de custodia es evitar cualquier manipulación no adecuada que afecte a la integridad de la evidencia, además también de tener un control total sobre los elementos incautados, quien o quienes tienen acceso a esta además de un registro con las fechas en las cuales fueron manipuladas, por quien o quienes y con qué objetivo.

Según (Rivas, 2014), para la preservación de evidencia digital hay que tener en cuenta lo siguiente:

- Luego de ser recolectada la evidencia, al ser preparada para el transporte del lugar de los hechos al laboratorio se debe tener en cuenta

los medios necesarios para evitar golpes o caídas fortuitas. Para mayor referencia se puede consultar y considerar las recomendaciones contenidas en la ISO 17799:2005 en su apartado 10.7.

- La documentación de la cadena de custodia debe contener todos los lugares por donde ha pasado la evidencia, quien realizo su transporte y quien tuvo acceso a la misma.
- Antes de ser almacenados se debe considerar la naturaleza del elemento confiscado para utilizar los medios más adecuados para el mismo, por ejemplo en el caso de discos duros, CD, Cintas de Copias de seguridad o similares, deben ser protegidos contra electricidad estativa por lo cual se debe utilizar bolsas antiestáticas para evitar la pérdida o daño en los datos contenidos.
- Mientras los elementos estén en el laboratorio y no estén siendo manipulados constantemente, es necesario embalarlos con etiquetas informativas que contengan al menos datos como:
    - Identificador único para cada elemento.
    - Nombre del técnico responsable del material.
    - Descripción del mismo.
    - Propietario.
    - Lugar en que fue confiscado.
    - Fecha y hora del evento.
    - Observaciones.

- **Fase 4: Analizar las evidencias obtenidas**

  La fase del análisis culmina solamente cuando se logra determinar que o quien causo el incidente, como lo hizo, porque y que repercusiones tuvo esto. Es decir esta fase es en sí es el porqué de la investigación y esta dará el máximo de información posible para poder documentar todo adecuadamente y realizar los informes pertinentes del caso.

  Siempre antes de empezar el análisis hay que tener en cuenta lo siguiente:

  - Como se ha indicado en las fases anteriores nunca se debe trabajar con los datos originales sino con copias del mismo.
  - Se debe respetar las leyes correspondientes de cada jurisdicción en donde se lleve a cabo la investigación.
  - Los resultados obtenidos deben ser completamente verificables y reproducibles.
  - Disponer de una documentación adicional a la información de diversa índole por ejemplo:
    - Sistema operativo del sistema.
    - Programas instalados en el equipo.
    - Hardware, accesorios y periféricos que forman parte del sistema.
    - Datos relativos a la conectividad del equipo:
      - Si dispone de firewall, ya sea físico o lógico.
      - Si el equipo se encuentra en zonas de red especiales, por ejemplo, DMZ.
      - Si tiene conexión a Internet o utiliza Proxy.

- Datos generales de la configuración que puedan ser de interés para el investigador.

Es importante tener en cuenta que no existe un proceso estandarizado que norme la investigación por lo cual será necesario analizar cada caso por separado teniendo en cuenta las particularidades de cada uno. También no se actuara de la misma forma con todos los casos pero se puede destacar varios pasos esenciales recomendados por (Rivas, 2014):

- Preparar un entorno de trabajo adaptado a las necesidades del incidente.
  - Aquí se deberá decidir el tipo de análisis que se va a hacer en caliente o en frio.
  - En el caso de análisis en caliente hay tener en cuenta los riesgos que esta tiene debido a que se trabajará sobre la evidencia original y cualquier error puede ser fatal.
  - El análisis en frio es más recomendable ya que se podrá reproducir y ejecutar sin miedo los eventos sin que la copia original resulte afectada.
- Reconstruir una línea temporal con los hechos sucedidos.
  - Para crear la línea temporal lo más sencillo es referirse a las fechas de modificación, acceso, cambio y borrado.
  - Es importante tener en cuenta el huso horario del lugar del evento y del lugar del análisis.
  - Acudir a los registros del sistema operativo el cual brindará una completa información desde que fue instalado.

  - Con lo anteriormente mencionado se podrá crear un esbozo de los puntos clave en el tiempo que puedan aportar o afianzar la evidencia.
- Determinar que procedimiento se llevó a cabo por parte del atacante.
  - Se debe llevar a cabo la investigación sobre la memoria del equipo para lo cual el volcado de memoria facilita la obtención de cierta información.
  - Con programas adecuados para estos fines se tendrá que visualizar los procesos visibles y ocultos, saber que ejecutables inician los procesos en ejecución y que librerías se ven involucradas.
- Identificar el autor o autores de los hechos.
  - El volcado de memoria también proporciona información sobre las conexiones de red abiertas y las que están preparadas para enviar o recibir datos. Esta información puede ayudarnos a relacionar el posible origen del ataque buscando datos como la dirección IP. Aunque se debe actuar con cautela ya que existen diferentes técnicas para distribuir los ataques o falsear la dirección IP.
  - Se debe considerar los distintos perfiles de atacantes que existen hoy día en este ámbito para intentar mimetizarse y entender quién pudo ser el autor.
- Evaluar el impacto causado y si es posible la recuperación del sistema.
  - Es difícil calcular el impacto de un incidente debido a los distintos factores a ser considerados y a que no hay un método estándar para su cálculo. Sin embargo existen métodos como BIA (Business Impact Analysis) que determinan el impacto de ciertos eventos ayudando a valorar los daños económicamente.

- No solo se puede calcular económicamente el impacto causado puede haber una larga cadena de sucesos los cuales pueden ser:
    - Repercusiones en el trabajo de los colaboradores.
    - Malversación de información y desacreditación.
    - Difusión de información confidencial.

- **Fase 5: Redactar informes sobre los resultados**

  La última fase de análisis forense consiste en la elaboración de los informes que documentaran los antecedentes al evento, todo el trabajo realizado, el método seguido y las conclusiones e impacto.

  Para esto se deben red informes, el técnico y el ejecutivo los cuales explican el mismo hecho de un enfoque y grado de detalle diferente.

  Informe ejecutivo

  Este informe será un resumen de toda la tarea llevada a cabo pero no tendrá una extensión amplia comparada con el informe técnico pero deberá contener al menos los siguientes apartados según (Rivas, 2014):

  - Motivos de la intrusión.
    - ¿Por qué se ha producido el incidente?
    - ¿Qué finalidad tenía el atacante?
  - Desarrollo de la intrusión.
    - ¿Cómo lo ha logrado?
    - ¿Qué ha realizado en los sistemas?
  - Resultados del análisis.
    - ¿Qué ha pasado?

- ¿Qué daños se han producido o se prevé que se producirán?
- ¿Es denunciable?
- ¿Quién es el autor o autores?

- Recomendaciones.
  - ¿Qué pasos dar a continuación?
  - ¿Cómo protegerse para no repetir los hechos?

Informe técnico

Este informe será mucho más extenso que el anterior debido a que se presenta con mayor detalle y con profundidad en la tecnología usada y los hallazgos.

Para este informe se debe redactar al menos:

- Antecedentes del incidente.
  - Puesta en situación de cómo se encontraba la situación anteriormente al incidente.
- Recolección de datos.
  - ¿Cómo se ha llevado a cabo el proceso?
  - ¿Qué se ha recolectado?
- Descripción de la evidencia.
  - Detalles técnicos de las evidencias recolectadas, su estado, su contenido, etcétera.
- Entorno de trabajo del análisis.
  - ¿Qué herramientas se han usado?
  - ¿Cómo se han usado?

- Análisis de las evidencias.
    - Se deberá informar del sistema analizado aportando datos como las características del sistema operativo, las aplicaciones instaladas en el equipo, los servicios en ejecución, las vulnerabilidades que se han detectado y la metodología usada.
- Descripción de los resultados.
    - ¿Qué herramientas ha usado el atacante?
    - ¿Qué alcance ha tenido el incidente?
    - Determinar el origen del mismo y como se ha encontrado.
- Dar la línea temporal de los hechos ocurridos con todo detalle.
- Redactar unas conclusiones con las valoraciones que se crean oportunas a la vista de todo el análisis realizado.
- Dar unas recomendaciones sobre cómo proteger los equipos para no repetir el incidente o sobre cómo actuar legalmente contra el autor.

3.2. Herramientas para análisis forense.

La informática forense es una rama muy importante de la ciencia de la computación en relación con los crímenes de computadora e Internet. El objetivo principal de la informática forense es desarrollar investigación de crímenes usando evidencias de la información digital y encontrar quien fue el responsable y que efectos tuvo este ataque.

Para una mejor investigación los desarrolladores han creado muchas herramientas para el análisis forense. Los departamentos de policía y agencias de

investigación de seleccionar las herramientas basadas en varios factores, incluyendo el presupuesto y los expertos disponibles en el equipo.

Estas herramientas de informática forense pueden también ser clasificadas en varias categorías:

- Disco de datos y herramientas de captura
- Herramientas de análisis de archivos
- Herramientas de análisis del registro
- Herramientas de análisis de Internet
- Herramientas de análisis de correo electrónico
- Herramientas de análisis de dispositivos móviles
- Herramientas de análisis de Mac OS
- Herramientas forenses para el análisis de la red
- Herramientas forenses para el análisis de base de datos

Tabla 3
Comparación de herramientas OpenSource con características básicas

	RedoBackup	**Recuva**	**Speecy**	**File.net**	**Process Explorer**
Software / Licencia	Gratuito	Gratuito	Gratuito	Gratuito	Comercial
Plataforma Soportada	Windows 8, 7,Vista, Linux	Windows 8, 7,Vista, XP	Windows 8, 7,Vista	Windows 8,7,Vista, XP	Windows 8, 7,Vista, XP
Desarrollador	RedoBackUp.org	Piriform	Piriform	Windows Partner	Windows Sysinternals
Rendimiento	Alto	Bajo	Alto	Alto	Alto
Utilidad	Bueno	Medio	Bueno	Bueno	Bueno

Fuente: (Dhwaniket & Nilakshi, 2015)

En la tabla 3 se comparara algunas características entre las herramientas forenses más populares tomando en cuenta el tipo de software

3.3. Cadena de custodia

La caracterización de la cadena de custodia se da por una serie de rasgos distintivos que proveen una certificación del uso adecuado del proceso, entre las características más importantes se encuentran:

- Inicia desde la recolección y conocimiento de las pruebas, finaliza con el juez y los funcionarios.
- La cadena de custodia es un proceso manual en toda su vida útil.
- La custodia se aplica a todo elemento probatorio físico. Extendiendo la misma a la documentación que acompañe al material.
- La cadena de custodia están formados por personas que tienen la responsabilidad de proteger a los elementos de prueba.
- La cadena de custodia tendrá el registro de: fecha, hora, nombre y firma de quien recibe y de quien entrega.

3.3.1. Importancia

La importancia de la cadena de custodia radica en asegurar la integridad de las pruebas recolectadas identificando certeramente a las personas involucradas en la cadena, es decir todos las personas que tuvieron algún contacto con las evidencias, por mínimo e insignificante que este contacto fuera, también establecer la relación de la evidencia con el hecho, el sitio o lugar del hecho, asimismo los involucrados, víctima y victimario. (García, 2014)

3.3.2. Principios de cadena de custodia

- Aseguramiento de la prueba: protección de medios probatorios.
- Licitud de la prueba: medios de obtención de pruebas legales.
- Veracidad de la prueba: obtención y preservación de la autenticidad de las pruebas.
- Necesidad de la prueba: prueba útil a la investigación y que puede probar un hecho

CAPÍTULO 4

APLICACIÓN DE LA GUÍA METODOLÓGICA EN LA RESOLUCIÓN DE UN CASO PRÁCTICO WINDOWS 8

4.1. Antecedentes

Se plantea el caso de la intrusión al computador de la administradora de la empresa INDUSTEC quien reporta la pérdida de información valiosa sobre el KNOW-HOW de la empresa la cual ha sido borrada del equipo y además reporta transacciones no autorizada y de las cuales no tiene conocimiento desde la cuenta bancaria de la empresa. Como medida de seguridad se cambiaron todas las claves que están a cargo de esta persona y se dejó de utilizar el equipo presuntamente infectado.

Según información proporcionada, se pudo identificar los siguientes incidentes llevados a cabo en el ataque:

- Eliminación de archivos importantes y presunto robo de la misma.
- Posible acceso a las cuentas sociales las cuales la administradora tenía siempre abiertas en su computador.

4.2. Entorno de investigación

El entorno de investigación como su nombre lo indica es aquel en cual se va a llevar a cabo la aplicación de las diferentes técnicas y herramientas de análisis forense que permitan resolver el caso.

4.2.1. Herramientas utilizadas

Tabla 4
Herramientas utilizadas para la investigación

Software	Observación
Virtual Box 5.0	Software virtualizador para arquitecturas x86/amd64, desarrollado por la empresa Oracle Corporation. Es de libre distribución. https://www.virtualbox.org/wiki/Downloads
Recuva v1.52.1086	Software de recuperación de archivos de todo tipo desde cualquier dispositivo de almacenamiento. Su versión básica es de libre distribución y su versión profesional se distribuye bajo licencia. http://www.piriform.com/recuva/download/standard
eSupport UndeletePlus v 3.0.6	Software de recuperación de archivos de todo tipo desde cualquier dispositivo de almacenamiento. Es de licencia privativa. http://www.undeleteplus.com/
Speccy v1.29.714	Software que muestra información detallada acerca del hardware y software del computador. Su versión básica es de libre distribución y su versión profesional se distribuye bajo licencia. https://www.piriform.com/speccy/download/standard
CPU-Z v1.75	Software que muestra información detallada acerca del hardware y software del computador. Su versión básica es de libre distribución y su versión profesional se distribuye bajo licencia. http://www.cpuid.com/softwares/cpu-z.html
File.net	Página Microsoft Partner la cual contiene una amplia base de datos acerca de archivos de Windows desde 2005. Es de libre acceso. http://www.file.net/
Process Explorer v1	Software que provee la funcionalidad de la administración de Tareas pero con varias opciones para recolectar información acerca de los procesos que están siendo corridos en el sistema del usuario. Es de libre distribución. https://technet.microsoft.com/en-us/sysinternals/processexplorer.aspx
Process Hacker v2.3.4.3.	Software que provee la funcionalidad de la administración de tareas pero con varias opciones para recolectar información acerca de los procesos que están siendo corridos en el sistema del usuario. Es de libre distribución. http://processhacker.sourceforge.net/
Visor de Sucesos de Windows 8.1.	Herramienta predeterminada de Windows que permite visualizar los diferentes sucesos del sistema. Viene integrado en el sistema Windows 8.1.
Event Log Explorer 4.5.3	Software que permite el análisis sucesos del sistema y guardar el respaldo en formato para abrirlo en cualquier visor de sucesos predeterminado de Windows. Su licencia es pagada. http://eventlogxp.com/download.html
Redo v1.0.4	Software para creación de respaldos y recuperación de desastres de software. Es de libre distribución. https://sourceforge.net/projects/redobackup/
Acronis True Image 2016	Software para creación de respaldos y recuperación de desastres de software. Es de licencia pagada. http://www.acronis.com/en-us/personal/computer-backup/

Fuente: (Sanchez Herrera & Basantes Salazar)

4.2.2. Lugar de análisis

Lugar de residencia de Katherine Sánchez. Laboratorio técnico.

4.3. Metodología del análisis forense

Después de evaluar lo manifestado por la administradora, se obtiene la todas las evidencias que puedan ser de ayuda para la resolución de este caso y así poder determinar el alcance del delito.

4.3.1. Cadena de Custodia.

La cadena de custodia es una herramienta que tiene un valor muy significativo en el ámbito forense, esto se inicia con la recolección de la evidencia en el lugar donde sucedió el incidente y termina cuando se entrega a la autoridad designada. Esta es tan importante que si se interrumpe en algún momento no se tiene seguro de que la prueba sea válida.

En una cadena de custodia es necesario que la información no sea modificada, por ese motivo es necesario el uso de las normas de bioseguridad y respetar el orden a seguir en la inspección. (Zapata, 2013).

El juez tiene que confiar en dichos elementos digitales, ya que son los conocidos “testigos mudos”, por este motivo su identificación, recolección, protección, reguardo, empaque y traslado de la evidencia del lugar hasta su presentación como elemento probatorio. Este debe garantizar que la evidencia recolectada en la escena del crimen es la misma que se está presentando al evaluador. Por este motivo es necesario establecer un riguroso registro, indicando lugar, hora, fecha, nombre, dependencia involucrada, interacción posterior y su depósito en la sede

que corresponda. Si no tiene ninguno de estos componentes, la prueba recolectada no habrá alcanzado el objetivo probatorio. (Palencia, Romero, & de Danielle, 2008).

4.3.2. Asegurar la escena

Una vez determinado el incidente ocurrido con el computador, se procede a asegurar la escena del crimen y recolectar las evidencias posibles.

En primera instancia se toma fotografías del lugar y de cómo se encontró el equipo, como se indica en la Figura 17.

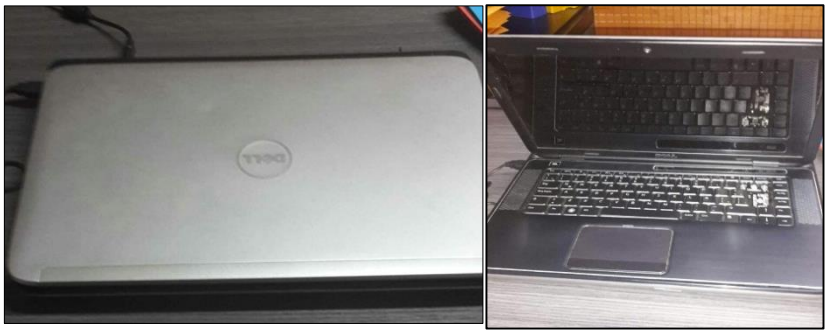


Figura 16 Condiciones en las que se encontró el computador

(Sanchez Herrera & Basantes Salazar)

A continuación se procede hacer una inspección del lugar tomando en cuenta cualquier particular que pueda estar involucrado en el caso realizando lo siguiente:

- Se anotó la hora y fecha de todos los computadores, y se identificó que no existe ningún desfase en el huso horario.
- Se verifica los periféricos conectados al computador encontrando una impresora de marca EPSON, mouse, teclado e impresora conectada vía Wi-Fi.

En la Tabla 5 se hace una pequeña descripción de la escena del crimen, con los datos anteriormente descritos.

Tabla 5
Descripción de la escena de los hechos

Lugar	Oficina administración empresa Industec
Fecha y Hora	17/02/2016 14:00:00
Número de Personas en el lugar	4
Listado de Personas en el lugar	• Mireya Barragán (Administradora). • Lady Salazar (Contadora). • Elizabeth Chano (Secretaria).
Ubicación física del equipo vulnerado	Escritorio perteneciente a la Administradora
Personas que tienen acceso al equipo vulnerado	Mireya Barragán (Administradora)
Descripción Física del Equipo	• Color: Plateado. • Dimensiones 38x27. • Estado: Medio Uso.
Descripción de hardware del Equipo	• Windows 8.1 Pro 64-bit. • Intel Core i5. • RAM: 4gb. • Almacenamiento: 465 Gb.
Periféricos conectados al Equipo	Mouse, Teclado, Impresora (Vía Wi-fi).
Conexión a Internet	Si
Persona quien toma custodia de la evidencia	Katherine Sanchez
Medidas de seguridad tomadas para la custodia.	Se coloca el equipo dentro de una funda protectora de neopreno para evitar cualquier daño del equipo que altere la información.

Fuente: (Sanchez Herrera & Basantes Salazar)

4.3.3. Identificar, recolectar y preservar las evidencias

4.3.3.1. Identificación

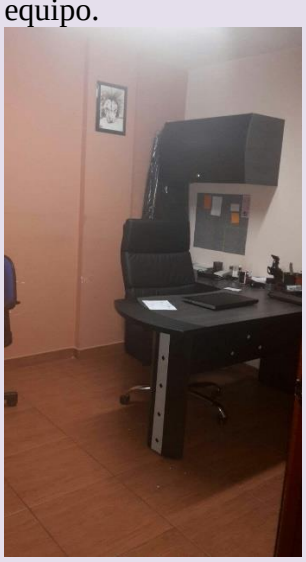
En esta fase es importante tomar en cuenta el hardware que pueda albergar aquella información que sea relevante al momento de la investigación. Las evidencias digitales que se encontró se describirán en las tablas 6,7 y 8.

Tabla 6
Descripción de evidencia 1

Evidencia #1	
Computador Portátil: Detalle de hardware	Modelo Dell XPS 15. CPU: Intel Core i5 2.53GHz. RAM: 4GB DDR3. Gráficos: 1023 MB NVIDIA Geforce GT 420M. Disco Duro: 465GB SATA.
Estado Físico del Equipo.	Vida útil media, tiene el teclado con teclas faltantes por lo cual utilizan otro teclado externo.
Dimensiones del Equipo.	38x27cm.

Fuente: (Sanchez Herrera & Basantes Salazar)

Tabla 7
Descripción de evidencia 2

Evidencia 2	Fotografías
Fotografía del lugar del incidente:	Oficina administración empresa Industec, escritorio donde se encontró el equipo. 

Fotografía de las inmediaciones:	

Fuente: (Sanchez Herrera & Basantes Salazar)

Tabla 8
Descripción de evidencia 3

Evidencia 3	**Testimonios**
Mireya Barragán (Administradora)	- El equipo fue recientemente formateado ya que todos los equipos de computación de la empresa entraron en un plan de mantenimiento en el cual el técnico entregó todos los equipos en las condiciones acordadas y todos los equipos se entregaron con la misma contraseña para luego ser cambiadas al gusto de los usuarios sin embargo este computador aún no había sido actualizado por lo cual podía ser accesado por cualquier persona de la oficina. - El equipo funcionó en estas condiciones desde el 08/02/2016 hasta el 17/02/2016 que ocurrió el incidente. - El día del incidente la administradora se da cuenta que ciertos archivos muy importantes no se encuentran en la dirección usual, ni en la papelera o en cualquier otro directorio por lo cual decide solicitar ayuda profesional principalmente para la recuperación de la información perdida.

Fuente: (Sanchez Herrera & Basantes Salazar)

4.3.3.2. Recolección

Tabla 9
Recolección evidencia 1

Evidencia 1	
Computador portátil	
	Utilización de una funda de neopreno anti golpes para resguardar el equipo.
Custodio	Katherine Sánchez
Lugar de destino	Residencia de Katherine Sánchez laboratorio de análisis.

Fuente: (Sanchez Herrera & Basantes Salazar)

Tabla 10
Recolección evidencia 2

Evidencia 2	
Fotografías	
	Utilización de cámara en teléfono celular.
Custodio	Katherine Sánchez
Lugar de destino	Residencia de Katherine Sánchez laboratorio de análisis.

Fuente: (Sanchez Herrera & Basantes Salazar)

4.3.4. Análisis de evidencia

Esta fase es la parte neurálgica de todo el proceso ya que aquí se examina la evidencia. A continuación se muestran los diferentes pasos a seguir para realizar un análisis forense óptimo.

4.3.4.1. Preparación de entorno de trabajo

Para el análisis de la evidencia se utilizara las diferentes herramientas citadas en la Tabla 4.

4.3.4.1.1. Creación de imagen

RedoBackup

Utilizando la herramienta Redo v1.0.4 se extrajo dos copias exactas del equipo en las condiciones que fue encontrado luego del ataque. Una de estas copias será virtualizada para su análisis usando Virtual Box 5.0 en combinación de Redo v1.0.4 para realizar la restauración de la copia.

Lo primero a realizar fue el backup del disco utilizando Redo. Se tiene que bootear con Redo para proseguir al backup. En las Figuras 18, 19, 20 y 21 se describen los pasos a seguir:

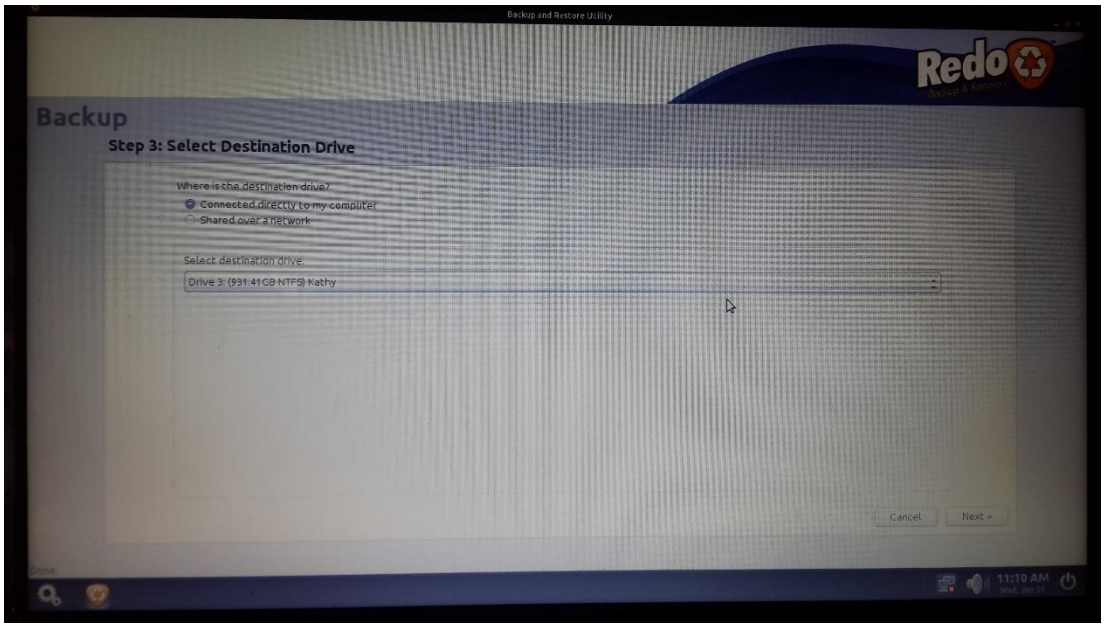


Figura 17 Selección del directorio en donde se guardara el backup

Fuente: (Sanchez Herrera & Basantes Salazar)

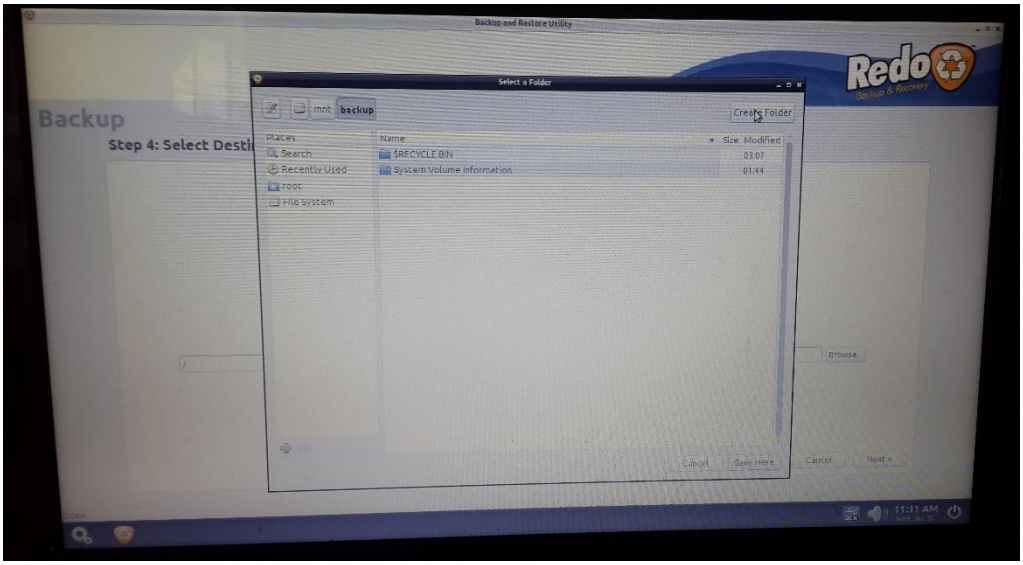


Figura 18 Se crea una carpeta para guardar el backup

Fuente: (Sanchez Herrera & Basantes Salazar)

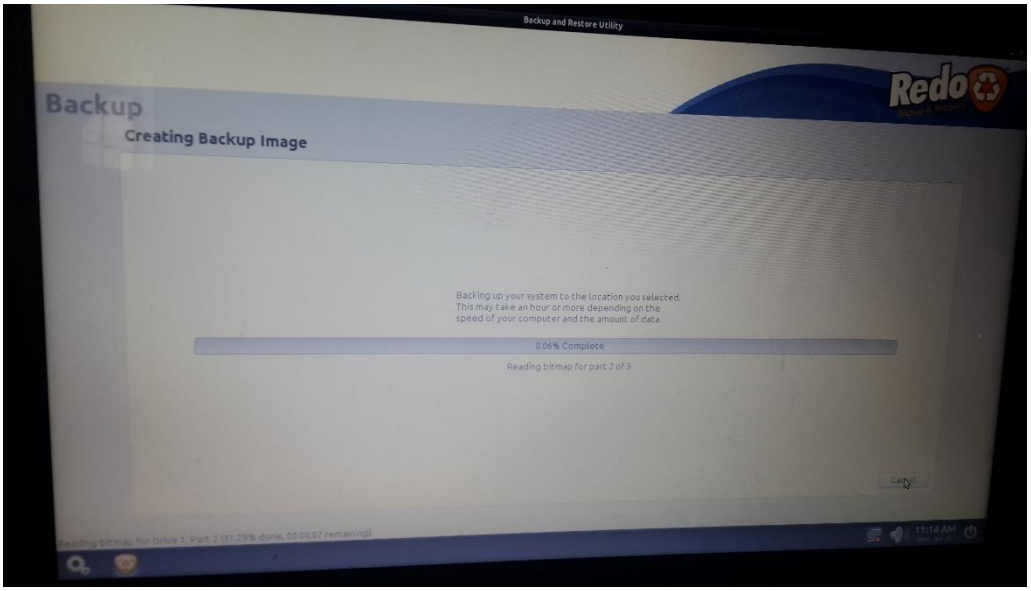


Figura 19 Comenzara a crear la imagen del disco

Fuente: (Sanchez Herrera & Basantes Salazar)

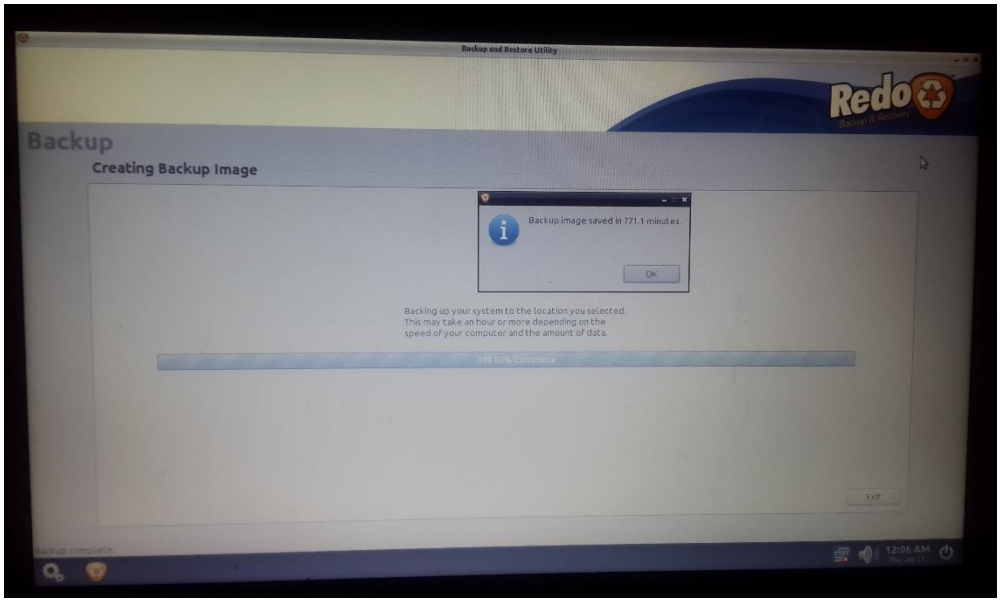


Figura 20 Finalización del proceso de backup del disco

Fuente: (Sanchez Herrera & Basantes Salazar)

Una vez realizado el backup se procede a crear una máquina virtual en la que se procede a instalar una imagen del disco. Para esto se utiliza de igual manera la herramienta REDO, como se muestra en las Figuras 22, 23, 24, 25, 26, 27 y 28.

Figura 21 Pantalla de inicio de RedoBackup

Fuente: (Sanchez Herrera & Basantes Salazar)

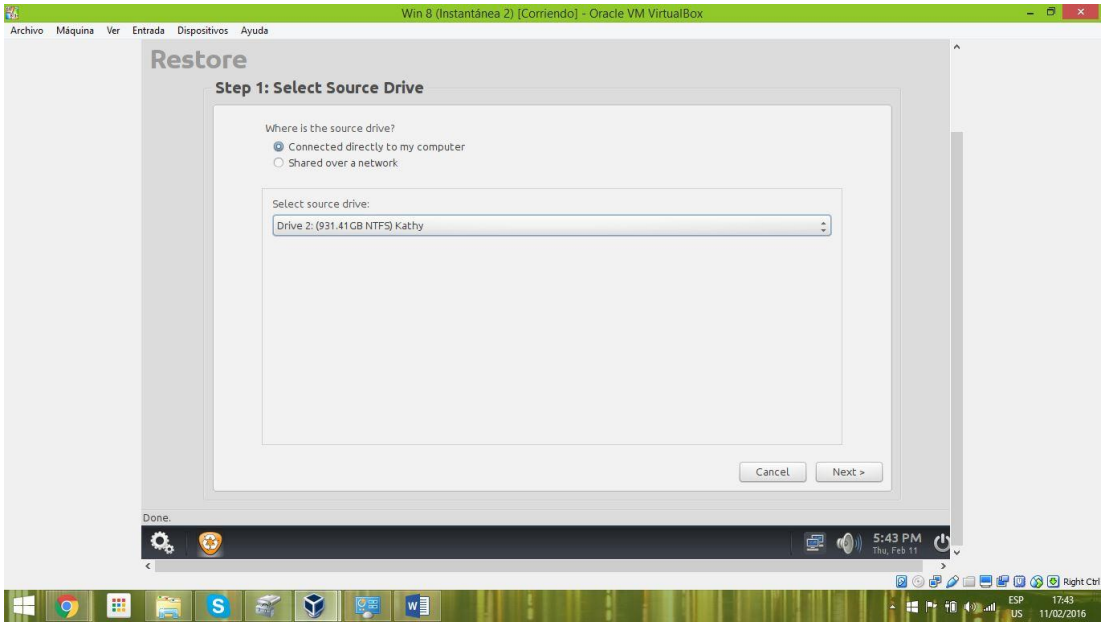


Figura 22 Pantalla de Selección Fuente de Imagen

Fuente: (Sanchez Herrera & Basantes Salazar)

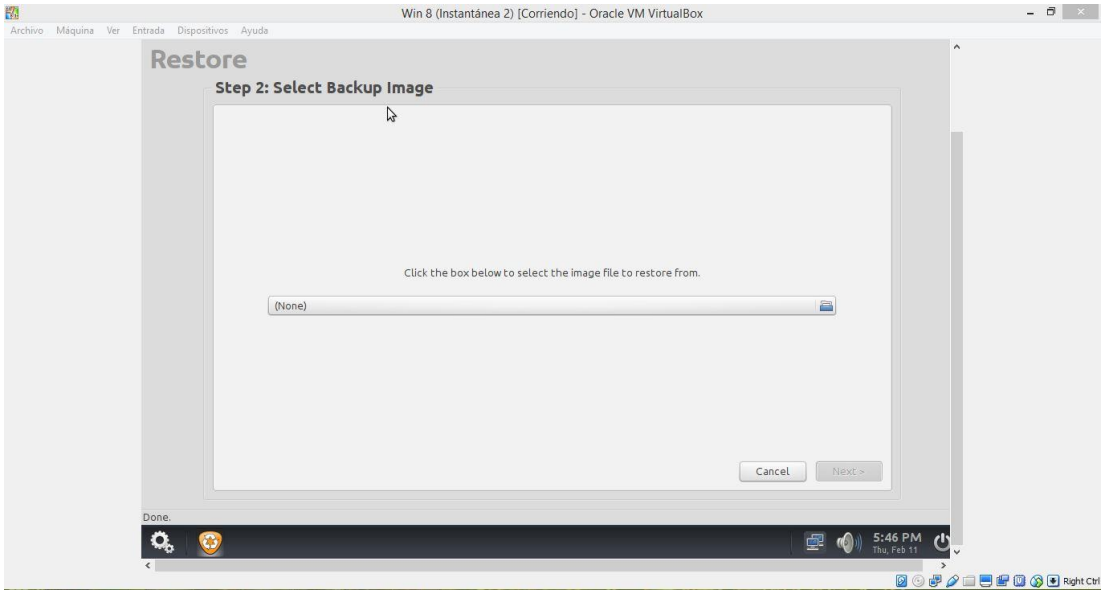


Figura 23 Pantalla de selección fuente de imagen

Fuente: (Sanchez Herrera & Basantes Salazar)

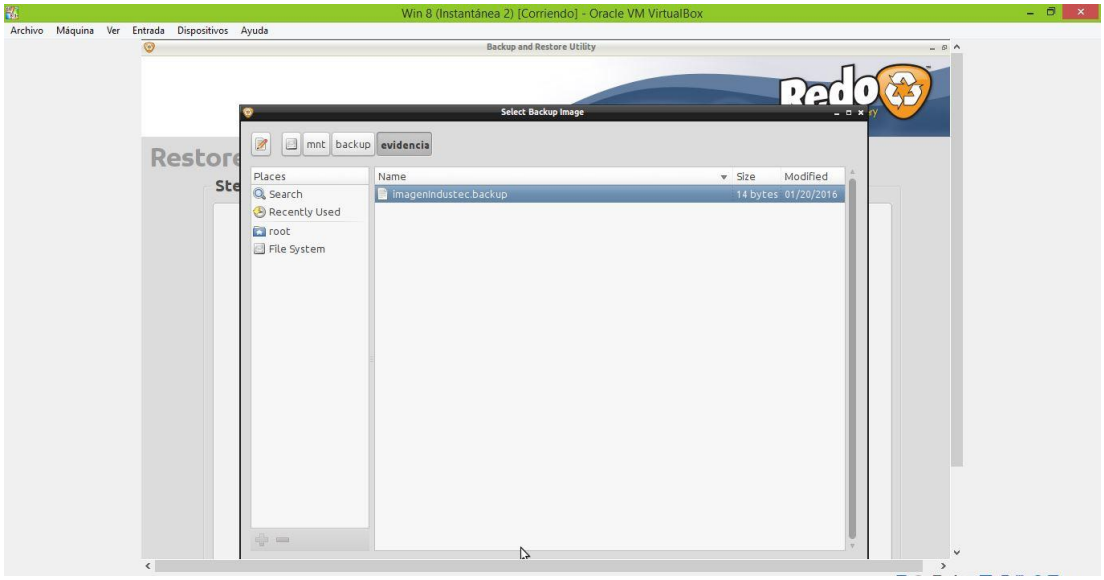


Figura 24 Pantalla de selección donde se encuentra backup

Fuente: (Sanchez Herrera & Basantes Salazar)

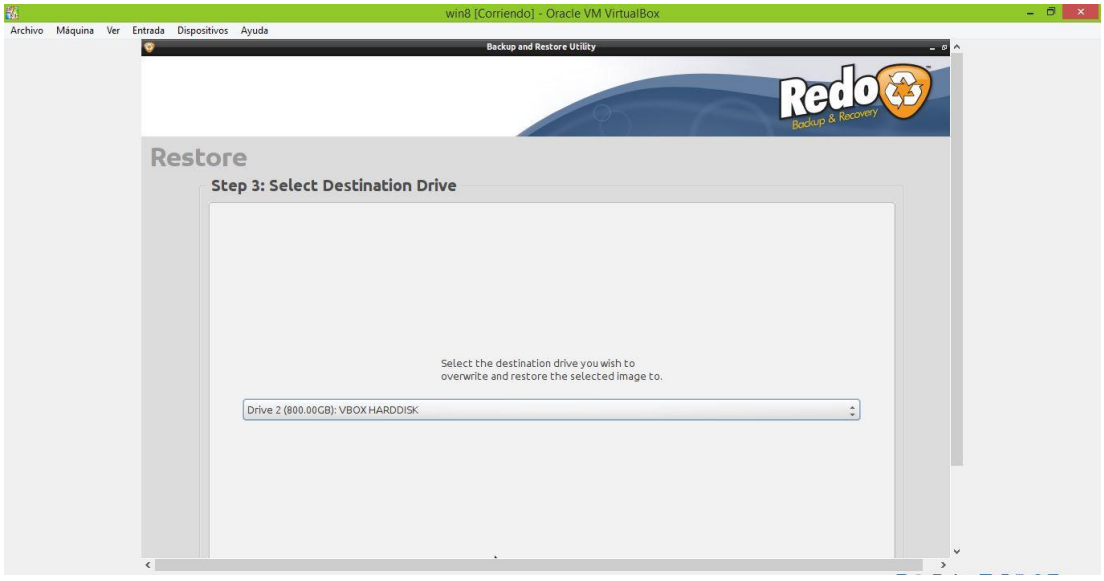


Figura 25 Pantalla de selección de disco duro

Fuente: (Sanchez Herrera & Basantes Salazar)

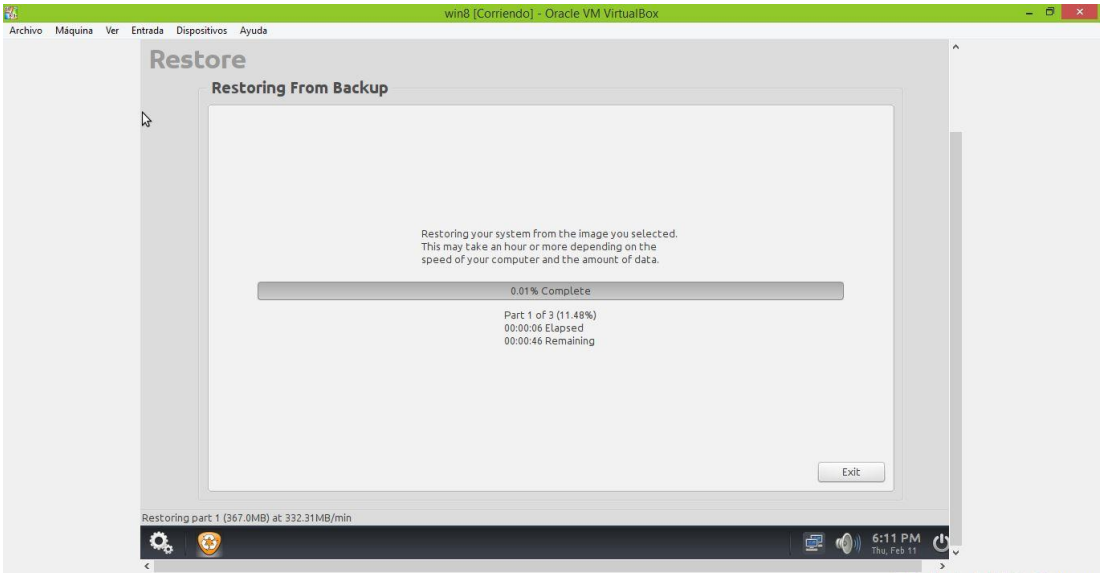


Figura 26 Proceso de instalación

Fuente: (Sanchez Herrera & Basantes Salazar)

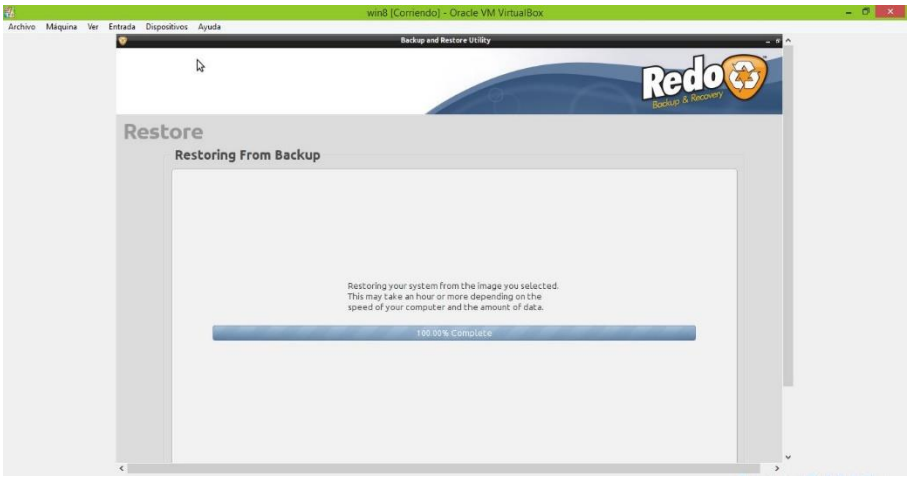


Figura 27 Pantalla de restauración de Backup

Fuente: (Sanchez Herrera & Basantes Salazar)

Acronis True Image

Acronis True Image es una visión completamente nueva de la copia de seguridad. Es la tecnología de sincronización más reciente. Es almacenamiento en el

cloud. True Image compatible con dispositivos nuevos. Se utilizará ésta herramienta para hacer una comparación de tiempo y desempeño entre dos herramientas de backup.

Para este caso se necesita descargar la herramienta e instalarla en el computador e iniciarla como se indica en las Figuras 29 y 30.

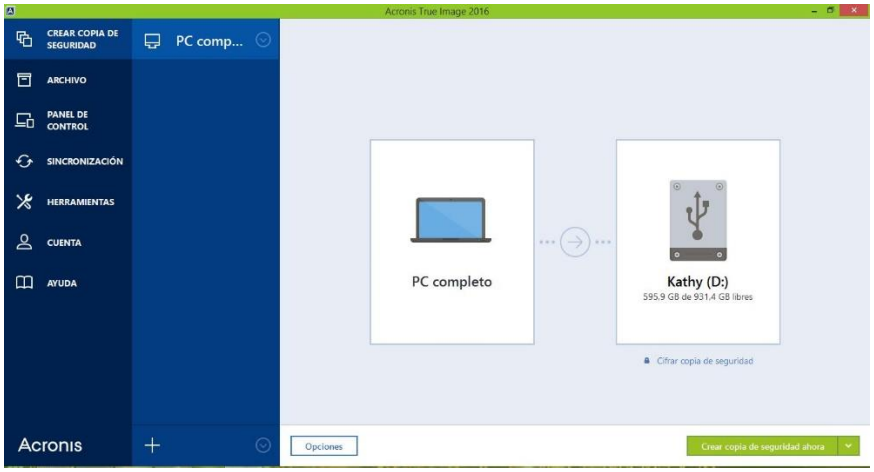


Figura 28 Pantalla de selección de disco a ser clonado

(Sanchez Herrera & Basantes Salazar)

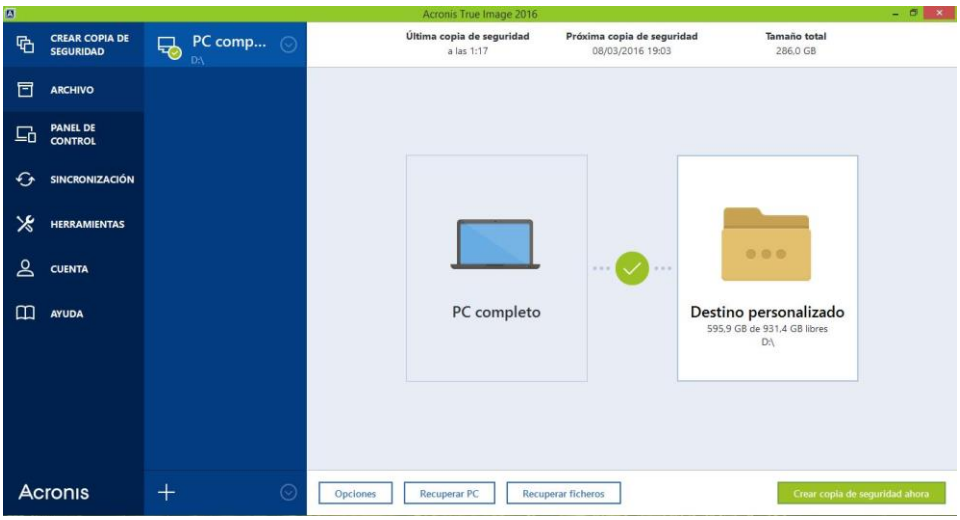


Figura 29 Finalización de la clonación

(Sanchez Herrera & Basantes Salazar)

Resultados

Una vez realizado el backup del disco duro con las dos herramientas antes descritas, se obtuvo los siguientes resultados que se encuentra descritos en las Tablas 11 y 12:

Tabla 11
Características del disco duro

Propiedades del dispositivo:	
Descripción del controlador	ST9640320AS
Fecha del controlador	21/06/2006
Versión del controlador	6.3.9600.16384
Proveedor del controlador	Microsoft
Información física del dispositivo de disco:	
Fabricante	Seagate
Nombre del disco duro	Momentus 5400.7 640320
Forma	2.5"
Capacidad formateado	465 GB
Discos	2
Superficies de grabación	4
Dimensiones físicas	100.35 x 69.85 x 9.5 mm
Peso máximo	100 g
Latencia media de rotación	5.5 ms
Velocidad de rotación	5400 RPM
Tasa máx. de datos interna	1175 Mbit/s
Tiempo de búsqueda medio	13 ms
Búsqueda pista a pista	1.5 ms
Búsqueda completa	27 ms
Interfaz	SATA-II
Tasa de búfer hacia host	300 MB/s
Tamaño del búfer	8 MB
Fabricante del dispositivo:	
Nombre de la empresa	Seagate Technology LLC
Información del producto	http://www.seagate.com/gb/en

(Sanchez Herrera & Basantes Salazar)

Tabla 12
Cuadro comparativo de dos herramientas para el backup de discos

Software	Licencia	Antivirus	Clave acceso	Firewall	Archivos Copiados	Duración	Observaciones
RedoBackup	Gratuita	Avast Antivirus	Si	Activado	268 GB	771.1 minutos	La licencia es gratuita pero su interfaz no es de fácil utilización para personas con poco conocimiento
Acronis True Image	Pagada	Avast Antivirus	Si	Activado	285 GB	145.6 minutos	Su utilización es mucho más sencilla debido a que se instala en el computador

(Sanchez Herrera & Basantes Salazar)

4.3.4.2. Recuperación de archivos perdidos utilizando RECUVA

Luego de descargar la herramienta gratuita de la página oficial https: //www.piriform.com, de la cual existen versiones de pago con mejores opciones pero ponen a nuestra disposición totalmente gratis la versión básica, la cual será de gran importancia al momento de recuperación de datos e información perdida.

Recuva ofrece una interface bastante fácil de usar y bastante interactiva con el usuario detallando claramente cada fase a seguir.

- **Utilización de la herramienta.**

Para iniciar Recuva presenta un asistente el cual resulta bastante útil para filtrar mejor la información, como se puede apreciar en la Figura 31.

Figura 30 Página principal del asistente de Recuva.

Fuente: (Sanchez Herrera & Basantes Salazar)

Se procede a seleccionar el tipo de archivo que se requiere recuperar en este caso Documentos, como se puede observar en la Figura 32.

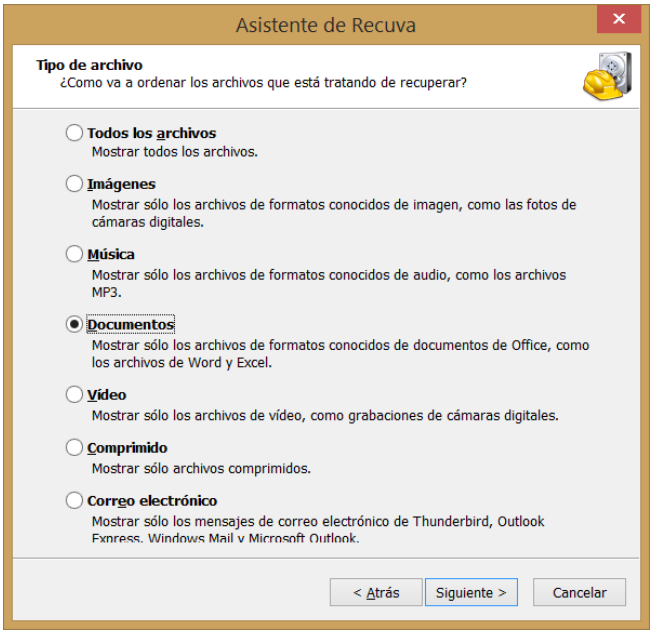


Figura 31 Tipo de archivo que se quiere recuperar

Fuente: (Sanchez Herrera & Basantes Salazar)

En la Figura 33 se observa la ubicación que proporciono el cliente, en donde se encontraban estos archivos.

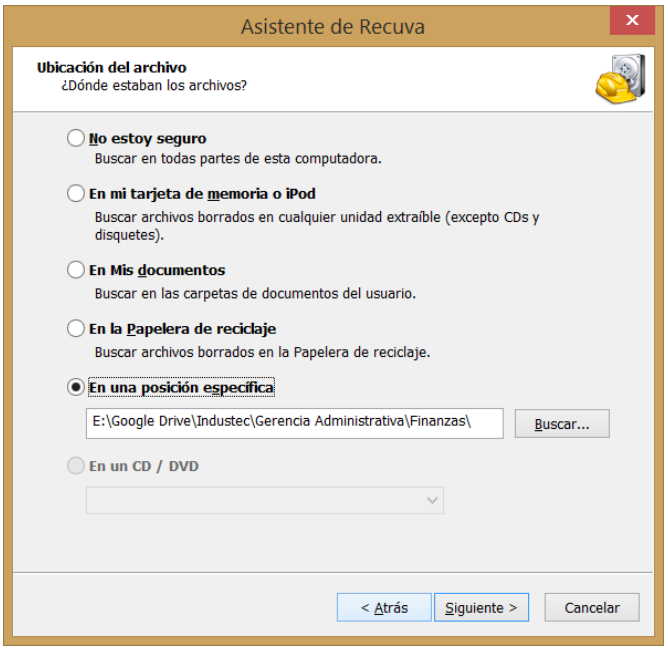


Figura 32 Selección de la ubicación de los archivos

Fuente: (Sanchez Herrera & Basantes Salazar)

Finalmente se procede con el escaneo profundo del directorio, el cual toma más tiempo pero reduce la probabilidad de cualquier error u omisión de información, como se aprecia en la Figura 34.

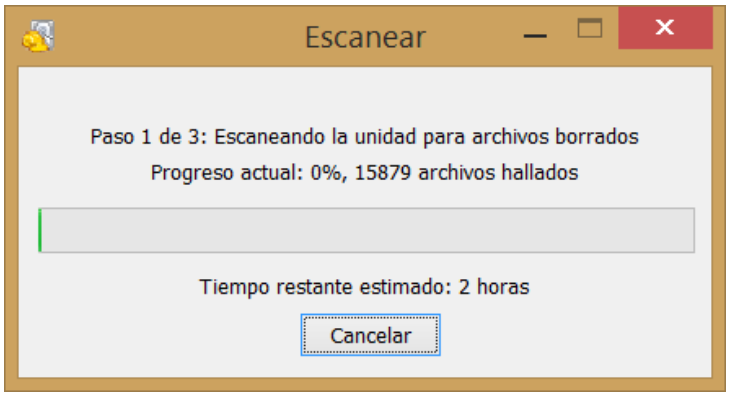


Figura 33 Proceso de escaneo profundo

Fuente: (Sanchez Herrera & Basantes Salazar)

Al final del análisis se encontró los archivos mencionados por el cliente de los cuales se procede con la recuperación y además con el listado (Figura 35) de los elementos encontrados aparte de los solicitados.

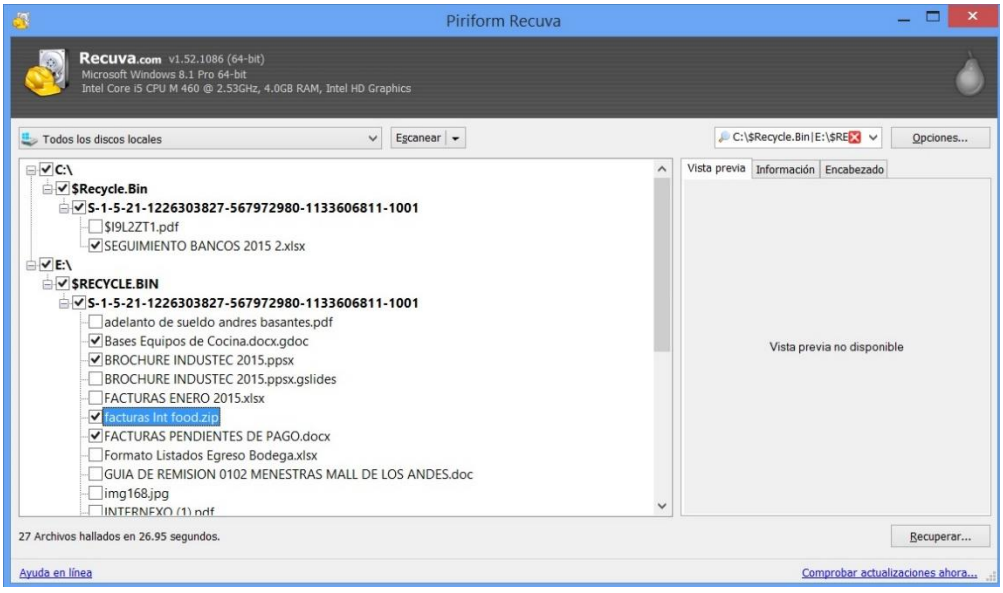


Figura 34 Búsqueda del archivo borrado

Fuente: (Sanchez Herrera & Basantes Salazar)

Continuando con el proceso, se procede como norma de seguridad a hacer un análisis profundo tanto del estado del hardware como del software instalado y los procesos en ejecución con el objetivo encontrar cualquier anomalía y encontrar pistas de software malicioso utilizado para este ataque.

4.3.4.2.1. Recuperación de Archivos perdidos utilizando eSupport UndeletePlus

Luego de descargar la herramienta gratuita de la página oficial https: //www.undeleteplus.com/, de la cual hay una versión de evaluación que permite realizar la examinación gratis pero en el momento de proceder con la recuperación de los archivos solicita la adquisición de una licencia.

- **Utilización de la herramienta.**

  Se inicia seleccionando las ubicaciones que se van a analizar, como se puede apreciar en la Figura 36.

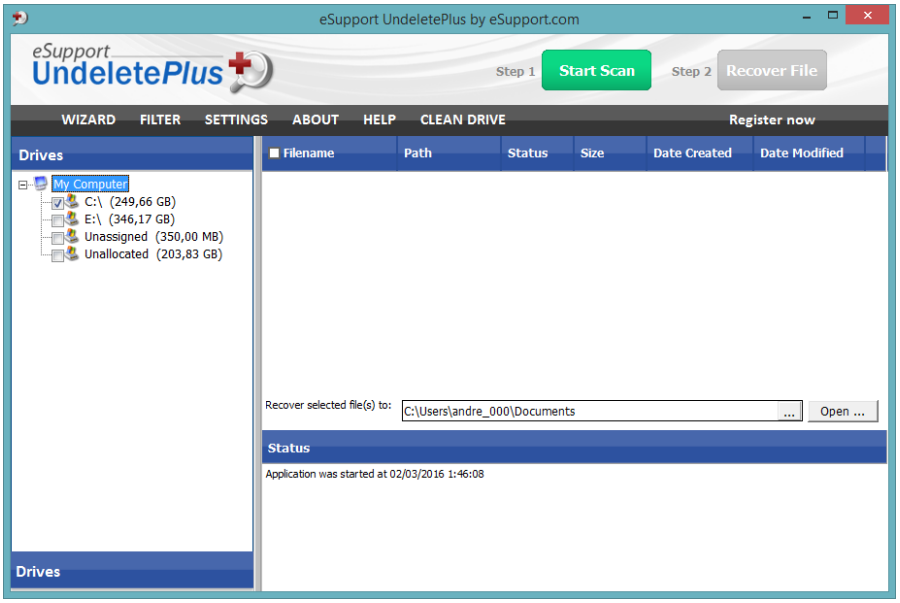


Figura 35 Página principal de eSupport UndeletePlus

Fuente: (Sanchez Herrera & Basantes Salazar)

La herramienta posee un proceso Wizard que permite seleccionar de mejor forma los criterios de búsqueda, como se puede observar en las Figuras 37.

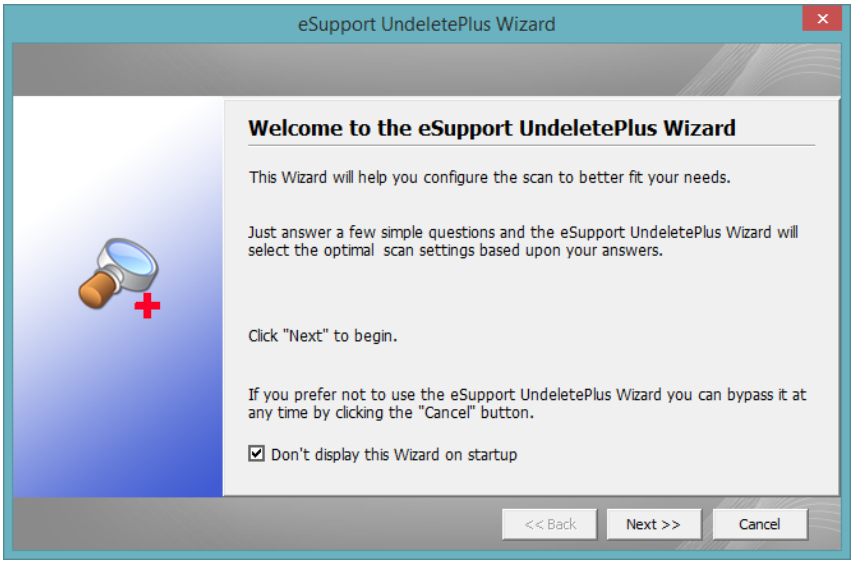


Figura 36 Tipo de archivo que se quiere recuperar

Fuente: (Sanchez Herrera & Basantes Salazar)

La herramienta posee un proceso Wizard que permite seleccionar de mejor forma los criterios de búsqueda, como se puede observar en las Figuras 38, 39, 40, 41 y 42.

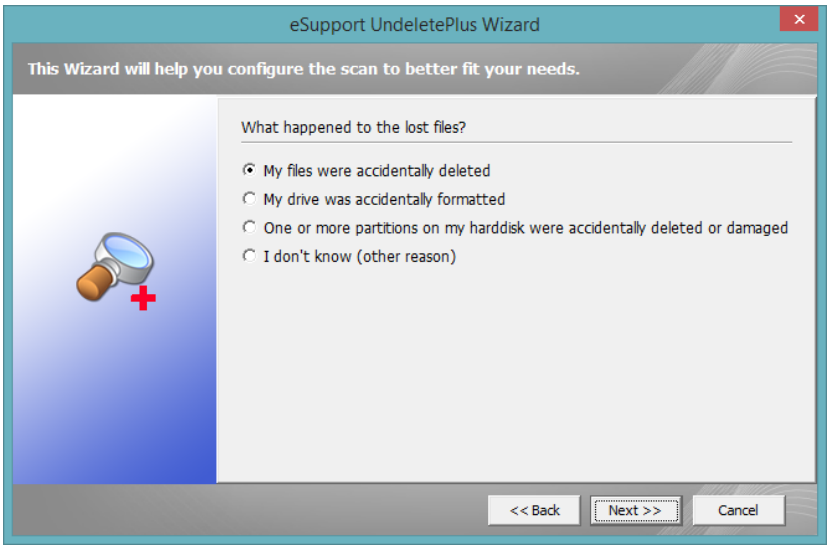


Figura 37 Wizard de recuperación eSupport UndeletePlus

Fuente: (Sanchez Herrera & Basantes Salazar)

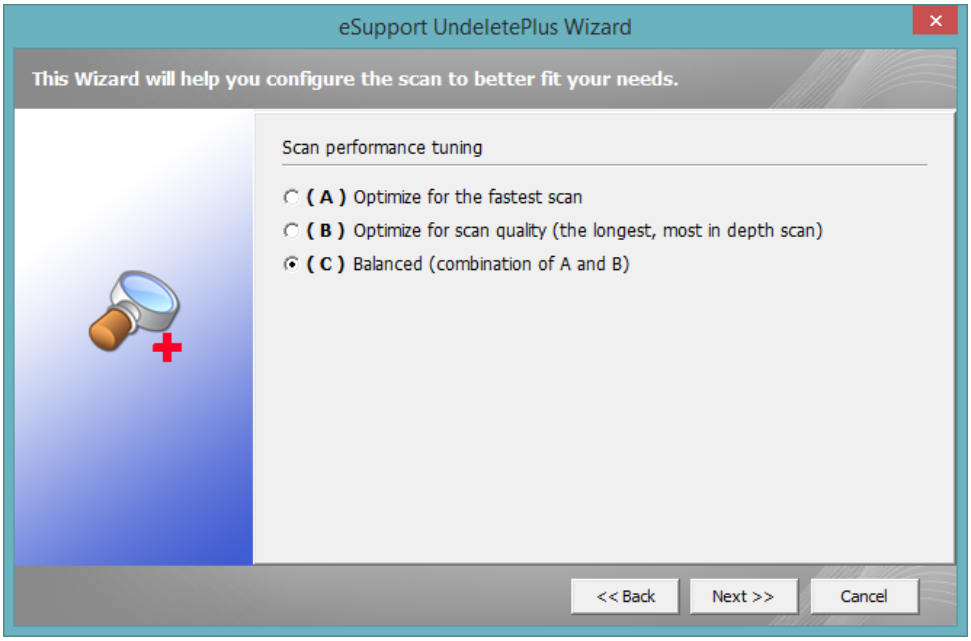


Figura 38 Selección de Tipo de Búsqueda eSupport UndeletePlus

Fuente: (Sanchez Herrera & Basantes Salazar)

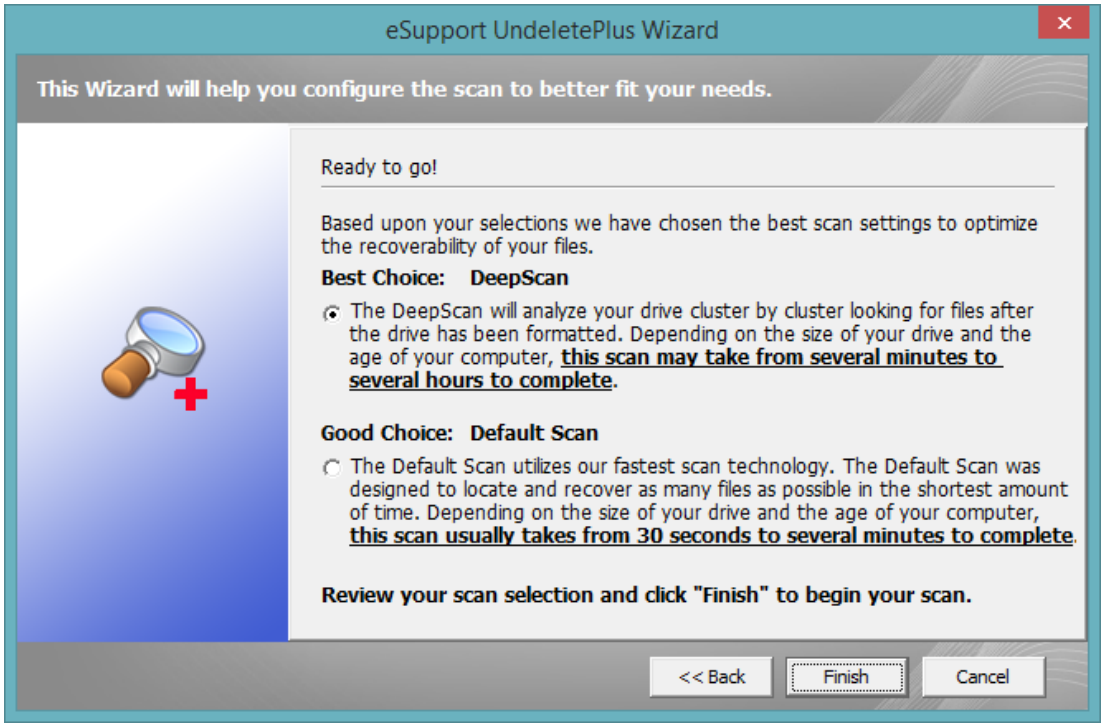


Figura 39 Selección de tipo de búsqueda eSupport UndeletePlus

Fuente: (Sanchez Herrera & Basantes Salazar)

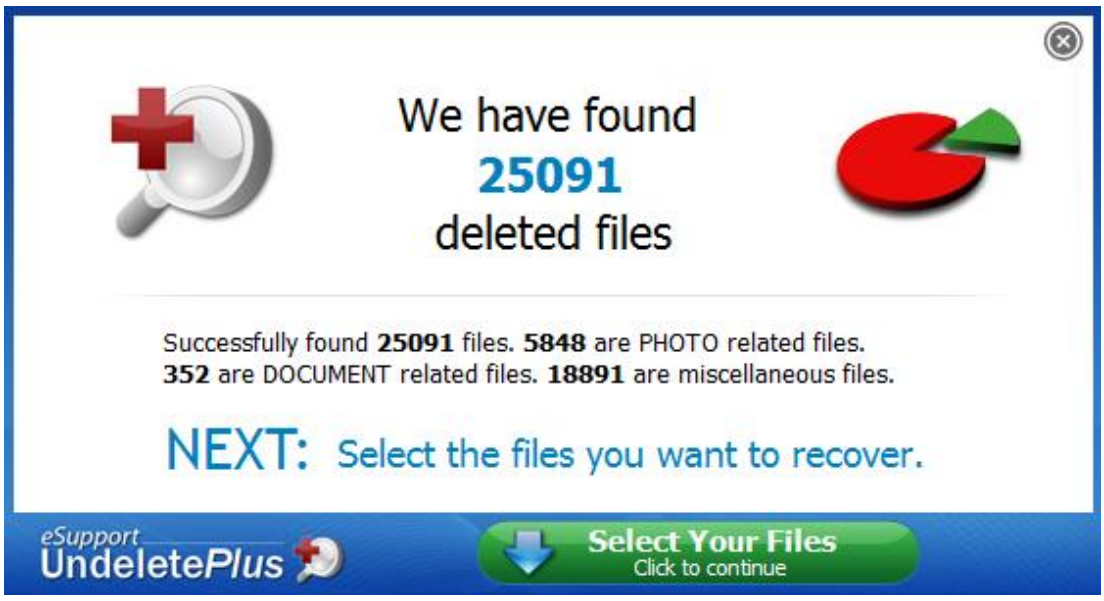


Figura 40 Resultado de búsqueda eSupport UndeletePlus

Fuente: (Sanchez Herrera & Basantes Salazar)

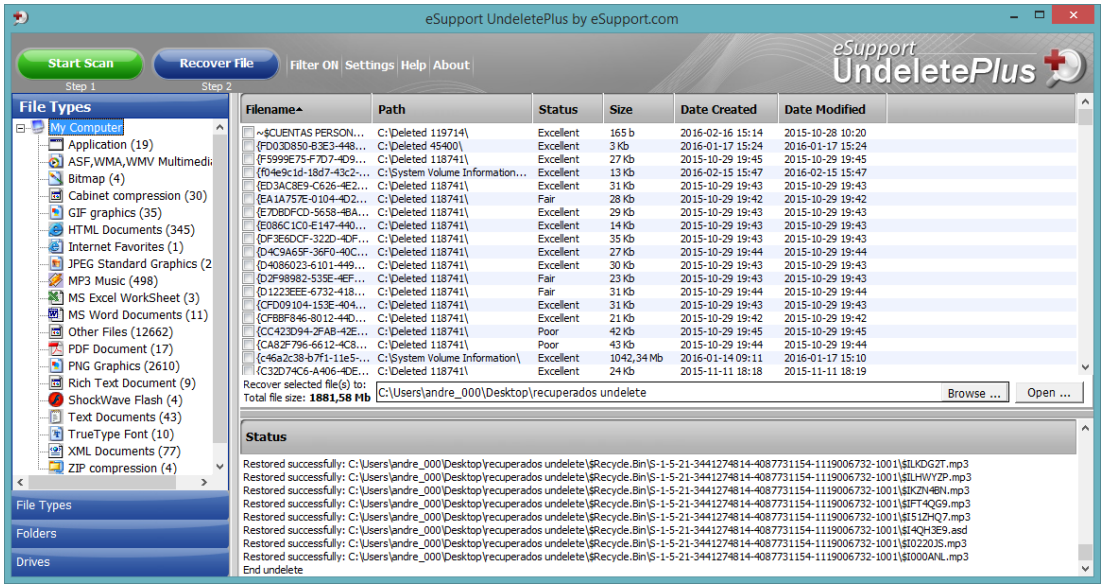


Figura 41 Finalización de recuperación de búsqueda eSupport UndeletePlus

Fuente: (Sanchez Herrera & Basantes Salazar)

Resultado

La utilización de dos diferentes softwares al momento de recuperar archivos ha dado los resultados que se observaran en la Tabla 13.

Tabla 13
Comparación entre herramienta de recuperación de archivos

CARACTERÍSTICAS	SOFTWARE	LICENCIA	TIPO DE ANÁLISIS	TIEMPO DE ANÁLISIS	# ARCHIVOS RECUPERADOS	USO	EFECTIVIDAD	OBSERVACIONES
WINDOWS 8.1 PRO 64BIT INTEL CORE I5 4GB RAM NVIDIA GEFORCE GT 420 1023MB 465 GB	RECUVA 1.52.1086	GRATIS	PROFUNDO	91min	64 recuperados 134 parcialmente recuperados (608 MB)	FÁCIL	ALTO	Tiene una fácil visualización de los archivos a recuperarse. Al final de la recuperación muestra el detalle de la operación realizada indicando el tiempo de demora y el número de archivos recuperados.
WINDOWS 8.1 PRO 64BIT INTEL CORE I5 4GB RAM NVIDIA GEFORCE GT 420 1023MB 465 GB	eSupport UndeletePlus 3.0.6.1019	PAGADA	PROFUNDO	19 min 6 sec	198 recuperados (608 MB)	FÁCIL	BAJO	Muestra una visualización general para la recuperación con opciones de visualización pero son muy generales. Al final de la recuperación no emite ningún informe sobre el proceso de recuperación.

(Sanchez Herrera & Basantes Salazar)

La utilización del software eSupport entrego la mayor cantidad de archivos en la menor cantidad de tiempo, pero su efectividad no es tan alta. Lo que se puede determinar la utilización de los dos es muy sencillo.

4.3.4.3. Comprobación de hardware utilizando Speecy

Esta herramienta de la misma familia de Recuva ayudar a visualizar el estado y la información completa del hardware instalado. Es importante este análisis ya que por medio del chequeo de temperatura de los procesadores, consumo de memoria, utilización del disco, etc., se puede evidenciar anomalías que indicarían repercusiones severas del ataque. Al igual que Recuva Speccy tiene una interfaz bastante sencilla.

Al iniciar la herramienta se encontrara un resumen general del equipo en el cual de entrada proporciona información de la temperatura del equipo y que dispositivos tiene conectado para lo cual en nuestro caso se puede decir que todo se encuentra dentro de la temperatura normal y se puede observar hardware extraño instalado, tal y como se puede visualizar en la Figura 43.

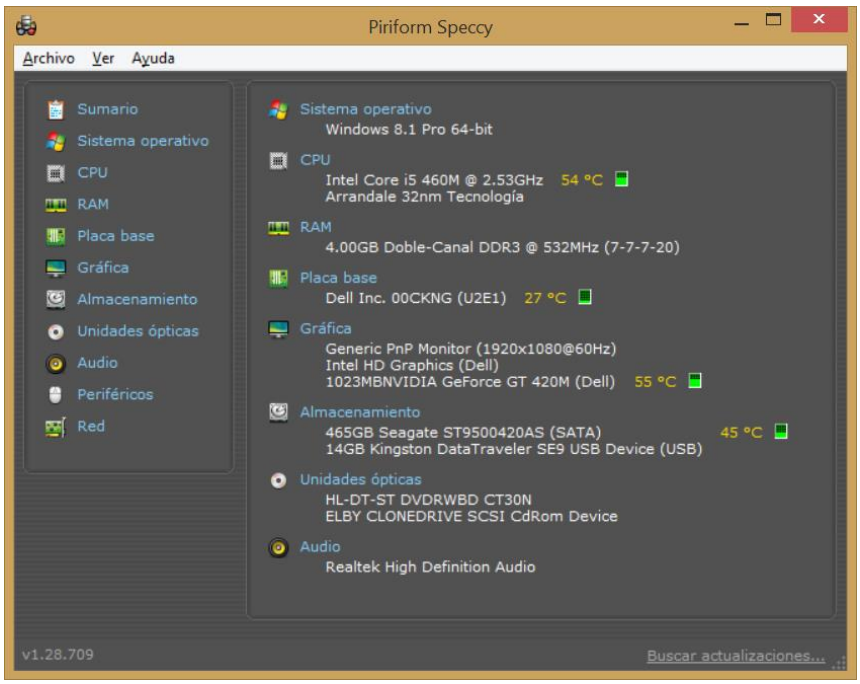


Figura 42 Interfaz principal de Speccy

Fuente: (Sanchez Herrera & Basantes Salazar)

En la información del CPU se puede observar toda la información dentro de los rangos normales no se muestra ninguna anomalía.

En la memoria RAM la cual es la que principalmente delata procesos maliciosos ya que tienden a consumir los recursos del computador. En este caso se ve un consumo bastante bajo inclusive en relación a lo normal por lo cual se descarta por el momento cualquier afección al hardware pero por rutina se da un vistazo a todos los resúmenes detallados que brinda Speccy, descritos en la Figura 44.

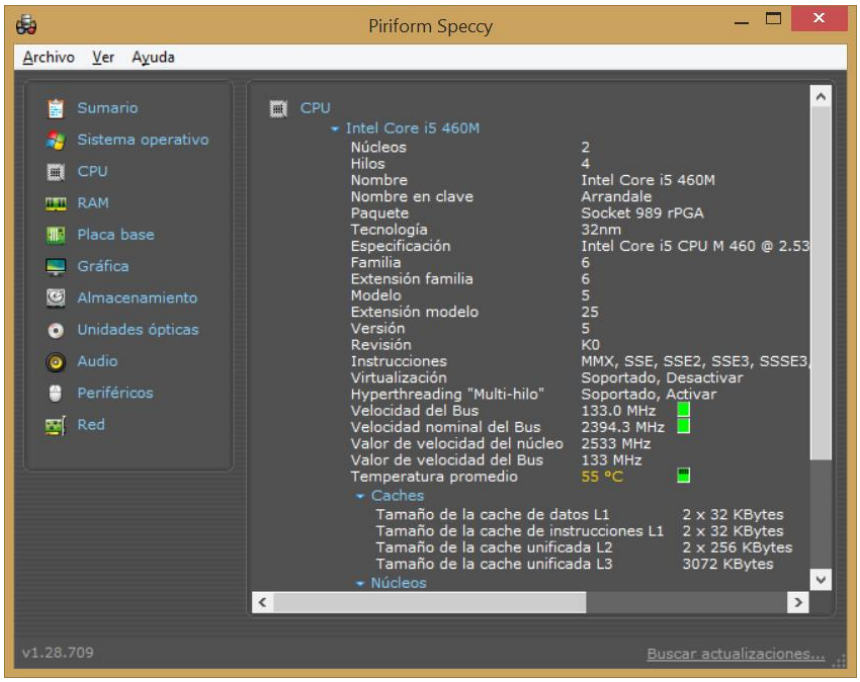


Figura 43 Principales características del computador de INDUSTEC

Fuente: (Sanchez Herrera & Basantes Salazar)

En la información del CPU se observa toda la información dentro de los rangos normales no se muestra ninguna anomalía.

4.3.4.3.1. Comprobación de hardware utilizando CPUID CPU-Z

Luego de descargar el software de su página oficial http://www.cpuid.com/softwares/cpu-z.html se procede con la instalación del mismo. Al inicial el software se muestra una ventana como se muestra en la Figura 45.

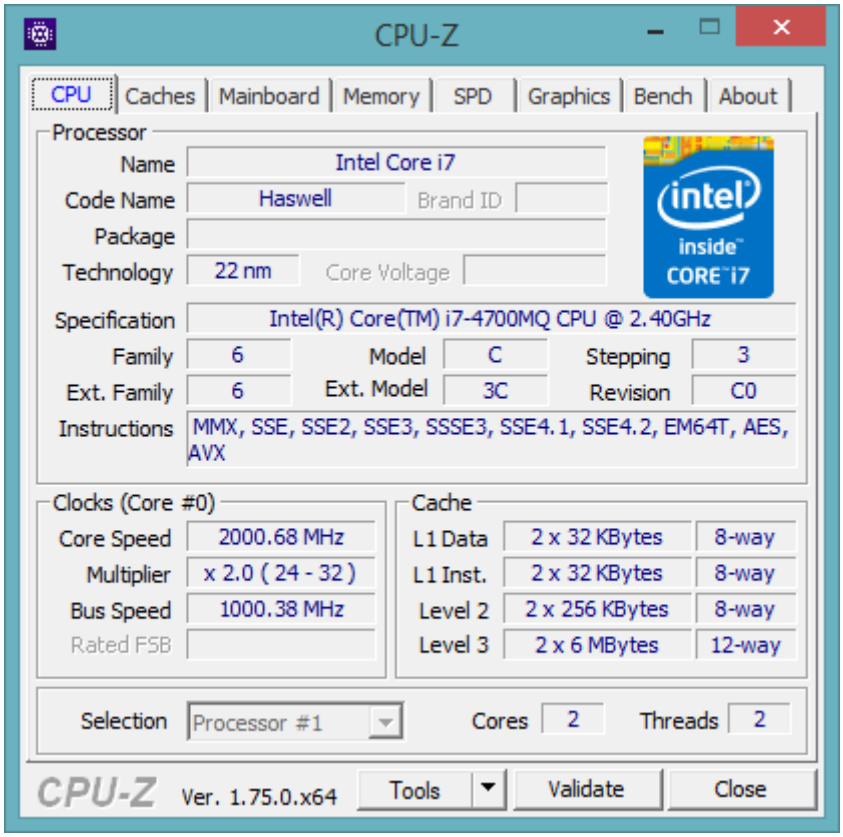


Figura 44 Pantalla inicial de CPU-Z

Fuente: (Sanchez Herrera & Basantes Salazar)

Se puede visualizar la información del hardware más esencial, y que toda la información solamente se refiere al hardware más no a los datos del sistema operativo ni de los procesos y servicios en ejecución. Además también ofrece la posibilidad de realizar el test de benchmarking al procesador como se muestra en la Figura 46.

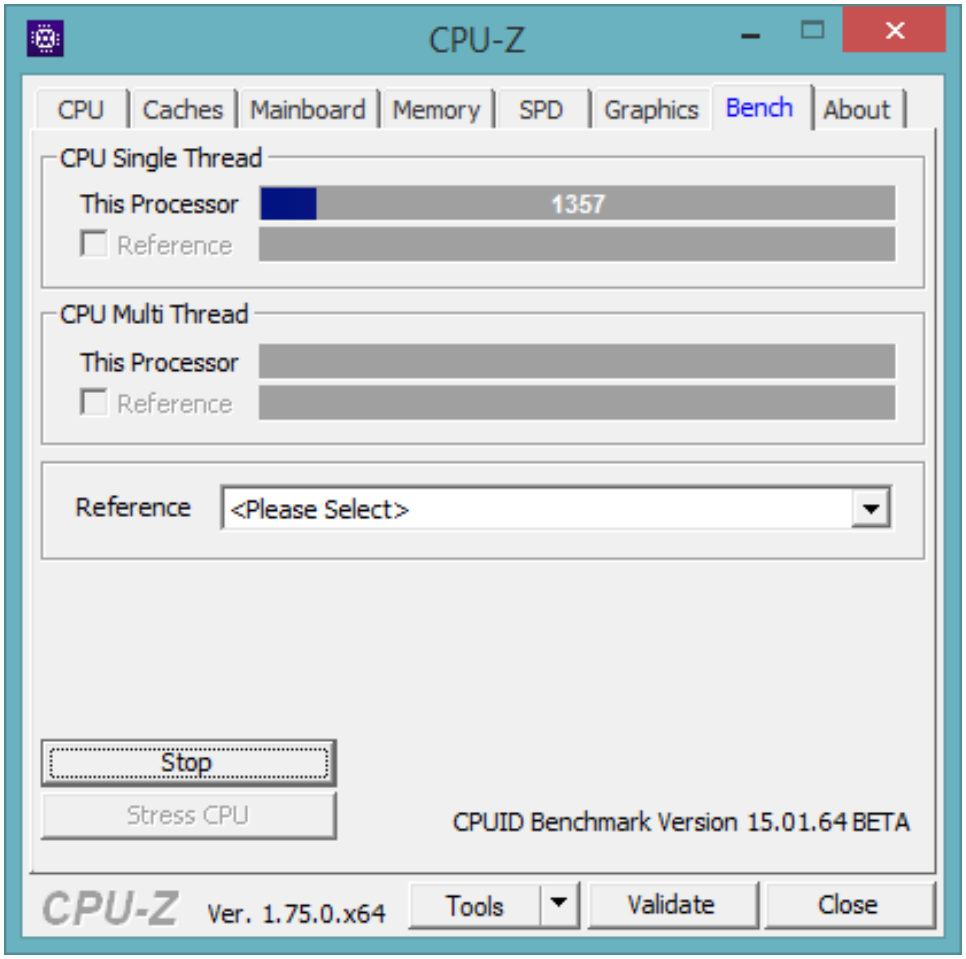


Figura 45 Ventana opción benchmark de CPU-Z

Fuente: (Sanchez Herrera & Basantes Salazar)

Resultado

En la Tabla 14 se observa la comparación entre dos herramientas para el análisis del hardware que tiene un computador.

Tabla 14
Comparación entre software de análisis de procesos

CARACTERÍSTICAS	SOFTWARE	LICENCIA	DETALLE DE RESULTADOS	USO	EFECTIVIDAD	OBSERVACIONES
WINDOWS 8.1 PRO 64BIT INTEL CORE I5 4GB RAM NVIDIA GEFORCE GT 420 1023MB 465 GB	VISOR DE SUCESOS DE WINDOWS 8.1 PRO	GRATIS	MEDIO	FÁCIL	MEDIO	Muestra la información básica sobre los eventos del sistema. No permite guardar los logs mostrados.
WINDOWS 8.1 PRO 64BIT INTEL CORE I5 4GB RAM NVIDIA GEFORCE GT 420 1023MB 465 GB	EVENT LOG EXPLORER 4.5.3.2069	EVALUACIÓN	ALTO	FÁCIL	ALTA	Ofrece la posibilidad de agregar filtros que permiten hacer una búsqueda más precisa. Permite guardar el log de eventos el cual puede ser visualizado con el visor de eventos predeterminado de Windows.

(Sanchez Herrera & Basantes Salazar)

4.3.4.4. Comprobación de procesos en ejecución utilizando Process Explorer

Luego de descargar la herramienta Process Explorer de www.sysinternals.com, se procede con el análisis de los procesos en ejecución en nuestro equipo, esta herramienta brinda una vista bastante detallada, en la cual se puede visualizar el uso de CPU por aplicación, memoria RAM, y principalmente permite controlar los procesos con opciones como definir prioridades o matar procesos, reiniciarlos, suspenderlos e incluso visualizar sus propiedades, como se muestra a continuación en las Figuras 47 y 48.

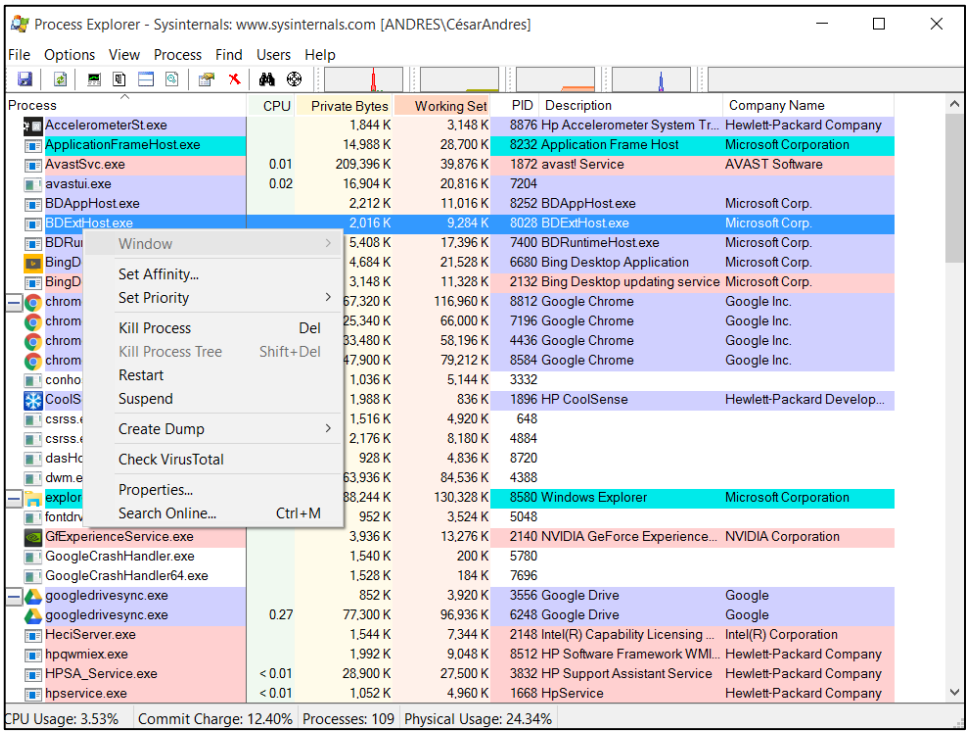


Figura 46 Pantalla principal del Process Explorer

Fuente: (Sanchez Herrera & Basantes Salazar)

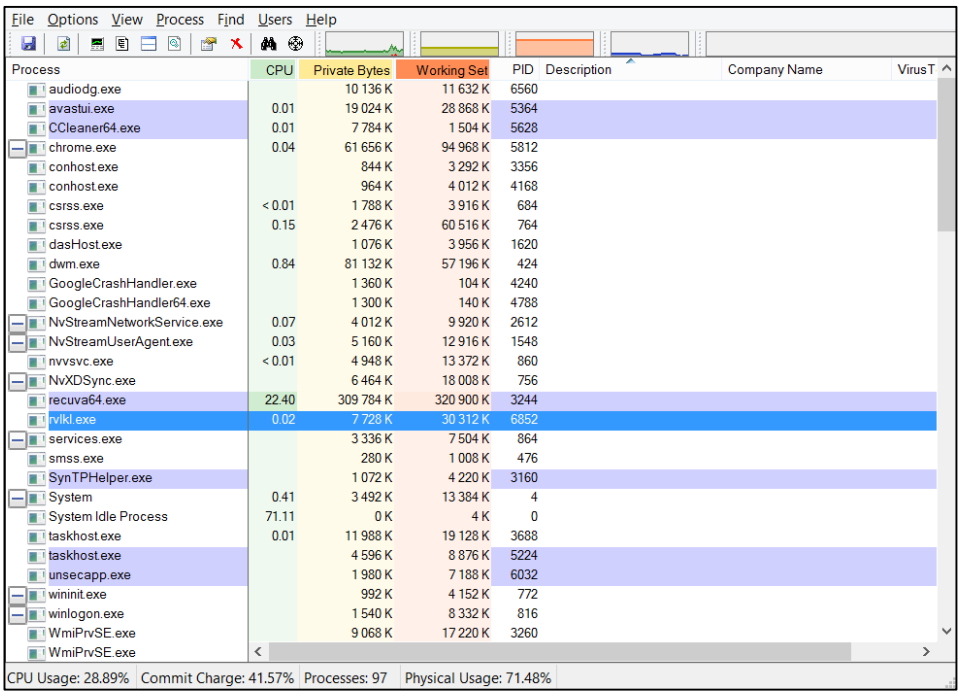


Figura 47 Proceso extraño ejecutándose en el computador

Fuente: (Sanchez Herrera & Basantes Salazar)

4.3.4.4.1. Comprobación de procesos en ejecución utilizando Process Hacker

Luego de descargar el software desde http://processhacker.sourceforge.net/ se procede con la instalación del mismo. Este software nos presenta una vista detallada de la actividad del sistema, entre una de sus funcionalidades más importantes, nos permiten determinar que procesos son usados para cada archivo, que programas tienen conexiones de red activas, información en tiempo real del acceso en disco, etc. Como se muestra a continuación en la Figura 49.

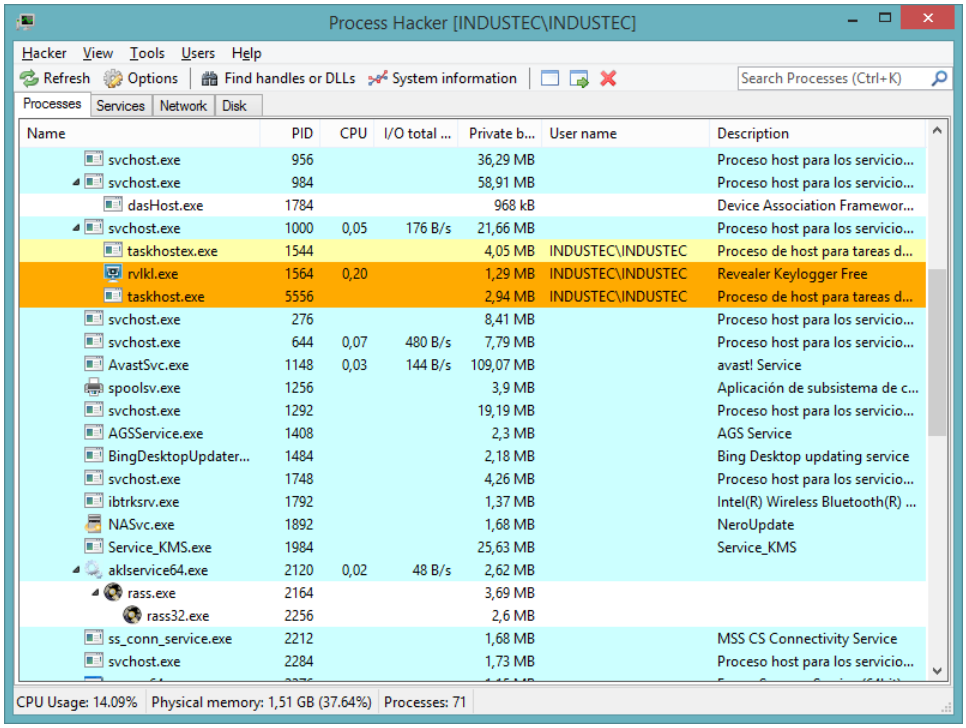


Figura 48 Ventana de ejecución de Process Hacker

Fuente: (Sanchez Herrera & Basantes Salazar)

Resultados

En la Tabla 15 se observa la comparación entre dos herramientas para el análisis de los procesos que están corriendo en un computador.

Tabla 15
Cuadro comparativo entre Speecy y CPU-Z

CARACTERÍSTICAS	SOFTWARE	LICENCIA	NIVEL DE DETALLE DE RESULTADOS	DIFICULTAD DE USO	GRADO DE EFECTIVIDAD	OBSERVACIONES
WINDOWS 8.1 PRO 64BIT INTEL CORE I5 4GB RAM NVIDIA GEFORCE GT 420 1023MB 465 GB	SPECCY 1.29.714	GRATIS	ALTO	FÁCIL	ALTO	El programa a más de mostrar una interfaz bastante detallada y bien clasificada. Sobre el hardware, muestra también una información completa de los servicios y procesos ejecutándose. Genera un reporte bastante completo y entendible.
WINDOWS 8.1 PRO 64BIT INTEL CORE I5 4GB RAM NVIDIA GEFORCE GT 420 1023MB 465 GB	CPU-Z 1.75.0	GRATIS	BAJO	FÁCIL	MEDIO	Ofrece la posibilidad de ejecutar el Benchmarking del CPU y estresarlo para obtener datos de su rendimiento, sin embargo ofrece muy poco detalle del hardware. No muestra ninguna información de software. Genera un reporte bastante básico

Fuente: (Sanchez Herrera & Basantes Salazar)

Haciendo un minucioso estudio de los procesos utilizando a la par la base de datos de procesos de Microsoft en la página http://www.file.net/ se pudo encontrar que dentro de los procesos se encontraba instalado un Keylogger el cual sería la evidencia contundente de que se realizó algo más que el borrado de los archivos. Este tipo de software malicioso registra en un archivo plano todo lo que es digitado en el teclado, muestra información sobre cuando se escribió, e incluso en el caso de páginas de Internet en que paginas estaba cuando se estaba tecleando.

Una de las características principales de este tipo de software es que no consume gran cantidad de recursos lo cual depende directamente del tiempo que ha estado instalado ya que poco a poco sigue creando archivos de texto plano almacenando la información.

La utilización de este software es bastante sencilla y no requiere de mucho tiempo para ser instalada y puesta en marcha. Además como se observa en la Figura 30, el Keylogger instalado en el computador fue Revealer Keylogger en su versión de prueba la cual limita al atacante a tener que volver físicamente para extraer la información ya que solamente las versiones de paga permiten el envío automático vía email. También basándose en la fecha de creación de los ficheros de instalación de este programa se percata de que este software fue instalado el 04/02/2016 encontrando al principal implicado, el técnico que dio mantenimiento al equipo, sin embargo como se mencionó anteriormente debido a que el programa es una versión de prueba existe un implicado más quien debió acceder para recoger el resultado del programa luego de todo el tiempo de funcionamiento y se presume la complicidad de un atacante interno quien pudiere acceder al computador sin complicaciones, como se visualiza en la Figura 50.

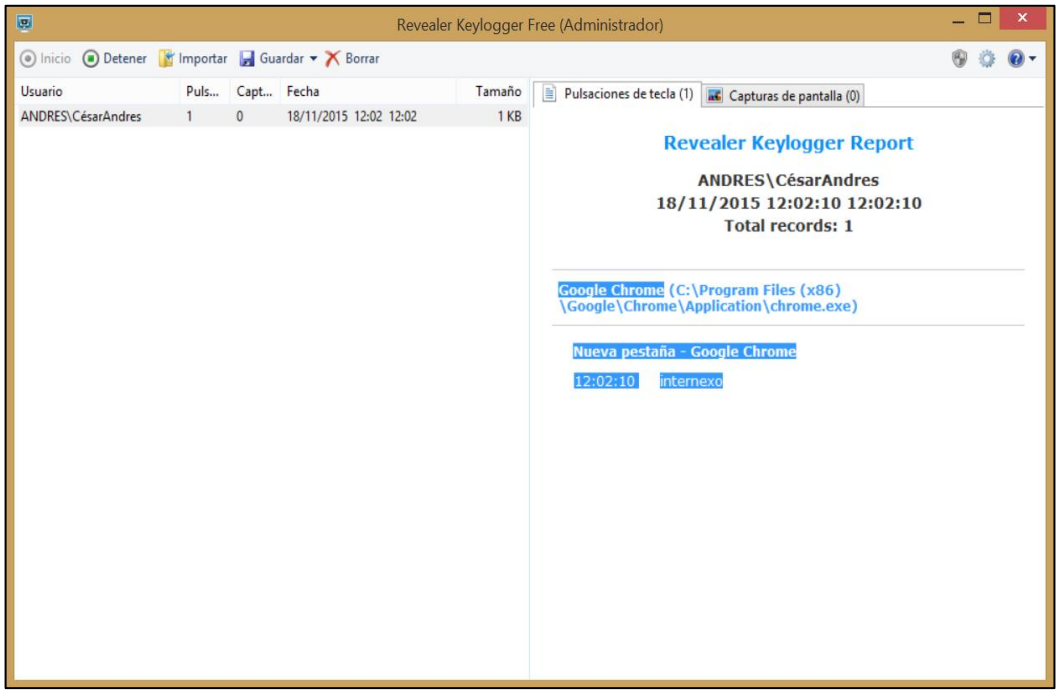


Figura 49 Pantalla principal del Keylogger instalado ocultamente

Fuente: (Sanchez Herrera & Basantes Salazar)

Aquí el programa desplegara una pantalla del Keylogger usado por el atacante el cual muestra el suficiente detalle para poder acceder a información personal.

Bajo la sospecha del atacante interno, se procede a realizar más preguntas a la administradora acerca de posibles sospechosos a lo cual supo manifestar que recientemente hubo un recorte de personal administrativo y existen tres personas quienes se encuentran trabajando el periodo final de 15 días antes de cesar sus labores y además comenta que durante el tiempo que trabajó con el computador luego de pasar por el programa de mantenimiento, ella siempre estuvo en la oficina excepto un día en el cual se ausentó durante todo el día por motivos personales.

A continuación luego de entender cómo se realizó el ataque, se tiene que saber cuándo se realizó el ataque y además se tiene un día especifico el cual el computador no estuvo bajo uso de la administradora da la pauta para realizar una análisis de inicios

de sesión en búsqueda de irregularidades lo cual le brindará al cliente la evidencia suficiente para poder encontrar a un culpable.

4.3.4.5. Auditoria de inicio de sesión

Por medio de la utilización de la herramienta de Windows Visor de Eventos, dentro de los registros de Windows en la opción de seguridad, se encontró un completo detalle de los inicios de sesión realizados.

En la Figura 51 y 52 se puede visualizar que en la fecha indicada cuando el cliente se ausento existe un inicio de sesión lo cual proporciona la hora exacta de la intrusión y a usuario que se accedió.

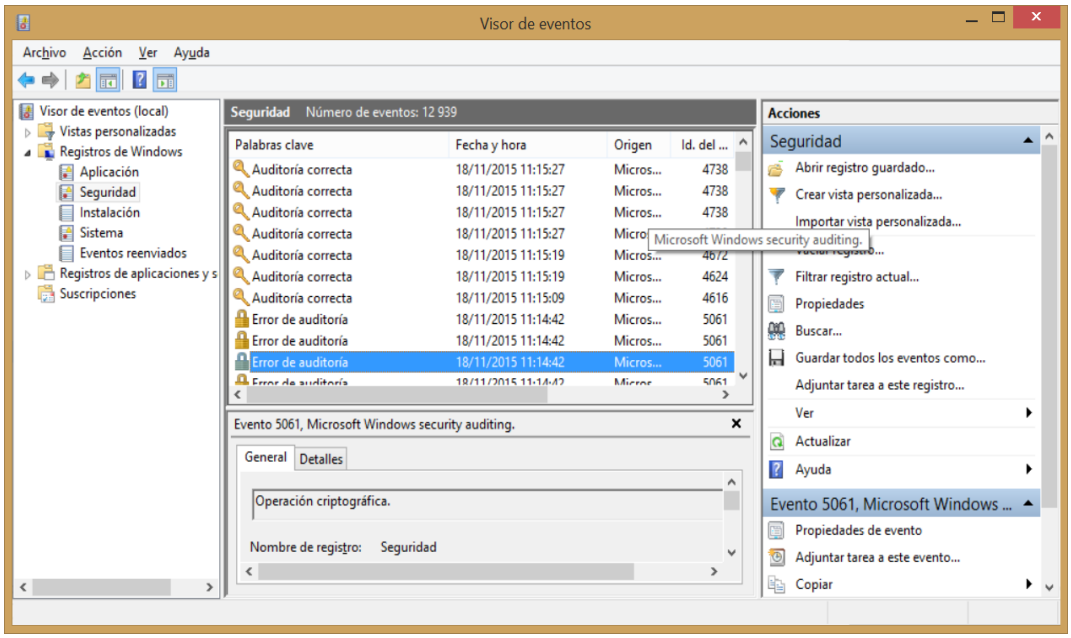


Figura 50 Visualización de los eventos ocurridos el día del crimen

Fuente: (Sanchez Herrera & Basantes Salazar)

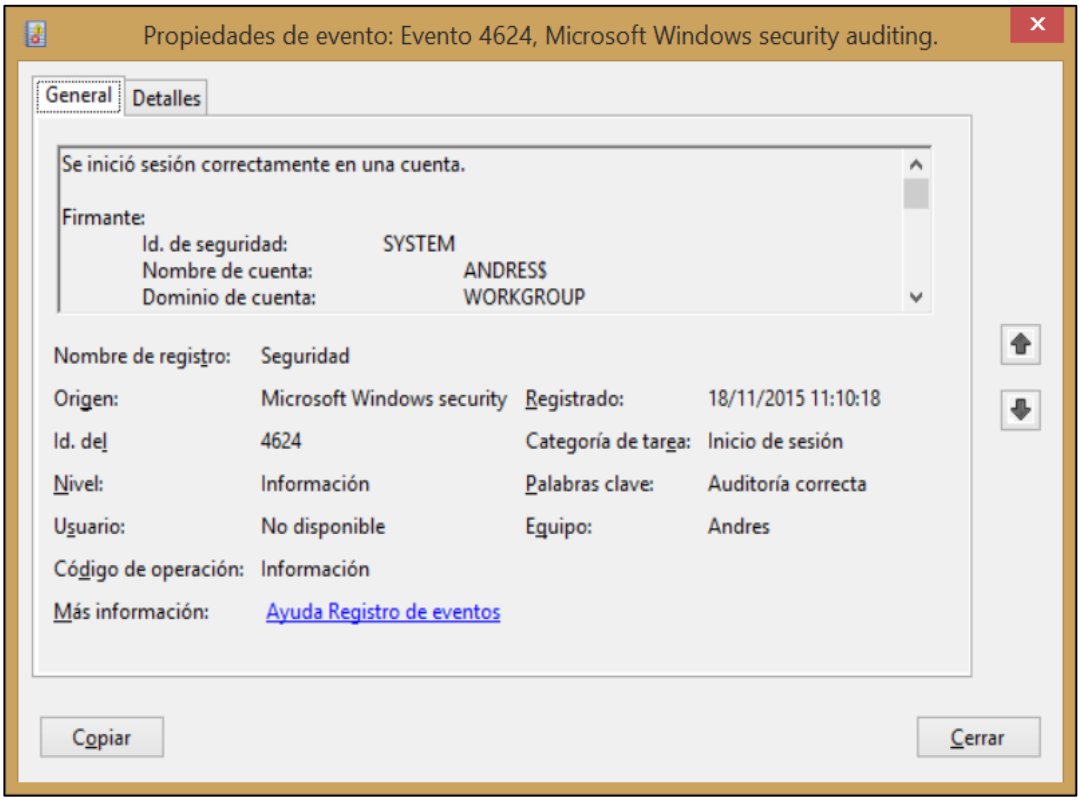


Figura 51 Descripción de usuario que accedió en las horas mencionadas por el cliente

Fuente: (Sanchez Herrera & Basantes Salazar)

Dentro de este análisis, se encontró un acceso no autorizado a las 11:10:18 del 15/02/2016.

Utilizando esta información el cliente pudo detectar por medio de la revisión de las cámaras de seguridad del lobby el cual enfoca parte de la entrada de su oficina en la cual uno de los empleados ingresa a la oficina del cliente y sale unos minutos después corroborando la información proporcionada y validando la evidencia.

4.3.4.5.1. Auditoria de inicio de sesión con Event Log Explorer

Luego de descargar el software de su página oficial http://www.eventlogxp.com/ , se procede con la instalación la cual es bastante sencilla. Al ejecutar el software se visualiza la pantalla que se muestra en la Figura 53.

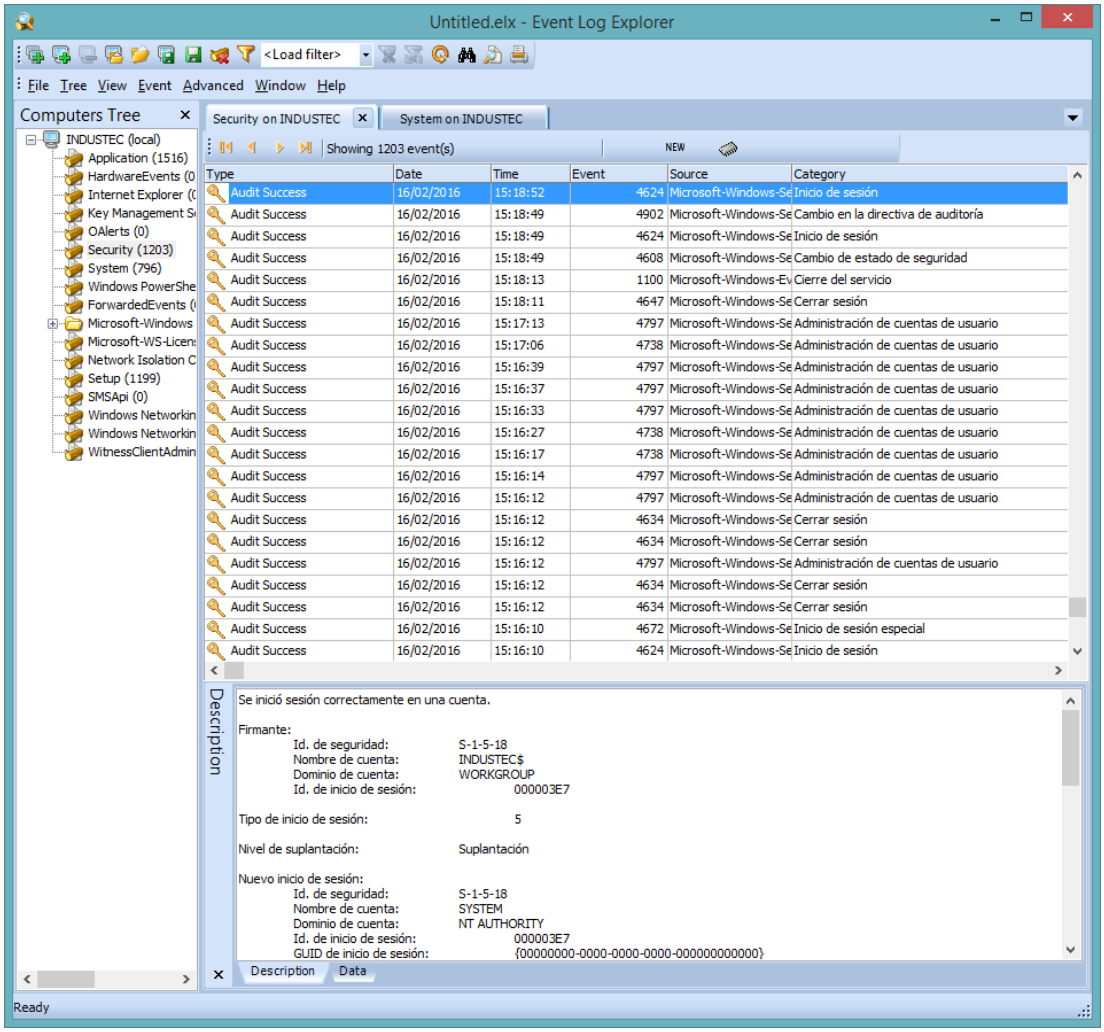


Figura 52 Ventana principal Event Log Explorer

Fuente: (Sanchez Herrera & Basantes Salazar)

Como se visualiza en la Figura 65, Event Log Explorer nos ofrece una gran cantidad de detalle pero principalmente permite guardar los registros que se está

mostrando ya sea alguno en específico o todos y este log puede ser visualizado también en el visor predeterminado de Windows.

Resultados

En la Tabla 16 se observa la comparación entre dos herramientas para el análisis de inicio de sesión de un computador.

Tabla 16
Comparación de software para el análisis de inicio de sesión

CARACTERÍSTICAS	SOFTWARE	LICENCIA	DETALLE DE RESULTADOS	USO	EFECTIVIDAD	OBSERVACIONES
WINDOWS 8.1 PRO 64BIT INTEL CORE I5 4GB RAM NVIDIA GEFORCE GT 420 1023MB 465 GB	PROCESS EXPLORER v16.12	GRATIS	MEDIO	FÁCIL	ALTA	Muestra la información bastante detallada pero todo dentro de un solo resumen sin embargo es útil la cantidad de detalles y nos facilita la visualización de la actividad del sistema mediante gráficos bien explicados.
WINDOWS 8.1 PRO 64BIT INTEL CORE I5 4GB RAM NVIDIA GEFORCE GT 420 1023MB 465 GB	PROCESS HACKER v2.38.343	GRATIS	ALTO	FÁCIL	ALTA	Ofrece una vista más individualizada por pestañas que muestran los procesos, servicios, red y disco. Ofrece gráficos del desempeño del sistema. También tiene varias opciones adicionales que nos permiten realizar varias pruebas por ejemplo la facultad de ejecutar un proceso como administrador o como un usuario limitado

4.3.4.6. Creación de línea temporal

Id	Nombre de tarea
1	Instalación y puesta en marcha de Sistema Windows 8.1 Pro 64-bit
2	Equipos de oficina entran en programa de mantenimiento en el cual se quitan las claves de seguridad de todos los equipos para poder
3	Instalación de programa espía
4	Entrega del equipo luego del mantenimiento sin contraseña para ser establecida por el usuario
5	Eliminación del Know-how de la Empresa
6	Ingreso al Sistema por parte del usuario
7	Se tiene acceso al lugar de los hechos y se prosigue con la recuperación de la evidencia
8	**Se inicia con el proceso de análisis forense**
9	Creación de la imagen utilizando RedoBackUp
10	Se analiza la imagen y se procede con la recuperación de archivos utilizando RECUVA
11	Se procede a analizar la imagen con Speecy para determinar su rendimiento
12	Utilizamos la herramienta Process Explorer para analizar los procesos que se encuentran ejecutándose
13	Se informa al cliente sobre las peculiaridades encontradas
14	Se realiza una auditoria al Inicio de Sesión utilizando el visor de eventos de Windows
15	Se elaboran informes Ejecutivos y Técnicos
16	Se entregan resultados y se da recomendaciones pertinentes

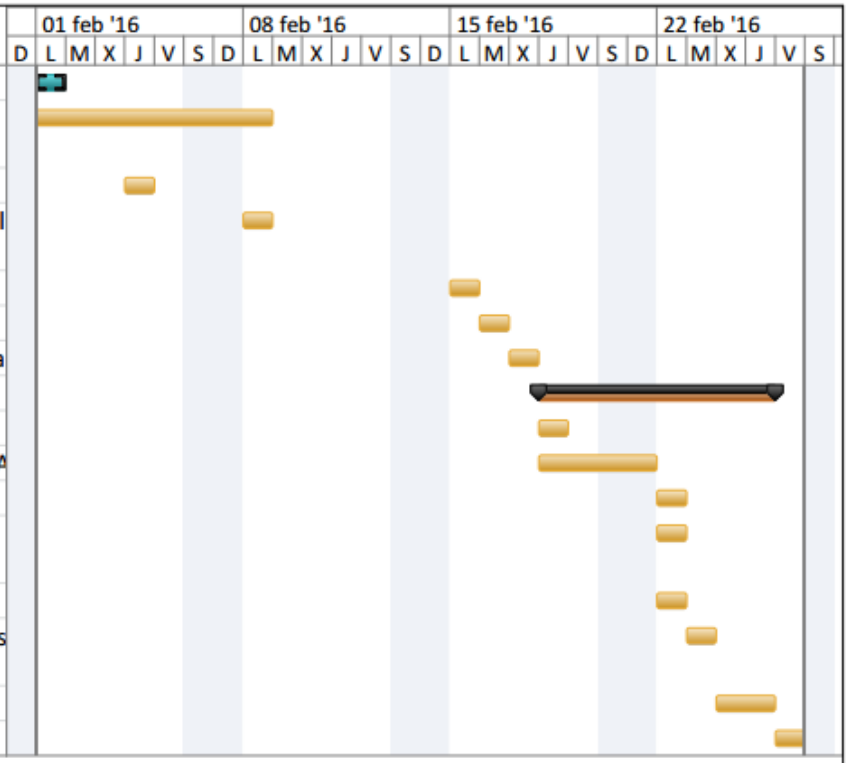


Figura 53 Línea de tiempo en el análisis forense

(Sanchez Herrera & Basantes Salazar)

4.4. Informe ejecutivo

El informe ejecutivo del presente análisis forense, se encuentra en el Anexo A.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Usar Software Open Source en el análisis forense de sistemas privativos como Windows 8, provee de resultados suficientemente válidos para poder ser utilizados en la elaboración de un informe final que contribuya en la ejecución de cualquier proceso judicial. En la tabla 17 se muestra los resultados obtenidos de las herramientas utilizadas.

Tabla 17
Resultados de software obtenidos

TAREA	SOFTWARE	LICENCIA	DETALLE DE RESULTADOS	USO	EFECTIVIDAD	OBSERVACIONES
ANÁLISIS DE PROCESOS	PROCESS HACKER v2.38.343	GRATIS	ALTO	FÁCIL	ALTA	Ofrece una vista más individualizada por pestañas que muestran los procesos, servicios, red y disco. Ofrece gráficos del desempeño del sistema. También tiene varias opciones adicionales que nos permiten realizar varias pruebas por ejemplo la facultad de ejecutar un proceso como administrador o como un usuario limitado
ANÁLISIS DE EVENTOS WINDOWS	VISOR DE SUCESOS DE WINDOWS 8.1 PRO	GRATIS	MEDIO	FÁCIL	MEDIO	Muestra la información básica sobre los eventos del sistema. No permite guardar los logs mostrados.
ANÁLISIS DE INFORMACIÓN DE HARDWARE	SPECCY 1.29.714	GRATIS	ALTO	FÁCIL	ALTO	El programa a más de mostrar una interfaz bastante detallada y bien clasificada. Sobre el hardware, muestra también una información completa de los servicios y procesos ejecutándose. Genera un reporte bastante completo y entendible.
RECUPERACIÓN DE ARCHIVOS ELIMINADOS	RECUVA 1.52.1086	GRATIS	PROFUNDO	FÁCIL	ALTO	Tiene una fácil visualización de los archivos a recuperarse. Al final de la recuperación muestra el detalle de la operación realizada indicando el tiempo de demora y el número de archivos recuperados.
CREACIÓN DE IMAGEN DE SISTEMA	RedoBackup	GRATIS	Avast Antivirus	FÁCIL	ALTO	La licencia es gratuita pero su interfaz no es de fácil utilización para personas con poco conocimiento

Fuente: (Sanchez Herrera & Basantes Salazar)

La utilización de una buena guía metodología comprende desde el aseguramiento de la escena hasta la elaboración del informe con el fin de entregar resultados necesarios para la resolución de un caso. Además es de vital importancia la aplicación de la cadena de custodia que asegure la integridad de la evidencia durante todo el proceso de investigación.

Actualmente Ecuador ha avanzado en la sanción de delitos informáticos. El COIP contiene algunos artículos referentes al delito informático dentro de los más importantes están: acoso sexual y oferta de servicios sexuales con menores de edad vía medios electrónicos, apropiación fraudulenta de información y de dinero, reprogramación o modificación de información de equipos terminales móviles (tabletas, celulares, IPad, etc.), interceptación ilegal de datos hasta el acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

Como conclucion del caso práctico se obtuvo que la persona quien llevo a cabo el delito, fue un miembro interno de la empresa, que con el fin de perjudicar a esta borro información importante, la cual fue recuperada exitosamente con el uso de la herramienta RECUVA..

5.2. Recomendaciones

Se recomienda el uso de herramientas Open Source que ayuden a lo largo del proceso investigativo para el análisis informático forense.

Es recomendable el uso de una guía metodológica que implemente procedimientos de la cadena de custodia que ayudara a mantener la integridad de la información y garantizara la calidad en la investigación.

Es necesario desarrollar e implementar mejores sanciones a los delitos informáticos que se encuentran tipificados dentro de el COIP en el uso de las TICs.

Se debería realizar un mejor estudio en el perfil del candidato al momento de pasar por los proceso de incorporación a la empresa. Se debería realizar un mejor estudio en el perfil del candidato al momento de pasar por los proceso de incorporación a la empresa.

BIBLIOGRAFÍA

Acurio, S. D. (2007). *Introducción a la informática forense.* Quito.

Ardita, J. (11 de Jul de 2007). *Metodología de Análisis forense Informático. .* Obtenido de http://www.cybsec.com/upload/ADACSI_Ardita_Analisis_forense_Informaticov2.pdf

Azas Manzano, M. F. (Julio de 2015). DISEÑO DE UN MODELO PARA LA CADENA DE CUSTODIA Y HERRAMIENTAS PARA EL ANÁLISIS FORENSE DE EQUIPOS TECNOLÓGICOS EN PROCESOS JUDICIALES EN EL ECUADOR. Quito: Universidad Internacional SEK.

Bolzas, G. M. (2006). Utilización de una guía para la elaboración del Informe Técnico. España.

Cano, J. (2006). *Introducción a la informática forense.* Bogota: Asociación Colombiana deIngenieros de Sistemas.

CFE, J. J. (2009). *Computacion forense.* Mexico: Alfaomega Grupo Editor.

Constitucion. (2014). *Codigo Penal Legal.*

Constitucional, T. (2008). *Constitución de la República del Ecuador.* Quito: Registro Oficial.

Contreras Clunes, A. (2003). *Delitos Informáticos: Un importante precedente.* Talca: Ius et Praxis.

Dhwaniket , R. K., & Nilakshi, J. (02 de 2015). *Advanced Embedded Solutions.* Recuperado el 21 de 08 de 2015, de http://embeddedsw.net/doc/Digital_forensic_tools_a_comparative_approach.pdf

Flynn, I., & Mclver, A. (2001). *Sistemas Operativos.* Mexico: International ThomsonEditores.

Furnell, S. (2002). *cyber-crime: Vandalizing the information society.* London: Addison-Wesley.

G. Arias, M. A. (2012). *La Guía de Windows 8. Paso a Paso.*

Galban, L. S. (Marzo de 2009). Propuesta de una metodologia de analis forense para dispositivos de telefonia celular. Mexico, Mexico: Instituto Politecnico Nacional.

García, C. (1 de Feb de 2014). *CADENA DE CUSTODIA DIGITAL DE LAS EVIDENCIAS.* Recuperado el 13 de Agos de 2015, de http://biblioteca.usac.edu.gt/tesis/08/08_0755_CS.pdf

Gutiérrez, G. Z. (noviembre de 2006). *informática forense.* Obtenido de http://pegasus.javeriana.edu.co: http://pegasus.javeriana.edu.co/~edigital/Docs/informatica%20forense/informatica%20forense%20v0.6.pdf,

INEI. (2001). Delitos Informáticos. *Trabajo de Investigación, Lima: Oficina Técnica de Administración*.

Lima, M. d. (1984). Delitos Electronicos. En M. d. Lima, *Delitos Electronicos* (pág. 100). Mexico: Ediciones Porrua.

López, O., Amaya, H., & León, R. (s.f.). *informática forense: GeneralidadesAspectos Técnicos y Herramientas.* Universidad de los Andes.

Martinez, P. (1997). *Sistemas Operativos: Teoria y Practica.* Espana: Ediciones Diaz de Santos S.A.

Más, F. R., & Rosado, A. D. (s.f.). *La informática forense: El Rastro Digital Del Crimen.* Qdc (SECCIF).

Matthew Meyers, M. R. (2004). *Computer Forensics:The Need for Standardization and.* Obtenido de http://www.utica.edu:

http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-

Mosquera, J., Certain Jaramillo, F., & Cano, J. (2005). *EvidenciaDigital: contexto, situación, e implicaciones nacionales.* Universidad de los Andes.

Palazzi, P. (2000). DELITOS INFORMÁTICOS. En P. Palazzi, *DELITOS INFORMÁTICOS* (pág. 38).

Palencia, A., Romero, G., & de Danielle, E. (2008). *Las muestras en toxicología forense. Importancia de la cadena de custodia.*

Perez Marques, M. (2012). *Windows 8 en profundidad.* Madrid: Grupo RC.

Portantier, F. (2013). *seguridad informatica.*

Rivas, C. G. (2014). *Metodologia para un analisis forense.* Catalunya.

Romero Echevarria, L. (2005). *Marco conceptual de los delitos informáticos.Marco Conceptual.* Lima: Universidad Mayor de San Marcos.

Sanchez Herrera, K. E., & Basantes Salazar, C. A. (s.f.).

Silberschatz, A. P., James, L., Galvin, P. B., Morales Peake, E., & García Escrivá, J. R. (1998). *Sistemas operativos: conceptos fundamentales.*

Stallings, W. (1997). *Sistemas operativos (Vol. 732). .* Prentice Hall.

Tanenbaum, A. (2003). *Sistemas Operativos Modernos.* Mexico: Pretince Hall.

Valdés, J. T. (1996). Derecho Informático. En J. T. Valdés, *Derecho Informático.* México.: Mc Graw Hill.

Zapata, A. M. (2013). *Cadena de custodia. INNOVACIENCIA.*

Zdnet. (2012). *Zdnet*. Recuperado el 11 de 08 de 2015, de http://www.zdnet.com/microsoft/?p=264