PROPUESTA DE GUÍAS DE LABORATORIO PARA LA ASIGNATURA DE INFORMÁTICA FORENSE DEL PROGRAMA DE INGENIERÍA DE SISTEMAS DE LA UNIVERSIDAD ECCI

SERGIO CAMILO ORTEGA RUIZ

STIVEN PAEZ DIAZ

UNIVERSIDAD ECCI

Programa Tecnología en Desarrollo Informático

Bogotá D.C.

2020

PROPUESTA DE GUÍAS DE LABORATORIO PARA LA ASIGNATURA DE INFORMÁTICA FORENSE DEL PROGRAMA DE INGENIERÍA DE SISTEMAS DE LA UNIVERSIDAD ECCI

Presentador por:

SERGIO CAMILO ORTEGA RUIZ

STIVEN PAEZ DIAZ

Presentado a:

ANA ROCIO LEÓN LUGO

INGENIERA DE SISTEMAS

DIRECTORA

CARLOS ALBERTO PRIETO HURTADO

ECONOMISTA

MBA

ASESOR METODOLÓGICO Y CORRECTOR DE ESTILO

UNIVERSIDAD ECCI

Programa Tecnología en Desarrollo Informático

Bogotá D.C.

2020

Tabla de Contenido

Lista de Abreviaturas y Siglas

.doc Documento.

.exe Ejecutable.

.jpg Grupo conjunto de expertos en fotografía

CF Computer forensics.

IF Informática forense.

IFE Imagen forense.

IP Protocolo de internet.

MD5 Algoritmo de resumen del mensaje 5.

OS Sistema operativo.

RAM Memoria de acceso aleatorio.

SHA Algoritmo de hash seguro.

TICs Tecnologías de la información y la comunicación

Lista de Imágenes

Lista de Tablas

Glosario

Bluekeep: Es una vulnerabilidad de seguridad que fue descubierta en el Protocolo de Escritorio Remoto de Microsoft, que permite la posibilidad de ejecución remota de código.

Cabecera: Identifica que tipo de archivo y formato es, para que así la computadora sepa con que programa abrirlo.

Dentro de la cabecera de un archivo puede haber varia información como:

- Dimensiones
- Duración
- Formato
- Modificaciones
- Tamaño

Exploit: Software malicioso que explota las vulnerabilidades detectadas en determinados programas. Los hay de diversas clases en relación al tipo de flaqueza que exploten.

Hash: Conjunto de caracteres que identifican unívocamente a un archivo. Es un código que lo diferencia del resto.

Hexadecimal: Es el sistema de numeración posicional que tiene como base el 16. Su uso actual está muy vinculado a la informática y ciencias de la computación donde las operaciones de la CPU suelen usar el byte u octeto como unidad básica de memoria.

IP: Es forma estándar de identificar un equipo que está conectado a Internet, de forma similar a como un número de teléfono identifica un número de teléfono en una red telefónica.

Metadatos: Son datos que describen otros datos. En general, un grupo de metadatos se refiere a un grupo de datos que describen el contenido informativo de un objeto al que se denomina recurso.

Parche: Cuando en informática hablamos de un parche informático, nos estamos refiriendo a los distintos cambios que se han aplicado a un programa para corregir errores, actualizarlo, eliminar secciones antiguas de software o simplemente añadirle funcionalidad.

Pentester: Auditor técnico, el cual su función es identificar fallos, vulnerabilidades y riesgos de un sistema informático.

Protocolo: Un protocolo es el lenguaje (conjunto de reglas formales) que permite comunicar nodos (computadoras) entre sí. Al encontrar un lenguaje común no existen problemas de compatibilidad entre ellas. Existen infinidad de protocolos (a nivel de aplicación) en internet u otras redes, por ejemplo: HTTP, FTP, TCP, POP3, SMTP, SSH, IMAP, etc.

Puerto: Es una interfaz a través de la cual se pueden enviar y recibir los diferentes tipos de datos. La interfaz puede ser de tipo física (hardware) o puede ser a nivel lógico o de software, en cuyo caso se usa frecuentemente el término puerto lógico (por ejemplo, los puertos de redes que permiten la transmisión de datos entre diferentes computadoras).

Sector: Un sector de un disco duro es la sección de la superficie del mismo que corresponde al área encerrada entre dos líneas radiales de una pista. También es una superficie que almacena información de un usuario.

Service Pack: Es un conjunto de programas informáticos que consisten en un grupo de actualizaciones que corrigen y mejoran aplicaciones y sistemas operativos.

Sniffer: Programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador.

Trama: Es una unidad de envío de datos. Es una serie sucesiva de bits, organizados en forma cíclica, que transportan información y que permiten en la recepción extraer esta información.

Viene a ser el equivalente de paquete de datos o Paquete de red, en el Nivel de red del modelo OSI.

Unix: Es una familia de sistemas operativos tanto para ordenadores personales como para mainframes. Soporta gran número de usuarios y posibilita la ejecución de distintas tareas de forma simultánea (multiusuario y multitarea). Su facilidad de adaptación a distintas plataformas y la portabilidad de las aplicaciones (está escrito en lenguaje C) que ofrece hacen que se extienda rápidamente.

Abstract

This document evidences the application of a series of knowledge and skills developed by the authors to generate a series of laboratories or guides that serve as support to the subject of IF of the Systems Engineering Program.

As a result of the present project, the University is given a complete document that has as its central axis the subject of IF and that functions as a reference for the student who wishes to learn about this science in addition to being a support material for the subject with the same name.

What we want to achieve is to guide the less inexperienced student in this science, that is to say, to be able to give him an information so that he can familiarize himself with the IF.

To achieve the proposed results, information is consulted from the most basic to the most complex about FI, define the concept of computer science and what is forensic in order to better cover the subject accompanied by content such as chain of custody, laws, evidence collection processes, forensic tools among others.

Resumen Ejecutivo

En el presente documento se evidencia la aplicación de una serie de conocimientos y habilidades desarrolladas por los autores para generar una sucesión de laboratorios o guías que sirvan como apoyo a la asignatura de IF del Programa de Ingeniería de Sistemas.

Como resultado del presente proyecto, se entrega a la Universidad un documento completo que tenga como eje central el tema de IF y que funcione como referencia para el estudiante que desee aprender sobre esta ciencia además de ser un material de apoyo para la asignatura con el mismo nombre.

Lo que se quiere conseguir es orientar al estudiante menos inexperimentado en esta ciencia, es decir, poderle entregar una información para que logre familiarizarse con la IF.

Para lograr los resultados propuestos, se consulta información desde la más básica hasta la más compleja sobre IF, definir el concepto de informática y lo que es forense para así poder abarcar de mejor manera el tema acompañado de contenidos como cadena de custodia, leyes, procesos de recolección de evidencia, herramientas forenses entre otros.

Introducción

Hace unos años atrás la ciencia forense no contemplaba la posibilidad de presentar como evidencia información digital para la demostración de un hecho, con el tiempo se fue haciendo uso de las huellas digitales y el análisis genético para aclarar los mismos. De un tiempo para acá se identificó que los usos de los diferentes aparatos tecnológicos estaban implicados en infracciones a la ley y que servían como evidencia en un caso.

Fue así que, en EEUU, se crearon organizaciones para generar estándares para la recolección y cadena de custodia de evidencia digital, hoy en día es una ciencia más desarrollada y fue así que se dio a conocer al mundo pues hay un crecimiento considerable de delitos informáticos como robo de información, piratería, fraudes, amenazas, acceso ilícito a sistemas entre otros.

Debido a los precedentes tan alarmantes sobre ciberdelitos en Colombia y en el mundo, la Universidad decide involucrar en su programa de Ingeniería de Sistemas como asignatura la informática forense. Bajo este contexto se desarrolla este trabajo, uno de los objetivos es ser pioneros en cuanto a material generado sobre el tema en la Universidad ECCI para que haya un precedente sobre el mismo en futuras investigaciones, crear un material de referencia para la asignatura y motivar al estudiante a continuar con este tema tan extenso.

El documento pretende explicar los conceptos principales sobre esta ciencia, temas como ¿qué es?, historia, conceptos, herramientas, procedimientos entre otros, se hace así para brindar una información completa y dinámica ya que cuenta con una serie de laboratorios realizados paso a paso.

En este documento se encontrará bibliografía extensa, sobre la historia de la IF la cual se desarrolla en el capítulo 5.1. No obstante el documento también cuenta con el marco legal (Capítulo 5.3), el cual es un elemento relevante ya que el individuo que se incursione en el área

de la IF. Este apartado es clave, ya que si no cuenta con el conocimiento del contexto legal podría verse involucrado en un delito.

Pero no todo es teoría, más delante de lo ya anteriormente mencionado, se encontrará la parte de los ejercicios desarrollados a través de laboratorios (Capítulo7.3.1 al 7.3.5), los cuales consisten en plasmar ejercicios en un ambiente controlado, para que así el lector tenga las herramientas, para poder elaborar futuros proyectos, bien sea replicando los mismos ejercicios o proponiendo nuevas prácticas.

Capítulo 1. Título de la Investigación

El programa de Ingeniería de Sistemas de la Universidad ECCI, en el proceso de actualización del registro calificado, realizó una tarea de evaluación del perfil profesional del estudiante del programa, para cumplir con las necesidades de la sociedad. Como resultado de la evaluación de dicho perfil, se realizó un cambio en las líneas curriculares del programa y se crearon asignaturas como IF. Dicha asignatura impartirá por primera vez en el período 2020-1, por lo que el presente proyecto se encargará de proponer unas guías de apoyo a la cátedra y sus resultados se tomarán en cuenta para la solicitud de los requerimientos necesarios para la implementación de laboratorios de seguridad y forense para la Universidad ECCI.

Por ello, en este proyecto se tratarán temas acerca del concepto de IF, su utilidad, el marco legal colombiano sobre delitos informáticos, metodologías de investigación para mantener la evidencia y una serie de laboratorios que se llevarán a cabo con el fin de afianzar todos estos conocimientos y de esta manera generar un contenido útil para la asignatura de IF.

La IF como rama de estudio se ha vuelto fundamental debido a la cantidad delitos informáticos generados al año. Así lo reveló el ministro de Defensa, Guillermo Botero, durante la apertura de la Conferencia de Ciberdefensa del Hemisferio Occidental. manifestando que al cierre de 2018 se registró un aumento de 40 por ciento en las cifras relacionadas con delitos informáticos, que pasaron de 15.962 en 2017 a 22.366 casos registrados por las autoridades. De ahí se evidencia la necesidad de ingenieros que manejen las metodologías y herramientas forenses que soporten los casos y que expliquen el origen de los incidentes de seguridad que aquejan a las organizaciones colombianas.

Capítulo 2. Problema de la Investigación

2.1 Descripción del Problema

Lo que se pretende con la realización de este proyecto es contribuir en el refuerzo de las competencias de en gestión de la infraestructura y gestión de la seguridad de la información para hacer al Ingeniero de Sistemas de la Universidad ECCI mas competente y de la misma manera dar un apoyo hacia la nueva asignatura IF que tiene muy poca precedencia en la Universidad ECCI.

También se busca alentar a los estudiantes por el conocimiento sobre la IF, el cual es un campo bastante amplio, que sirve como área de especialización para los futuros Ingenieros de Sistemas, que deben dar respuestas asociadas al origen de los incidentes de seguridad y la investigación de delitos que tengan componentes de TICs.

¿Cómo lo hacemos?, La propuesta consiste en desarrollar las siguientes fases:

- Revisión del contenido de la asignatura.
- Propuesta de laboratorios.
- Implementación de los laboratorios.
- Análisis de resultados.
- Propuesta de infraestructura para la sala de seguridad y IF.

2.2 Formulación del Problema

¿Cómo plantear las guías de laboratorio de IF para coadyuvar a la generación de profesionales expertos que estudien los delitos informáticos y los incidentes de seguridad de la información de las organizaciones?

Capítulo 3. Objetivos de la Investigación

3.1 Objetivo General

Diseñar e implementar un conjunto de laboratorios basados en las competencias a desarrollar en la asignatura de IF, asignatura que se impartirá en el nuevo pensum del Programa de Ingeniería de Sistemas de la Universidad ECCI.

3.2 Objetivos Específicos

- Analizar el micro currículo de la asignatura de IF, que se impartirá en el nuevo contenido programático del Programa de Ingeniería de Sistemas.
- Analizar diferentes tipos de incidentes informáticos donde es aplicable la IF, para inferir la utilidad de las herramientas utilizadas.
- Proponer un conjunto de laboratorios para la adquisición de las competencias asociadas a la asignatura.
- Realizar la implementación de los laboratorios en entornos de prueba controlados, haciendo uso de herramientas de Software libre.
- Generar las guías de laboratorio, para que sirvan de soporte a los docentes de las asignaturas y como requerimientos para el laboratorio de seguridad informática.

Capítulo 4. Justificación y Delimitaciones de la Investigación

4.1 Justificación

El programa de Ingeniería de Sistemas está trabajando con una nueva malla curricular desde el semestre 2019-1, donde se enfatizan las competencias asociadas al perfil del Ingeniero de Sistemas especializado en infraestructura de TICs, que debe haber desarrollado habilidades en torno a la Seguridad de la Información, donde la IF es una de las asignaturas que desarrolla dichas competencias. Dicha asignatura se impartirá a partir del primer semestre de 2020-1.

El proyecto busca dar apoyo a la asignatura mencionada, brindando un material el cual abarca prácticas, herramientas de Software y Hardware para realizar pruebas forenses y el conocimiento en asignatura de legislación sobre el manejo de la evidencia digital. El proyecto realiza la propuesta de dichas prácticas para que estudiantes y docentes tengan un soporte y aprovechen al máximo los laboratorios y la Dirección de Ingeniería de Sistemas solicite la compra de Hardware y Software para desarrollar dichos laboratorios, cuyo objetivo es trabajar en técnicas científicas y analíticas especializadas a infraestructura tecnológica, que permitan identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

4.2 Delimitación

Dado que la Universidad ECCI a partir del 2019-1 desarrolla un nuevo contenido curricular con cambios en los contenidos y materias de la carrera Ingeniería de Sistemas, se decide trabajar en la línea de infraestructura de TICs en la asignatura IF para brindar unas guías de laboratorios de seguridad e IF para la asignatura del mismo nombre y definir el Software y Hardware para los laboratorios que se solicitarán a la Universidad para impartir de una manera adecuada el programa de dicha asignatura.

Las guías se basan en ejercicios y la manera en la que se encontraron los daños causados del ataque, los causantes y las medidas para prevenirlos, el contexto en que se realizaron y herramientas utilizadas. Los procesos que se llevaron a cabo de la documentación para exponer la validez de la misma de acuerdo a leyes colombianas y la estrategia de investigación.

Capítulo 5. Marco de Referencia de la Investigación

5.1 Marco Teórico

La mira central del proyecto estará enfocada a dar un soporte a la nueva asignatura de IF, para esto será necesario plantear algunos parámetros que sirvan de ejes conceptuales. Para empezar, entenderemos el concepto de informática "La informática es una ciencia vinculada al desarrollo de la computadora su nombre viene del francés informatique y el inglés computer science, utiliza métodos, técnicas y procesos para el procesamiento automático de información mediante sistemas informáticos llamados ordenadores o computadoras prácticamente se basa en dos palabras Hardware que son las máquinas y el Software que nos permite decirles que queremos que hagan. La asignatura prima de esta ciencia es la información, mientras que su objetivo es el poder almacenarla, procesarla y transmitirla." (Adicra, s.f.).

Recapitulando se puede decir que la informática es entonces una ciencia con el propósito de almacenar, procesar y transmitir información y datos en forma digital, en si las personas están ya muy familiarizadas con esta ciencia pues un resultado de esta son los dispositivos que utilizamos a diario como lo son computadores, tablets, celular entre otras, pero que es forense "Las Ciencias Forenses son un conjunto de disciplinas científicas que ayudan a la policía y la justicia a determinar las circunstancias exactas de la comisión de una infracción y a identificar a sus autores, el término latino forensis llegó a nuestro idioma como forense, se refiere a una discusión o examen realizado en público. Su objetivo recoger, preservar y analizar la evidencia científica durante el curso de una investigación proporcionando pruebas imparciales para su uso en los tribunales para establecer o descartar la relación que hay entre la infracción y el acusado. En la Antigua Roma, una imputación por crimen suponía presentar el caso ante un grupo de personas notables en el foro (tribunal, curia, audiencia o juzgado). Tanto la persona que se la acusaba por

haber cometido el crimen como el denunciante tenían que explicar su versión de los hechos. La argumentación, las pruebas y el comportamiento de cada persona determinaba el veredicto o sentencia del caso" (Conicet, s.f.).

Una vez explicado los términos informática y forense podemos abarcar lo que es la IF que en sí es una ciencia moderna que permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad. Este análisis puede determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un intruso en los sistemas afectados por un incidente de seguridad.

Una vez dicho esto la IF es un proceso entre varios procesos, técnicos y científicos, que deben estar sujetos a una metodología para la recogida y análisis de datos digitales de un dispositivo electrónico con la capacidad de guardar, procesar o transmitir información con el fin de presentar evidencia ante un foro (tribunal, curia, audiencia o juzgado). "Tuvo su origen a comienzo de los años 90 en EEUU por el FBI surgió a partir de la observación de que las pruebas o evidencias digitales tenían la potencia de convertirse en un elemento de prueba poderoso en un foro, a finales de los años 90 se creó IOCE (International Organization of Computer Evidence/ Organización Internacional de Pruebas Informáticas) con la intención de compartir información de herramientas procedimientos y metodologías para la IF" (Rodríguez Más & Doménech Rosado, 2011).

En 1910 Edmond Locard sentó las bases de la ciencia forense, diciendo que "siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto" (Manual. Vigilantes de Seguridad. Área Técnico/Socio-Profesional e Instrumental Vol. II, 2016) o en otras palabras todo contacto deja un rastro. Esto significa que cualquier tipo de delito, incluidos los relacionados con la informática que son los que nos atañen, dejan un rastro por lo que mediante el proceso de análisis forense se pueden obtener evidencias.

5.2 Marco Conceptual

La IF lleva a cabo una serie de procesos y herramientas para poder presentar la evidencia en un respectivo foro por lo tanto es importante tener claro cuáles son y cómo se procede para llegar a la evidencia por medio de las siguientes herramientas, métodos y conceptos.

Ataque informático

Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el Software, en el Hardware, e incluso, en las personas que forman parte de un ambiente informático, a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización (Mieres, 2009) .

Cadena de custodia

Consiste en un informe detallado que documenta la manipulación y el acceso a las pruebas objeto de la investigación. La información contenida en el documento debe ser conservada adecuadamente y mostrará los datos específicos, en particular todos los accesos con fecha y hora determinada (Marqués Arpa & Serra Ruiz, 2014) .

Copia

Por “copia de respaldo o de seguridad” (backup) se entiende una copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación. Las copias de seguridad son útiles ante distintos eventos y usos: Recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque, restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas, guardar información histórica de forma más económica que los discos duros y además permitiendo el traslado a ubicaciones distintas de la de los datos originales, etc. (Vietes, 2014).

Delito informático

Los delitos informáticos son conductas en que el o los delincuentes se valen de programas informáticos para cometer delitos como implantación de virus, suplantación de sitios web, estafas, violación de derechos de autor, piratería, etc. (Policia Nacional de Colombia, s.f.).

Evidencia digital

Se denomina así a cualquier elemento que proporcione la información, mediante el cual se pueda deducir alguna conclusión o que constituya un hallazgo relacionado con el hecho que esté bajo investigación (Marqués Arpa & Serra Ruiz, 2014).

Ficheros

Dentro del ordenador la información se almacena en el disco duro (de forma permanente) o en la memoria (de forma temporal, para realizar las operaciones). La información se guarda en forma de archivos o ficheros. Así, una imagen es un archivo y una carta escrita en un procesador de textos es otro archivo distinto. Pero esta información debe estar organizada, para hacer posible un acceso de modo claro y rápido. Los archivos o ficheros tienen un nombre y una extensión para diferenciarlos unos de otros. Lógicamente dentro de una carpeta no puede haber dos ficheros (o dos carpetas) que se llamen igual, ya que esto impediría identificar cada uno de ellos. Las carpetas o directorios son agrupaciones de ficheros. Es como si el disco duro fuera un gran archivador. Cada cajón sería una carpeta, que puede tener dentro archivos u otros directorios. (Albors Pérez, Palacio Junquera, & García Reyes, 2010).

Hash

Una función criptográfica hash - usualmente conocida como “hash”- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de

salida tendrá siempre la misma longitud. Una de sus utilidades es proteger la confidencialidad de una contraseña, asegurar la integridad de la información, sirve como firma digital entre otras (Donohue, 2014).

IFE

Una IFE es una copia bit a bit exacta de un dispositivo de almacenamiento. Es también conocido como una imagen de flujos de bits. En otras palabras, cada bit (1 o 0) es duplicado en otro dispositivo limpio desde la perspectiva forense, como un disco duro. (Caballero Quezada, Imágenes Forenses, 2018).

Recuperación datos

La recuperación de datos es un procedimiento para recuperar datos del disco duro de un equipo que se han perdido debido a un fallo del sistema o a un mal funcionamiento mecánico. La recuperación de datos también se puede utilizar para recuperar datos que han sido sobrescritos o borrados accidentalmente en una computadora. Hay empresas y personas que se especializan en la recuperación de datos, y programas que tratan de extraer los datos de los equipos que aún tienen algún nivel de funcionamiento. (Mendes, s.f.).

Sistemas operativos

Un OS es el Software o programa más importante que se ejecuta en un computador, nos permite usarlo y darle órdenes para que haga lo que necesitamos. Son importantes, porque te permiten interactuar y darle órdenes al computador. Sin un OS el computador es inútil.

Sin el OS, no tendrías la plataforma que soporta los programas que te permiten hacer cartas, escuchar música, navegar por internet o enviar un correo electrónico. Administra los recursos del computador, es decir, el Software y Hardware de su equipo. Es la estructura que soporta y maneja todos los programas y partes de tu computador. (GCFGLOBAl, s.f.).

Virtualización

La virtualización crea un entorno informático simulado, o virtual, en lugar de un entorno físico. A menudo, incluye versiones de Hardware, sistemas operativos, dispositivos de almacenamiento, etc., generadas por un equipo. Esto permite a las organizaciones particionar un equipo o servidor físico en varias máquinas virtuales. Cada máquina virtual puede interactuar de forma independiente y ejecutar sistemas operativos o aplicaciones diferentes mientras comparten los recursos de una sola máquina host (Microsoft Azure, s.f.).

Virus

Es un programa informático desarrollado en un determinado lenguaje (ensamblador. C, C++, Visual Basic, Java entre otros), capaz de infectar un sistema informático mediante distintos mecanismos de propagación, que contiene una determinada carga dañina para el sistema infectado y que además puede incorporar algunas medidas de autoprotección para "sobrevivir". (Vietes, 2014).

Volcado de memoria

Volcar la memoria consiste en copiar el contenido de la memoria principal en un archivo, el cual puede ser analizado posteriormente para obtener información del estado de la computadora en el momento del volcad (Bernal Michelena, 2013) o..

5.3 Marco Legal

Las instancias legales que afectan o están directamente implicadas en relación con el proyecto, son bastantes, ya que la rama de la IF involucra o aplica la Ley en ciertos campos, generando una labor conjunta con las autoridades pertinentes en distintas instancias. Esto permite y genera que el trabajo realizado sea transparente y profesional, es decir, que el personal que esté a cargo de esta área se encuentre capacitado para cualquier tipo de situación.

Un problema que se tiene con el Cibercrimen es que las Leyes y la aplicación de las mismas puede variar ya que cada país tiene su metodología y forma de gobernar y aplicar sus Leyes. Sin embargo, existen acuerdos que abarcan un grupo de país que adoptan ciertas Leyes, esto genera que la Ley pueda ser aplicada de manera correcta y oportuna ante el Cibercriminal. Como ejemplo el 23 de noviembre de 2001 se firma en Budapest un convenio de Ciberdelincuencia del Consejo de Europa al que se suman también EEUU, Canadá y Japón, y que luego es también suscrito posteriormente por otros países en el marco europeo e internacional, y queda abierta la inclusión por invitación o requerimiento de cualquier país al que quiera suscribirse.

En el caso de nuestro país, Colombia existen entidades del Estado, específicamente el cuerpo policial, el cual cuenta con un cuerpo especializado para las distintas situaciones o casos en los cuales intervienen dispositivos electrónicos bien sea: móviles, laptops y/o desktops y tablets.

En Colombia se ha creado la Ley 1273 DE 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Todos los delitos informáticos en Colombia, cuenta con una multa económica que va desde los 100 hasta 1.500 salarios mínimos legales vigente, dependiendo del delito, e incurrirá en pena de prisión sin el beneficio de libertad domiciliaria.

Ahora después de la Ley impuesta en el 2009, empezaron a regir unos artículos los cuales complementan de forma adecuada la Ley tales como:

– Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la

voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes (Daccach T, s.f.).

– Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor (Daccach T, s.f.).

– Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses (Daccach T, s.f.).

– Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes (Daccach T, s.f.).

– Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional Software malicioso u otros programas de computación de efectos dañinos, incurrirá en

pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes (Daccach T, s.f.).

– Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes (Daccach T, s.f.).

Al respecto es importante aclarar que la Ley 1266 de 2008 definió el término dato personal como "cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica". Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la Ley obliga a quien "sustraiga" e "intercepte" dichos datos a pedir autorización al titular de los mismos.

– Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave (Daccach T, s.f.).

– Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239[3] manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio

semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal [4], es decir, penas de prisión de tres (3) a ocho (8) años (Daccach T, s.f.).

– Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes (Daccach T, s.f.).

5.4 Marco Histórico

La necesidad que surgió a partir de la falta de resultados en las investigaciones de casos, en diferentes escenarios, ya sea un asesinato o un suicidio, dio cabida a las ciencias forenses ya que estas son las encargadas de llevar a cabo una investigación pertinente la cual tiene un objetivo, por lo tanto, tiene subprocesos los cuales son la guía para llegar a dicho objetivo.

La definición de informática forense, pertenece a un conjunto de ciencias las cuales están involucradas directa o indirectamente. Para poder entender el porqué de la informática forense, se debe partir del principio de las ciencias forenses.

En Francia, Vidoc crea las bases de La Sureté en 1810, y en 1823 Purkinje desarrolla un estudio sobre la doxología y el órgano cutáneo, en 1829 se crea, en la calle Henry Fielding, de Bow, un agrupamiento de investigación, en 1833 nace el primer antecedente de la antropometría o fotografía forense, con Bertillón y el famosísimo «bertillonaje».

Teniendo claro el concepto por cual las ciencias forenses fueron creadas, a continuación, se mostrará la evolución que ha tenido la informática forense:

La informática forense nace en los años 80, ya que por esta época las computadoras personales se encontraban en auge, ya que los precios se volvieron accesibles hacia los consumidores. Pasados 4 años con la revolución de las computadoras personales o bien llamadas Laptops, esto generó que en el año 1984 se creará un programa dirigido por el FBI llamado como CART (Computer Analysis Respone Team). Uno de los primeros nombres importantes en la informática forense es Michael Anderson, el cual era el director de un proyecto enfocado a la informática forense en una División de la IRS. Anderson trabaja con dicha organización hasta los años 90, decide dar un paso al costado y crear su propia empresa llamada New Technologies Inc, el cual tenía como misión seguir expandiendo el campo de la informática forense desde un campo privatizado.

La década de los 90 fue fructífera, ya que la disciplina se vio en constante desarrollo, a tal punto de que, en el año 1993, fue organizada la primera conferencia con respecto a dicha temática. La conferencia fue enfocada hacia la recopilación de pruebas sobre equipos. Al ver el impacto positivo de esta área, la IOCE (International organization On Compueter Evidence), fue creada y posteriormente establecida.

Corrido el año 1999, la CART, llegó a analizar 17 Terabytes de datos en los casos previamente tomados. Por otro lado, en el año 2003 se llegó a la cifra de 782 Terabytes en tan solo un año. Con estas cifras se puede ver claramente que la informática forense tomo un papel casi que esencial en los casos otorgados a los agentes del orden, se convirtió en una gran herramienta que permite tener procesos ágiles, y con un porcentaje bastante bajo de error, lo cual colaboró y sigue siendo primordial, para que los casos en los cuales se tenga que ver involucrada, se puedan llegar a tener resultados exitosos.

La informática forense a través del tiempo amplió su campo ya que con los avances que ha tenido la tecnología, se encuentra que ya no son solo laptops o desktops, si no que encontramos Tablets, Smartphones, Wearables, pen drives. Cada uno de estos dispositivos cuenta con unas memorias la cuales tienen como propiedad almacenar información, la cual es usada por la informática forense.

Capítulo 6. Tipo de Investigación

Se puede mencionar que en el presente proyecto se presentan dos tipos de investigación:

Investigación documental

Este tipo de investigación permite indagar sobre los temas usando referencias escritas como bibliográficas, hemerográficas y archivísticas. Se implementa porque para el desarrollo del proyecto se acudió a diferentes fuentes bibliográficas y hemerográficas, que permitieron conocer sobre los proyectos relacionados con el tema de investigación que ya se han implementado para que sirvan de apoyo para el desarrollo del proyecto. También para profundizar el conocimiento sobre IF.

Investigación experimental

Es un tipo de investigación que bien utiliza experimentos y los principios encontrados en el método científico. Los experimentos pueden ser llevados a cabo en el laboratorio o fuera de él (entorno natural). Estos generalmente involucran un número relativamente pequeño de personas y abordan una pregunta bastante enfocada. Los experimentos son más efectivos para la investigación explicativa y frecuentemente están limitados a temas en los cuales el investigador puede manipular la situación en la cual las personas se hallan.

Capítulo 7. Diseño Metodológico

Para este proyecto la metodología a seguir estará compuesta por tres etapas las cuales son obtención de conocimientos, marco legal y laboratorios, en la primera nos enfocaremos en consultar diferentes fuentes bibliográficas para obtención de conocimientos de IF. En la segunda etapa se busca conocer el marco legal que cobija esta asignatura, en la tercera aplicaremos los conocimientos y recolección de evidencias de los diferentes laboratorios que se hagan.

Para la primera etapa de adquisición de conocimientos y estudio en asignatura nos enfocaremos en consultar diferentes tipos de bibliografía para conocer qué es la IF, que la compone y diferentes herramientas para la realización de laboratorios.

La segunda etapa estará enfocada en consultas y noticias de diferentes fuentes sobre Leyes y delitos informáticos que nos permitan establecer que ampara y que no ampara la Ley en Colombia.

En la última etapa se recolectarán diferentes tipos de incidentes informáticos reales o no reales para su posterior análisis, ejecutar pruebas, exámenes muy detallados y los diferentes procesos involucrados en el ataque, así mismo llegar a la conclusión de quien, y como estuvieron involucrados.

7.1 Temas de la asignatura de IF del nuevo pensum

La asignatura de IF trae como objetivo instruir a los futuros Ingenieros de Sistemas en temas como explotación y detención de vulnerabilidades, análisis de protocolos de red por medio de sniffers y análisis de memorias volátil y no volátil por medio de volcados e imágenes forenses.

Debilidades en las plataformas

Uno de los temas de la asignatura es la detección de debilidades los sistemas, los sistemas de información son susceptibles a fallos y errores internos que generen agujeros o puertas traseras

que exponen al sistema a delincuentes, al fin y al cabo, son hechos por humanos y herrar es de humanos, la importancia de como aprender a encontrarlas, eliminarlas son ejes fundamentales de la asignatura y está implícita como laboratorio en el proyecto.

Análisis de protocolos

El análisis de protocolos por medio de sniffer tema fundamental en la asignatura que tendrá como utilidad enseñarles a los estudiantes el análisis de fallos para arreglar problemas de la red, la medición de tráfico que es fundamental en una organización, detención de intrusos entre otros.

Obtención y manejo de pruebas digitales

La creación de imágenes forenses y el volcado de memoria RAM son pan de cada día para un perito, la imagen se obtiene mediante un método que no altera, en ninguna manera, dato alguno de la memoria que está haciendo duplicada tiene que ser precisa, verificable y reproducible.

7.2 Algunas herramientas para empezar en IF

Un perito informático es una persona especialista en el análisis y recolección de evidencias en TICs, su función es ser auxiliar de cualquier entidad que recurra a sus servicios llámese juez, empresa o una persona en particular. Su trabajo consiste presentar pruebas informáticas o digitales sobre delitos informáticos, es su obligación siempre decir la verdad y emitir su respectivo dictamen sobre lo sucedió para esclarecer los hechos, uno de los objetivos de un procedimiento forense es preservar la evidencia a su forma más original (Alamillo, 2013)

Clonezilla: Herramienta que nos permite crear imágenes de discos, también nos permite crear copias de seguridad y restauración de sistemas (Clonezilla, s.f.).

FTK Imager: Herramienta que nos permite crear una imagen de la memoria RAM y de discos (ACCESDATA, s.f.).

DumpIt; Es una herramienta que permita el volcado de memoria RAM es muy sencilla y eficaz pues no trae mucha que configurar (Zeltser, 2017).

Regripper: Es una herramienta que nos permite análisis los registros de sistemas operativos como Windows, una de sus utilidades es analizar archivos que se encuentran en la carpeta confg de syste32 por medio de ejecución de plugins (Caballero Quezada, 2014).

Autopsy: Es una herramienta que nos permite analizar evidencia digital, tal vez una de las más usadas por peritos informáticos. Dentro de sus cualidades nos permite calcular hash, recuperar archivos borrados, segmentación de información detallada como tamaño de la imagen, información sobre OS, superación por tipo de archivos(png.zip.mkv) entre otras (Sleuth Kit, s.f.).

Wireshark: Es una de las herramientas más utilizadas para solucionar problemas en redes y el análisis de protocolos de red, permite la captura de conversaciones y archivos que son pruebas muy importantes para un perito (Wireshark, s.f.).

Caine: Es una distro de linux especializada en análisis forense cuenta un kit completo de herramientas para el análisis forense, es de origen italiano y open source.

Kali: Es una distro de linux basada en debían especialista en auditoría y seguridad informática, pero también tiene un modo forense que es muy útil para peritos (Kali Linux, s.f.)

7.3 Laboratorios

Se diseñaron 5 laboratorios que van relacionados con el temario de la asignatura de IF que se proponen como guías para ser usadas en la asignatura. Entre los laboratorios están los siguientes:

- Vulnerabilidad de un sistema.
- Análisis a un disco y recuperación de archivos.
- Análisis de sistemas Windows.
- Análisis con sniffer 1.

- Análisis con sniffer 2.

Con el objetivo de organizar la información de cada uno de los casos a trabajar en los laboratorios de clase se diseñó la siguiente plantilla:

Tabla 1. Plantilla para la solución de los laboratorios

Id del caso: 0000	Fecha: 00/00/0000	Forense: xxxxxxxxxxxxxxxx
Descripción del delito		
Objetivos de la investigación		
Evidencia		
Análisis forense		
Conclusiones		

Fuente: Los Autores 2019

7.3.1 Laboratorio #1 vulnerabilidad de un sistema

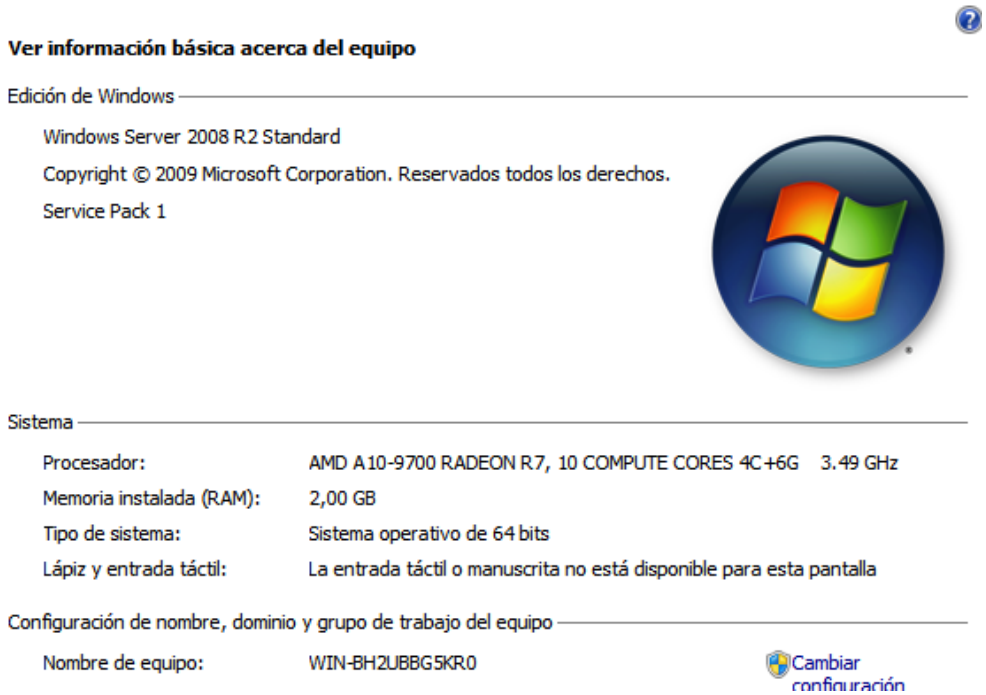
Tabla 2. Solución laboratorio de vulnerabilidad

Id del Caso: 001	Fecha: 17/05/2019	Penterster o Auditor técnico: Sergio Camilo Ortega Ruiz y Stiven Paez Diaz
¿Qué es una vulnerabilidad de un sistema de información?		
Una vulnerabilidad de un sistema de información es una debilidad que expone al sistema a un ataque poniendo en riesgo su funcionamiento, información y disponibilidad. Puede generarse por una mal configuración o error de diseño		
Vulnerabilidad Bluekeep		
¿Qué es Bluekeep (CVE-2019-0708)? Bluekeep es el nombre que recibió la vulnerabilidad que afecta los sistemas de Microsoft como lo son Windows NT, Windows 2000 hasta Windows Server 2008 R2 y Windows 7, esta vulnerabilidad permite la ejecución de código remoto, es posible explotar el fallo (tanto para un ataque de denegación de servicio como para realizar un ataque de ejecución remota de código (RCE), fue publicada por primera vez en mayo de 2019 y la solución es actualizar los sistemas ya que Microsoft lanzo el parche para esta vulnerabilidad.		

Explotación de la vulnerabilidad Bluekeep

Para la explotación de esta vulnerabilidad crearemos una máquina con el OS Windows Server 2008 R2 Serví Pack 1 y como sistema de ataque utilizamos Kali. Después de instalar la máquina no actualizamos nada ya que el exploit solo afecta a máquinas sin parchar.

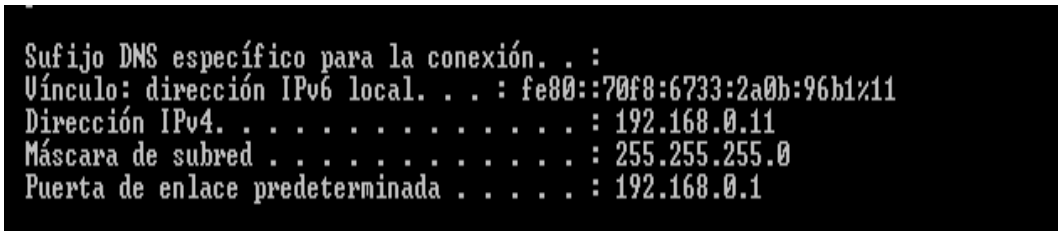
Imagen 1. Versión del OS de la máquina virtual



Fuente: Los Autores 2019

Se utiliza el comando ipconfig para averiguar nuestra ip.

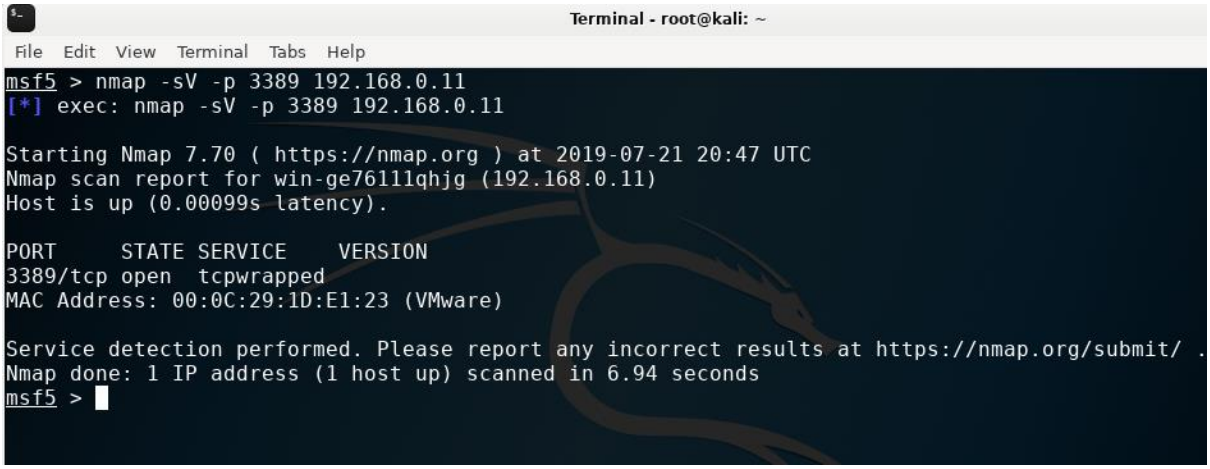
Imagen 2. IP de la máquina virtual



Fuente: Los Autores 2019

Desde kali se realiza un escaneo con nmap para el puerto 3389 a la dirección 192.168.0.11.

Imagen 3. Escaneo puerto 3389 de la máquina virtual



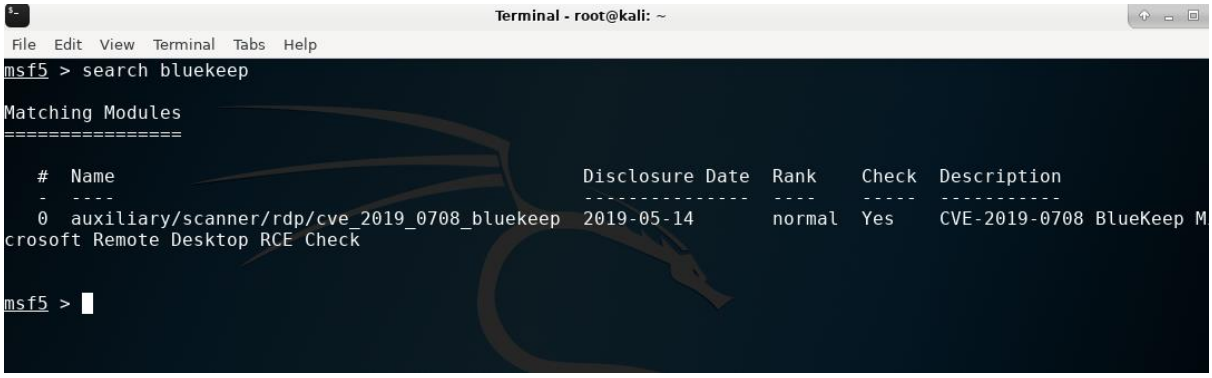
Fuente: Los Autores 2019

Se muestra que el puerto 3389 está abierto, procedemos a buscar un scanner auxiliar en

metasploit que nos permita averiguar si la maquina es vulnerable o no.

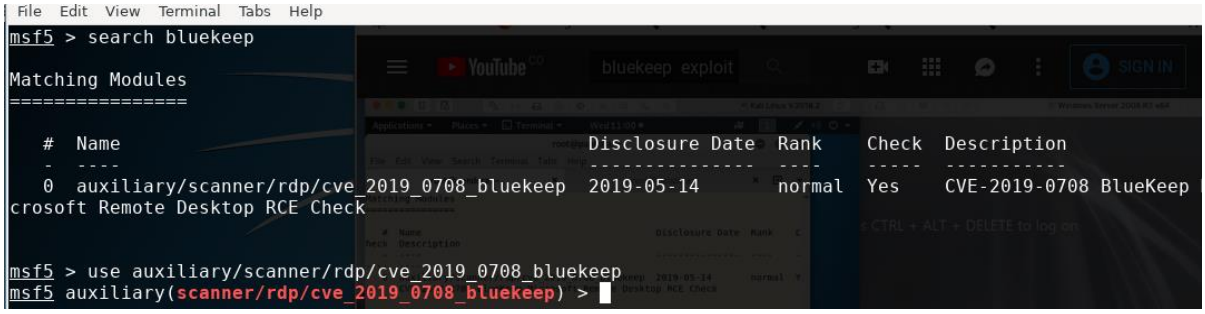
aparece uno con la etiqueta de Bluekeep y la fecha reciente de mayo/19.

Imagen 4. Búsqueda del scanner auxiliar para Bluekeep



Fuente: Los Autores 2019

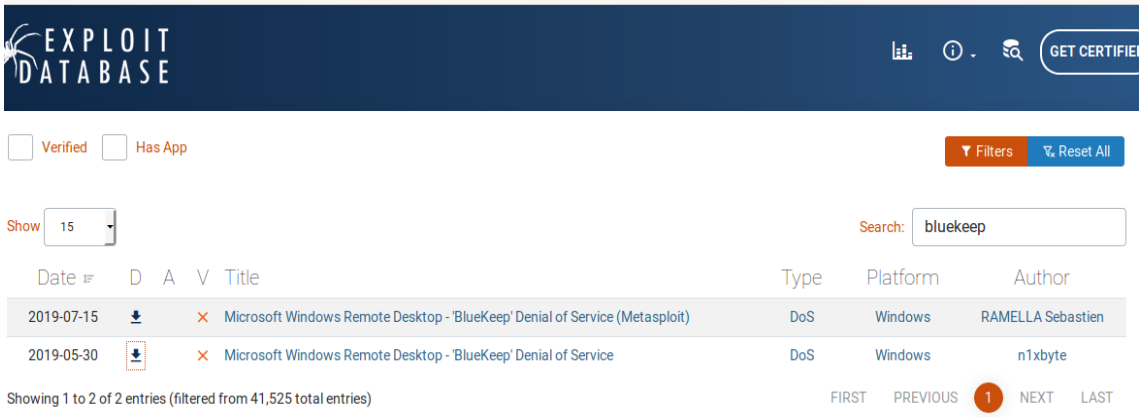
Imagen 5. Escáner auxiliar para Bluekeep



Fuente: Los Autores 2019

Después de usarlo arroja que la máquina se puede atacar, se procede a buscar el exploit en la base datos de kali con el nombre de Bluekeep.

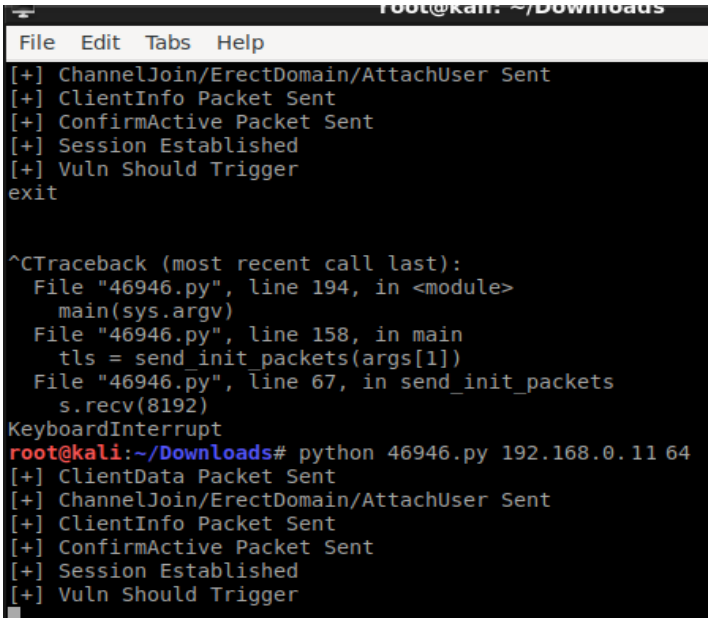
Imagen 6 Exploit Bluekeep



Fuente: Los Autores 2019

Se descarga y se ataca, indicamos la ruta donde se guardó el archivo, la ip y la versión del sistema si es de 64 o 32 bits.

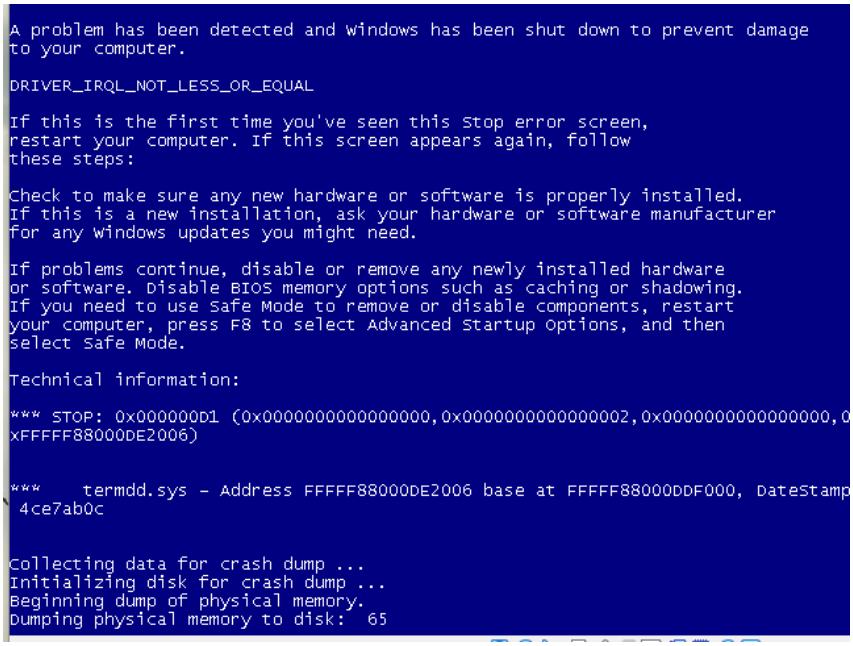
Imagen 7 Ataque a la máquina virtual



Fuente: Los Autores 2019

Como resultado en la maquina donde se tiene el Windows server 2008 r2 se obtiene el famoso pantallazo azul y una alerta del sistema por reinicio inesperado.

Imagen 8. Resultado del ataque a la máquina



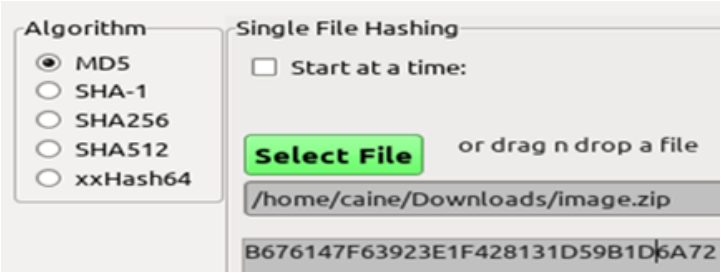
Fuente: Los Autores 2019

Conclusiones
Esta vulnerabilidad que afecta a los sistemas de Microsoft (Windows XP, Windows Vista, Windows Server R2 y Windows 7) como menciona anteriormente es preocupante pues son muchos los equipos que aún no se han actualizado, aunque Microsoft ya no brinda de manera oficial soporte para estos sistemas emitió un parche para proteger el sistema de esta vulnerabilidad. Blueekee no solo permite un ataque de denegación de servicio que fue el que nosotros hicimos si no que permite ejecución de código remoto (RCE).

Fuente: Los Autores 2019

7.3.2 Laboratorio #2 análisis a un disco y recuperación de archivos

Tabla 3. Solución laboratorio 2

Id del caso: 0002	Fecha: 05/07/2019	Forense: Sergio Camilo Ortega Ruiz y Stiven Paez Diaz
Descripción del delito		
Un colegio de EEUU a través de medios tecnológicos, fuentes humanas y trabajos de seguimiento se descubrió que uno de los estudiantes estaba comercializando drogas ilícitas dentro y fuera de esta institución, la policía incauto un disco duro donde se cree hay información relevante que ayude esclarecer el caso y llevar tras las rejas a todos los culpables.		
Objetivos de la investigación		
¿Quién es el proveedor de marihuana de Joe Jacob's el estudiante que comercializaba la droga? ¿Qué dirección posee dicho proveedor? ¿Hay alguna otra escuela secundaria además de la Smith Hill que Joe Jacob's frecuente?		
Evidencia		
Como evidencia se tiene un archivo comprimido con la imagen de un disco duro con el siguiente hash: md5: B676147F63923E1F428131D59B1D6A72 Imagen 9. Hash a imagen del laboratorio 2  Fuente: Los Autores 2019		

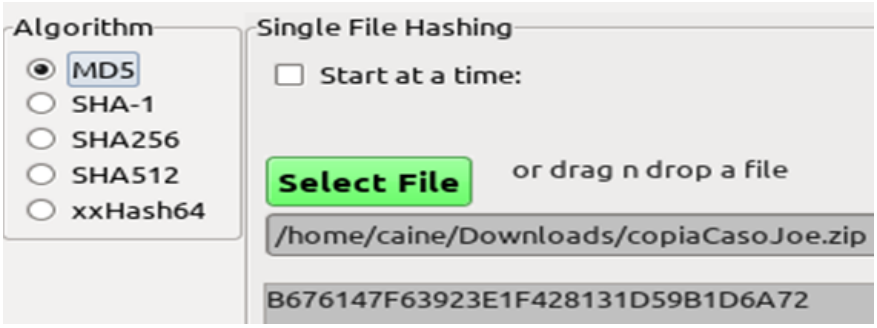
Análisis forense

Se procede a realizar una copia bit a bit y calcular su md5 para garantizar que la información con la que estamos trabajando es legítima.

Imagen 10. Copia bit a bit de la imagen del laboratorio

Fuente: Los Autores 2019

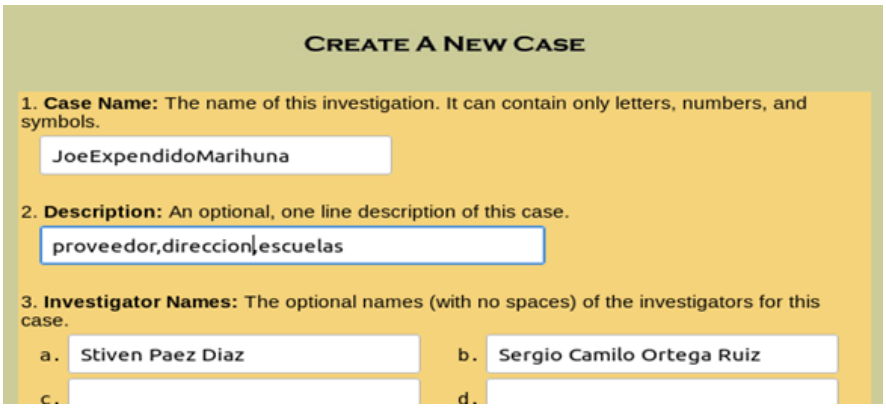
Imagen 11. Hash a la copia de la imagen forense laboratorio 2



Fuente: Los Autores 2019

Procedemos a montar la imagen en Autopsy para comenzar hacer su análisis.

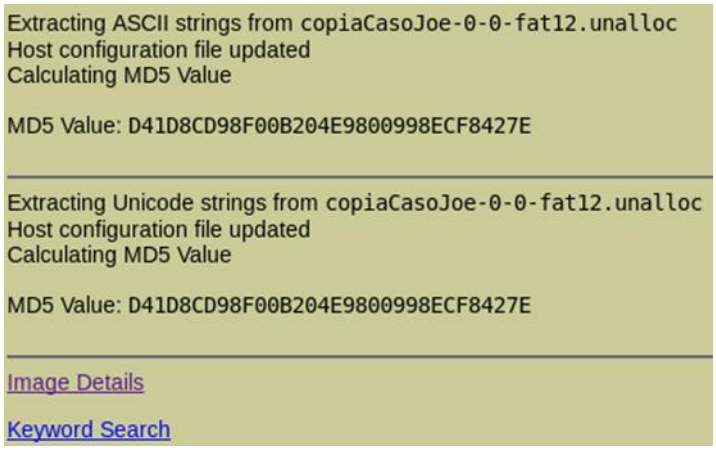
Imagen 12. Creación del caso del laboratorio 2 en Autopsy



Fuente: Los Autores 2019

Después de descomprimir el archivo montamos la imagen del disco.

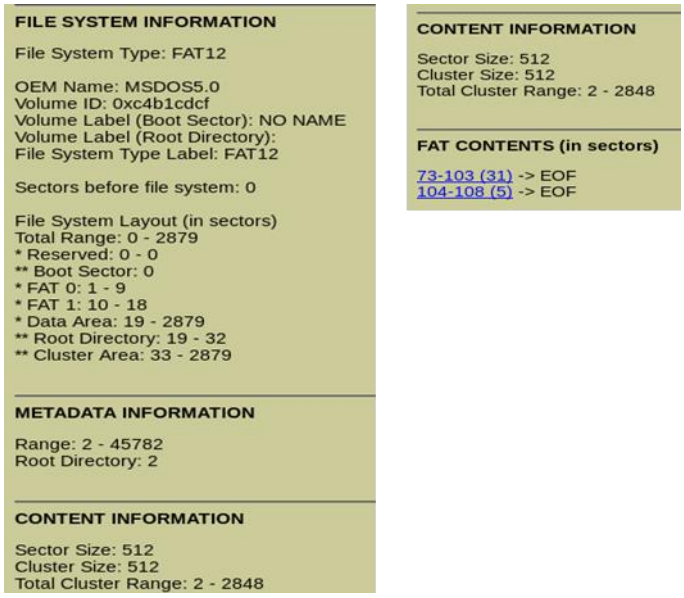
Imagen 13. Calculo md5 imagen forense laboratorio 2



Fuente: Los Autores 2019

Obtenemos los siguientes detalles de la imagen.

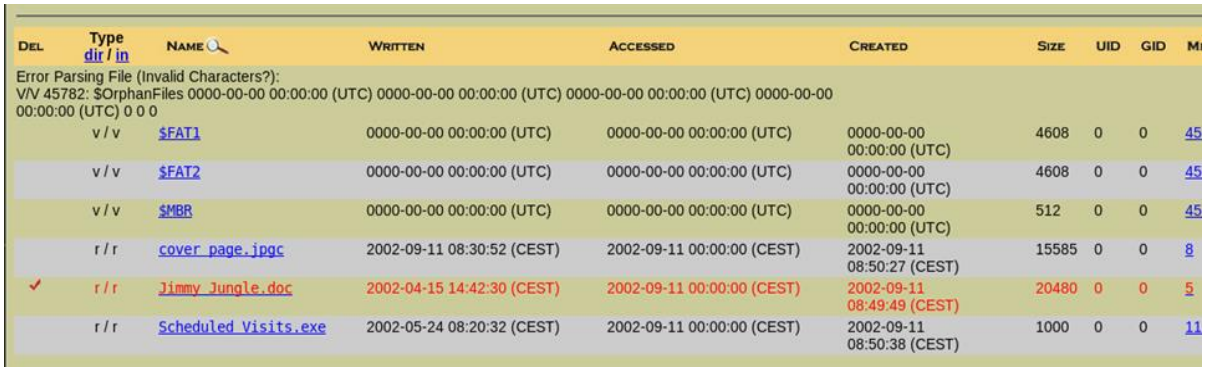
Imagen 14. Detalles imagen laboratorio 2



Fuente: Los Autores 2019

Encontramos 6 archivos en la imagen del disco.

Imagen 15. Archivos encontrados en la imagen del laboratorio 2



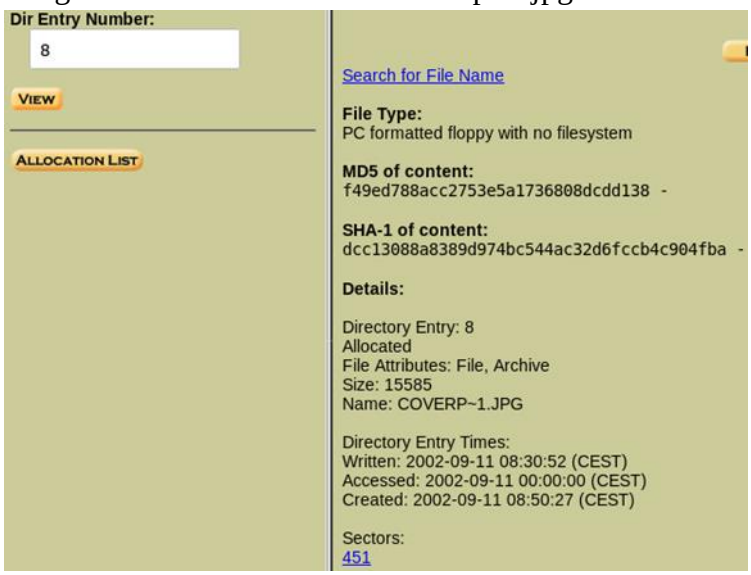
Del	Type dir / in	Name	Written	Accessed	Created	Size	UID	GID	M
Error Parsing File (Invalid Characters?): V/V 45782: $OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0									
	v / v	$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	45
	v / v	$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	45
	v / v	$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	45
	r / r	cover page.jpgc	2002-09-11 08:30:52 (CEST)	2002-09-11 00:00:00 (CEST)	2002-09-11 08:50:27 (CEST)	15585	0	0	8
✓	r / r	Jimmy Jungle.doc	2002-04-15 14:42:30 (CEST)	2002-09-11 00:00:00 (CEST)	2002-09-11 08:49:49 (CEST)	20480	0	0	5
	r / r	Scheduled Visits.exe	2002-05-24 08:20:32 (CEST)	2002-09-11 00:00:00 (CEST)	2002-09-11 08:50:38 (CEST)	1000	0	0	11

Fuente: Los Autores 2019

Se comienza analizar el archivo cover page.jpgc, a simple vista se observa una extensión rara.

Podría ser un archivo jpg.

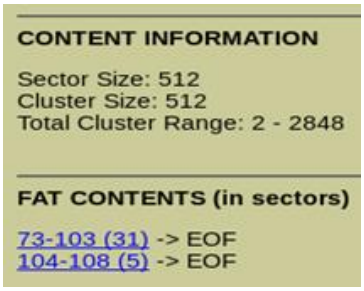
Imagen 16. Metadatos archivo coverp -1.jpg



Fuente: Los Autores 2019

Gracias a los metadatos del archivo, se identifica la verdadera extensión del archivo. Se nota algo inusual en el tamaño del archivo no es congruente con el del sector.

Imagen 17. Tamaño del sector



Fuente: Los Autores 2019

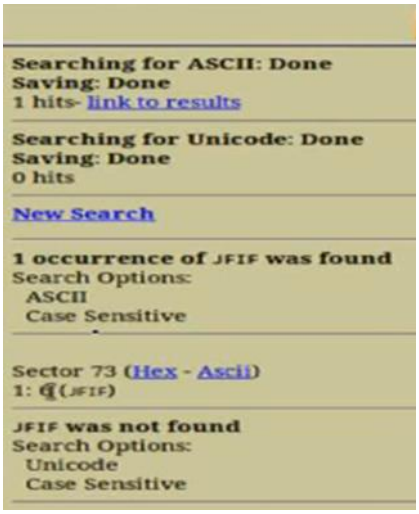
Procedeos a buscar la cabecera de un archivo jpg por medio de una herramienta de auptosy llamada búsqueda de palabras claves.

Imagen 18. Búsqueda cabecera de un archivo jp

Fuente: Los Autores 2019

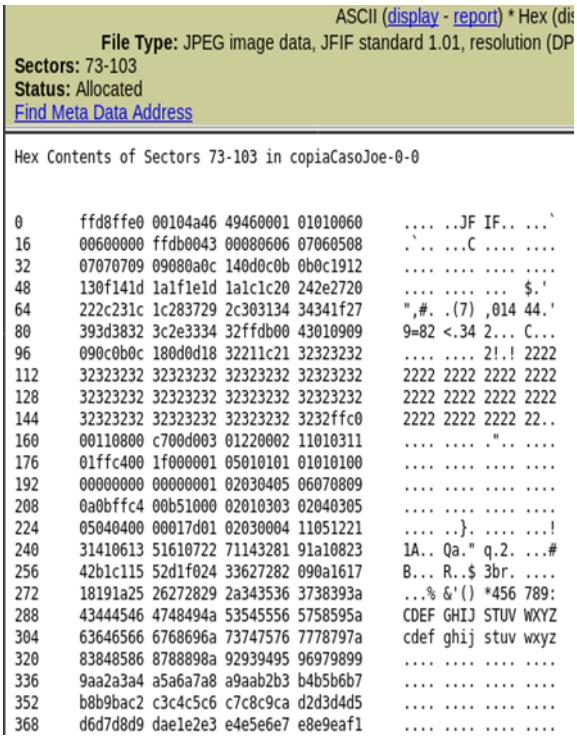
Autopsy nos arroja como resultado un archivo en el sector 73.

Imagen 19. Archivo encontrado el sector 73 con formato jpg



Fuente: Los Autores 2019

Imagen 20. Cabecera en hexadecimal de un archivo jpg



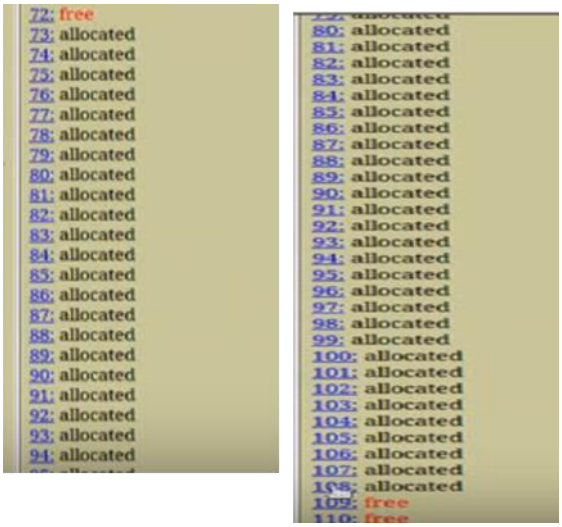
Fuente: Los Autores 2019

Sabemos que el archivo jpg empieza desde el sector 73 y vamos descubrir dónde termina por medio de la función data unit 

>>>>>>>> 

.

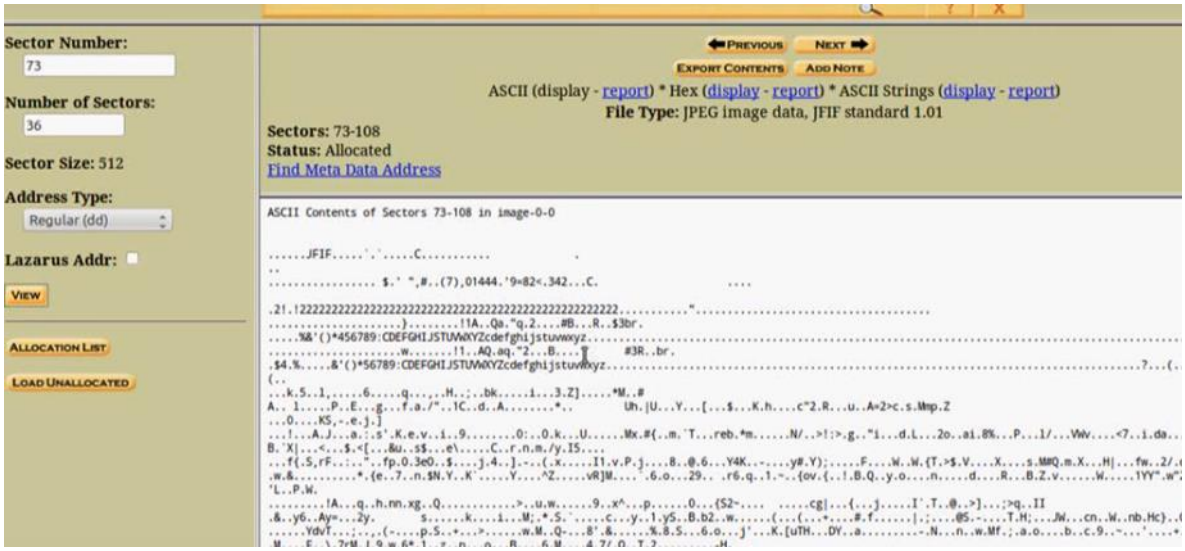
Imagen 21. Cantidad de sectores asignados desde el 73-108



Fuente: Los Autores 2019

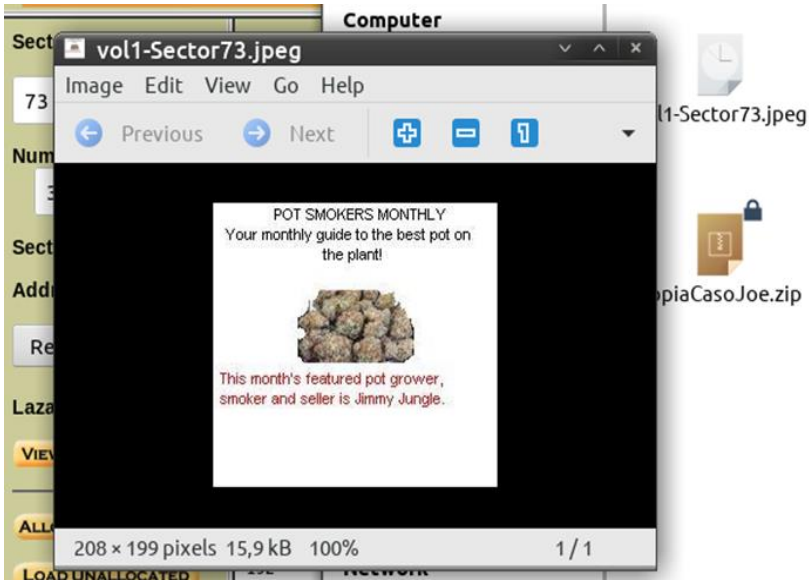
Se evidencia que desde el sector 73 que es donde empieza la asignación del archivo jpg hasta el 108 es donde termina dado que después de 108 está libre, se procede a exportar dichos sectores en formato jpg.

Imagen 22. Archivo a recuperar desde el sector 73-108



Fuente: Los Autores 2019

Imagen 23. Archivo recuperado cover-1.jpeg

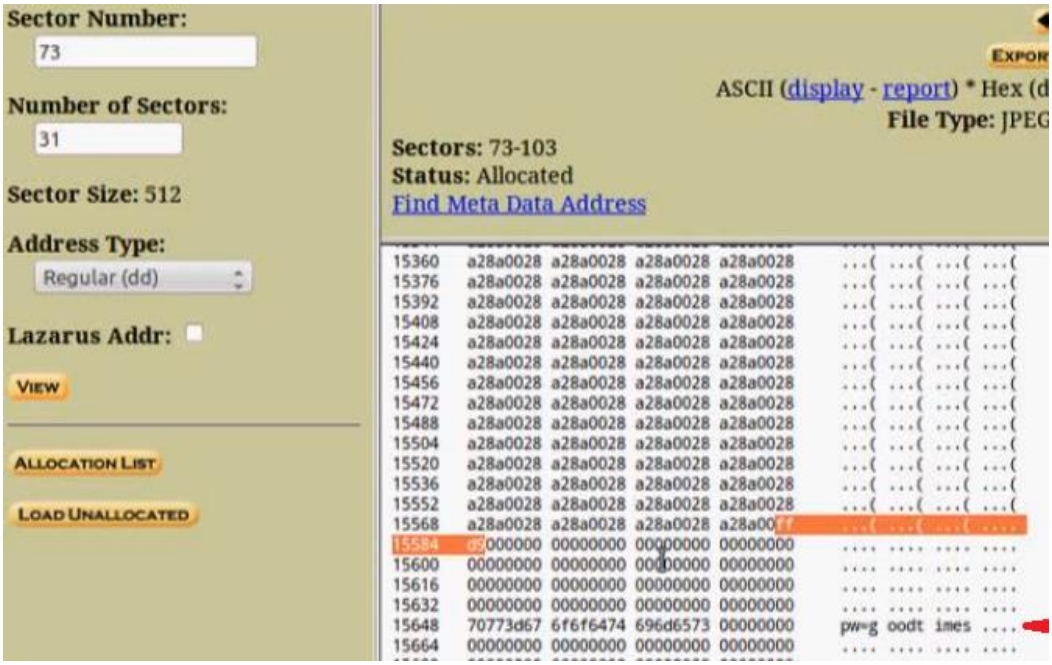


Fuente: Los Autores 2019

En la imagen se encuentra el nombre de “Jimmy Jungle” presunto proveedor de Joe.

Se determina la cantidad de sectores que debe de ocupar el tamaño de este archivo por medio del siguiente calculo 15585/512=30,439453125 aprox. 31, al visualizar el código hexadecimal se encuentra un texto insertado en la imagen.

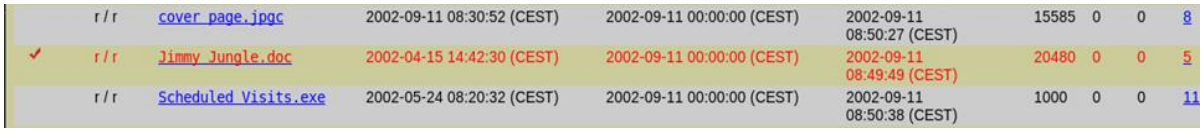
Imagen 24. Código hexadecimal del archivo jpg con una clave oculta



Fuente: Los Autores 2019

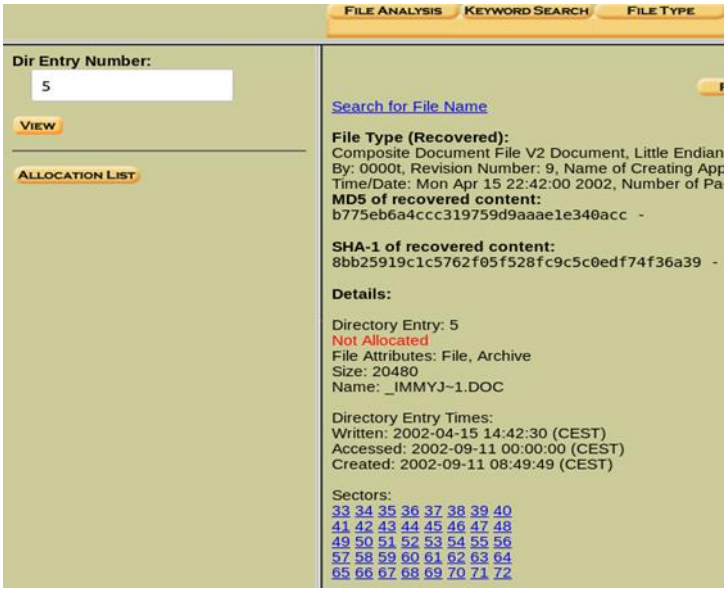
Ahora se analiza el archivo Jimmy jungle.doc el cual Autopsy resalta como eliminado.

Imagen 25. Archivo eliminado de la imagen del laboratorio 2



Fuente: Los Autores 2019

Imagen 26. Metadatos archivo eliminado Jimmy jungle.doc



Fuente: Los Autores 2019

Calculamos el número de sectores que ocuparía el archivo para proceder a su exportación

20480/512=40.

Imagen 27. Código hexadecimal del archivo Jimmy jungle.doc desde el sector 33-73

Fuente: Los Autores 2019

Contenido del documento recuperado.

Imagen 28. Documentos word que estaba eliminando del laboratorio 2

Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 11111

Jimmy:

Dude, your pot must be the best – it made the cover of High Times Magazine! Thanks for sending me the Cover Page. What do you put in your soil when you plant the marijuana seeds? At least I know your growing it and not some guy in Columbia.

These kids, they tell me marijuana isn't addictive, but they don't stop buying from me. Man, I'm sure glad you told me about targeting the high school students. You must have some experience. It's like a guaranteed paycheck. Their parents give them money for lunch and they spend it on my stuff. I'm an entrepreneur. Am I only one you sell to? Maybe I can become distributor of the year!

I emailed you the schedule that I am using. I think it helps me cover myself and not be predictive. Tell me what you think. To open it, use the same password that you sent me before with that file. Talk to you later.

Thanks,

Joe

Fuente: Los Autores 2019

Se analiza el otro archivo que aparentemente es un ejecutable de sistemas Windows.

Imagen 29. Archivo engañoso con extensión .exe

r / r	Scheduled Visits.exe	2002-05-24 08:20:32 (CEST)	2002-09-11 00:00:00 (CEST)	2002-09-11 08:50:38 (CEST)	1000	0	0	11

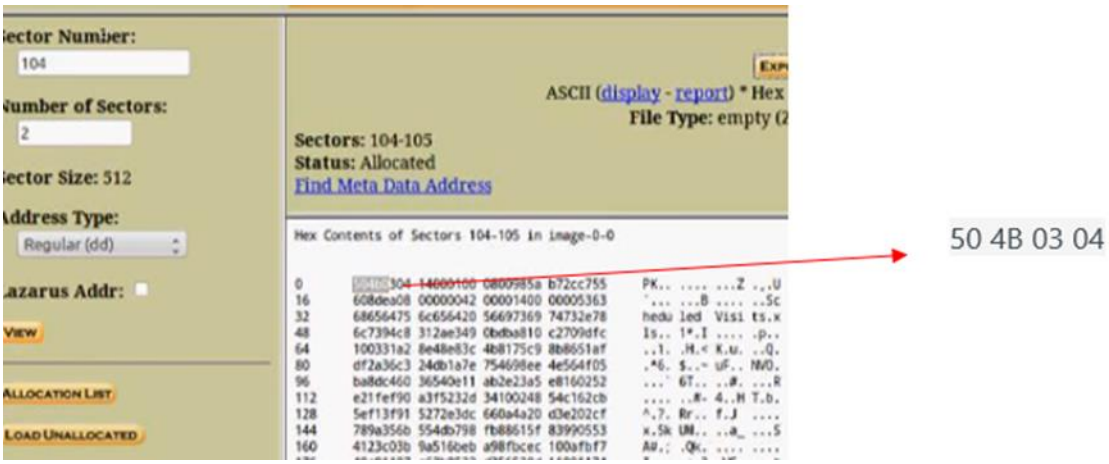
Fuente: Los Autores 2019

Imagen 30. Metadatos archivo .exe del laboratorio 2

Fuente: Los Autores 2019

El documento no es un .exe como pensamos es un archivo comprimido, calculamos la cantidad de sectores que se necesitan para almacenar el tamaño de este archivo por medio del siguiente calculo 1000/512=1,953125 aproximado 2.

Imagen 31. Cabecera archivo .zip



Fuente: Los Autores 2019

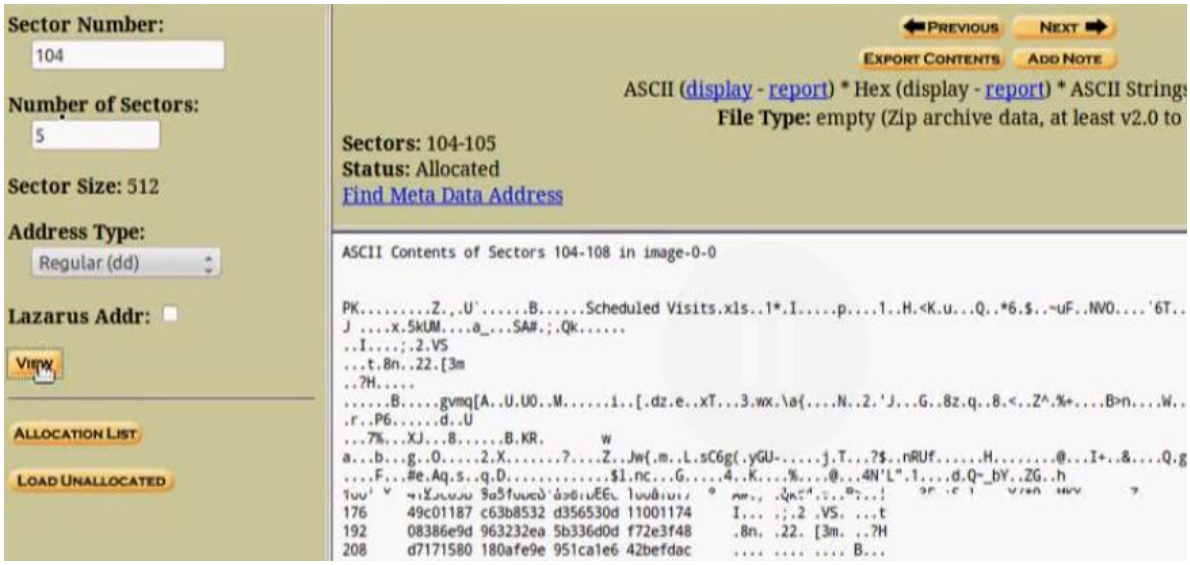
Se procede a extraer como un .zip, al tratar de descomprimirlo arroja una alerta de archivo corrupto y no continua con el proceso. Puede ser el que el archivo este compuesto por varias partes o no esté completo.

Al mirar los sectores asignados nos damos cuenta que el archivo está compuesto desde el sector 104 hasta el 108 y no desde hasta 105 como se creía.

Imagen 32. Sectores del archivo .exe laboratorio 2

Fuente: Los Autores 2019

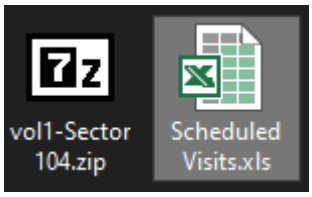
Imagen 33. Cabecera del archivo .zip desde el sector 105-108



Fuente: Los Autores 2019

Procedemos a exportarlo nuevamente como archivo. Zip y al tratar de descomprimirlo nos pide una clave, que encontramos en el texto extra encontrado en la imagen 24.

Imagen 34. Archivo descomprimido



Fuente: Los Autores 2019

Después de exportar el archivo .zip encontramos un archivo Excel con nombres y fechas de diferentes colegios que frecuentaba para hacer sus distribuciones.

Imagen 35. Archivo excel encontrado laboratorio 2

Month	DAY	HIGH SCHOOLS
2002		
April	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Key High School (B)
	Wednesday (3)	Leetch High School (C)
	Thursday (4)	Birard High School (D)
	Friday (5)	Richter High School (E)
	Monday (1)	Hull High School (F)
	Tuesday (2)	Smith Hill High School (A)
	Wednesday (3)	Key High School (B)
	Thursday (4)	Leetch High School (C)
	Friday (5)	Birard High School (D)
	Monday (1)	Richter High School (E)
	Tuesday (2)	Hull High School (F)
	Wednesday (3)	Smith Hill High School (A)
	Thursday (4)	Key High School (B)
	Friday (5)	Leetch High School (C)
	Monday (1)	Birard High School (D)
	Tuesday (2)	Richter High School (E)
	Wednesday (3)	Hull High School (F)
	Thursday (4)	Smith Hill High School (A)
	Friday (5)	Key High School (B)
	Monday (1)	Leetch High School (C)

Fuente: Los Autores 2019

Conclusiones

El archivo jpg se utilizó para guardar una contraseña.

Se encontró una carta de agradecimiento de Joe a su proveedor que había sido eliminada.

Se encontró una lista de colegios y fechas.

¿Quién es el proveedor de marihuana de Joe Jacob’s el estudiante que comercializaba la droga?

Jimmy Jungle

Imagen 36. Dirección del proveedor de Joe

Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 11111

Fuente: Los Autores 2019

¿Hay alguna otra escuela secundaria además de la Smith Hill que Joe Jacob’s frecuente?

- Key High School (B)
- Leetch High School (C)
- Birard High School (D)
- Richter High School (E)
- Hull High School (F)

Fuente: Los Autores 2019

7.3.3 Laboratorio #3 análisis a sistemas Windows

Tabla 4. Solución laboratorio 3.

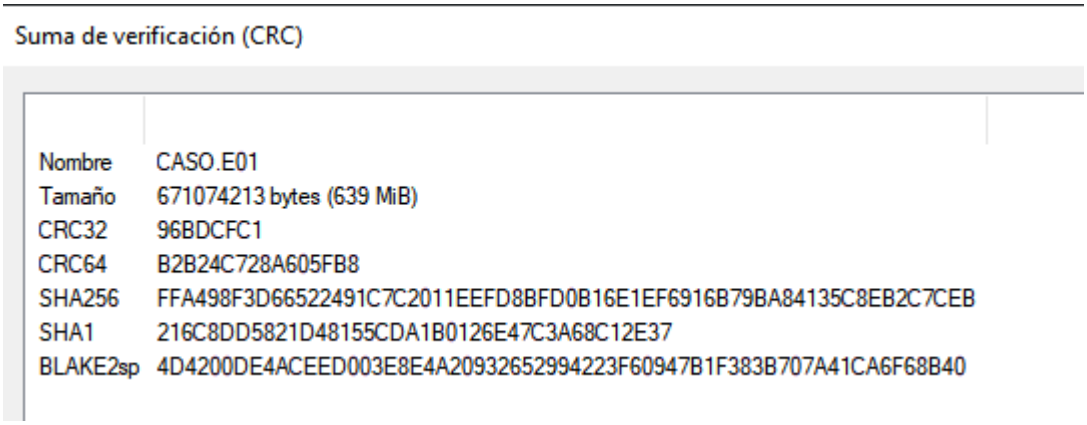
Id del caso: 0003	Fecha: 12/07/2019	Forense: Sergio Camilo Ortega Ruiz y Stiven Paez Diaz
Descripción del delito		
En una entrada y registro policial en un domicilio compartido por varias personas, se localiza y decomisa un computador personal que, pudiera estar relacionado con un presunto delito de tráfico de substancias ilícitas. A raíz del decomiso, una brigada especializada de un cuerpo policial realiza la clonación del disco duro contenido en el ordenador y tramita su IFE al laboratorio para que se realice un informe pericial de su contenido. Para llevar a cabo esta tarea se dispone de una autorización del juez que instruye el caso, por la cual se puede analizar cualquier contenido local del disco duro intervenido.		
Objetivos de la investigación		
Recaudar evidencia que permita esclarecer el caso en, encontrando información tal como: • ¿Cuál es el OS instalado en el sistema informático que estás analizando? • ¿Cuál es el tamaño, particiones y número de serie del disco? • ¿Sistema y versión del OS instalado? • ¿Nombre del usuario y organización registrados? • ¿Cuál es el “Product ID” asociado al sistema? • ¿Cuál es el “Service Pack” instalado? • ¿Cuál es la fecha y hora de instalación del OS? • ¿Cuál es la fecha y hora del último “shutdown? • ¿Cuáles son los usuarios creados en el sistema? • ¿Hay archivos eliminados?		

- ¿Hay archivos que estén ligados a delitos?
- ¿En el navegador hay información que esté implicada en los delitos?

Evidencia

Imagen de un disco duro con el siguiente hash:

Imagen 37. Hash imagen laboratorio 3

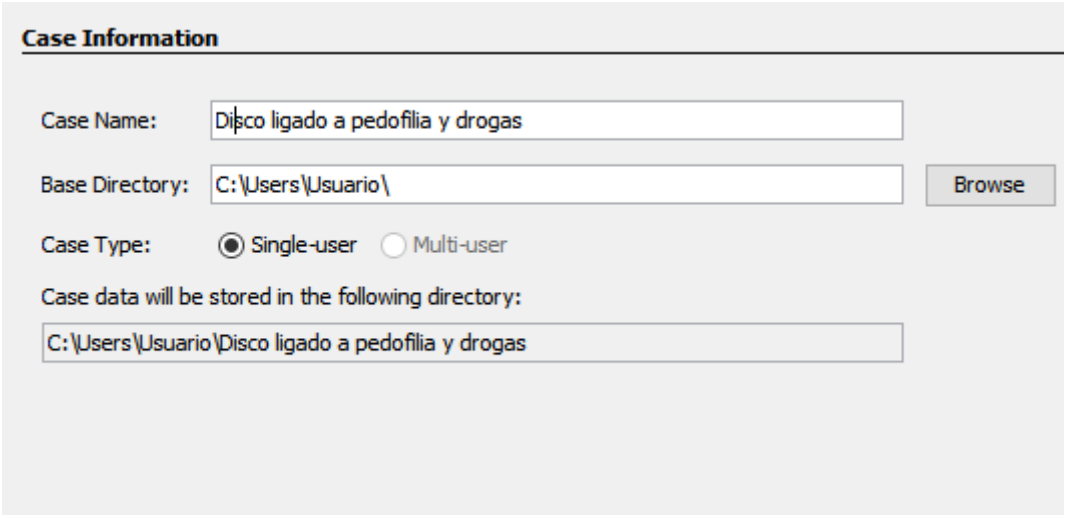


Fuente: Los Autores 2019

Análisis forense

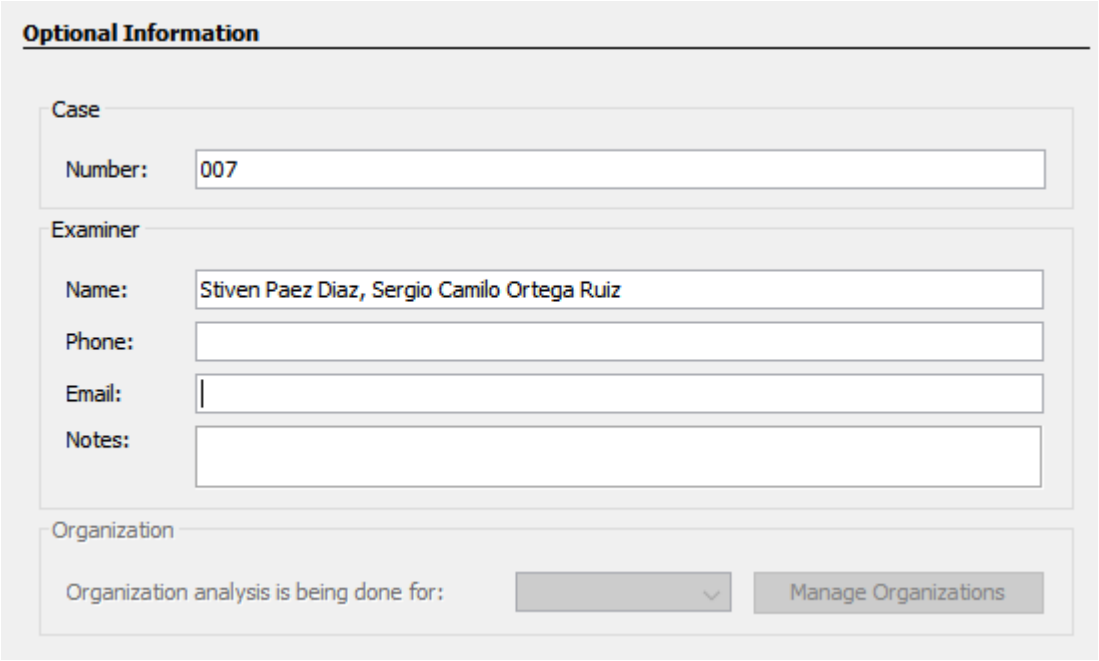
Se procede a montar la imagen en Autopsy.

Imagen 38. Creando el caso laboratorio 3



Fuente: Los Autores 2019

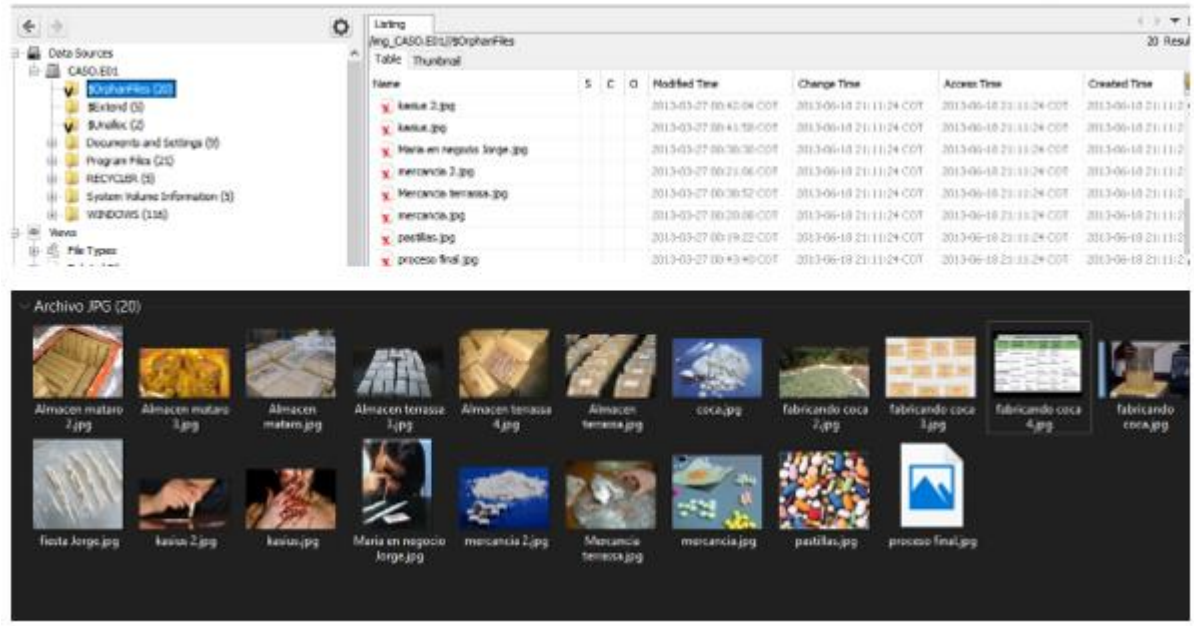
Imagen 39. Creando el caso laboratorio 3 Parte 2



Fuente: Los Autores 2019

Se procede a restaurar los archivos eliminados.

Imagen 40. Imágenes recuperadas del laboratorio 3

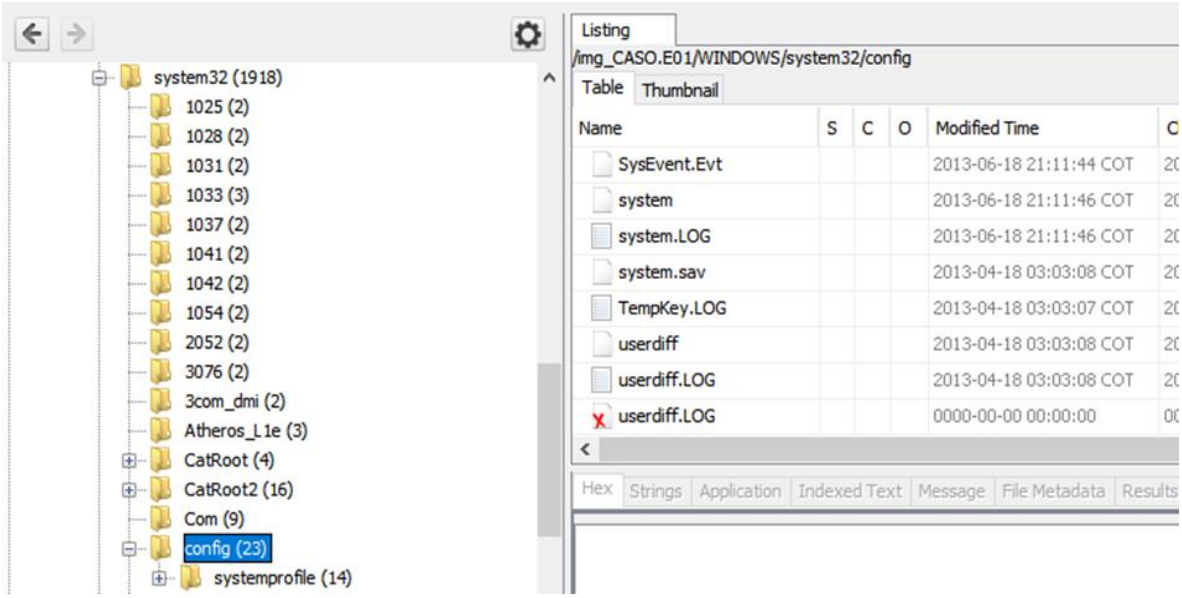


Fuente: Los Autores 2019

Se encuentran imágenes de almacenes, cargamentos y fórmulas de fabricación de drogas

Se extraer la carpeta system32/conf para averiguar información del sistema, usuarios entre otros con el Software regripper v2.8.

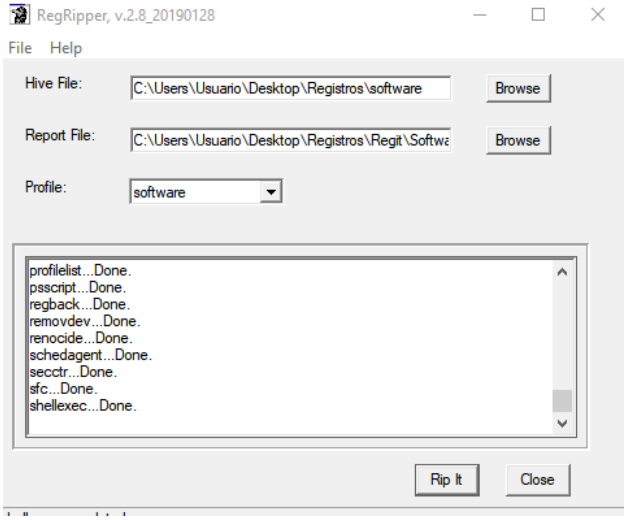
Imagen 41. Directorio de la imagen del laboratorio 3, carpeta system32/config



Fuente: Los Autores 2019

Se realizó la extracción de la carpeta config del directorio de Windows que está en la imagen y analizó el archivo con nombre Software y nos arroja información valiosa como la siguiente.

Imagen 42. Analizando el archivo Software



Fuente: Los Autores 2019

Imagen 43. Resultado del análisis del archivo Software

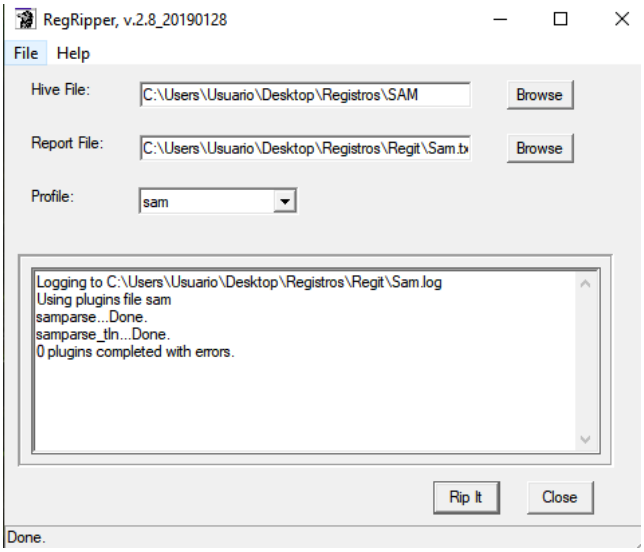
```
  SubVersionNumber :
  RegDone :
  CurrentVersion : 5.1
  RegisteredOrganization : home
  RegisteredOwner : John
  CurrentBuildNumber : 2600
  SoftwareType : SYSTEM
  SourcePath : D:\I386
  SystemRoot : C:\WINDOWS
  PathName : C:\WINDOWS
  CSDVersion : Service Pack 3
  CurrentType : Multiprocessor Free
  ProductName : Microsoft Windows XP
  BuildLab : 2600.xpsp.080413-2111
  ProductId : 76487-341-1072684-22504
  InstallDate : Thu Apr 18 15:17:02 2013 (UTC)
  CurrentBuild : 1.511.1 () (Obsolete data - do not use)
  LicenseInfo : e7 11 ea a1 e5 61 f8 35 10 d2 d7 7e 85 20 c
  DigitalProductId : a4 00 00 00 03 00 00 00 37 36 34 38 37
  00 31 2f 33 9f
----------------------------------------
winver v.20081210
(Software) Get Windows version

ProductName = Microsoft Windows XP
CSDVersion  = Service Pack 3
InstallDate = Thu Apr 18 15:17:02 2013
```

Fuente: Los Autores 2019

Arrojando que el equipo tenía como OS Windows XP, con Servi Pack 3, que el propietario se llama Jhon y que fue instalado el 18/04/2013 a las 15:17:02, también se encontró que la última vez que se apagó el equipo fue 19/06/2013 a las 02:11:46.

. También se analizó el archivo con nombre sam con el fin de saber los usuarios que tenía el sistema y horas de acceso.

Imagen 44. Analizando el archivo sam



Fuente: Los Autores 2019

Imagen 45. Datos del usuario John

```
Username        : John [1003]
SID             : S-1-5-21-1343024091-152049171-725345543-1003
Full Name       :
User Comment    :
Account Type    : Default Admin User
Account Created : Thu Apr 18 15:18:44 2013 Z
Name            :
Last Login Date : Thu Mar 28 03:10:49 2013 Z
Pwd Reset Date  : Thu Apr 18 15:18:44 2013 Z
Pwd Fail Date   : Never
Login Count     : 16
  --> Password does not expire
  --> Normal user account
```

Fuente: Los Autores 2019

Se descubrió que el usuario John tiene derechos de administrador, su ultimo acceso fue

28/03/2013 a las 03:10:49 y tiene 16 accesos al sistema.

Imagen 46. Datos del usario Ian

```
Username         : Ian [1004]
SID              : S-1-5-21-1343024091-152049171-725345543-1004
Full Name        :
User Comment     :
Account Type     : Default Admin User
Account Created  : Thu Apr 18 15:18:44 2013 Z
Name             :
Last Login Date  : Thu Apr 25 02:06:52 2013 Z
Pwd Reset Date   : Thu Apr 18 15:18:44 2013 Z
Pwd Fail Date    : Never
Login Count      : 10
   --> Password does not expire
   --> Normal user account
```

Fuente: Los Autores 2019

Se descubrió que el usuario Ian tiene derechos de administrador, su ultimo acceso fue 25/04/2013 a las 02:06:52 y 10 accesos al sistema.

Imagen 47. Datos del usuario Jessy

```
Username         : Jessy [1005]
SID              : S-1-5-21-1343024091-152049171-725345543-1005
Full Name        :
User Comment     :
Account Type     : Default Admin User
Account Created  : Thu Apr 18 15:18:44 2013 Z
Name             :
Last Login Date  : Tue Apr 23 02:18:56 2013 Z
Pwd Reset Date   : Thu Apr 18 15:18:44 2013 Z
Pwd Fail Date    : Never
Login Count      : 8
   --> Password does not expire
   --> Normal user account
```

Fuente: Los Autores 2019

Se descubrió que el usuario Jessy tiene derechos de administrador, su ultimo acceso fue 23/04/2013 a las 02:18:56 y tiene 8 accesos al sistema.

En el análisis del disco se encontraron archivos asociados a los delitos de pornografía infantil y expendido de droga.

Archivos encontrados.

Imagen 48. Datos encriptados hallados en el disco

Listing - Editor

Listing

Encryption Detected

Table | Thumbnail

Source File	S	C	O	Comment	Data Source
Contactes.xls				Password protection detected.	CASO.E01
pedofilia.zip				Content-only Encryption (Archive File)	CASO.E01
pedofilia.zip				Content-only Encryption (Archive File)	CASO.E01

Fuente: Los Autores 2019

Imagen 49. Historial de búsquedas implicadas en delitos

index.dat	clients1.google.es	cocaine	2013-04-24 01:59:09 COT
index.dat	www.google.es	cocaine price	2013-04-24 01:59:11 COT
index.dat	www.google.es	cocaine price	2013-04-30 23:01:30 COT
index.dat	www.google.es	cocaine price	2013-04-24 01:59:11 COT
index.dat	www.bing.com	codigo penal espa;ol	2013-04-25 23:01:20 COT
index.dat	www.bing.com	codigo penal espa;ol	2013-04-30 23:01:30 COT
index.dat	www.bing.com	codigo penal espa;ol	2013-04-25 23:01:20 COT
index.dat	www.bing.com	cotilleos corazon	2013-04-23 02:24:45 COT
index.dat	www.bing.com	cotilleos corazon	2013-04-23 02:24:45 COT
index.dat	clients1.google.es	foros ped	2013-04-24 01:58:27 COT
index.dat	clients1.google.es	foros pedo	2013-04-24 01:58:28 COT
index.dat	clients1.google.es	foros pedof	2013-04-24 01:58:28 COT
index.dat	clients1.google.es	foros pedofi	2013-04-24 01:58:28 COT
index.dat	www.google.es	foros pedofilia	2013-04-24 01:58:31 COT
index.dat	clients1.google.es	ill	2013-04-23 02:16:07 COT
index.dat	clients1.google.es	ille	2013-04-23 02:16:07 COT
index.dat	clients1.google.es	illeg	2013-04-23 02:16:08 COT
index.dat	clients1.google.es	illega	2013-04-23 02:16:08 COT
index.dat	clients1.google.es	illegal	2013-04-23 02:16:08 COT
index.dat	clients1.google.es	illegal p	2013-04-23 02:16:08 COT
index.dat	clients1.google.es	illegal po	2013-04-23 02:16:09 COT
index.dat	www.google.es	illegal porn	2013-04-23 02:16:20 COT

Fuente: Los Autores 2019

Imagen 50. Archivo encontrado en la carpeta del usuario Jhon que contiene datos de los proveedores de drogas

Name	Location	Modified Time	Size
providers.ico	/img_CASO.E01/Documents and Settings/John/Desktop/providers.ico	2013-04-17 12:24:42 COT	38400
winword.doc	/img_CASO.E01/Documents and Settings/Default User/Templates/winword.doc	2008-04-14 07:00:00 COT	4608
winword.doc	/img_CASO.E01/WINDOWS/system32/config/systemprofile/Templates/winword.doc	2008-04-14 07:00:00 COT	4608
winword.doc	/img_CASO.E01/Documents and Settings/John/Templates/winword.doc	2008-04-14 07:00:00 COT	4608
winword.doc	/img_CASO.E01/Documents and Settings/Jessy/Templates/winword.doc	2008-04-14 07:00:00 COT	4608
winword.doc	/img_CASO.E01/Documents and Settings/Ian/Templates/winword.doc	2008-04-14 07:00:00 COT	4608

Hoja de coca Mikel Ezberria 666556655 llamar solo los lunes tarde

Punto de encuentro: zarragoza, gasolinera la pausa a2 km 40

Pasta base Luisma (badia) 666112211

Punto de encuentro: badia c/ oporto bar "pep"

MDA foro motor.net , contacto "Ian34"

Metilanfetamina ebay contacto "roxy2332"

Dietilamina foro motor.net, contacto "Merkel69"

_1427699432.doc

Proveedores productos

Hoja de coca

Mikel Ezberria

666556655 llamar solo los lunes tarde

Fuente: Los Autores 2019

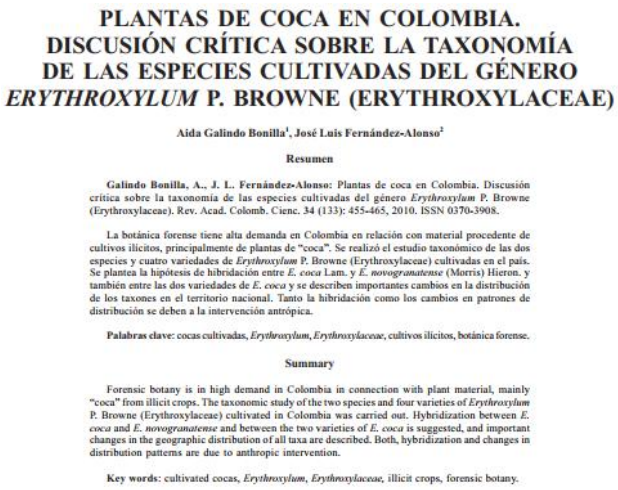
Imagen 51. Búsqueda pornografía infantil, un delito

index.dat	clients1.google.es	porn	2013-04-23 02:15:49 COT
index.dat	clients1.google.es	porn	2013-04-23 02:15:41 COT
index.dat	clients1.google.es	porn	2013-04-23 02:15:38 COT
index.dat	www.google.es	porn 10 years	2013-04-23 02:15:57 COT
index.dat	www.google.es	porn 10 years	2013-04-23 02:15:57 COT
index.dat	clients1.google.es	porn b	2013-04-23 02:15:46 COT
index.dat	clients1.google.es	porn ba	2013-04-23 02:15:47 COT
index.dat	www.google.es	porn baby	2013-04-23 02:15:48 COT
index.dat	www.google.es	porn baby	2013-04-23 02:15:48 COT
index.dat	www.google.es	porn bibies	2013-04-23 02:15:44 COT
index.dat	www.google.es	porn bibies	2013-04-23 02:15:44 COT
index.dat	www.google.es	porn pedofil	2013-04-23 02:15:52 COT
index.dat	www.google.es	porn pedofil	2013-04-23 02:15:52 COT

Fuente: Los Autores 2019

Imagen 52. Archivo pdf relacionada con la droga

Name	Location	Created Time	Size
coca.pdf	/img_CASO.E01/Documents and Settings/John/Desktop/coca.pdf	2013-04-22 19:58:42 COT	5826655
manufacturing amfetas.link	/img_CASO.E01/Documents and Settings/John/Desktop/manufa...	2013-04-22 19:58:52 COT	133681
manufacturing.link	/img_CASO.E01/Documents and Settings/John/Desktop/manufa...	2013-04-22 19:58:52 COT	669101
Dc1.link	/img_CASO.E01/RECYCLER/S-1-5-21-1343024091-152049171-...	2013-04-22 19:58:58 COT	336765



PLANTAS DE COCA EN COLOMBIA. DISCUSIÓN CRÍTICA SOBRE LA TAXONOMÍA DE LAS ESPECIES CULTIVADAS DEL GÉNERO *ERYTHROXYLUM* P. BROWNE (ERYTHROXYLACEAE)

Aida Galindo Bonilla[1], José Luis Fernández-Alonso[2]

Resumen

Galindo Bonilla, A., J. L. Fernández-Alonso: Plantas de coca en Colombia. Discusión crítica sobre la taxonomía de las especies cultivadas del género *Erythroxylum* P. Browne (Erythroxylaceae). Rev. Acad. Colomb. Cienc. 34 (133): 455-465, 2010. ISSN 0370-3908.

La botánica forense tiene alta demanda en Colombia en relación con material procedente de cultivos ilícitos, principalmente de plantas de "coca". Se realizó el estudio taxonómico de las dos especies y cuatro variedades de *Erythroxylum* P. Browne (Erythroxylaceae) cultivadas en el país. Se plantea la hipótesis de hibridación entre *E. coca* Lam. y *E. novogranatense* (Morris) Hieron. y también entre las dos variedades de *E. coca* y se describen importantes cambios en la distribución de los taxones en el territorio nacional. Tanto la hibridación como los cambios en patrones de distribución se deben a la intervención antrópica.

Palabras clave: cocas cultivadas, *Erythroxylum*, *Erythroxylaceae*, cultivos ilícitos, botánica forense.

Summary

Forensic botany is in high demand in Colombia in connection with plant material, mainly "coca" from illicit crops. The taxonomic study of the two species and four varieties of *Erythroxylum* P. Browne (Erythroxylaceae) cultivated in Colombia was carried out. Hybridization between *E. coca* and *E. novogranatense* and between the two varieties of *E. coca* is suggested, and important changes in the geographic distribution of all taxa are described. Both, hybridization and changes in distribution patterns are due to anthropic intervention.

Key words: cultivated cocas, *Erythroxylum*, *Erythroxylaceae*, illicit crops, forensic botany.

Fuente: Los Autores 2019

Los archivos están ligados a los usuarios John e Ian.

Conclusiones

Con esto se concluye que los usuarios Ian y John tenían en su cuenta archivos sobre pornografía infantil, creación y expendido de cocaína, el análisis arroja que las fechas de los registros de la creación de estos archivos concuerdan con los accesos al sistema desde estas cuentas, también se evidencia que los archivos están ligados a los diferentes directorios creados por el sistema para estos usuarios.

Fuente: Los Autores 2019

7.3.4 Laboratorio #4 análisis con sniffer 1

Tabla 5. Solución laboratorio 4

Id del caso: 0004	Fecha: 05/07/2019	Forense: Sergio Camilo Ortega Ruiz y Stiven Paez Diaz

Descripción del delito

Desserts and Delights S.A, sospecha que uno de sus empleados, Ann Dercover, es realmente un agente secreto que trabaja para su competidor. Ann tiene acceso a una receta muy importante de la compañía ganadora de un premio a nivel mundial, esta receta es secreta. El personal de seguridad está preocupado de que Ann intente filtrar la receta secreta de la compañía.

El personal de seguridad ha estado monitoreando la actividad de Ann por algún tiempo, pero hasta ahora no ha encontrado nada sospechoso. Hoy, una computadora portátil inesperada apareció brevemente en la red inalámbrica de la compañía. El personal cree que podría haber sido alguien en el estacionamiento, porque no se vio a extraños en el edificio. La computadora de Ann (I.P: 192.168.1.158) envió mensajes instantáneos a través de la red inalámbrica a esta computadora. El portátil falso desapareció poco después.

Objetivos de la investigación

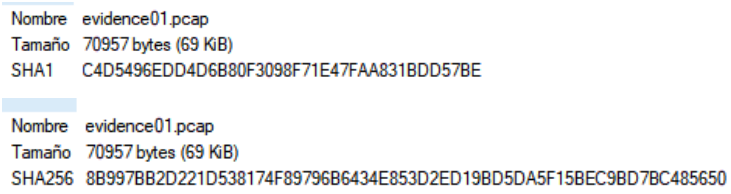
- ¿Cuál es el nombre de la amiga de Ann?
- ¿Cuál fue el primer comentario en la conversación?
- ¿Cuál es el nombre del archivo que Ann transfirió?
- ¿Cuál es el número mágico del archivo que desea extraer (primeros cuatro bytes)?
- ¿Cuál fue la suma MD5 del archivo?
- ¿Cuál es la receta secreta?

Evidencia

El departamento de TICs de la empresa obtuvo la captura de paquetes de dicha conversación inusual iniciada desde la computadora de Ann.

La cual se nos entrega mediante este link:
http://forensicscontest.com/contest01/evidence01.pcap

Imagen 53. Hash realizado a la evidencia



Fuente: Los Autores 2019

Análisis forense

Después de obtener la evidencia, se hace el análisis utilizado dos herramientas en especial, Wireshark que nos va a permitir analizar la trama, NetworkmMner para la recuperación de archivo además de Autopsy para ir llevando el caso.

El análisis se hace a partir de la identificación de la conversación entre el equipo de Ann con IP 192.168.1.158 y la otra máquina.

Después de hacer el respectivo análisis, se empezó a resolver las preguntas:

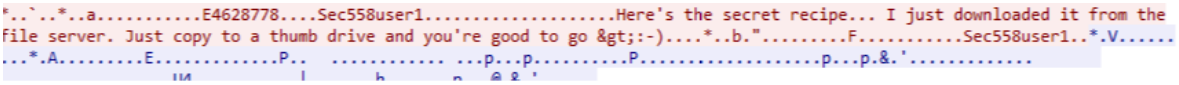
Nombre de la amiga de Ann IM:

Imagen 54. Usuario encontrado laboratorio 4

Fuente: Los Autores 2019

El mensaje capturado:

Imagen 55. Mensaje capturado

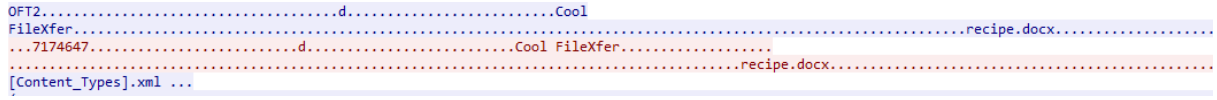


Fuente: Los Autores 2019

Para poder observar el mensaje, lo que se hizo fue identificar los equipos que más comunicación tenían y se procedió a seguir las “tramas”, lo cual con la herramienta WireShark, permite seguir TCP Streams, como se evidencia en la imagen y posteriormente nos muestra el mensaje solicitado.

Nombre del archivo enviado:

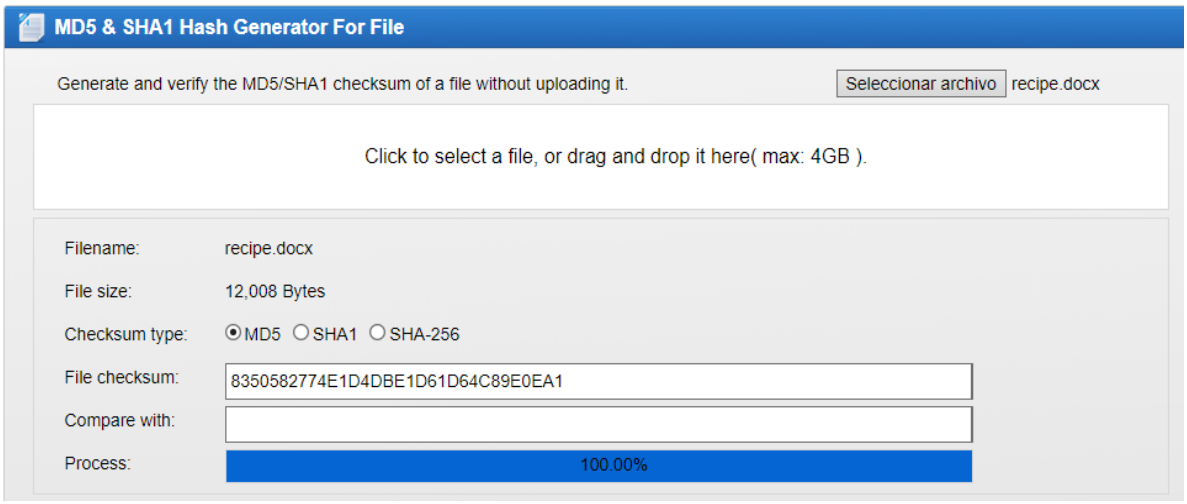
Imagen 56. Imagen 56. Seguimiento de trama



Fuente: Los Autores 2019

Número mágico del archivo encontrado:

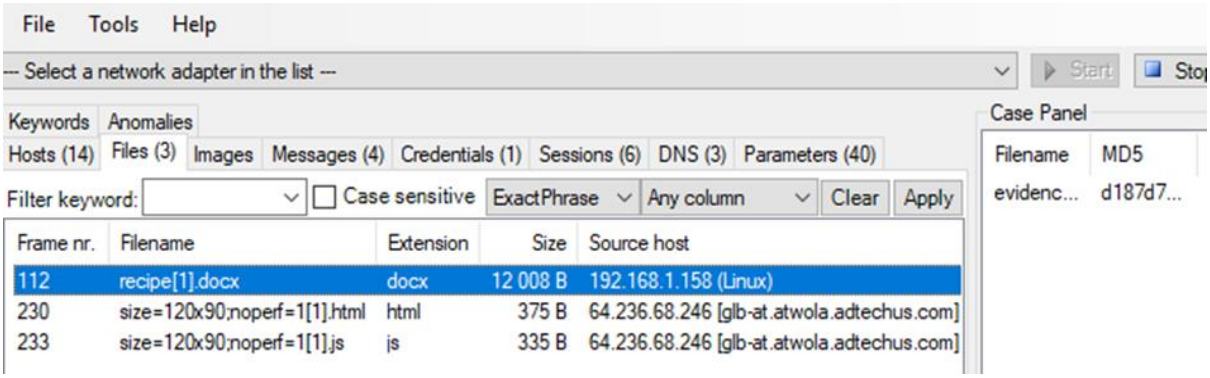
Imagen 57. Hash MD5



Fuente: Los Autores 2019

¿Cuál era la receta secreta que contenía el archivo?

Imagen 58. Recuperación de archivo .doc



Fuente: Los Autores 2019

Al analizar las tramas se encontró un mensaje donde se evidencia la transferencia de un archivo con extensión .doc, se procedió a buscarlo y extraerlo.

Imagen 59. Contenido de archivo

Recipe for Disaster:

1 serving

Ingredients:

4 cups sugar

2 cups water

In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.

Fuente: Los Autores 2019

Conclusiones

Gracias a la información brindada por el personal de seguridad y posteriormente del análisis forense realizado, se concluye que la empleada Ann Decover ha estado realizando procesos indebidos con información sensible y privada de la empresa, puesto que se ha encontrado que la empleada revelo la receta secreta de la empresa.

Fuente: Los Autores 2019

7.3.5 Laboratorio #5 análisis con sniffer 2

Tabla 6. Solución laboratorio 5.

Id del caso: 0005	Fecha: 05/07/2019	Forense: Sergio Camilo Ortega Ruiz y Stiven Paez Diaz

Descripción del delito

Después de ser liberada bajo fianza, ¡Ann Dercover desaparece! Afortunadamente, los investigadores estaban monitoreando cuidadosamente la actividad de su red antes de que se saliera de la ciudad.

"Creemos que Ann puede haberse comunicado con su amante secreto, el Sr. X, antes de irse", dice el jefe de policía. "La captura de paquetes puede contener pistas sobre su paradero".

Objetivos de la investigación

- ¿Cuál es la dirección de correo electrónico de Ann?
- ¿Cuál es la contraseña de correo electrónico de Ann?
- ¿Cuál es la dirección de correo electrónico de la amante secreta de Ann?
- ¿Qué dos artículos le dijo Ann a su amante secreto para traer?
- ¿Cuál es el NOMBRE del archivo adjunto que Ann le envió a su amante secreto?
- ¿Cuál es la suma MD5 del archivo adjunto que Ann le envió a su amante secreto?
- ¿En qué CIUDAD y PAÍS es su punto de encuentro?
- ¿Cuál es la suma MD5 de la imagen incrustada en el documento?

Evidencia

Después de la captura de Ann Dercover, por filtrar información de la empresa, más concreto, la receta secreta, Ann sale bajo fianza, posterior a esto Ann recurre a romper su fianza e huir. Lo que no sabía era que seguía vigilada, por lo tanto, se tiene conocimiento de su tráfico de red, esto permite que la investigación tenga pistas para poder resolver los objetivos de la investigación.

Evidencia entregada mediante el siguiente link:

http://forensicscontest.com/contest02/evidence02.pcap

Imagen 60. Hash evidencia laboratorio 5

Nombre	evidence02.pcap
Tamaño	335144 bytes (327 KiB)
CRC32	3B1F0584
CRC64	34E21624050CFD12
SHA256	290F495DF4D30038E0DB638AC9A0EE24AFD9C708ACBF1BD86BEC9F0C45FC061C
SHA1	CC649705CEF9F42FD2ECD6F5B949D5B7C4901C3D
BLAKE2sp	98D3C7154A3F9813D39AFF01AB24A4D3E203777A80A80C3B6710C8443A83457A

Fuente: los Autores

Análisis forense

Para empezar a resolver los objetivos para este caso, se procede a escoger las herramientas adecuadas. Las escogidas fueron WireShark y NetworkMiner. Como primer objetivo es con la evidencia obtenida, es buscar la dirección de correo electrónico de Ann Dercover.

Se abre la captura y se empieza a buscar en que parte de la trama se encuentra la mayor comunicación entre origen y destino, después de hallada esta área se procede a seguir la trama. Siguiendo dicho tramo de la captura se puede observar la dirección de correo de Ann como se muestra:

Imagen 61. Email de Ann

```
354 START MAIL INPUT, END WITH "." ON A LINE BY ITSELF
Message-ID: <001101ca49ae$e93e45b0$9f01a8c0@annlaptop>
From: "Ann Dercover" <sneakyg33k@aol.com>
```

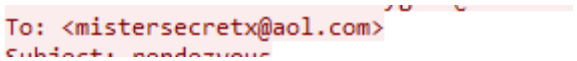
Fuente: Los Autores 2019

¿Cuál es la contraseña de correo electrónico de Ann?

¿Cuál es la dirección de correo electrónico de la amante secreta de Ann?

Para obtener el correo de Mr X, se procedió a seguir la misma trama con la cual se hayo el correo de Ann ya que fue la captura de unos correos que se enviaron.

Imagen 62. Email Mrx

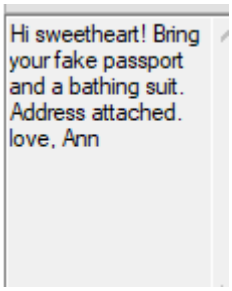


Fuente: Los Autores 2019

¿Qué dos artículos le dijo Ann a su amante secreto para traer?

Para este punto, se usó la herramienta NetworkMiner, con su amigable interfaz, se abre la captura, y se dirige a el apartado “Messages”, y en el primero que aparece, dice lo siguiente:

Imagen 63. Mensaje de correo electrónico

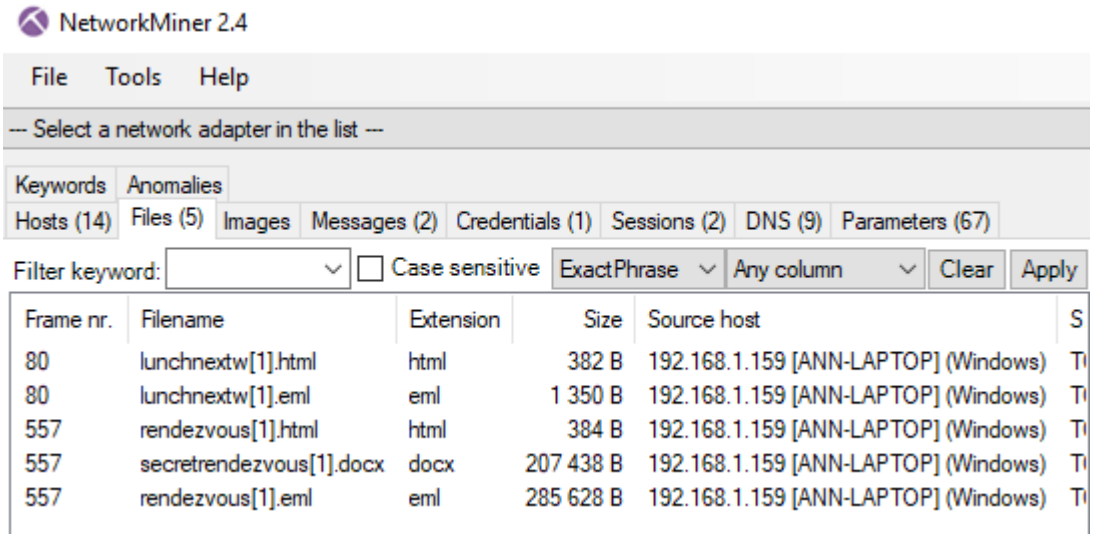


Fuente: Los Autores 2019

¿Cuál es el NOMBRE del archivo adjunto que Ann le envió a su amante secreto?

En este punto, lo que se utilizó NetworkMiner. Se dirige al apartado de “Files”, y ahí encontramos un archivo .docx, como se observa en la evidencia:

Imagen 64. Nombre de archivo .doc

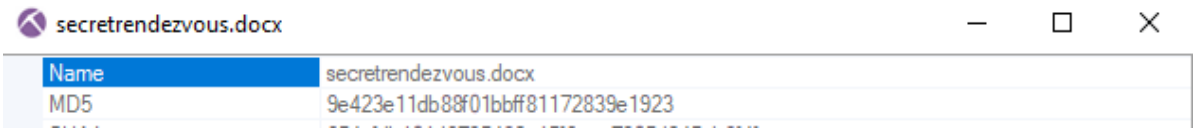


Fuente: Los Autores 2019

¿Cuál es la suma MD5 del archivo adjunto que Ann le envió a su amante secreto?

Para hacer el hash de este archivo usamos la herramienta NetworkMiner, la cual nos permite hacer este procedimiento.

Imagen 65. Hash MD5 del archivo encontrado

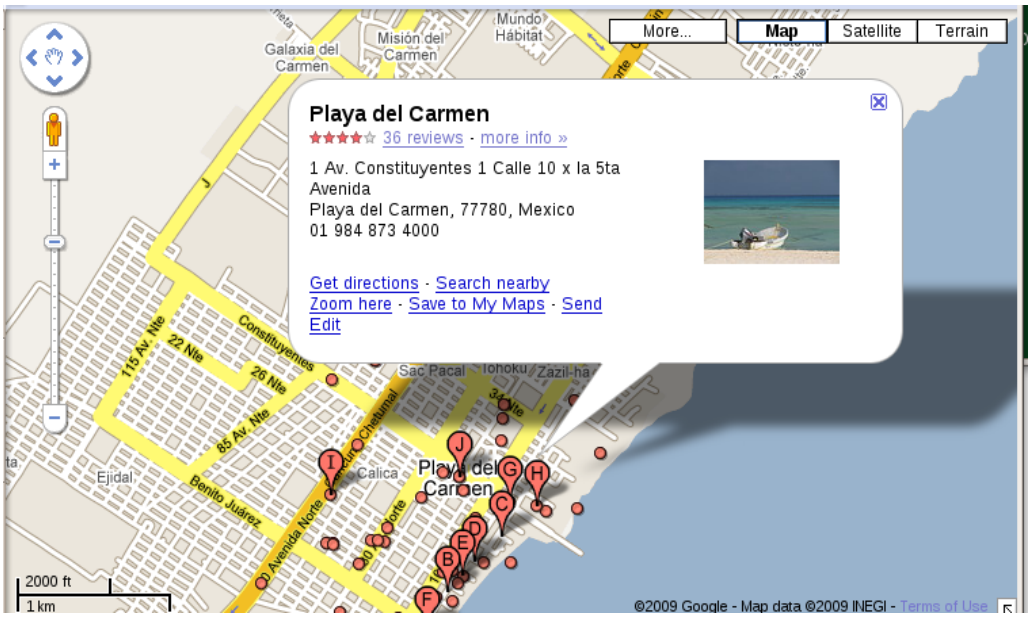


Fuente: los Autores 2019

¿En qué CIUDAD y PAÍS es su punto de encuentro?

Para poder obtener esta información necesitamos usar NetworkMiner, ya que como con su función de recuperación de archivos encontrados en la captura, se procese a recuperar el documento y este en su interior nos da una información la cual es:

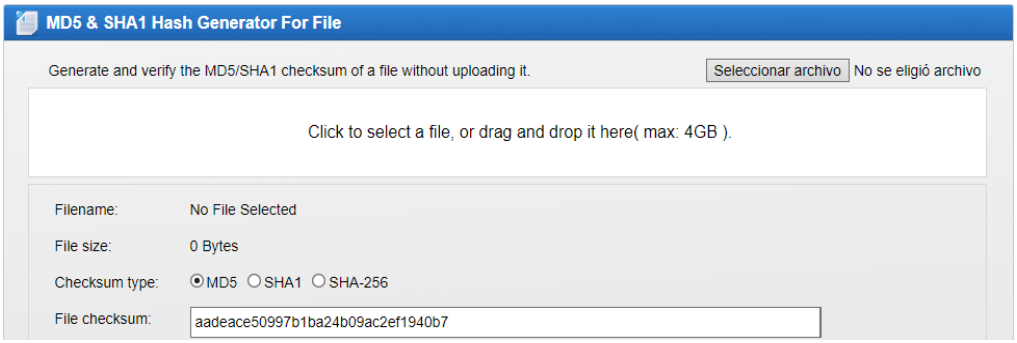
Imagen 66. Localización del individuo en cuestión



Fuente los Autores 2019

¿Cuál es la suma MD5 de la imagen incrustada en el documento?

Imagen 67. Hash de la imagen del archivo



Fuente: Los autores 2019

Conclusiones

Cabe resaltar que a pesar de que Ann Dercover se encontraba en libertad condicional se le seguía vigilando, gracias a esto, nos da una evidencia con la cual se tiene un punto de partida para poder dar con el paradero de Ann. Gracias al análisis forense hecho, se puede resolver los objetivos propuestos, esto permite que las autoridades competentes puedan recuperar la custodia de la acusada.

Fuente: Los Autores 2019

Capítulo 8. Fuentes para la Obtención de Información

A continuación, se citan las múltiples fuentes que fueron consultadas durante el desarrollo de este proyecto, las cuales por su relevancia aportaron de una forma notoria a lo que fue el levantamiento de información de una manera correcta, para así poder alinear las diferentes fases del proyecto presentado.

8.1 Fuentes Primarias

Chavez, A., & Villota Jimenez, W. A. (2018). *Análisis forense y sus herramientas*. Cali: UNICATÓLICA Fundación Universitaria Católica Lumen Gentium.

Haydée Di Iorio, A., Mollo, M., Cistoldi, P., Lamperti, S., Fernanda Giaccaglia, M., Malaret, P., . . . Constanzo, B. (2016). Consideraciones para el diseño de un Laboratorio Judicial en Informática Forense. (U. FASTA, Ed.) *Universidad FASTA*, 1-6. Recuperado el 11 de 12 de 2018, de http://redi.ufasta.edu.ar:8080/xmlui/handle/123456789/1564

Rifà Pous, H., Serra Ruiz, J., & Rivas López, J. (2009). *Análisis forensede sistemasinformáticos*. Barcelona: EURECA MEDIA S.L.

Castillo Saavedra, L. F., & Bohada Jaime, J. A. (2015). Informática Forense en Colombia. *Ciencia, Innovación y Tecnología*, 94.

8.2 Fuentes Secundarias

Informática Forense Colombia. (31 de 07 de 2019). *Informática Forense* . Obtenido de Informática Forense Colombia: https://www.informaticaforense.com.co/category/iforense/

Malagón, V. (15 de 05 de 2019). *Los delitos informáticos se triplican en un año en los juzgados de Baleares*. Obtenido de Ultimahora:

https://www.ultimahora.es/noticias/local/2019/05/15/1080005/delitos-informaticos-triplican-ano-juzgados-baleares.html

Mora Mendoza, V. H. (09 de 09 de 2013). *https://www.eluniversal.com.co*. Obtenido de https://www.eluniversal.com.co: https://www.eluniversal.com.co/tecnologia/asi-funciona-la-informatica-forense-en-colombia-134018-CQEU222347

Capítulo 9. Recursos

Recursos humanos:

Tabla 7. Recursos humanos

No.	Nombres y Apellidos	Profesión básica	Post - grado	Función básica dentro del proyecto	Dedicación hs/semana	Duración
1	Sergio Camilo ortega Ruiz	Tecnólogo en Desarrollo Informático		Consultar bibliografía, diseñar, crear y solucionar laboratorios de IF	2 horas	4 semanas
2	Stiven Paez Diaz	Tecnólogo en Desarrollo Informático		Consultar bibliografía, diseñar, crear y solucionar laboratorios de IF	2 horas	10 semanas

Fuente: Los Autores 2019

Recursos físicos:

Tabla 8. Recursos físicos

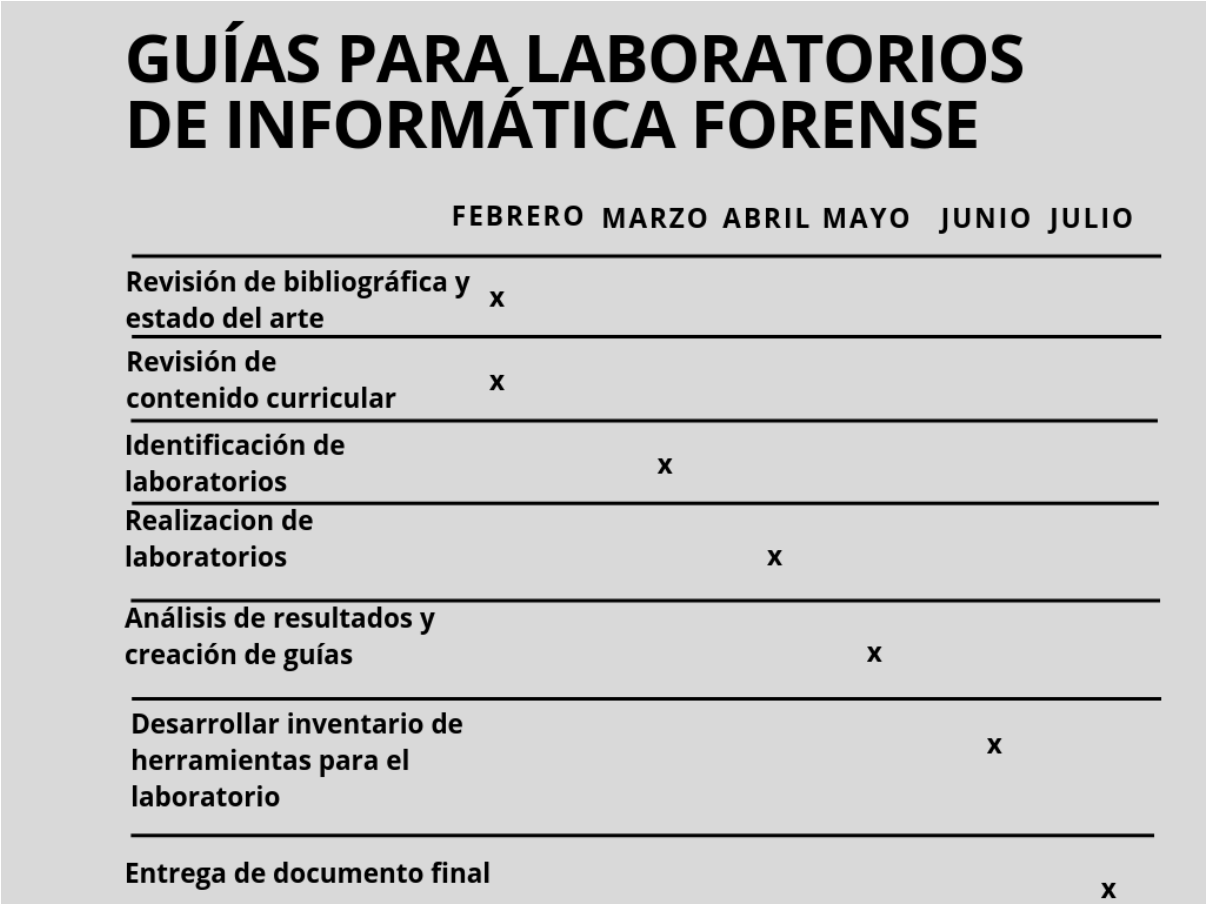
Descripción del equipo	Propósito fundamental del equipo en el proyecto	Actividades en las cuales se utiliza primordialmente	Costo miles de pesos	Total
HP Pavilion Desktop PC 570-p00	Montaje de laboratorios	Virtualización, escaneo, ataques entre otras	$ 1.500.0000	$ 1.500.0000
Portátil Toshiba Satélite c655	Recolección de información relacionado con la IF	Consultar, analizar y redactar información sobre IF	$ 900.000	$ 900.000

Fuente: Los Autores 2019

Capítulo 10. Cronograma

En este capítulo se va a representar el cronograma de actividades donde están plasmadas las actividades completas a realizar del documento:

Imagen 68. Cronograma



Fuente: Los Autores 2019

Conclusiones

De acuerdo con lo visto a lo largo del documento se puede concluir que la IF es un campo bastante amplio en la Ingeniería de Sistemas. Los temas propuestos se explicaron paso a paso, para que la persona que tenga la oportunidad de tomar como guía la documentación brindada, cuente con la facilidad de entender cada tema expuesto y con sus debidos ejemplos.

Esto brinda una bibliografía para los futuros estudiantes para la asignatura “IF”. Y no solo tendrán ejemplos y/o laboratorios, sino que también se cuenta con los marcos referenciales que permiten saber de qué se está hablando y por su puesto como no hablar del marco legal en Colombia que en esta área es uno de los más involucrados y que más impacto tiene en la asignatura, es un régimen que tienen los peritos para basarse y tomar acción en cada caso.

Con este documento se busca generar un impacto positivo entre el estudiantado, ya que en la actualidad los temas expuestos no tienen el grado de profundización que se requiere, por lo tanto, con estas bases el estudiante tendrá los instrumentos necesarios para continuar y ampliar su conocimiento.

Según nuestros objetivos planteados al inicio del documento, se puede decir que fueron cumplidos, ya que fueron objetivos alcanzables, y realizados en su totalidad en el tiempo establecido. Se evidencia que el análisis de los laboratorios propuestos se hizo, y por ende se continuo con la realización de los mismos, ya que se contaba con las herramientas necesarias para ello. En los resultados de que cada laboratorio nos arroja datos bastante sólidos y claros según los objetivos de cada uno de ellos.

Recomendaciones

Hay que tener unos conceptos claros para antes abordar la IF, tales como:

- Conocimientos básicos en redes, más especialmente en el área de monitoreo de redes, ya que, si no se tiene estos conceptos claros no podrá aprovechar herramientas para sniffer fundamentales en una investigación.
- Debe estar familiarizado con ambientes Linux, ya que cuenta con gran variedad de sistemas operativos con kits de herramientas muy completos para el análisis forense.
- En cada caso que sea tratado, se debe tener conceptos legales claros, ya que esta área de IF, está regida por parámetros legales tanto nacionales, como internacionales, estos estándares deben estar claros para el perito en cuestión.
- Contar con un buen equipo es fundamental, pues si se corren sistemas en modo live la cantidad de memoria RAM tiene que ser considerable, se recomienda mínimo 8gb.
- Tener las diferentes herramientas actualizadas es fundamental pues en el trascurso del laboratorio #1, tuvimos problemas con la distro Kali por actualizaciones.
- El NIST (Instituto Nacional de Estándares y Tecnología), tiene un repositorio muy completa de herramientas para IF.
- Tener claro las cabeceras de los diferentes archivos es fundamental, esto ahorrara trabaja para identificar un archivo.
- Un curso de IF nivel intermedio credo por RIT (Rochester Institute of Technology) alojado en la plataforma Edx.

Bibliografía

Castillo Saavedra, L. F., & Bohada Jaime, J. A. (10 de 12 de 2015). Informática Forense en Colombia. *Ciencia, Innovación y Tecnología, II*, 83-94. Recuperado el 17 de 03 de 2019, de https://www.jdc.edu.co/revistas/index.php/rciyt/article/view/113/102

Chavez, A., & Villota Jimenez, W. A. (2018). *Análisis forense y sus herramientas*. Cali: UNICATÓLICA Fundación Universitaria Católica Lumen Gentium.

Daccach T, J. C. (s.f.). *www.deltaasesores.com*. Recuperado el 31 de 07 de 2019, de www.deltaasesores.com: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Zeltser, L. (31 de 07 de 2017). *https://zeltser.com*. Recuperado el 01 de 08 de 2019, de https://zeltser.com: https://zeltser.com/memory-acquisition-with-dumpit-for-dfir-2/

ACCESDATA. (s.f.). *https://accessdata.com*. Recuperado el 01 de 08 de 2019, de https://accessdata.com: https://accessdata.com/products-services/forensic-toolkit-ftk

Adicra. (s.f.). *https://adicra.org.ar*. Recuperado el 24 de 02 de 2019, de https://adicra.org.ar: https://adicra.org.ar/informatica/

Alamillo, J. R. (08 de 10 de 2013). *https://peritoinformaticocolegiado.es*. Recuperado el 01 de 08 de 2019, de https://peritoinformaticocolegiado.es: https://peritoinformaticocolegiado.es/blog/peritaje-informatico/

Albors Pérez, L., Palacio Junquera, L., & García Reyes, M. (2010). *Iniciación a la informática. Formación en red*. (I. d. Educación, Ed.) Madrid, España: Ministerio de Educación. Recuperado el 17 de 03 de 2019, de

https://books.google.com.co/books?id=gaqtDAAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Bernal Michelena, D. E. (01 de 04 de 2013). Herramientas en seguridad. *Seguridad Cultura de prevención para TI, 17*, 08-11. Recuperado el 17 de 03 de 2019, de Wikipedia: https://revista.seguridad.unam.mx/sites/default/files/revistas/pdf/Seguridadnum17.pdf

Caballero Quezada, A. E. (20 de 05 de 2014). *http://www.reydes.com*. Recuperado el 03 de 10 de 2019, de http://www.reydes.com: http://www.reydes.com/d/?q=Extraer_Informacion_del_Registro_de_Windows_con_RegRipper

Caballero Quezada, A. E. (04 de 04 de 2018). *http://www.reydes.com*. Recuperado el 17 de 03 de 2019, de http://www.reydes.com: http://www.reydes.com/d/?q=Imagenes_Forenses

Clonezilla. (s.f.). *https://clonezilla.org*. Recuperado el 01 de 08 de 2019, de https://clonezilla.org: https://clonezilla.org

Conicet. (s.f.). *https://www.conicet.gov.ar*. Recuperado el 24 de 02 de 2019, de https://www.conicet.gov.ar: https://www.conicet.gov.ar/programas/ciencia-y-justicia/ciencia-forense/

Donohue, B. (10 de 04 de 2014). *https://latam.kaspersky.com*. Recuperado el 17 de 03 de 2019, de https://latam.kaspersky.com: https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

DragonJAR. (s.f.). *https://www.dragonjar.org*. Recuperado el 03 de 10 de 2019, de https://www.dragonjar.org: https://www.dragonjar.org/laboratorios-informatica-forense-introduccion-y-contenido.xhtml

Garitano, I., Iturbe, M., Arenaza Nuño, I., Uribeetxeberria, R., & Zurutuza, U. (2014). *Sistema de detección de anomalías para protocolos propietarios de control industrial*. Alicante: Universidad de Alicante.

GCFGLOBAl. (s.f.). *https://edu.gcfglobal.org*. Recuperado el 17 de 03 de 2019, de https://edu.gcfglobal.org: https://edu.gcfglobal.org/es/informatica-basica/que-es-un-sistema-operativo/1/

Guerrero Paiva , A. (2018). Informática forense y sus beneficios. *Revista de Información, Tecnología y Sociedad*.

Haydée Di Iorio, A., Mollo, M., Cistoldi, P., Lamperti, S., Fernanda Giaccaglia, M., Malaret, P., . . . Constanzo, B. (2016). Consideraciones para el diseño de un Laboratorio Judicial en Informática Forense. (U. FASTA, Ed.) *Universidad FASTA*, 1-6. Recuperado el 11 de 12 de 2018, de http://redi.ufasta.edu.ar:8080/xmlui/handle/123456789/1564

Informática Forense Colombia. (31 de 07 de 2019). *Informática Forense* . Obtenido de Informática Forense Colombia: https://www.informaticaforense.com.co/category/iforense/

Intef. (s.f.). *http://www.ite.educacion.es*. Recuperado el 03 de 10 de 2019, de http://www.ite.educacion.es: http://www.ite.educacion.es/formacion/materiales/13/cd/windows_xp/libro_wxp/Modulo4.pdf

Kali Linux. (s.f.). *https://www.kali.org*. Recuperado el 03 de 10 de 2019, de https://www.kali.org: https://www.kali.org/about-us/

Malagón, V. (15 de 05 de 2019). *Los delitos informáticos se triplican en un año en los juzgados de Baleares*. Obtenido de Ultimahora: https://www.ultimahora.es/noticias/local/2019/05/15/1080005/delitos-informaticos-triplican-ano-juzgados-baleares.html

Manual. Vigilantes de Seguridad. Área Técnico/Socio-Profesional e Instrumental Vol. II (Vol. II). (2016). Madrid, España: EDITORIAL CEP. Recuperado el 26 de 08 de 2019, de https://books.google.com.co/books?id=wqxCDwAAQBAJ&printsec=frontcover&dq=Manual.+Vigilantes+de+Seguridad.+%C3%81rea+T%C3%A9cnico/Socio-Profesional+e+Instrumental+Vol.+II&hl=es&sa=X&ved=0ahUKEwj6tYWqrJLnAhVRjlkKHfrZCnwQ6AEIKDAA#v=onepage&q=Manual.%20Vigila

Marqués Arpa, T., & Serra Ruiz, J. (08 de 09 de 2014). Cadena de custodia en el análisis forense. Implementación de un marco de gestión de la evidencia digital. (U. d. Alicante, Ed.) *Universidad de Alicante*, 1-6. Recuperado el 17 de 03 de 2019, de http://hdl.handle.net/10045/40423

Mendes, J. (s.f.). *https://techlandia.com*. Recuperado el 17 de 03 de 2019, de https://techlandia.com: https://techlandia.com/recuperacion-datos-sobre_510114/

Microsoft Azure. (s.f.). *https://azure.microsoft.com*. Recuperado el 17 de 03 de 2019, de https://azure.microsoft.com: https://azure.microsoft.com/es-es/overview/what-is-virtualization/

Mieres, J. (05 de 01 de 2009). Ataques informáticos Debilidades de seguridad comúnmente explotadas. *Academia*, 1-17. doi:8522766

Mora Mendoza, V. H. (09 de 09 de 2013). *https://www.eluniversal.com.co*. Obtenido de https://www.eluniversal.com.co: https://www.eluniversal.com.co/tecnologia/asi-funciona-la-informatica-forense-en-colombia-134018-CQEU222347

Organización de los Estados Americanos. (25 de 7 de 2019). *https://www.oas.org*. Obtenido de https://www.oas.org: https://www.oas.org/juridico/spanish/cyber/cyb40_imaging_sp.pdf

Policia Nacional de Colombia. (s.f.). *https://www.policia.gov.co*. Recuperado el 17 de 03 de 2019, de https://www.policia.gov.co: https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Policia Nacional de Colombia. (s.f.). *https://www.policia.gov.co*. Recuperado el 10 de 09 de 2019, de https://www.policia.gov.co: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Revista, P. (Febrero de 2017). *www.portafolio.co*. Obtenido de Portafolio: http://www.portafolio.co/innovacion/emprendimiento-colombiano-cifras-155078

Rifà Pous, H., Serra Ruiz, J., & Rivas López, J. (2009). *Análisis forensede sistemasinformáticos*. Barcelona: EURECA MEDIA S.L.

Rivas López, J. L. (2009). *Análisis forensede sistemas informáticos* (Primera ed.). (FUOC, Ed.) Barcelona, España: EURECA MEDIA S.L. Obtenido de http://jlrivas.webs.uvigo.es/downloads/publicaciones/Analisis%20forense%20de%20sistemas%20informaticos.pdf

Rodríguez Más, F., & Doménech Rosado, A. (25 de 08 de 2011). LA INFORMÁTICA FORENSE: EL RASTRO DIGITAL DEL CRIMEN. *Dialnet*, *Universidad de la Rioja*, 1-9. doi:5497990

Sleuth Kit. (s.f.). *https://www.sleuthkit.org/*. Recuperado el 03 de 10 de 2019, de https://www.sleuthkit.org/: https://www.sleuthkit.org/autopsy/

Turriago Díaz, M. (Abril de 2017). *conocimientosenseguros.blogspot.com.co*. Obtenido de Legislación de seguros en colombia: http://conocimientosenseguros.blogspot.com.co/p/pag5.html

Vietes, Á. G. (2014). *Enciclopedia de la Seguridad Informática. 2ª edición* (Segunda ed.). (S. RA-MA, Ed.) Madrid, España: RA-MA, S.A. Recuperado el 17 de 03 de 2019, de https://books.google.com.co/books?id=Bq8-DwAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Wireshark. (s.f.). *https://www.wireshark.org*. Recuperado el 03 de 10 de 2019, de https://www.wireshark.org: https://www.wireshark.org