Universidad de las Ciencias Informáticas

Facultad 2

Trabajo de Diploma para Optar por el Título de Ingeniero en Ciencias Informáticas.

Título: Metodología para el análisis forense de los principales incidentes de seguridad Informática en la UCI.

Autores:

Miruleidis Gómez Pérez.

Daniela Borges Crosa.

Tutores:

Jesse Daniel Cano Otero.

Alexander Fernández Castro.

Ciudad de La Habana, junio del 2011

"Año 50 de la Revolución"

Declaración de Autoría

Declaramos que somos las únicas autoras de este trabajo y autorizamos a la Universidad de las Ciencias Informáticas a hacer uso del mismo en su beneficio.

Para que así conste firmamos la presente a los ____ días del mes de _____ del año _____.

_____ _____

Autor: Miruleidis Gómez Pérez. **Autor: Daniela Borges Crosa.**

_____ _____

Tutor: Ing. Jesse Daniel Cano Otero. **Tutor: Ing. Alexander Fernández Castro.**

“…el futuro de nuestra Patria, tiene que ser necesariamente, un futuro de hombres de ciencias…”

Fidel Castro

Datos de Contacto

Lic. Alexander Fernández Castro

Profesor licenciado en Ciencia de la Computación, Ministerio de Educación Superior en la Universidad de Oriente. Categoría Docente Principal de Instructor, Ministerio de Educación Superior, Universidad de las Ciencias Informáticas. Actualmente labora como especialista en la Dirección de Redes y Seguridad Informática de la Universidad de Ciencias Informáticas.

Empresa: UCI Dirección: Carretera a San Antonio Km. 2 1/2 Reparto Torrens, Ciudad Habana

e-mail: alexanderfc@uci.cu.

Ing. Omar Pimentel Alonso

Instructor recién graduado de Ingeniería en Ciencias Informática en el año 2009. Actualmente labora como especialista en redes y seguridad informática.

Empresa: UCI Dirección: Carretera a San Antonio Km. 2 1/2 Reparto Torrens, Ciudad Habana

e-mail: opimentel@uci.cu.

Ing. Jesse Daniel Cano Otero

Profesor graduado de Ingeniería en Ciencias Informática en el año 2009. Actualmente labora como profesor de Ingeniería de Software y radica en el departamento central de ingeniería de software.

Empresa: UCI Dirección: Carretera a San Antonio Km. 2 1/2 Reparto Torrens, Ciudad Habana

e-mail: jdcano@uci.cu.

Dedicatoria

De Miru:

A Dios, por darme la oportunidad de formarme en esta universidad y ver hoy mí sueño hecho realidad.

A mami y a papi por darme la vida y ser más que mis padres, mis confidentes y amigos eternos.

A mi tía Mirulgia Andujar Pérez que a pesar de no estar presente en cuerpo pero si su alma, sé que donde esté he sido un orgullo para ella....te quiero mucho.

A mis hermanos ya que he sido el mechero de sus sueños.

A mi abuela Miriam, mi tía Maura, mi primito Frank.…gracias por estar para mí.

A mi familia en general por todo lo que han sido para mí en el trayecto de mi vida.

A todos mis amigos especialmente a Yudenia, Frank, Edel, Elier, Nadiezka, Leidis que me han apoyado y ofrecido una palabra de aliento cuando la he necesitado…gracias.

A todos los profes que han contribuido con mí formación.

De Daniela:

Este trabajo de diploma está dedicado a mis padres por ser los motores impulsores en mi formación. Especialmente dedicado al bebé que estoy esperando y a mi novio. En general se lo dedico a mi familia completa que tanto apoyo y fuerzas me han dado a lo largo de mi vida, que cuando se creía que todo estaba perdido siempre existieron palabras de fe y esperanza.

Agradecimientos

De Miru:

A las personas más importantes de mi vida:

Mami y Papi. Sin los cuales no estaría donde estoy ni sería hoy quien soy.
A Modesto (mi cosita) por su confianza, apoyo y amor incondicional…gracias
A Yudenia, Frank, Edel y Elier mis hermanos…gracias
Al tribunal de esta Tesis por señalarme con paciencia mis errores...gracias
A mi tutor Jesse Daniel cano Otero por su apoyo y ayuda en el desarrollo de la investigación.
A mis Co-tutores Alexander Fernández Castro y Omar Pimentel Alonso porque sin ellos no hubiera podido terminar el desarrollo de esta investigación…gracias

A todas las personas que me han ayudado o han ayudado a las personas que quiero, directa o indirectamente.

De Daniela:

Agradecerle a mi tutor y mis coo-tutores que sin su apoyo y experiencia no hubiera sido posible el desarrollo de este trabajo. A mis padres por su apoyo incondicional, a mi familia por creer en mí. Especialmente a mi novio Yoel, que tanto me ayudó y

me dio las fuerzas necesarias para seguir adelante en esta labor. A todas mis amistades de los años que he estudiado en esta universidad que aunque algunas se han quedado en el camino, otros han demostrado su valor y han perdurado todos estos años, gracias a todos por estar presentes en mi vida enriqueciéndola cada día más.

Resumen

Actualmente en el mundo las tecnologías han mostrado un gran avance, el alto crecimiento en el desarrollo de software y la competencia hace que cada día se impongan productos con mayor calidad. Teniendo esto en cuenta, en la Universidad de Ciencias Informáticas (UCI) se vincula el estudio y la producción a través de la participación de los estudiantes en proyectos productivos reales, dentro de sus principales objetivos están: impulsar la informatización de la sociedad e ir al frente en el desarrollo de software. Entre sus disímiles actividades se encuentra la atención a los incidentes informáticos de seguridad, mediante la dirección de redes y seguridad informática de la universidad.

El seguimiento y la solución a estos problemas se realiza basándose en la experiencia adquirida por cada profesional inmiscuido en este aspecto, es decir que cada cual le da la solución al problema en dependencia de la previa investigación que haya desarrollado, con la base de casos anteriores y con la utilización de muchos procedimientos y herramientas ya existentes. El objetivo del presente trabajo de diploma es la elaboración de una metodología para el análisis forense a los principales incidentes de seguridad informática presentes en la UCI, que favorezca este proceso llevado a cabo por los especialistas de la universidad.

El uso de esta metodología facilitará considerablemente el trabajo de los especialistas de seguridad informática dedicados a este tipo de labor que es el análisis forense, ya que servirá de guía para la realización de este trabajo. En ella podrán encontrar los principales tipos de delitos informáticos que ocurren en la Universidad de Ciencias Informáticas, los pasos a seguir para su solución así como las herramientas a utilizar para dicho procedimiento.

Palabras claves: Incidentes informáticos, seguridad, metodología, análisis forense.

Índice:

INTRODUCCIÓN

Años atrás, las computadoras eran máquinas colosales que sólo eran utilizadas por corporaciones multinacionales y agencias gubernamentales en países poderosos. Estos artefactos eran tan grandes y tan complejos, que inclusive requerían sus propios ambientes con temperatura controlada, para que funcionaran apropiadamente. Desde ese tiempo, se puede decir que han sufrido una enorme metamorfosis, hasta convertirse en equipos domésticos comunes, tan usuales que en la mayoría de las ocasiones llegan a formar parte de la vida cotidiana de la persona; como un teléfono o un televisor.(1)

Con el creciente desarrollo computacional y con este el surgimiento y perfeccionamiento de las redes se ha logrado la combinación de los conocimientos y habilidades en la obtención de herramientas y técnicas para alcanzar resultados exitosos en el cumplimiento de un objetivo. Un ejemplo de una rama de gran relevancia y que combina múltiples procedimientos para lograr objetivos que a veces parecen inalcanzables, es la Ciencia Forense la cual es la aplicación de prácticas científicas dentro del proceso legal, es decir es un conjunto de ciencias que la ley usa para atrapar a un criminal, ya sea física, química, matemática. (2)

En la actualidad con el progresivo avance de las tecnologías, el mundo de la informática con el de la ciencia forense de cierta forma ha tenido su fusión ya que como la mayoría de las personas usan las computadoras para comunicarse, aprender, trabajar e inclusive para entretenimiento. Estos dispositivos, en la mayoría de los casos, contienen información muy importante que puede ser usada como prueba o evidencia en procesos legales, tanto en materia penal como en civil, incluso en el caso en que la evidencia no sea directamente relacionada con estas. Es aquí donde aparece un área nueva de la ciencia forense, como es la Informática Forense.

La informática forense combina técnicas especializadas con el uso de software sofisticado para ver y analizar información a la que no puede acceder el usuario ordinario. Esta información pudo haber sido "borrada" por el usuario meses o años antes de la investigación o inclusive pudo no haber sido guardada, pero puede aún estar presente del todo o parte de ella, en el disco duro de la computadora. (3)

Con el fin de dar seguimiento a los delitos informáticos que ocurren a diario existen múltiples instituciones en todo el mundo que se dedican a dar solución a estos incidentes, Que pueden ir desde robo de la propiedad intelectual hasta lavado de dinero, fraude, destrucción de información confidencial, acoso sexual y amenazas vía e-mail, corrupción, pornografía en todas sus formas incluyendo la más catastrófica, la pornografía infantil.

Como ejemplo de estas empresas se pueden mencionar Chase The Sun la cual es una compañía creada por un grupo de profesionales expertos en tecnologías de la información, los cuales son pioneros en la introducción del Análisis Forense Informático en España, tienen un record del 100% de juicios ganados con su apoyo como peritos.(4) Tecnolinks, S.A, empresa del área de tecnología de información dedicada a prestar servicios de Informática Forense, recuperación de datos en dispositivos de almacenamiento, seguridad Informática, respaldo de Información y eliminación de virus informáticos.(5) KPMG Forensic es una de las cuatro mayores firmas de servicios profesionales a nivel internacional, la cual combina conocimientos tecnológicos especializados con una amplia experiencia en análisis independientes, pruebas periciales e investigaciones de fraudes.(6)

Deloitte Forensic Spain es una empresa dedicada al análisis forense, la cual ofrece servicios de prevención, investigación, así como soluciones informáticas y análisis de datos para la detección del fraude, además cuenta con un grupo de profesionales que poseen una amplia experiencia en tribunales y, en general, en todo tipo de situaciones de conflicto, apoyados por investigadores informáticos y otros especialistas. (7)

Cuba no se queda rezagada en el desarrollo computacional y con este el de las redes y la seguridad informática, existe una institución para la atención, seguimiento y control de las redes informáticas. La entidad encargada de atender este aspecto en Cuba es La Oficina de Seguridad para las Redes Informáticas (OSRI), la cual es la encargada de llevar a cabo la prevención, evaluación, aviso, investigación y respuesta a las acciones, tanto internas como externas, que afecten el normal funcionamiento de las tecnologías de la información en el país, trabaja para fortalecer la seguridad durante el empleo de las Tecnologías de la Información. Su propósito consiste en implementar un sistema que contribuya al ordenamiento de las actividades asociadas con las redes informáticas y de comunicaciones, mediante el establecimiento de un esquema que garantice niveles aceptables de seguridad.

Dentro de La Oficina de Seguridad para las Redes Informáticas (OSRI) se encuentra el Equipo de Respuesta a Incidentes Computacionales de Cuba (CuCERT), el cual tiene la misión de prevenir y responder a los incidentes computacionales en Cuba. Esta organización tiene en su membrecía a profesionales en Seguridad Informática, y cuenta con colaboradores pertenecientes a otras entidades del país. Su misión es la detección y respuesta a incidentes computacionales que se presenten en el país, informar sobre vulnerabilidades y amenazas de seguridad informática, educar a la comunidad en general, sobre temas de seguridad informática, elaborar estadísticas e informes, gestionar las reclamaciones internacionales.(8)

Por idea del Comandante en Jefe Fidel Castro Ruz y como parte de la batalla de ideas surge el proyecto educativo informático de la Universidad de las Ciencias Informáticas (UCI). En la misma se vincula el estudio y la producción a través de la participación de los estudiantes en proyectos productivos reales, dentro de sus principales objetivos están: impulsar la informatización de la sociedad e ir al frente en el desarrollo de software. Entre sus disímiles actividades se encuentra la atención a los incidentes de seguridad, mediante la Dirección de Redes y Seguridad Informática de la universidad contando con profesionales en el ámbito de la seguridad informática.

Formando parte de la Dirección de Redes y Seguridad Informática de la UCI, se encuentra el Equipo de Respuesta a Incidentes Informáticos (CERT), contando con una herramienta que convierte a este equipo de trabajo en un auténtico CERT. Esta herramienta es conocida como OTRS (Open-source Ticket Request System), la cual es un sistema que se ha destacado por su robustez y estabilidad, está diseñado de forma general para servir a muchos tipos de procesos empresariales y se brinda su instalación de forma gratuita. En la UCI está funcionando actualmente una variante de este sistema OTRS, con la autenticación, tipos de usuarios, tipos de incidentes, colas y roles definidos formalmente según las características del entorno. Gracias a esto el trabajo de los especialistas se ha humanizado en gran medida, al punto que se ha convertido oficialmente en la herramienta de trabajo de la Dirección de Redes y Seguridad Informática, con la cual se manejan más de 20 tipos de incidentes, no solo de seguridad sino también de servicios, y la asignación de tareas ahora es también automatizada, en general ha sido un gran impulso en la gestión centralizada del trabajo diario de los profesionales.

A pesar de contar con una herramienta que a gran escala es verdaderamente imprescindible, existen algunos tipos de delitos informáticos que necesitan un estudio más profundo como es el caso de los

incidentes que requieren análisis forense, por lo que surge la siguiente **situación problémica**: En la Universidad de las Ciencias Informáticas (UCI) ocurren regularmente incidentes de Seguridad Informática que requieren análisis forense. El seguimiento y solución a estos problemas se realiza basándose en la experiencia adquirida por cada profesional inmiscuido en este aspecto, los cuáles dedican muchas horas de esfuerzo y trabajo para solucionarlos. Los profesionales se apoyan en la previa investigación realizada, con la base de casos anteriores y con la utilización de muchos procedimientos y herramientas ya existentes. Pero no existe una filosofía estandarizada que unifique el proceso de análisis forense en los casos reportados.

A raíz de la situación actual y las insuficiencias existentes, conllevan a que los esfuerzos estén encaminados al siguiente **problema a resolver**: ¿Cómo unificar las herramientas y procedimientos a seguir para darle tratamiento a los distintos tipos de incidentes de seguridad informática que requieren análisis forense presentes en la UCI? enmarcando como **objeto de estudio:** los procedimientos, herramientas y métodos que se utilizan para el tratamiento a los incidentes informáticos de seguridad que necesiten análisis forense, donde su **campo de acción** se enfoca, en las herramientas y métodos a seguir para el análisis forense a los principales incidentes de seguridad informática presentes en la UCI, que precisen análisis forense. El **objetivo general** del presente trabajo es: diseñar una metodología para la investigación forense de los principales incidentes de Seguridad Informática en la UCI.

Para dar cumplimiento al objetivo general se proponen las siguientes **tareas de la investigación:**

- Identificar y definir los principales conceptos asociados al dominio del problema.
- Valorar las tendencias actuales de las metodologías existentes a nivel mundial que tributen a la solución del problema planteado.
- Analizar los tipos de incidentes informáticos que se manejan en la actualidad que requieran análisis forense.
- Realizar un análisis de las herramientas y métodos que utilizan los especialistas en la UCI y en Cuba.
- Establecer criterios comparativos entre la UCI y Cuba en cuanto a la solución de los delitos informáticos que requieren análisis forense, que a su vez tributen a la posterior elaboración de la metodología a proponer.
- Elaborar un estándar para la metodología a proponer.

Métodos de Investigación

- **Métodos Teórico**
- 1.1. Lógico.
- 1.1.1. Modelación: Para crear una metodología que explique el resultado final de la investigación.
- 1.2. Histórico: Para el estudio de los antecedentes que existen respecto a la informática forense.
- **Métodos Empíricos**
- 2.1. Revisión de documentos para apoyar el estudio de las herramientas y metodologías utilizadas actualmente para el tratamiento a los delitos informáticos que requieran análisis forense, tanto en el ámbito internacional como nacional.

El presente documento está estructurado en tres capítulos como se presenta a continuación, estos contienen todo lo relacionado con el trabajo investigativo realizado.

- **Capítulo 1. Fundamentación Teórica:** En este capítulo se realiza un estudio del estado del arte a nivel nacional e internacional. Se establece un marco conceptual en correspondencia con la información que será manipulada. Se describen los conceptos fundamentales, asociados al dominio del problema, así como las tendencias de las tecnologías actuales a tener en cuenta.
- **Capítulo 2. Diagnóstico Actual:** En este capítulo se fundamenta la metodología a proponer, es decir, por qué es necesaria la existencia de una guía para el análisis forense.
- **Capítulo 3. Propuesta de Metodología:** En este capítulo se propone la metodología, basada en la investigación realizada.

CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA

En este capítulo se exhiben los resultados del proceso investigativo llevado a cabo para la elaboración del presente trabajo de diploma. Se muestran los conceptos fundamentales asociados al dominio del problema. Se expone el estado del arte de la investigación, es decir, las metodologías, herramientas o procedimientos empleados actualmente tanto en el ámbito internacional como nacional para los incidentes informáticos que requieran análisis forense, con el fin de sentar las bases para la posterior propuesta de una metodología que guie este análisis.

1.1 Conceptos fundamentales

La informática forense está en una etapa de desarrollo continuo y grandes cambios, todo esto con el fin de lograr que esta área se haga cada vez más fuerte y eficiente para el logro de sus objetivos, es decir para el claro y eficaz análisis a todos los incidentes de seguridad informática que requieran este tipo de estudio. Para ello es necesario conocer conceptos y definiciones que permitan su entendimiento y profundización:

Informática Forense

La **informática forense**, también llamada cómputo forense, computación forense, análisis forense digital o exanimación forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Estas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

La informática forense no solo requiere de tecnología de punta para poder mantener la integridad de los datos y el procesamiento de estos, sino también necesita de una especialización y conocimientos avanzados en materia de informática y sistemas, para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido.(9)

Evidencia digital

La **evidencia digital** es la información almacenada digitalmente que puede llegar a ser presentada como prueba en un proceso judicial, es decir, es sumamente frágil por lo que con solo darle doble clic a un

archivo se modifica hasta la última fecha de acceso del mismo. La importancia de estos datos y el poder mantener su integridad se basa en este tipo de evidencia. (10)

Herramientas informáticas

Las **herramientas informáticas** son dispositivos o procedimientos que aumentan la capacidad de llevar a cabo determinadas tareas. De las mismas existen dos tipos. (11)

Las **herramientas de hardware** son herramientas físicas como un destornillador o martillo, que no necesitan mucho entrenamiento o conocimiento técnico para usarla, su uso se basa principalmente en la experiencia práctica, primordialmente se necesita fuerza motriz para usarla, y se desgasta con el uso.(12)

Las **herramientas de software** son herramientas lógicas o intangibles, que permiten depurar o diseñar nuevo software y se necesita cierto entrenamiento para poder usarla ya que generalmente se utiliza para tareas complicadas. No se daña con el uso, y se puede mejorar sin necesidad de adquirir otra. Este último tipo de herramienta es la que se utiliza generalmente para el cómputo forense, por lo cual son de gran utilidad para la recuperación de evidencias y por lo que se hace necesario que sean cada vez más sofisticadas debido a la gran cantidad de datos que pueden estar almacenados en un computador.(13)

Metodologías

Las **metodologías** son un conjunto de métodos por los que se regirá una investigación científica. Es el procedimiento que se llevará a cabo en orden a la consecución de determinados objetivos. La metodología estudia los métodos para luego determinar cuál es el más adecuado a aplicar o sistematizar en una investigación o trabajo. (14)

1.2 Dispositivos a analizar en el análisis forense

Se debe analizar todo aquello que tenga una memoria (informática), por la razón de que estos dispositivos pueden contener o de ellos se puede recuperar información que en muchos casos sirve de evidencia para un proceso legal de la índole de la informática forense. Por ejemplo los siguientes dispositivos:

- Teléfono Móvil o Celular, parte de la telefonía celular.
- Agendas Electrónicas (PDA).
- Dispositivos de GPS.
- Impresoras.
- Memorias USB. Teléfono Móvil o Celular, parte de la telefonía celular.

1.3 Pasos a seguir para la informática Forense

La informática forense está estructurada en varios pasos que se deben seguir a la hora de realizar el análisis forense a una computadora, a continuación se muestran estos pasos:

- **Preservación**

En este paso se incluye la revisión y duplicación de las imágenes forenses de la evidencia, para poder realizar el análisis. Esta duplicación se realiza utilizando tecnología avanzada para poder mantener la integridad de la evidencia y la cadena de custodia que se requiere. Dicha **cadena de custodia** es el proceso ilimitado y documentado que permite demostrar la autenticidad de la evidencia física.

Realizar una imagen forense, es el proceso requerido para generar una copia bit-a-bit de todo el disco, la cual permitirá recuperar en el posterior paso, toda la información contenida en el disco duro, de igual forma si es borrada será recuperada.

- **Análisis**

Es el proceso de aplicar técnicas científicas y analíticas a las imágenes obtenidas en el paso anterior para poder encontrar pruebas de ciertas conductas. Se pueden realizar búsquedas de cadenas de caracteres, acciones específicas del o de los usuarios de la máquina, como son el uso de dispositivos de USB (marca, modelo), búsqueda de archivos específicos, recuperación e identificación de correos electrónicos, recuperación de los últimos sitios visitados, recuperación del caché del navegador de Internet, entre otros.

- **Presentación**

Es el proceso de recopilación de toda la información que se obtuvo a partir del análisis para realizar el reporte y la presentación a los abogados. (15)

1.4 Principales delitos informáticos a nivel mundial.

- Fraudes cometidos mediante manipulación de ordenadores.
- Manipulación de programas.
- Manipulación de datos de salida.
- Fraude efectuado por manipulación informática o por medio de dispositivos informáticos.
- Falsificaciones informáticas.
- Sabotaje informático.
- Virus, gusanos y bombas lógicas.
- Acceso no autorizado a Sistemas o Servicios de Información.
- Reproducción no autorizada de programas informáticos de protección legal.
- Producción / Distribución de pornografía infantil usando medios telemáticos.
- Amenazas mediante correo electrónico.
- Juego fraudulento on-line.

1.5 Antecedentes

La Informática forense es una ciencia relativamente nueva y no existen estándares aceptados. Hace su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garantizar la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso. Tiene un papel, en primer lugar, como sistema preventivo. Sirve para auditar, mediante la práctica de diversas técnicas para probar que los sistemas de seguridad instalados cumplen con ciertas condiciones básicas de seguridad.

1.5.1 Hechos que dieron inicio a la informática forense

- En 1978 Florida reconoce los crímenes de sistemas informáticos en el Computer Crimes Act, en casos de sabotaje, copyright, modificación de datos y ataques similares.

- En 1981 nace Copy II PC de Central Point Software. También es conocida como copy2pc, se usa para la copia exacta de disquetes, que generalmente están protegidos para evitar copias piratas. El producto será posteriormente integrado en las PC Tools. La compañía es un éxito y es comprada por Symantec en 1994.
- En 1982 Peter Norton publica UnErase: Norton Utilities 1.0, la primera versión del conjunto de herramientas Norton Utilities, entre las que se destaca UnErase, una aplicación que permite recuperar archivos borrados accidentalmente. Otras aplicaciones también serán útiles desde la perspectiva forense, como FileFix o TimeMark. Con el éxito de varias de aplicaciones, Peter publica varios libros técnicos, como Inside the I. B. M. Personal Computer, Access to Advanced Features and Programming, de este último se publica su octava edición en 1999, 11 años después de la primera edición. La compañía será vendida a Symantec en 1990.
- En 1984 el FBI forma el Magnetic Media Program, que más tarde, en 1991, será el Computer Analysis and Response Team (CART).
- En 1986 Clifford Stoll colabora en la detección del hacker Markus Hess. En 1988 se publica el documento Stalking the Wily Hacker contando lo ocurrido. Este documento es transformado 1989 en el libro El huevo del cuco, anticipando una metodología forense.
- En 1987 se crea la High Tech Crime Investigation Association (HTCIA), asociación de Santa Clara que agrupa a profesionales tanto de agencias gubernamentales, como compañías privadas para centralizar conocimiento e impartir cursos. John C. Smith detalla la historia de esta organización aún vigente en su página web.
- En 1987 nace la compañía Access Data, pionera en el desarrollo de productos orientados a la recuperación de contraseñas y el análisis forense con herramientas, como la actual Forensic Toolkit (FTK).
- En 1988 se crea la Asociación Internacional de Especialistas en Investigación Informática (International Association of Computer Investigative Specialists), que certificará a profesionales de agencias gubernamentales en el Certified Forensic Computer Examiner (CFCE), una de las certificaciones más prestigiosas en el ámbito forense.
- En este mismo año se desarrolla el programa Seized Computer Evidence Recovery Specialists o SCERS, con el objetivo de formar a profesionales en informática forense.

- El libro A Forensic Methodology for Countering Computer Crime, de P. A. Collier y B. J. Spaul acuña en 1992 el término informática forense. Otros libros posteriores continuarán desarrollando el término y la metodología, como: High-Technology Crime e Investigating Cases Involving Computers de Kenneth S. Rosenblatt.
- En 1995 se funda el International Organization on Computer Evidence (IOCE), con objetivo de ser punto de encuentro entre especialistas en la evidencia electrónica y el intercambio de información.
- A partir de 1996 la Interpol organiza el simposio internacional de ciencia forense, como foro para debatir los avances forenses, uniendo fuerzas y conocimientos.
- En agosto de 2001 nace la Digital Forensic Research Workshop (DFRWS), un nuevo grupo de debate y discusión internacional para compartir información.(16)

1.6 Estado del Arte

La informática forense es un arma fundamental en la obtención de pruebas sólidas para darle respuesta a los incidentes informáticos que cada vez son más frecuentes en el mundo actual, para ello existen una gran variedad de herramientas con la finalidad de ayudar y hacer más eficiente el trabajo diario.

Entre estas herramientas se pueden encontrar algunas que son las más fiables, eficientes y libres a la hora de obtener información digital.

KeyLogger:

Es una herramienta que puede ser útil cuando se quiere comprobar actividad sospechosa, guarda los eventos generados por el teclado, por ejemplo, cuando el usuario teclea la tecla de retroceder, esto es guardado en un archivo o enviado por e-mail. Los datos generados son complementados con información relacionada con el programa que tiene el foco de atención, con anotaciones sobre las horas, y con los mensajes que generan algunas aplicaciones.

Existen dos versiones: la registrada y la de demostración. La principal diferencia es que en la versión registrada se permite correr el programa en modo escondido. Esto significa que el usuario de la máquina no notará que sus acciones están siendo registradas. (17)

EnCase:

ENCASE es un ejemplo de herramienta para la recolección de evidencia digital. Desarrollada por Guidance Software Inc. Permite asistir al especialista forense durante el análisis de un crimen digital. Es un software propietario. Algunas de las características más importantes son:

- Copiado comprimido de discos fuente:

Emplea un estándar sin pérdida (loss-less) para crear copias comprimidas de los discos origen. Los archivos comprimidos resultantes, pueden ser analizados, buscados y verificados, de manera semejante a los normales (originales). Esta característica ahorra cantidades importantes de espacio en el disco del computador del laboratorio forense, permitiendo trabajar en una gran diversidad de casos al mismo tiempo, examinando la evidencia y buscando en paralelo.

- Búsqueda y análisis de múltiples partes de archivos adquiridos:

Permite al examinador buscar y analizar múltiples partes de la evidencia. Muchos investigadores involucran una gran cantidad de discos duros, discos extraíbles, discos zip y otros tipos de dispositivos de almacenamiento de la información. Con Encase, el examinador puede buscar todos los datos involucrados en un caso en un solo paso. La evidencia se clasifica, si esta comprimida o no, y puede ser colocada en un disco duro y ser examinada en paralelo por el especialista.

- Diferente capacidad de almacenamiento:

Los datos pueden ser colocados en diferentes unidades, como Discos duros IDE o SCSI, drives ZIP, y Jazz. Los archivos pertenecientes a la evidencia pueden ser comprimidos o guardados en CD-ROM manteniendo su integridad forense intacta, estos archivos pueden ser utilizados directamente desde el CD-ROM evitando costos, recursos y tiempo de los especialistas.

- Varios campos de ordenamiento, incluyendo estampillas de tiempo:

Permite al especialista ordenar los archivos de la evidencia de acuerdo a diferentes campos, incluyendo campos como las tres estampillas de tiempo (cuando se creó, último acceso, última escritura), nombres de los archivos, firma de los archivos y extensiones.

- Análisis compuesto del documento:

Permite la recuperación de archivos internos y meta-datos con la opción de montar directorios como un sistema virtual para la visualización de la estructura de estos directorios y sus archivos, incluyendo el slack interno es decir la parte interna débil y los datos del espacio sin asignar.(18)

Forensic Toolkit:

Es un conjunto de herramientas para el análisis de las propiedades de ficheros, examina los ficheros de un disco en busca de actividad no autorizada y los lista por su última fecha de acceso, permitiendo realizar búsquedas en franjas horarias, búsqueda de archivos eliminados, entre otros. (19)

md5deep:

Es un conjunto de programas que permiten calcular resúmenes MD5, SHA-1, SHA-256, Tiger Whirlpool, de un número arbitrario de ficheros. Funciona sobre Windows. Linux, Cygwin, BSD, OS X, Solaris, entre otros. Similar en funcionalidad al programa md5sum se diferencia en las siguientes características:

- Recursividad.
- Estimación del tiempo de duración del proceso.
- Modo comparativo.
- Permite trabajar sobre un tipo de fichero determinado.(20)

Gpart:

Es un programa que permite recuperar la tabla de particiones de un disco cuyo sector 0 este dañado, sea incorrecto o haya sido eliminado, puede escribir el resultado obtenido a un fichero o dispositivo. (21)

TestDisk:

Es un programa que permite chequear y recuperar una partición eliminada. Soporta BeFS (BeOS), BSD disklabel (FreeBSD/OpenBSD/NetBSD), CramFS (Sistema de Ficheros Comprimido), DOS/Windows, Linux Swap (versiones 1 y 2), FAT12, FAT16, FAT32, HFS, JFS, Ext2, Ext3, Linux, RaidLVM, LVM2, Netware NSS, NTFS (Windows NT/2K/XP/2003), ReiserFS 3.5, ReiserFS 3.6, UFS, XFS y SGIs Journaled File System.(22)

Fccu.evtreader:

Es una herramienta para el análisis forense, que permite al investigador analizar ficheros de log de

eventos de Windows. Se trata de un script de perl que puede funcionar bajo Linux, y que debe funcionar en otros sistemas. (23)

GrokEVT:

Es un conjunto de scripts en python que permiten analizar ficheros de registros de eventos de Windows NT. También permite extraer cualquier otro tipo de log y convertirlo en un formato legible. (24)

Event Log Parser:

Es un script php que, pasándole un fichero de log de Windows, permite extraer su contenido en un fichero de texto ASCII. (25)

Srprint:

Es una herramienta que permite volcar el contenido de los ficheros de log de utilidad de restauración del sistema de Windows XP. Estos tipos de logs permiten averiguar la fecha de creación y borrado de ficheros que ya no estén presentes en el sistema. (26)

Galleta:

Una herramienta para el análisis forense de los cookies del Internet Explorer. Convierte la información de un fichero de cookie obteniendo como resultado campos separados por tabuladores que pueden importarse fácilmente a una hoja de cálculo. 27)

Pasco:

Permite analizar los ficheros de registro de la actividad del internet explorer. Convierte la información de un fichero index.dat, obteniendo como resultado campos separados por tabuladores que pueden importarse fácilmente a una hoja de cálculo. (28)

Web Historian:

Es un asistente para la recuperación de las URL de los sitios almacenados en los ficheros históricos de los navegadores más habituales, incluyendo: MS Internet Explorer, Mozilla Firefox, Netscape, Opera y Safari. (29)

Rifiuti:

Es una herramienta para el análisis forense de la información almacenada en la papelera de reciclaje de

un sistema Windows. Convierte la información de un fichero INFO2, obteniendo como resultado campos separados por tabuladores que pueden importarse fácilmente a una hoja de cálculo. (30)

Allimage:

Esta herramienta para Windows permite crear imágenes bit a bit de cualquier tipo de dispositivo de almacenamiento de datos (diskettes, cdroms, unidades usb, discos duros). Incluye un gestor para montaje de particiones de forma que puede resultar muy útil para asignar una letra de unidad a un fichero de imagen de un sistema Windows, de forma que pueda realizarse un análisis post-mortem. (31)

ProDiscover Basic Edition:

Es un entorno gráfico para el análisis forense de sistemas bajo entorno Windows. Permite realizar imágenes, preservar, analizar y realizar informes de los elementos contenidos en el dispositivo sujeto del análisis. Esta versión es completamente gratuita. (32)

PyFlag:

Es una avanzada herramienta para el análisis forense de grandes volúmenes o imágenes de log. Desarrollada en python posee un interfaz accesible mediante un navegador web. Entre sus características se encuentra: la integración rápida, facilitando de esta forma el análisis de ficheros de imagen de la memoria física de un sistema Windows. (33)

Volatility Framework:

Es un framework completo desarrollado en Python que permite el análisis de un volcado de la memoria física de un sistema Windows. Además de ser multiplataforma ofrece las siguientes funcionalidades:

- Obtener fecha y hora del contenido de la imagen.
- Listado de los procesos en ejecución.
- Interruptores (sockets) de red abiertos.
- Conexiones de red abiertas.
- DLL cargadas por cada proceso.
- Ficheros abiertos por cada proceso.
- Claves del registro abiertas por cada proceso.
- Direcciones de memoria asignadas a cada proceso.

- Módulos del núcleo (kernel).
- Extracción de ejecutables almacenados en memoria.(34)

Sleuth Kit 2.05:

Es una colección de herramientas forenses del sistema de ficheros que podemos usar en Linux, permite investigar los sistemas de ficheros: NTFS, FAT, FFS, EXT2FS y EXT3FS de una computadora sospechosa de un ataque informático. Las herramientas están diseñadas para extraer datos de las estructuras internas del sistema de ficheros. Estas herramientas no confían en el sistema operativo para procesar el contenido suprimido y ocultado de los sistemas de ficheros. Con esta herramienta podemos obtener datos como: fecha en que se han modificado, creado o accedido cualquiera de los ficheros de un sistema de ficheros. (35)

The Sleuth Kit y Autopsy:

Es una interfaz grafica que trabaja en conjunto con las herramientas utilizadas para el análisis forense. Entre sus características se encuentran:

- Analiza discos y sistema de archivos (NTFS, FAT, UFS1/2, Ext2/3).
- Muestra el detalle de información sobre datos eliminados y estructuras del sistema de ficheros.
- Permite el acceso a estructuras de archivos y directorios de bajo nivel y eliminados.
- Genera la línea temporal de actividad de los archivos de fecha y hora (timestamp).
- Permite buscar datos dentro de las imágenes por palabras clave.
- Permite crear notas del investigador e incluso genera informes y muchas tareas.
- Utiliza interfaz grafica que facilita notablemente el trabajo.
- Se ejecuta cuando la evidencia encontrada, posee un Sistema Operativo (Windows/Linux). (36)

Autopsy Forensic Browser: Es una interfaz gráfica para las herramientas de línea de comandos de investigación digital en The Sleuth Kit. Juntos, le permiten investigar el sistema de archivos y volúmenes de una computadora. (37)

Helix/FIRE:

Posee una variedad de herramientas para realizar un análisis forense tanto a equipos como imágenes de discos. Entre sus características se encuentran:

- Para MS Windows posee un conjunto de herramientas de 90 Mbyte, permitiendo trabajar con sistemas vivos, y recuperar información volátil.
- En el entorno Linux, dispone de un Sistema Operativo completo, con un núcleo modificado para conseguir una excelente detección de hardware.
- Es muy bueno para el análisis de equipos muertos, sin que se modifiquen las evidencias pues montará los discos que encuentre en el sistema en modo sólo lectura.
- Contiene nuevas versiones de SleuthKit y Autopsy.
- Está pensado específicamente para no realizar ningún tipo de alteración sobre los sistemas en los que se usa.
- Tiene una configuración auto-ejecutable (auto-run) para Windows.
- No requiere instalación (Live CD).(38)

BackTrack:

Es una de las más conocidas y apreciadas distribuciones GNU/Linux. Entre sus características se encuentran:

- No requiere de instalación, es decir se presenta como un live CD.
- Posee 300 herramientas de todo tipo (sniffers, exploits, auditoría wireless, análisis forense), perfectamente organizadas.
- La versión 2 utiliza un núcleo (kernel) 2.6.20 con varios parches e incluye soporte para tarjetas inalámbricas.
- Los programas que trae este software ya vienen todos configurados y listos para ser usados, por lo que no se debe emplear tiempo en buscarlos e instalarlos.

Además de la gran gama de herramientas con que cuenta la informática forense, existen metodologías empleadas con este fin, describiendo en el presente documento aquellas a las que se tiene acceso dado que la gran mayoría son privadas y comerciables.(39)

Codes of Practices for Digital Forensics (CP4DF):

Iniciativa española para el desarrollo de una metodología de procedimientos para Análisis Forense. Es una selección de criterios para guiar y asegurar actividades concernientes al análisis de evidencia digital, provee recomendaciones y cubre aspectos legales, policiales y operacionales como requerimientos técnicos para adquisición, análisis y reporte de evidencia, colaboración con otros grupos de investigación, gestión de casos, soporte a la fuerza de la ley, desarrollo de políticas de seguridad para respuesta a incidentes y plan preventivo y de continuidad. No es un manual técnico para análisis forense, es un manual basado en criterios siguiendo el asesoramiento de la comunidad y expertos.

Entre sus características se encuentran:

- Es un proyecto abierto para cualquier fuente.
- Cubre cinco fases del análisis forense:

Fase 1: Aseguramiento de la escena.

Fase 2: Identificación de las evidencias digitales.

Fase 3: Preservación de las evidencias digitales.

Fase 4: Análisis de las evidencias digitales.

Fase 5: Presentación y reportes.

Proyecto CTOSE

CTOSE (Cyber Tools On-Line Search for Evidence) es un proyecto de investigación mantenido por la Comisión Europea. El propósito del proyecto es recopilar el conocimiento disponible de diferentes fuentes expertas en todos aquellos procesos relacionados en la recuperación de evidencias digitales, y crear una metodología para definir como debe llevarse a cabo dicha recuperación cuando sea necesaria; como resultado de cualquier tipo de disputa en la que se vean envueltas transacciones electrónicas u otro tipo de crímenes relacionados con las nuevas tecnologías. Esto también incluye todas las preguntas sobre cómo ser capaz cada uno en su empresa de manejar estos tipos de incidentes y la información asociada a éstos.

1.6.1 Proyectos para el análisis forense y de redes

OWASP (Proyecto de seguridad de aplicaciones web abiertas) es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. Es un organismo que apoya y

gestiona los proyectos e infraestructura de OWASP. La comunidad OWASP está formada por empresas, organizaciones educativas y particulares de todo el mundo. Juntos constituyen una comunidad de seguridad informática que trabaja para crear artículos, metodologías, documentación, herramientas y tecnologías que se liberan y pueden ser usadas gratuitamente por cualquiera.

OWASP AntiSamy

El proyecto OWASP AntiSamy es unas cuantas cosas. Técnicamente, es una interfaz de aplicación programable (API) para asegurarse que las entradas html/ccs del usuario estén en cumplimiento con las reglas de la aplicación, es decir, es una interfaz que ayuda a asegurarse que los clientes no provean código malicioso en el html que proveen para su perfil y que se quedan almacenados en el servidor. El termino código malicioso en términos de aplicaciones web, es generalmente relacionado solo con JavaScript. Las hojas de estilo en cascada (CSS) son consideradas maliciosas cuando invocan a JavaScript, sin embargo, hay muchas situaciones donde html y ccs pueden ser usados de una forma maliciosa.

Filosóficamente, AntiSamy es una desviación de todos los mecanismos contemporáneos de seguridad. Generalmente, los mecanismos de seguridad y los usuarios tienen una comunicación que es virtualmente de una vía. Dejar al atacante potencial saber detalles acerca de la validación no se considera prudente, ya que permite que el atacante aprenda y reconstruya el mecanismo para debilidad. Estos tipos de fuga de información pueden también dañar en formas que no se espera. Un mecanismo de ingreso que le dice al usuario, usuario invalido, revela el hecho de que un usuario con ese nombre no existe. Un usuario podría usar un diccionario o directorio telefónico o ambos para obtener remotamente una lista de usuarios válidos. Usando esta información, un atacante podría lanzar un ataque de fuerza bruta o negación de servicio masivo de bloqueo de cuentas.

OWASP CLASP

CLASP (Proceso de seguridad en aplicación completo y ligero) proporciona un enfoque bien organizado y estructurado para mover las inquietudes de seguridad a las fases iniciales del ciclo de vida de desarrollo de software, cuando esto sea posible.

Es un conjunto de piezas de proceso que puede ser integrado en cualquier proceso de desarrollo de software. Está diseñado para ser fácil de adaptar y efectivo a la vez. Toma un enfoque prescriptivo, documentando las actividades que las organizaciones deberían estar haciendo. Y proporciona una amplia riqueza de recursos de seguridad que hacen razonable implementar esas actividades.

OWASP DirBuster

DirBuster es una aplicación Java multi-hilo diseñada para obtener por fuerza bruta los nombres de directorios y archivos en servidores web de aplicación. A menudo ocurre que lo que ahora parece un servidor web en una fase de instalación por omisión no lo es, y tiene páginas y aplicaciones ocultas, DirBuster trata de encontrar estos.

Sin embargo, las herramientas de esta naturaleza a menudo son solo tan buenas como la lista de archivos y directorios con los que vienen. Un enfoque diferente fue usado para generar esto. La lista fue generada desde cero, rastreando en internet y colectando los directorios y archivos que son realmente usados por los desarrolladores. DirBuster viene con un total de 0 listas diferentes, esto lo hace extremadamente efectivo, encontrando esos archivos y directorios ocultos. Tiene la opción de realizar fuerza bruta pura, lo que no les deja lugar para esconderse a los archivos y directorios ocultos.

OWASP Enterprise Security API

Es una colección gratis y abierta de todos los métodos de seguridad que un desarrollador necesita para construir una aplicación web segura. Puede usar la implementación de referencia como un punto de inicio. En concepto, la API es independiente del lenguaje. Sin embargo, los primeros entregables del proyecto son una API Java y una referencia de implementación Java.

Las plataformas disponibles y herramientas (JavaEE, Struts, Spring) simplemente no proporcionan protección suficiente. Esto deja a los desarrolladores con la responsabilidad de diseñar y construir mecanismos de seguridad.

OWASP Insecure Web App

Insecure Web App es una aplicación que incluye vulnerabilidades comunes en aplicaciones web. Es un objetivo de pruebas de penetración automatizadas y manuales, análisis de código fuente, evaluaciones de vulnerabilidades y modelado de amenazas.

Es una ayuda para desafiar y mejorar las habilidades de diseño y codificación segura. Arquitectos y desarrolladores necesitan aprender a identificar las vulnerabilidades en una aplicación web real.

Los objetivos de esta herramienta son de tres tipos:

1) Demostrar lo peligrosas que pueden ser las vulnerabilidades de las aplicaciones.

2) Cerrar la brecha que existe entre la teoría de seguridad en aplicaciones y la código que realmente se está diseñando y escribiendo.

3) Aprender como estas vulnerabilidades pueden ser arregladas.

OWASP LAPSE

LAPSE (Análisis Ligero para Seguridad en Programas en Eclipse), está diseñado para ayudar con la tarea de auditar aplicaciones Java J2EE para tipos comunes de vulnerabilidades encontradas en aplicaciones web.

OWASP Live CD

El **LiveCD de OWASP** es un CD de arranque, dedicado a la seguridad de aplicaciones. Servirá como un vehículo y medio de distribución para las herramientas y guías de OWASP.

La versión 2 del LiveCD de OWASP está enfocada en las herramientas y documentación de OWASP. La estructura del menú ha sido construida en torno a los tres niveles de estado de los proyectos (Releases, Alpha y Beta). Cada área ha sido separada en documentos y herramientas, para hacer más simples las actualizaciones.

OWASP Pantera Web Assessment Studio

Pantera proporciona una poderosa máquina de análisis de aplicaciones web. El objetivo principal es combinar las capacidades automáticas con pruebas manuales completas para obtener los mejores resultados de pruebas de intrusión.

OWASP Validation

El proyecto de validación de OWASP fue creado para proveer guía y herramientas relacionadas a la validación. Filosofía que es requerida para cada petición html, incluyendo cabeceras, cadenas, cookies, formas, campos y campos ocultos.

OWASP WSFuzzer

WSFuzzer es un programa LGPL, escrito en Python, que actualmente apunta hacia web services. En la versión actual los servicios SOAP basados en http son el principal objetivo. Esta herramienta fue creada para automatizar el trabajo de pruebas de intrusión manual para SOAP en el mundo real. Esta herramienta no está destinada para ser un reemplazo del análisis humano manual sólido. Es una herramienta para aumentar el análisis realizado por profesionales reconocidos y competentes. Los servicios web no son de naturaleza trivial así que la experiencia en esta área es necesaria para las correctas pruebas de intrusión.

Seguridad de aplicaciones web es un componente esencial de cualquier proyecto exitoso, ya sea de código abierto de aplicaciones php, servicios web, tales como procesamiento directo, o de propiedad sitios web de negocios. Los proveedores rechazan código inseguro, y los usuarios evitan servicios inseguros que lleven al fraude. El objetivo de esta guía de desarrollo es permitir a las empresas, desarrolladores, diseñadores y arquitectos producir aplicaciones web seguras.

A diferencia de otras formas de seguridad (tales como cortafuegos y cierres de seguridad), las aplicaciones web tienen la capacidad de hacer, un atacante experto rico, o hacer la vida de una víctima una completa miseria. La aplicación debe ser auto-defensa. La guía de desarrollo se ha escrito para cubrir todas las formas de las cuestiones de seguridad en aplicaciones web, inyección de SQL, a través de las preocupaciones modernas, tales como AJAX, suplantación de identidad, el manejo de tarjetas de crédito, la fijación del período de sesiones, falsificaciones de páginas web de solicitud, el cumplimiento y cuestiones de privacidad.

1.7 Conclusiones Parciales

En el capítulo se ha realizado un estudio detallado de los principales conceptos asociados al dominio del problema para el total entendimiento de la situación planteada. Se ha profundizado en las principales herramientas y metodologías existentes en la actualidad en el mundo, en Cuba y en la UCI para dar fundamento respecto al tema en análisis y sentar las bases de la presente investigación.

Por ello mediante el estudio teórico realizado se decidió que la presente investigación se centrará en la situación existente en la UCI para el análisis forense a incidentes de seguridad informática, para la elaboración de una metodología para guiar a los especialistas que trabajan en este campo.

CAPÍTULO 2. DIAGNÒSTICO ACTUAL

Con el objetivo de evaluar y buscar posibles soluciones a los problemas existentes en la universidad de las ciencias informáticas con respecto al análisis forense a incidentes de seguridad que requieran este tipo de estudio, en toda investigación se debe realizar un examen valorativo y detallado de la situación real del tema.

El presente capítulo se basa en la aplicación de una entrevista y el análisis de los resultados de la misma para la obtención de respuestas acerca de la situación existente en la universidad con respecto al análisis forense a incidentes informáticos de seguridad que requieren este tipo de investigación.

La entrevista es una de las técnicas de recopilación de información más utilizadas, mediante ella se obtienen los datos más específicos, concretos y superiores a los adquiridos mediante otros métodos, por este motivo se decidió utilizarla como sustento de la investigación.

2.1 Descripción del proceso de análisis forense a incidentes informáticos en la UCI

En la UCI el análisis a los incidentes informáticos está organizado y estructurado por la dirección de redes y seguridad informática de la universidad. El proceso mediante el cual estos incidentes llegan a manos de los especialistas es mediante el portal: http: //reportesdrsi.uci.cu, en el cual los estudiantes pueden generar reportes acerca de los problemas que hayan tenido referente al tema en cuestión. Esta página es un sistema de tickets (así se conoce en la literatura), donde llega el reporte y va a parar a una cola de similares, donde esperan ser atendidos por especialistas encargados específicamente para cada tipo de reporte existente, con el fin de garantizar la rapidez y eficiencia del proceso.

El proceso de atención a estos reportes lo realiza cada especialista basándose en la experiencia adquirida en la realización de esta tarea ya que actualmente no se cuenta con una guía aprobada y eficiente que oriente al personal calificado a la hora de ejecutar esta tarea.

A continuación se muestran los distintos tipos de incidentes informáticos existentes en la UCI que requieren análisis forense.

- Robo de cuentas.
- Correos cadena (Hoax).

- Páginas web con desperfectos.
- Programas malignos.
- Extraoficial ha pedido del departamento central docente (Fraudes Académicos).
- Correos anónimos ofensivos.

2.2 Personal Encuestado

Las entrevistas fueron realizadas a los especialistas de la dirección de redes y seguridad informática de la universidad. Se decidió entrevistar específicamente al personal encargado de atender los delitos informáticos que ocurren en el entorno universitario, ya que no todos los especialistas vinculados a este centro tienen conocimiento del tema en cuestión y esto puede provocar confusiones y falsos resultados. (**Ver Anexo 1**).

Tabla 2.1: Muestra la cantidad de especialistas entrevistados por cada delito informático que atiende.

Nombre del especialista	**Especialidad**	**Tipo de delito informático**
Alexander Fernández Castro.	Especialista en redes y seguridad informática.	Robo de cuentas. Fraude académico.
Omar Pimentel Alonso.	Instructor recién graduado (Especialista en redes y seguridad informática).	Programas malignos.
Haidi Marlen Plaza Gil.	Técnico general (especialista en redes y seguridad informática).	Correos cadena.
Yilian Elena Matías León.	Recién graduado en adiestramiento (especialista en redes y seguridad informática).	Páginas web des-configuradas.
Pablo Yunier Medina Martínez	Especialista superior (Dirección de redes y seguridad	Está capacitado para atender todos los delitos informáticos que

	informática).	se presentan en la universidad principalmente: Fraude académico. Robo de cuentas. Correos cadena. Correos anónimos ofensivos.

Figura 2.1: Muestra el orden de prioridad con que ocurren los incidentes informáticos de seguridad en la Universidad de Ciencias Informáticas.

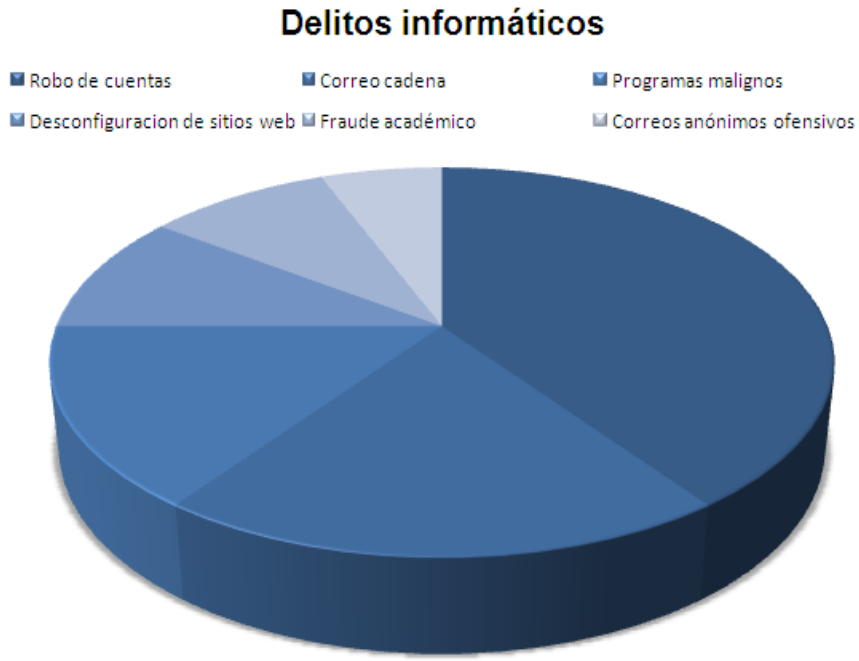

Figura 2.2: Principales tipos de delitos informáticos a los que se les realiza análisis forense en la universidad.

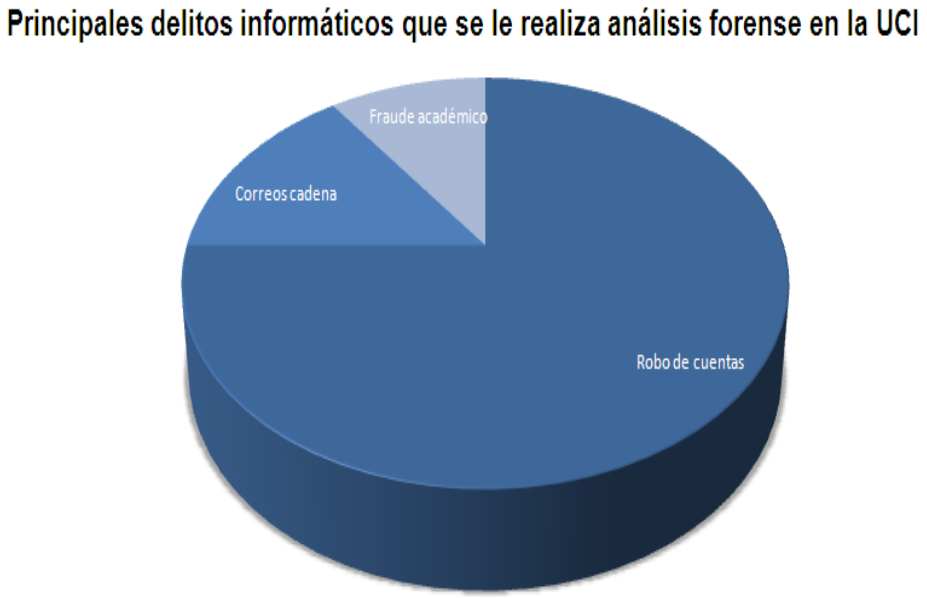

Tabla 2.2: Muestra los tipos de delitos informáticos que se le realiza análisis forense y si se utiliza una metodología oficial o personal.

Tipos de delitos informáticos	Metodología definida	Metodología personal
Robo de cuentas	no	si
Correos cadena	no	si
Fraude académico	no	si

Tabla 2.3: Muestra los tipos de delitos informáticos que se le realizan análisis forense y las herramientas utilizadas para este estudio.

Tipos de delitos informáticos	Herramientas

Robo de cuentas	SAWMILL, herramienta Web que reconoce varios formatos de logs.
Correo cadena	Encase en los casos donde se justifique la adquisición de evidencia digital.
Fraude académico	SAWMILL, herramienta Web que reconoce varios formatos de logs. Encase en los casos donde se justifique la adquisición de evidencia digital como prueba legal a presentar ante un tribunal.

2.3 Análisis y resultados del diagnóstico realizado a especialistas de la UCI.

El diagnóstico realizado contó con preguntas acerca de la aplicación y el funcionamiento del análisis forense a incidentes informáticos de seguridad que requieran este estudio en la UCI, lo cual permite evaluarlo cualitativamente. A continuación se presentan los resultados de interés a la investigación.

Tabla 2.4: Muestra los principales factores que se tuvieron en cuenta en la aplicación de las entrevistas.

Delito informático	Metodología definida	Metodología personal	Herramientas
Robo de cuentas	no	si	SAWMILL
Correo cadena	no	si	Encase
Fraude académico	no	si	SAWMILL, Encase
Programas malignos	no	no	Encase
Páginas web con desperfectos	no	no	Comandos ms-dos para su configuración

Correos anónimos ofensivos	no	no	Herramientas de análisis de temporales de los navegadores. Herramientas recuperadoras de contenidos borrados.

2.4 Descripción del proceso de análisis forense a incidentes informáticos en Cuba.

La institución rectora en redes y seguridad informática en Cuba como se especificó anteriormente es La Oficina de Seguridad para las Redes Informáticas (OSRI) y formando parte de la misma se encuentra el Equipo de Respuesta a Incidentes Computacionales de Cuba (CuCERT) el cual tiene entre sus responsabilidades la atención a los delitos informáticos de seguridad que demanden análisis forense. La investigación realizada fue profunda y precisa, pero a pesar del esfuerzo realizado no se logró obtener los resultados esperados debido a la privacidad respecto a la confidencialidad e integridad de la información con que allí se trabaja.

Por razones de seguridad el único especialista autorizado a brindar información fue Gerardo Gómez quien brindó una breve explicación acerca del tema en cuestión. Se precisó que por regla general cualquier incidente en el que se busque evidencia digital se le aplica informática forense, tales son los casos donde haya que identificar a un usuario, demostrar que el usuario estuvo usando un servicio no autorizado, dígase análisis del historial de aplicaciones, de logs de seguridad y recuperación de información borrada. El otro aspecto abordado fue que en Cuba el tema de leyes en el ámbito de la seguridad informática aun está en desarrollo, las leyes no están definidas todavía por tanto la informática forense que se realiza no se ajusta a las metodologías existentes en el mundo. El fuerte trabajo que se desarrolla se basa en los procesos que se presentan ante la justicia y tienen validez legal.

El organismo rector que rige a la OSRI en el tema de la informática forense es el Ministerio del Interior (MININT), específicamente los profesionales de Criminalística. El trabajo está estructurado de la siguiente forma: Como paso primordial no está permitido brindar información al personal ajeno al proceso forense

por tanto no se realizan entrevistas ni preguntas a los profesionales inmiscuidos en este tipo de labor. Para iniciar el proceso el MININT le solicita a la OSRI que inicien la investigación en la parte informática y los de Criminalística por su parte se dedican a la parte penal, después de todo el proceso investigativo realizado entre las dos partes se obtienen los resultados, y en dependencia de lo obtenido el caso pasa a los tribunales o no, es decir procede o no procede.

La solución a estos procesos de informática forense por parte de la OSRI se efectúa principalmente mediante la potente herramienta Encase, porque además de ser muy efectiva y eficaz; es muy utilizada para procesos penales e internacionales. En Cuba por los problemas existentes con respecto al bloqueo estadounidense la mayoría de las veces no hay posibilidad de comprar patentes para usar las mejores herramientas y son imprescindibles para los procesos penales, por este motivo se cuenta con la patente del Encase y el único personal autorizado en el país a utilizarla son los profesionales de la OSRI y del MININT.

2.5 Análisis y resultados del diagnóstico realizado a especialistas de la OSRI.

El diagnóstico efectuado permitió de forma general conocer que en Cuba el tema de leyes en el ámbito de la seguridad informática está evolucionándose aun, por tanto no se cuenta con una metodología descrita y definida para estos casos y además que el trabajo que se desarrolla actualmente en el campo de la informática forense está estructurado de forma confidencial y organizadamente distribuido. La presente investigación proporcionó gran ayuda en la adquisición de experiencias y conocimientos para la metodología a proponer.

2.5.1 Valoración General

Analizando los resultados obtenidos, a partir del diagnóstico realizado y de las entrevistas efectuada se puede decir que se ha logrado un gran avance en la aplicación de la informática forense tanto en el ámbito nacional como en el entorno universitario, pero no se puede obviar la necesidad de una metodología que unifique el desempeño de los especialistas en este aspecto, por tanto los esfuerzos deben estar enfocados a lograr este objetivo.

La encuesta realizada al personal de la Dirección de Redes y Seguridad Informática de la Universidad de las Ciencias Informáticas (UCI) evidenció que actualmente el proceso se ve afectado por varios factores

relacionados con la capacitación a los especialistas en el campo de la informática forense que ingresan al departamento. Los principales problemas detectados son los siguientes:

- Se evidenció que el personal que labora en la Dirección de Redes y Seguridad de la universidad no son especialistas en el tema de informática forense.
- El personal calificado para temas de seguridad tiene que prepararse en el aspecto de la informática forense para solucionar estos tipos de delitos informáticos que requieren análisis forense.
- La solución a estos tipos de delitos que requieren análisis forense se realiza basada en la experiencia adquirida por cada especialista.
- No se cuenta con un proceso escrito y bien definido para organizar y estructurar los pasos, métodos y herramientas utilizadas para dar solución a estos delitos que requieren análisis forense.

2.6 Conclusiones Parciales

En este capítulo se procesaron los datos obtenidos en la entrevista aplicada. Lo que permitió precisar el estado actual del proceso de análisis forense en Cuba y en la UCI, por lo cual se evidenció la necesidad de una vía de solución a las insuficiencias existentes. En el entorno UCI específicamente se detectaron problemas, descritos anteriormente, que hacen necesaria la existencia de una metodología para organizar y unificar las herramientas y métodos a seguir para darle tratamiento a los principales incidentes de seguridad informática que requieran análisis forense. Todo esto orientado a mejorar y erradicar el problema existente respecto al tema en cuestión.

CAPÍTULO 3. PROPUESTA DE METODOLOGÌA.

Después de realizar un análisis profundo del proceso de análisis forense en la Universidad de Ciencias Informáticas (UCI), se pudo comprobar que no es del todo satisfactorio. Lo que afecta el correcto funcionamiento del estudio y solución a los delitos informáticos que requieren análisis forense, por lo que se hace necesario, realizar una propuesta de una metodología para contribuir a la mejora del proceso de análisis forense y a la calidad del mismo.

3.1 Estructura de la metodología

La figura 3.1: Muestra la estructura de la metodología propuesta.

3.2 Metodología Propuesta

Tipo de delito informático	Pasos a seguir	Herramientas a utilizar
Robo de usuario	1. Verificar el gasto de la	SAWMILL, herramienta Web que

	cuota con algún software.	reconoce varios formatos de “logs” Comandos y Scripts en Phayton, Perl y AWK (utilizándose para funcionalidades específicas).
	2. Verificar las estadísticas de navegación. - Verificar que no esté gastado en los IPs regulares del usuario (posible equivocación del usuario). - Determinar Día-Hora-IP de los gastos más relevantes.	
	Con el Día-Hora-IP: 3. Buscar los usuarios que han usado algún servicio telemático (Jabber, Correo, Internet, Dominio) en los IPs detectados. Ampliar el margen de búsqueda (más menos) ±1 día.	
	4. Crear Línea de Tiempo con los gastos más relevantes del afectado que incluya accesos de otros usuarios intercalados.	

	5. Establecer sospechosos y estudiar comportamiento que delaten presencia. - Actividad en el Jabber y Buzón de Correo - Revisar la carpeta de Salvas. - Entrar a las PCs regulares de los sospechosos.	
	6. Coleccionar las pruebas incriminatorias y enviar el correo de citación.	
	7. Obtener declaración de responsabilidad de puño y letra firmada con datos explícitos de lo sucedido.	
	8. Escribir informe de la investigación.	

Tipo de delito informático	**Pasos a seguir**	**Herramientas a utilizar**
Fraude Académico	1. Buscar posibles usuarios de fraude. - Buscar toda la actividad que hayan tenido estos usuarios en los servicios (Jabber, Correo, Internet, Dominio), en computadoras y discos duros. 2. Proceder con las entrevistas. 3. Obtener Declaración de Responsabilidad de puño y letra firmado por el usuario implicado en el fraude con toda la evidencia recolectada. 4. Escribir informe de la investigación.	SAWMILL, herramienta Web que reconoce varios formatos de logs. Comandos y Scripts en Phayton, Perl y AWK (utilizándose para funcionalidades específicas). OpenVAS, herramienta usada para el escaneo de vulnerabilidades (virus, carpetas compartidas, PC sin antivirus). Sistema de Estadísticas de Navegación, herramienta que se utiliza para obtener información sobre los sitios más visitados por los usuarios en la universidad.
Correos Cadena	1. Se ponen filtros en el correo del especialista a cargo para buscar los correos que tengan de asunto: reenviar a todos, o	Scripts en el servidor de correo.

	aquellos correos que presenten muchas frases comunes, pues mientras más frases mejor el filtro. 2. Se hace un informe del caso. 3. Se le envía el usuario a un administrador para que le suspenda por 1 mes el acceso a la cuenta al usuario implicado. 4. Se envía el informe del caso a la Decana en caso de ser estudiante, o al director del área y al asesor de Seguridad Informática de esta área si es trabajador.	

3.3 Conclusiones Parciales

En este capítulo se elaboró la propuesta de metodología para el análisis forense a incidentes de seguridad informática en la UCI. Con su aplicación se espera que el proceso de análisis forense a los delitos informáticos que requieran este tipo de estudio por parte de los especialistas de la Dirección de Redes y Seguridad informática de la universidad, se organice y desarrolle de forma más factible disminuyendo el esfuerzo necesario para llevarlo a cabo, con el objetivo de mejorar los resultados logrados hasta el momento.

CONCLUSIONES GENERALES

Al concluir el presente trabajo de diploma se ha cumplido el objetivo y las tareas de la investigación. Se realizó la propuesta de una metodología para el análisis forense a incidentes de seguridad informática en la UCI. Se realizó un estudio de la situación actual del proceso de análisis forense a nivel mundial, nacional y específicamente en Universidad de Ciencias Informáticas. A partir del diagnóstico realizado se identificaron las insuficiencias que dificultan el proceso de análisis forense en la universidad y específicamente en la Dirección de Redes y Seguridad Informática, demostrando la necesidad de una guía que unificara las herramientas y métodos utilizados por los especialistas en el desarrollo de este proceso. Se diseñó una metodología para estructurar y organizar de forma más eficiente el proceso de análisis forense desarrollado por parte de la Dirección de Redes y Seguridad Informática de la Universidad de Ciencias Informáticas.

RECOMENDACIONES

REFERNCIAS BIBLIOGRÁFICAS

1. **Millán, LL.M. Adolfo Arturo Mercado.** Introduccion a la Informática Forense. [Online] [Cited: 3 5, 2011.] http://www.univalle.edu/publicaciones/brujula/brujula18/pagina05.htm.

2. **Discovery Channel.** Crimen y ciencia forense. [Online] Discovery Communications, Inc. [Cited: 4 12, 2011.] http://www.tudiscovery.com/crimen/ciencia_forense/index.shtml.

3. **Millán, LL.M. Adolfo Arturo Mercado.** Historia de la informática forense. [Online] Unidad Académica Cochabamba. [Cited: 3 25, 2011.] http://www.univalle.edu/publicaciones/brujula/brujula18/pagina05.htm.

4. **compañía inscrita en el Registro Mercantil de Madrid.** Chase The Sun. [Online] España. Madrid. [Cited: 4 2, 2011.] http://www.chasethesun.es.

5. **Insect.** Tecnolinks. [Online] Maracaibo. Venezuela. [Cited: 2 12, 2011.] http://www.tecnolinks.com.ve.

6. **S.A.** KPMG cutting throught complexity. [Online] sociedad anónima española. [Cited: 4 10, 2011.] http://www.kpmg.com/ES/es/QuienesSomos/Paginas/default.aspx.

7. **Deloitte Global Services Limited.** Deloitte. [Online] [Cited: 4 20, 2011.] http://www.deloitte.com/view/en_GX/global/services/index.htm.

8. **Oficina de seguridad para las redes informáticas(OSRI).** Cucert. Equipo de respuesta a incidentes computacionales de Cuba. [Online] Cuba. [Cited: 3 24, 2011.] http://www.cucert.cu/index.php/quienes-somos.html.

9. **Comunidad DragonJAR.** Dragonjar. [Online] Colombia. [Cited: 4 28, 2011.] http://dragonjar.org.

10. **Comunidad Dragonjar.** Dragonjar. [Online] Colombia. [Cited: 4 28, 2011.] http://www.dragonjar.org.

11. **Copyright © 2008 - Definición.de.** Definicion.de. [Online] [Cited: 4 28, 2011.] http://definicion.de.

12. **Comunidad Dragonjar.** Dragonjar. [Online] [Cited: 4 28, 2011.] http://anonym-url.com/.

13. **Copyright © 2011 Yahoo.** Yahoo Respuestas. [Online] España. [Cited: 4 28, 2011.] http://es.answers.yahoo.com/question/index.

14. Yahoo Respuestas. [Online] España. [Cited: 4 28, 2011.] http://es.answers.yahoo.com/question/index.

15. **Copyright © 2007 - 2011 Definicion ABC .** Definición ABC. [Online] Wordpress. [Cited: 4 28, 2011.] http://www.definicionabc.com/ciencia/metodologia.php.

16. **Security By Default.** Historia de la informática forense. [Online] España. [Cited: 4 29, 2011.] http://www.securitybydefault.com.

17. Ídem a referencia 9

18. Ídem a referencia anterior.

19. Ídem a referencia anterior.

20. Ídem referencia anterior.

21. Ídem a referencia anterior.

22. Ídem a referencia anterior.

23. Ídem a referencia anterior.

24. Ídem a referencia anterior.

25. Ídem a referencia anterior.

26. Ídem a referencia anterior.

27. Ídem a referencia anterior.

28. Ídem a referencia anterior.

30. Ídem a referencia anterior.

31. Ídem a referencia anterior.

32. Ídem a referencia anterior.

33. Ídem a referencia anterior.

34. Ídem a referencia anterior.

35. Ídem a referencia anterior.

36. Ídem a referencia anterior.

37. Ídem a referencia anterior.

38. Ídem a referencia anterior.

39. Ídem a referencia anterior.

BIBLIOGRAFÍA

1. **Millán, LL.M. Adolfo Arturo Mercado.** Introduccion a la Informática Forense. [Online] [Cited: 3,5, 2011.] http://www.univalle.edu/publicaciones/brujula/brujula18/pagina05.htm.

2. Anonymous. Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network, Second Edition. Indianapolis, Indiana: Sams, 1998.

3. Casey, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. San Diego: Academic Press, 2000.

4. National Institute of Justice. Crime Scene Investigation: A Guide for Law Enforcement. Washington, D.C.: U.S. Department of Justice, National Institute of Justice, 2000. NCJ 178280.

5. **Discovery Channel.** Crimen y ciencia forense. [Online] Discovery Communications, Inc. [Cited: 4 12, 2011.] http://www.tudiscovery.com/crimen/ciencia_forense/index.shtml.**o.** Introducción a la Informática Forense. [Online] [Cited: 3,5, 2011.] http://www.univalle.edu/publicaciones/brujula/brujula18pagina05.htm.

6. Http://www.dragonjar.org.

1. **Millán, LL.M. Adolfo Arturo Mercado.** Introduccion a la Informática Forense. [Online] [Cited: 3 5, 2011.] http://www.univalle.edu/publicaciones/brujula/brujula18/pagina05.htm.

2. **Discovery Channel.** Crimen y ciencia forense. [Online] Discovery Communications, Inc. [Cited: 4 12, 2011.] http://www.tudiscovery.com/crimen/ciencia_forense/index.shtml.

3. **Millán, LL.M. Adolfo Arturo Mercado.** Historia de la informática forense. [Online] Unidad Académica Cochabamba. [Cited: 3 25, 2011.] http://www.univalle.edu/publicaciones/brujula/brujula18/pagina05.htm.

4. **compañía inscrita en el Registro Mercantil de Madrid.** Chase The Sun. [Online] España. Madrid. [Cited: 4 2, 2011.] http://www.chasethesun.es.

5. **Insect.** Tecnolinks. [Online] Maracaibo. Venezuela. [Cited: 2 12, 2011.] http://www.tecnolinks.com.ve.

6. **S.A.** KPMG cutting throught complexity. [Online] sociedad anónima española. [Cited: 4 10, 2011.] http://www.kpmg.com/ES/es/QuienesSomos/Paginas/default.aspx.

7. **Deloitte Global Services Limited.** Deloitte. [Online] [Cited: 4 20, 2011.] http://www.deloitte.com/view/en_GX/global/services/index.htm.

8. **Oficina de seguridad para las redes informáticas(OSRI).** Cucert. Equipo de respuesta a incidentes computacionales de Cuba. [Online] Cuba. [Cited: 3 24, 2011.] http://www.cucert.cu/index.php/quienes-somos.html.

9. **Comunidad DragonJAR.** Dragonjar. [Online] Colombia. [Cited: 4 28, 2011.] http://dragonjar.org.

10. **Comunidad Dragonjar.** Dragonjar. [Online] Colombia. [Cited: 4 28, 2011.] http://www.dragonjar.org.

11. **Copyright © 2008 - Definición.de.** Definicion.de. [Online] [Cited: 4 28, 2011.] http://definicion.de.

12. **Comunidad Dragonjar.** Dragonjar. [Online] [Cited: 4 28, 2011.] http://anonym-url.com/.

13. **Copyright © 2011 Yahoo.** Yahoo Respuestas. [Online] España. [Cited: 4 28, 2011.] http://es.answers.yahoo.com/question/index.

14. Yahoo Respuestas. [Online] España. [Cited: 4 28, 2011.] http://es.answers.yahoo.com/question/index.

15. **Copyright © 2007 - 2011 Definicion ABC .** Definición ABC. [Online] Wordpress. [Cited: 4 28, 2011.] http://www.definicionabc.com/ciencia/metodologia.php.

16. **Security By Default.** Historia de la informática forense. [Online] España. [Cited: 4 29, 2011.] http://www.securitybydefault.com.

17. Ídem a referencia 9

18. Ídem a referencia anterior.

19. Ídem a referencia anterior.

20. Ídem referencia anterior.

21. Ídem a referencia anterior.

22. Ídem a referencia anterior.

23. Ídem a referencia anterior.

24. Ídem a referencia anterior.

25. Ídem a referencia anterior.

26. Ídem a referencia anterior.

27. Ídem a referencia anterior.

28. Ídem a referencia anterior.

30. Ídem a referencia anterior.

31. Ídem a referencia anterior.

32. Ídem a referencia anterior.

33. Ídem a referencia anterior.

34. Ídem a referencia anterior.

35. Ídem a referencia anterior.

36. Ídem a referencia anterior.

37. Ídem a referencia anterior.

38. Ídem a referencia anterior.

39. Ídem a referencia anterior.

GLOSARIO DE TÉRMINOS

UCI: Universidad de las Ciencias Informáticas.

OSRI: Oficina de Seguridad para las Redes Informáticas

CuCERT: Equipo de Respuesta a Incidentes Computacionales de Cuba.

CERT: Equipo de Respuesta a Incidentes Informáticos.

OTRS (Open-source Ticket Request System): es un sistema libre que cualquier institución puede utilizar para asignar identificadores únicos llamados tiques a solicitudes de servicio o de información, de forma que facilite el seguimiento y manejo de dichas solicitudes así como cualquier otra interacción con sus clientes o usuarios.

Computer Analysis and Response Team (CART): El análisis de Informática y Equipo de Respuesta presta asistencia a las oficinas de campo del FBI en la búsqueda e incautación de pruebas informáticas, así como los exámenes forenses y asistencia técnica para las investigaciones del FBI. Esta unidad incluye un laboratorio forense del estado de la técnica compuesta por especialistas en informática y una red de médicos forenses capacitados y equipados asignados a más de 50 oficinas sobre el terreno.

FileFix: es un virus que se propaga por internet. Este tipo de virus suele afectar a archivos de extensión DOC y PDF. Si un ordenador se contagia con este virus el usuario no podrá abrir este tipo de archivos ni tampoco acceder a la carpeta de Windows.

Detector de tensión (TimeMark): son componentes de alta calidad y durabilidad, están construido para el monitoreo de líneas trifásicas, monofásicas, sobre-corriente, bajo voltaje y desbalance de fase.

Symantec: es una corporación internacional que desarrolla y comercializa software para computadoras, particularmente en el dominio de la seguridad informática.

FBI: La Oficina Federal de Investigación o el Buró Federal de Investigación (en inglés: Federal Bureau of Investigation) es la principal rama de investigación del Departamento de Justicia de los Estados Unidos.

Forensic Toolkit (FTK): es un programa para la informática forense, realizado por Access Data. Analiza una unidad de disco duro en busca de información variada. Ejemplo, puede localizar mensajes de correo

electrónico eliminado, y escanear un disco para cadenas de texto para utilizarlos como una contraseña diccionario para romper el cifrado.

Guidance Software Inc.: es reconocido mundialmente como el líder de industria en soluciones de investigación digital.

Python: es un lenguaje de programación de alto nivel cuya filosofía hace hincapié en una sintaxis muy limpia y que favorezca un código legible. Se trata de un lenguaje de programación multi-paradigma ya que soporta orientación a objetos, programación imperativa y, en menor medida, programación funcional. Es un lenguaje interpretado, usa tipado dinámico, es fuertemente tipado y multi-plataforma.

Hojas de estilo en cascada (Ccs): es un lenguaje usado para definir la presentación de un documento estructurado escrito en HTML o XML (y por extensión en XHTML).

Lenguaje de Marcado de Hipertexto (Html): es el lenguaje de marcado predominante para la elaboración de páginas web. Es usado para describir la estructura y el contenido en forma de texto, así como para complementar el texto con objetos tales como imágenes.

Simple Object Access Protocol (SOAP): es un protocolo estándar que define cómo dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML.

AJAX: es una técnica de desarrollo web para crear aplicaciones interactivas o RIA (Rich Internet Applications). Estas aplicaciones se ejecutan en el cliente, es decir, en el navegador de los usuarios mientras se mantiene la comunicación asíncrona con el servidor en segundo plano. De esta forma es posible realizar cambios sobre las páginas sin necesidad de recargarlas, lo que significa aumentar la interactividad, velocidad y usabilidad en las aplicaciones.

Lenguaje de consulta estructurado (SQL): es un lenguaje declarativo de acceso a bases de datos relacionales, que permite especificar diversos tipos de operaciones en éstas. Una de sus características es el manejo del álgebra y el cálculo relacional permitiendo efectuar consultas con el fin de recuperar información de interés de una base de datos, así como también hacer cambios sobre ella.

MININT: Ministerio del Interior de la República de Cuba.

AWK: es un lenguaje de programación diseñado para procesar datos basados en texto, ya sean ficheros o flujos de datos.

ANEXO 1

Encuesta:

1- En el entorno informático ocurren múltiples incidentes de Seguridad Informática. De estos incidentes ejemplifique los más frecuentes que ocurren en la UCI.
2- De ellos diga cuales requieren análisis forense.
   ¿Usas algún estándar o alguna metodología conocida para el análisis forense?
3- Explica cuál usas.
4- Para qué incidente de seguridad informática la usas.
5- Por qué la usas para este tipo de incidente informático.
6- De las siguientes herramientas señale cuales utiliza para el análisis forense y explica para que tipo de incidente de seguridad informática la usas.

___ **Sleuth Kit (Forensics Kit):**

___ **AIRT Py-Flag (Forensics Browser):**

___ **Autopsy (Forensics Browser for Sleuth Kit):**

___ **Dcfldd (DD Imaging Tool command line tool and also works with AIR):**

___ **Foremost (Data Carver command line tool):**

___ **Air (Forensics Imaging GUI):**

___ **md5deep (MD5 Hashing Program):**

___ **Netcat (Command Line):**

___ **Cryptcat (Command Line):**

___ **NTFS-Tools:**

___ **Qtparted (GUI Partitioning Tool):**

___ **Regviewer (Windows Registry):**

___ **Viewer:**

___ **X-Ways WinTrace:**

___ **X-Ways WinHex:**

___ **X-Ways Forensics** t**:**

___ **R-Studio Emergency (Bootable Recovery media Maker):**

___ **R-Studio Network Edition:**

___ **Helix:**

___ **Rifiuti:**

___ **R Snort:**

___ **Encase:**

___ **R-Studio RS Agent:**

___ **Net resident:**

___ **Faces:**

___ **Ingeniería Inversa:**

___ **Arpwatch:**

___ **EnCase:**

___ **KeyLogger:**

__ **Otras:**

7- Si no utilizas ningún estándar, metodología o herramienta. Explique de qué forma realizas el análisis forense a los incidentes informáticos que requieran este tipo de análisis.