ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

DISEÑO Y PLAN DE IMPLEMENTACIÓN DE UN LABORATORIO DE CIENCIAS FORENSES DIGITALES

TESINA DE SEMINARIO

Previa a la obtención del Título de:

INGENIERO EN CIENCIAS COMPUTACIONALES
ESPECIALIZACIÓN SISTEMAS DE INFORMACIÓN

INGENIERO EN CIENCIAS COMPUTACIONALES
ESPECIALIZACIÓN SISTEMAS DE INFORMACIÓN

INGENIERO EN CIENCIAS COMPUTACIONALES
ESPECIALIZACIÓN SISTEMAS MULTIMEDIA

Presentado por:

Ricardo Gregorio Calderón Valdiviezo.
Gisell Stephanie Guzmán Reyes.
Jessica Margarita Salinas González.

Guayaquil-Ecuador
AÑO 2011

AGRADECIMIENTO

A Dios en primer lugar por bendecirnos durante este proceso, a nuestros padres y familiares por su apoyo incondicional, a nuestros amigos por ser partícipes de nuestra trayectoria universitaria.

DEDICATORIA

A nuestra familia, maestros y amigos.

TRIBUNAL DE SUSTENTACIÓN

Ing. Alfonso Aranda

Profesor de Seminario de Graduación

Ing. Ignacio Marín-García

Profesor Delegado del Decano de la FIEC

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Trabajo de Graduación, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

(Reglamento de graduación de la ESPOL)

Gisell Stephanie Guzmán Reyes

Jessica Margarita Salinas González

Ricardo Gregorio Calderón Valdiviezo

RESUMEN

El crecimiento que han tenido en la actualidad las Tecnologías de la Información y las Comunicaciones, ha dado lugar a que se tenga un acceso casi ilimitado a las fuentes de consulta de información. El beneficio para las empresas y personas naturales es notable cuando se aprovechan estas tecnologías, los inconvenientes se generan cuando las personas la utilizan para cumplir objetivos personales sin ética o utilizan la tecnología para causar daños a terceros, convirtiéndose en un delito informático.

Se realizó, durante la elaboración del proyecto, un breve análisis de cómo se procedía en el Ecuador ante este tipo de delitos, como se realizaban las investigaciones, y cuál era el trato que se le daba a la evidencia digital; en el trabajo también se analizarán diferentes normas y estándares internacionales para averiguar cual se ajusta mejor a las leyes y justicia Ecuatoriana.

En el trabajo se presentará el plan de implementación de un laboratorio de Ciencias Forenses Digitales donde se podrá aplicar la metodología para la búsqueda y el análisis de evidencias digitales, mediante la aplicación de técnicas científicas y analíticas, conocimientos tecnológicos y legales, para identificar, obtener, reconstruir, analizar y presentar información que pueda

ser válida dentro de un proceso legal en donde haya ocurrido un delito informático.

La formación de peritos de seguridad informática y el equipo de investigación es parte fundamental en el proceso de rastreo de los orígenes del delito; en este trabajo se buscará definir las funciones y métodos que utilicen los peritos para proceder a la recopilación de datos, pruebas, búsqueda y análisis de evidencias de aplicación en un asunto judicial, ya que para probar un delito deben existir evidencias que relacionen al sospechoso del crimen con el hecho.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

GLOSARIO

Archivo de intercambio.- Es un espacio en el disco duro usado como una extensión de la memoria RAM de la computadora [(1)].

Archivo BITMAP.- Es el formato propio del programa Microsoft Paint, que viene con el sistema operativo M Windows, extensión .BMP [(2)].

Bit SUID/SGID.- Es un procedimiento de asignación de permisos de los sistemas operativos basados en Unix, en el cual se le otorga al usuario o grupo privilegios de root o administrador, para realizar una tarea específica dentro del sistema [(3)].

Blu-Ray.- Es un formato de disco óptico de nueva generación que permite la grabación de video de alta definición y almacenamiento de grandes volúmenes de datos [(4)].

Bolsa antiestática.- Bolsa o funda diseñada para evitar el traspaso y la generación de electricidad estática sea por fricción o inducción, al almacenar o transportar hardware [(5)].

Bomba lógica.- Software, rutinas o modificaciones de programas que producen cambios, borrados de ficheros o alteraciones del sistema en un momento posterior a aquél en el que se introducen por su creador [(6)].

Botnet.- Es una red de equipos comprometidos, denominados zombies que recibe la orden de enviar simultáneamente tráfico de red a los sitios web que tienen por objetivo [(7)].

Bugs.- Son fallos o deficiencias en el proceso de creación de software que pueden ocasionar mal funcionamiento [(8)].

Bypass.- Es un sistema conformado por un enlace internacional, una instalación de equipos de telecomunicaciones y líneas telefónicas, lo cual produce que una llamada de origen internacional sea registrada, y por lo tanto facturada, por la operadora telefónica como una llamada local [(9) (10)].

Cookies.- Es un fragmento de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página [(11)].

Cibercriminal.- Persona que ha cometido o procurado cometer un crimen, es decir una acción ilegal, haciendo uso de medios informáticos [(12)].

Ciberdelincuencia.- Se define como cualquier tipo de actividad ilegal que utilice internet, una red pública o privada o un sistema informático [13].

Clonación (tarjetas).- Consiste en la duplicación de tarjetas de crédito o débito utilizando un dispositivo lector de bandas magnéticas, sin el consentimiento del dueño de la tarjeta [14].

Cortafuego.- Es una Herramienta de seguridad que controla el tráfico de entrada/salida de una red [15].

Criptografía.- Ciencia que estudia la manera de cifrar y descifrar los mensajes para que resulte imposible conocer su contenido a los que no dispongan de unas claves determinadas [16].

Directorio Activo.- Implementación de Microsoft del servicio de directorios LDAP para utilizarse en entornos Windows. Permite a los administradores poder implementar políticas a nivel empresa, aplicar actualizaciones a una organización completa y desplegar programas en múltiples computadoras [17].

Escáner.- Es un dispositivo que se utiliza para convertir, a través del uso de la luz, imágenes o documentos impresos a formato digital [18].

Esteganografía.- Es la ciencia de ocultar mensajes u objetos dentro de otros, llamados portadores, de modo que no se perciba su existencia a simple vista [19].

Exploits.- Software malicioso que se usa para tomar ventaja de bugs, fallas y vulnerabilidades existentes en programas o sistemas [20] [21].

Firewire.- Es un tipo de canal de comunicaciones externo caracterizado por su elevada velocidad de transferencia, empleado para conectar ordenadores y periféricos a otro ordenador, utilizando el Estándar IEEE 1394 [22].

Firma Digital.- Método que asegura la autoría del remitente en mensajes y documentos a través de una función criptográfica [23].

Flujos alternativos de datos.- Una característica del sistema de archivos NTFS que permite almacenar información y metadatos de manera oculta en un archivo [24].

Gusanos.- Es un software malicioso que reside en la memoria y que tiene la habilidad de duplicarse y propagarse por sí mismo, sin la intervención del usuario, existiendo dos tipos: el que consume recursos en el computador y el

que se propaga por una red auto replicándose enviando copias de sí mismo a otros nodos [25].

Hacker.- Término para designar a alguien con talento y conocimiento, especialmente relacionado con las operaciones de computadora, redes y seguridad [26].

Hash.- Algoritmo para generar claves para identificar de manera única a un documento, registro o archivo [27].

Log.- Archivo que registra movimientos y actividades de un determinado programa [28], usuario o proceso.

Malware.- Es una variedad de software que tiene como finalidad infiltrarse, dañar o causar un mal funcionamiento en un ordenador sin el consentimiento de su propietario, los virus y gusanos son ejemplos de este tipo de software [29].

Máquinas Virtuales.- Es la simulación de un computador real con todas sus características y funcionalidades [30].

Metadatos.- Son datos que describen o definen algún aspecto de un recurso de información (como un documento, una imagen, una página web, etc.) [(31)].

Phishing.- Es una modalidad de estafa informática que utiliza como medio un mensaje de texto, una llamada telefónica, una página web falsa, una ventana emergente o la más usada el correo electrónico suplantando la identidad de entidades o personas, con el objetivo de obtener de un usuario sus datos, claves, números de cuentas bancarias, números de tarjetas de crédito, identidades mediante el correo electrónico y servicios de mensajería instantánea y usar estos datos de manera fraudulenta [(32)].

Phreaking.- Actividad de manipular sistemas telefónicos complejos por personas que conocen el funcionamiento de teléfonos de diversa índole, tecnologías de telecomunicaciones, funcionamiento de compañías telefónicas, sistemas que componen una red telefónica y electrónica aplicada a sistemas telefónicos [(33)].

Script .- son un conjunto de instrucciones generalmente almacenadas en un archivo de texto que deben ser interpretados línea a línea en tiempo real para su ejecución, se distinguen de los programas, pues deben ser convertidos a un archivo binario ejecutable para correrlos [(34)].

Sistema Biométrico.- Es un sistema de autenticación para reconocimiento único de humanos, mediante huella digital, reconocimiento de rostro, reconocimiento de voz, reconocimiento de iris (ojo), entre otros [(35)].

Software.- o programa, es un conjunto de componentes lógicos necesarios que hacen posible la realización de tareas en una computadora [(36)].

Suma de Verificación.- Es una medida de seguridad que permite verificar que los datos no hayan sido modificados desde su publicación. El proceso consiste en sumar cada uno de los bytes y almacenar el valor del resultado. Posteriormente se realiza el mismo procedimiento y se compara el resultado con el valor almacenado, si ambas sumas concuerdan se asume que los datos no han sido corruptos [(37)].

Virus.- Un virus informático es software malicioso que necesita de la intervención del hombre para propagarse, se adjunta a un programa o archivo para replicarse a sí mismo y continuar infectando el ordenador [(38)].

Vulnerabilidades.- Es una debilidad en un sistema que puede permitir a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones [(39)].

ABREVIATURAS

ADS: Alternate Data Streams (Flujo Alternativo De Datos), son una característica del sistema de archivos NTFS de almacenar metadatos con un fichero.

ADN: Ácido desoxirribonucleico, es una macromolécula que identifica de manera única a los seres vivos mediante la información genética.

ARP: Address Resolution Protocol (Protocolo de Resolución de Direcciones), protocolo de la capa de nivel de enlace que permite identificar una MAC a partir de una dirección IP.

ASIC: Application-specific integrated circuit (Circuito Integrado para Aplicaciones Específicas), circuito integrado hecho a medida para un uso específico.

ATA: Advanced Technology Attachment (Adjunto de Tecnología Avanzada), especificaciones de diseño del interfaz IDE para conectar dispositivos de almacenamiento.

ATAPI: Advanced Technology Attachment Packet Interface (Interfaz de Paquetes De Tecnología Avanzada), estándar que designa los dispositivos que pueden conectarse a controladoras ATA (IDE).

BSA: Business Software Alliance (Alianza de Software para Negocios), es una asociación que actúa legalmente en contra de la piratería informática en el mundo.

CAT: Abreviatura utilizada para identificar la categoría de los cables de red.

CD: Compact Disc (Disco Compacto), es un medio de almacenamiento de datos digitales como audio, imágenes, videos o texto plano.

CDMA: Code Division Multiple Access (Acceso Múltiple con División de Código), término genérico para varios métodos de multiplexación o control de acceso al medio basados en la tecnología de espectro expandido.

CDR: Charging Data Record (Registro de Información para Facturación), es el registro producido por una central telefónica que contiene detalles de una llamada telefónica.

CIS: Card Information System (Sistema De Información de Tarjeta), es la estructura de la información que se encuentra almacenada en la tarjeta de memoria.

CONESUP: Consejo Nacional de Educación Superior en Ecuador, es el organismo planificador, regulador y coordinador del Sistema Nacional de Educación Superior.

CRC: Cyclic Redundancy Check (Código de Redundancia Cíclica), convierte una palabra binaria en un polinomio y utiliza un polinomio definido para la división polinomial.

DDR3: Double Data Rate Type 3 (Doble Velocidad De Datos Tipo 3), es un tipo de memoria RAM volátil, síncrona y dinámica que permite una alta velocidad de transferencia de datos.

DHCP: Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Host), protocolo utilizada en redes que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.

DVD: Digital Versatil Disc ó Digital Video Disc (Disco de Video Digital), es un formato de almacenamiento digital de datos con mayor capacidad que los CDs.

EIDE: Enhanced IDE (Extensión de IDE), es una extensión del IDE, una interfaz usada en los computadores para la conexión de discos duros.

eSATA: External Serial Advanced Technology Attachment (Dispositivo Serial De Tecnología Avanzada Externo), extensión de interfaz SATA que permite conectar dispositivos externos con el computador.

FAT: File allocation table (Tabla de Asignación de Archivos), sistema de archivos desarrollado para MS-DOS.

FTP: File Transfer Protocol (Protocolo de Transferencia de Archivos).

GB: Gigabyte, es una unidad de medida de almacenamiento de información equivalente a 10^9 bytes.

GPRS: General Packet Radio Service (Servicio General de Paquetes Vía Radio), es extensión del GSM, para la transmisión de datos no conmutada.

GSM: Global System for Mobil Communications (Sistema Global para la Comunicaciones Móviles), es un sistema estándar de telefonía celular.

HLR: Home Location Register (Registro de Ubicación Base), es una base de datos que almacena la posición del usuario dentro de la red de telefonía móvil.

HTML: HyperText Markup Language (Lenguaje de Etiquetas de Hipertexto), es un lenguaje de etiquetas utilizado en páginas web para describir la estructura y el contenido en forma de texto.

HTTPS: Hypertext Transfer Protocol Secure (Protocolo Seguro de Transferencia de Hipertexto), es un protocolo que crea un canal de comunicación seguro con el servidor web mediante encriptación.

IDE: Integrated Drive Electronics (Electrónica de Unidad Integrada), es un estándar de interfaz para la conexión de los dispositivos de almacenamiento masivo de datos y las unidades ópticas.

IDS: Intrusion Detection System (Sistema de Detección de Intrusos), es un programa usado para detectar accesos no autorizados a un computador o a una red.

IEC: International Electrotechnical Commission (Comisión Electrotécnica Internacional), es una organización de normalización en los campos eléctrico, electrónico y tecnologías relacionadas.

IEPI: Instituto Ecuatoriano de Propiedad Intelectual, es una institución comprometida con la promoción de la creación intelectual y su protección de acuerdo a la ley nacional, tratados y convenios internacionales vigentes.

IP (IP Address): Internet Protocol Address (Dirección de Protocolo de Internet), es una etiqueta numérica que identifica de manera única, lógica y jerárquica a un computador en una red.

ISO: International Standarization Organization (Organización Internacional para la Estandarización). Es la mayor organización que desarrolla y edita las normas internacionales.

ISP: Internet Service Provider (Proveedor de servicios de internet), es una empresa que brinda servicio de conexión a internet.

LAN: Local Area Network (Red de área local), es una interconexión de computadoras y dispositivos de red cuyo alcance se limita a un espacio físico, tiene un alcance aproximadamente de 200 metros.

LDAP: Lightweight Directory Access Protocol (Protocolo Ligero de Acceso a Directorios), un protocolo a nivel de aplicación el cual permite el acceso a un servicio de directorio para buscar información en un entorno de red.

MAC: Media Access Control (Control de Acceso al Medio). Se emplean en la familia de estándares IEEE 802 para definir la subcapa de control de acceso al medio.

MBR: Master Boot Record (Registro de Inicio Maestro), es un sector al principio del disco duro que contiene una secuencia de comandos necesarios para cargar un sistema operativo.

MD2: Message-Digest Algorithm 2 (Algoritmo de Resumen de Mensaje 2), es una función de hash criptográfica, este algoritmo está optimizado para computadoras de 8 bits. El valor hash de cualquier mensaje se forma haciendo que el mensaje sea múltiplo de la longitud de bloque en el computador (128 bits o 16 bytes) y añadiéndole un checksum.

MD4: Message-Digest Algorithm 4 (Algoritmo de Resumen de Mensaje 4), es una función de hash criptográfica que implementa una función criptográfica de hash para el uso en comprobaciones de integridad de mensajes. La longitud del resumen es de 128 bits.

MD5: Message-Digest Algorithm 5 (Algoritmo de Resumen de Mensaje 5), es un algoritmo de reducción criptográfico que fue desarrollado por Ronald

Rivest en 1995 y está basado en dos algoritmos anteriores MD2 y MD4, este algoritmo genera un número de 128 bits basado en el contenido de un fichero que ha sido publicado en la web.

MSC: Mobile Switching Center (Centro de Conmutación Móvil), es el nodo principal para la prestación de servicios GSM / CDMA.

NTFS: New Technology File System (Nueva Tecnología De Sistema De Archivos), es el estándar de sistema de archivos usada por Microsoft Windows sustituye al FAT.

OEA: Organización de Estados Americanos.

OMC: Operation and Maintenance Center (Centro de Operación y Administración).

ONU: Organización de Naciones Unidas.

PCI: Peripheral Component Interconnect (Interconexión de Componentes Periféricos), bus de datos que sirve para conectar dispositivos de hardware a un computador.

PDA: Personal Digital Assistant (Asistente Personal Digital), dispositivo móvil que sirve como un gestor de información personal.

PIN: Personal Identification Number (Número de Identificación Personal), es un código numérico utilizado en los dispositivos móviles para identificarlos u obtener acceso a información.

PPTP: Point to point Tunnelling Protocol (Protocolo De Túnel Punto a Punto), método para implementar redes virtuales privadas.

PUK: Personal Unlocking Key (Clave Personal de Desbloqueo).

RAID: Redundant Array of Independent Disks (Conjunto Redundante De Discos Independientes), es un sistema de almacenamiento de datos que usa múltiples discos duros o SSD entre los que distribuyen o replican los datos.

SAS: Serie Attached SCSI (Interfaz de Transferencia de Datos en Serie), interfaz que sirve para mover información desde y hacia un dispositivo de almacenamiento.

SATA: Serial Advanced Technology Attachment (Dispositivo Serial de Tecnología Avanzada), estándar de conexión de discos duros.

SCSI: Small Computers System Interface (Sistema de Interfaz para pequeñas computadoras), interfaz estándar para la transferencia de datos entre distintos dispositivos del computador.

SHA: Secure Hash Algorithm (Algoritmo Seguro De Hash), es una función hash criptográfica que fue diseñado por la Agencia de Seguridad Nacional,

es similar en su forma de operación al MD-5, pero produce un resumen con un incremento de 160 bits.

SIM: Subscriber Identity Mode (Módulo de Identificación del Suscriptor), es una tarjeta inteligente desmontable usada en teléfonos móviles.

SSD: Solid state drive (Unidad de Estado Sólido), dispositivo de almacenamiento de datos.

SSL: Secure Sockets Layer (Protocolo de Capa de Conexión Segura), protocolo criptográfico que proporciona comunicaciones seguras por una red

TDMA: Time division multiple Access (Acceso Múltiple por División de Tiempo), es una técnica que permite la transmisión de señales digitales.

TB: Terabyte, es una unidad de almacenamiento de información que equivale a 10^{12} bytes.

TLC: Tratado de Libre Comercio, es un acuerdo comercial regional o bilateral para ampliar el mercado de bienes y servicios entre los países participantes.

UNAM: Universidad Nacional Autónoma de México, es la universidad con mayor reconocimiento académico tanto en Iberoamérica, como en América Latina.

UPS / SAI: Uninterrupted Power System (Alimentación Eléctrica Ininterrumpida).

URL: Uniform Resource Locator (Localizador de Recurso Uniforme), es una secuencia de caracteres, de acuerdo a un formato modélico y estándar, que se usa para nombrar recursos en Internet para su localización o identificación.

USB: Universal Serial Bus (Bus universal en serie).

VLR: Visitor Location Register (Registro de Ubicación De Visitante), es una base de datos volátil que almacena, para el área cubierta por una central de conmutación móvil, los identificativos, permisos, tipos de abono y localizaciones en la red de todos los usuarios activos en ese momento y en ese tramo de la red.

VPN: Virtual Private Network (Red Privada Virtual), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

WAP: Wireless Application Protocol (Protocolo de Aplicaciones Inalámbricas), es un estándar abierto internacional para aplicaciones que utilizan las comunicaciones inalámbricas, especifica un entorno de aplicación y de un conjunto de protocolos de comunicaciones para normalizar el modo en que los dispositivos inalámbricos se pueden utilizar para acceder a correo electrónico, grupo de noticias y otros.

XML: Extensible Markup Language (Lenguaje de Etiquetas Extensible). Separa la estructura del contenido en la creación de páginas web.

XSL: Extensible StyleSheet Language (Lenguaje Extensible de Hojas de Estilo). Especificación para separar el estilo del contenido en la creación de páginas web.

INTRODUCCIÓN

El uso de los medios tecnológicos e información digital se ha incrementado, creando nuevos nexos de comunicación, enlaces entre las instituciones, empresas y/o personas, facilitando el manejo y almacenamiento de información. De la misma manera en que se puede aprovechar la tecnología positivamente, existen personas que utilizan estos medios con fines delictivos.

Cuando se comete un delito que involucra medios tecnológicos e información digital, la manera de abordar la investigación del caso, la recolección de evidencias, o rastros dejados por el autor del delito, es diferente a la tradicional, debido a ello, se deben aplicar metodologías especializadas en el tratamiento de tecnología informática.

Por lo expuesto anteriormente, es necesario contar con un laboratorio de Ciencias Forenses Digitales, el cual debe poseer el personal, la infraestructura física y tecnológica, y las herramientas informáticas para el análisis de datos, todo ello con el fin de recolectar evidencia y darle validez en un proceso judicial.

1. PLANTEAMIENTO DEL PROBLEMA

1.1. ANTECEDENTES

Tal como expuso la Dra. Sandra Morejón (Anexo A), fiscal de la Unidad de Delitos Informáticos y Telecomunicaciones; los delitos informáticos que han sido denunciados por lo general no llegan a culminar el proceso de análisis de evidencia ya que las víctimas retiran los cargos o simplemente no les interesa continuar con el proceso porque creen que es una pérdida de tiempo y dinero. También mencionó que algunos de los tipos de delitos conocidos a través de la prensa y opinión pública son el robo de información personal en redes sociales, bypass, la clonación de tarjetas de crédito por medio de escáneres y software, phishing.

En la Fiscalía General del Guayas, la Unidad Misceláneos se encargaba de las denuncias de delitos informáticos. “Hasta ahora se registran 221 indagaciones. De ese total, el 80% proviene de la clonación y robo de dinero a través de tarjetas de crédito, como el secuestro exprés. Sin embargo, estos casos se tratan como apropiación indebida penalizada en el Código Penal”, fue la declaración al respecto de los casos de delitos informáticos registrados en la fiscalía del Guayas [40].

Esta fiscalía maneja una estructura que ha tenido que variar para mejorar los procedimientos que se llevan a cabo al denunciar un delito informático, y así llevar un mejor control de las denuncias y documentación necesaria para un proceso judicial.

1.2. OBJETIVOS

1.2.1. OBJETIVOS GENERALES

- Plantear el diseño de un Laboratorio de Ciencias Forenses Digitales acorde a la situación actual en el Ecuador.
- Definir metodologías para la búsqueda y análisis de evidencia digital.

1.2.2. OBJETIVOS ESPECÍFICOS

- Determinar la situación actual de Laboratorios de Ciencias Forenses Digitales en el Ecuador.
- Definir los procedimientos tanto técnicos como operativos para el análisis de la evidencia digital.
- Definir los conceptos fundamentales en la formación de peritos en seguridad informática.
- Plantear opciones de implementación de un Laboratorio de Ciencias Forenses digitales.
- Analizar casos basados en hechos reales de delitos informáticos.

1.3. SITUACIÓN ACTUAL

En el año 2002 fue expedida la “Ley de comercio electrónico, firmas electrónicas y mensajes de datos” [41], la cual pretende dar protección a los usuarios de sistemas electrónicos mediante la regulación del uso de la tecnología y de estos medios, esta ley es de difícil cumplimiento debido a que en Ecuador actualmente no existe un laboratorio de Ciencias Forenses Digitales, no se cuenta con la integración de la tecnología y el personal especializado para realizar un análisis exhaustivo de evidencia digital relacionada en un proceso judicial (Anexo A).

La Fiscalía del Guayas, a diferencia de la provincia del Pichincha que ya contaba con una Unidad de Delitos Informáticos, propuso la idea de crear una unidad especializada para este tipo de casos. Esta iniciativa tuvo aceptación en la Fiscalía General de Estado y tuvo como consecuencia la creación de la Unidad de Delitos Informáticos y Telecomunicaciones en el año 2010, la cual tiene como misión fundamental "Investigar, perseguir y prevenir todo lo relacionado con la llamada criminalidad informática en todos sus espectros y ámbitos" [(42)], tal y como expresa en su artículo el Dr. Santiago Acurio del Pino.

La Unidad de Delitos Informáticos y Telecomunicaciones se encarga de llevar a cabo las investigaciones para rastrear al autor del delito una vez que se haya presentado la denuncia respectiva, como parte de la investigación está la aplicación de metodologías para recolectar evidencias digitales y con esto comenzar a generar procesos judiciales.

Para llevar una estandarización de las metodologías que se aplican en la evidencia digital, el Dr. Santiago Acurio del Pino, Director Nacional de Tecnología de la Información, publicó en el año 2009 el "Manual de Manejo de Evidencias Digitales y Entornos Informáticos" [(43)], el manual pretendía ser una guía para todo el personal que

interviniese en diferentes fases de las investigaciones y para el personal de la Fiscalía que estuvieren involucrados en la investigación de los casos, cuando en una escena de delitos se encontrasen dispositivos Informáticos o electrónicos. A pesar de la existencia de este manual de evidencias digitales, éste no es aplicado actualmente (Anexo A) y por ende no existe una metodología estandarizada.

1.4. JUSTIFICACIÓN

Debido a que en la actualidad no se cuenta con un laboratorio especializado en análisis de evidencia digital, las evidencias recolectadas pierden su validez por un tratamiento inadecuado.

El proyecto busca plantear unos procedimientos en tratamiento de evidencia con la implementación de metodología técnica y operativa, definición del perfil y de los conocimientos que debe poseer un perito informático, con la finalidad de garantizar la validez y confiabilidad del informe final posterior al análisis de evidencia; el proyecto pretende diseñar un laboratorio de ciencias forenses digitales que posiblemente se pueda implementar en la ESPOL.

1.5. ALCANCE

- Consolidar información de diferentes fuentes para generar un referente en la implementación de un Laboratorio de Ciencias Forenses Digitales.
- Analizar la legislación Nacional con respecto a delitos informáticos, y realizar comparaciones con legislaciones y convenios internacionales para determinar brechas legales.
- Definir el perfil ideal de un perito informático.
- Definir las metodologías de tratamiento de evidencia que se ajuste mejor a la situación actual.
- Realizar plan de factibilidad para la implementación del laboratorio de Ciencias Forenses Digitales en la ESPOL.

2. DELITO INFORMÁTICO

Los delincuentes informáticos afectan a los usuarios de medios digitales utilizando diferentes modalidades de delitos informáticos, ampliando el campo en el que incurren este tipo de delitos, por esto existen varios enfoques y criterios al momento de definirlos y clasificarlos según organismos y expertos en el tema, analizaremos dichos aspectos en este capítulo.

2.1. CONCEPTO DE DELITO INFORMÁTICO

Existen varios puntos de vista al momento de definir lo que es un delito informático, lo cual dificulta la creación de una definición universal, siendo así, se han creado conceptos o definiciones que tratan de ajustarse a la realidad jurídica de cada país. Un ejemplo de esto es la aportación de Wikipedia que define al delito informático como *"*el crimen genérico o crimen electrónico, que agobia con operaciones ilícitas realizadas por medio de Internet o que tienen

como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet" [44]. Por contrapartida, el Convenio de Ciberdelincuencia del Consejo de Europa define a los delitos informáticos como: "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos" [45].

En todas estas definiciones queda claro que los delitos informáticos atentan contra la privacidad de la información y utilizan medios tecnológicos como el internet y las redes para cometer actos ilícitos.

2.2. TIPOS DE DELITOS INFORMÁTICOS

Presentaremos algunas formas de clasificación de delito informático, según la ONU y la opinión de algunos expertos, las mismas que serán expuestas a continuación:

La ONU (Organización de las Naciones Unidas) [46] reconoce y clasifica a los delitos informáticos de la siguiente manera:

Fraudes cometidos mediante manipulación de computadoras, dentro de este tipo de delito se encuentran cuatro formas de llevarlos

a cabo. ***La manipulación de los datos de entrada,*** más conocida como sustracción de datos, se caracteriza porque es fácil de cometer y difícil de descubrir, no requiere conocimientos técnicos de informática, pudiendo ser realizado por cualquier persona que tenga acceso a los datos. ***La manipulación de programas,*** la cual consiste en modificar o añadir programas y rutinas en los sistemas. Se caracteriza por pasar inadvertido, es realizada por delincuentes que tienen conocimientos concretos de informática. ***La manipulación de datos de salida,*** que consiste en fijar un objetivo al funcionamiento del sistema informático, utilizando para ello equipos y programas especializados para codificar información electrónica falsificada en las bandas magnéticas de tarjetas bancarias y de crédito. Además existe ***la manipulación informática*** que es una técnica que consiste en ir sacando transacciones financieras apenas perceptibles de una cuenta y transferirlas a otra, aprovechando repeticiones automáticas de los procesos de cómputo.

Las falsificaciones informáticas, que pueden ser clasificadas de la siguiente manera: ***como objeto***, para la alteración de datos de los documentos almacenados en forma computarizada o ***como instrumentos***, donde se utilizan las computadoras para falsificar documentos de uso comercial.

Los daños o modificaciones de programas o datos computarizados, encasillados en este tipo de delitos encontramos: ***el sabotaje informático***, el cual consiste en borrar, suprimir o modificar sin los debidos permisos funciones o datos de un computador con el fin de obstaculizar el funcionamiento normal, utilizando para ello virus, gusanos y bombas lógicas o cronológicas, ***el acceso no autorizado a servicios o sistemas informáticos***, en el cual se puede acceder a los sistemas aprovechando las vulnerabilidades en las medidas de seguridad o en los procedimientos del sistema. De la misma manera, ***la reproducción no autorizada de programas informáticos*** significa una pérdida económica sustancial para los propietarios legítimos.

Por otro lado existe también la clasificación de los delitos informáticos según la opinión de algunos expertos.

El Dr. Julio Téllez Valdez, investigador del Instituto de Investigaciones Jurídicas de la UNAM, clasifica a los delitos informáticos basándose en dos criterios [47] [48]: ***Como instrumento o medio***, que aplican conductas criminales que usan las computadoras como método, medio o símbolo para cometer un acto ilícito, como por ejemplo la falsificación de documentos digitalmente, la variación

de la situación contable y la intervención de líneas de comunicación de datos o teleprocesos. ***Como fin u objetivo***, donde las conductas criminales van en contra de la computadora o programas como entidad física como por ejemplo instrucciones que producen un bloqueo parcial o total del sistema, la destrucción de programas por cualquier método y el atentado físico contra la computadora, sus accesorios o medios de comunicación.

Finalmente, la Doctora en Derecho María Luz Lima, catedrática de Derecho Penal, Penitenciario y Criminología en la Facultad de Derecho de la UNAM y actualmente presidenta de la Sociedad Mexicana de Victimología y Vicepresidenta de la Sociedad Mundial de Victimología, presenta una clasificación diferente [47] [49]: Los delitos informáticos ***como método***, donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito, ***como medio*** en los cuales para realizar un delito utilizan una computadora como medio o símbolo, y ***como fin*** que son dirigidos contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

3. LEGISLACIONES, CONVENIOS Y ORGANIZACIONES

Existen múltiples y variadas legislaciones a nivel nacional e internacional relacionadas con los delitos informáticos y digitales. Entre ellas podemos destacar como ejemplos:

3.1. LEGISLACIÓN NACIONAL

Ley Orgánica de Transparencia y Acceso a la Información Pública [(50)]**,** la cual garantiza el derecho fundamental de las personas para acceder libremente a la información de entidades del sector público, las mismas que deben publicar información acerca de la organización interna, directorio, remuneraciones, servicios que ofrece, contratos colectivos, formularios, presupuesto anual,

auditorias, procesos de contratación, incumplimiento de contratos, créditos internos y externos, rendición de cuentas, viáticos y del responsable de la información y además mantenerla actualizada.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos **(41),** la cual regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluyendo el comercio electrónico y la protección a los usuarios de estos sistemas.

Ley de Propiedad Intelectual **(51),** que garantiza y reconoce los derechos de autor y los derechos de los demás titulares sobre sus obras. El Instituto Ecuatoriano de Propiedad Intelectual (IEPI) es el organismo que a nombre del Estado protege los derechos de propiedad intelectual. El robo de información digital puede tratarse como una violación de la propiedad intelectual, ya que se trataría de información personal y de gran importancia para su propietario.

Ley Especial de Telecomunicaciones **(52),** la cual tiene por objeto normar en el territorio nacional la instalación, operación, utilización y desarrollo de toda transmisión, emisión o recepción de signos,

señales, imágenes, sonidos e información de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos.

Ley de Control Constitucional (Habeas Data) [(53)]**,** la cual establece que cualquier persona natural o jurídica sean nacionales o extranjeras y quieran acceder a documentos, bancos de datos e informes que estén en posesión de entidades públicas, de personas naturales o jurídicas privadas, conocer el uso y finalidad que se les haya dado o se les esté por dar, podrán interponer el recurso de hábeas data para requerir las respuestas y exigir el cumplimiento de las medidas tutelares prescritas en esta Ley, por parte de las personas que posean tales datos o informaciones.

Código Penal Ecuatoriano [(54)]**,** en el cual no se encuentran estipuladas sanciones específicas para delitos informáticos, por lo tanto no son sancionados adecuadamente o en relación a la gravedad del delito.

3.2. EJEMPLOS DE LEGISLACIÓN INTERNACIONAL

Al igual que en Ecuador existen diversas legislaciones que puede ser utilizadas para perseguir el delito informático, a nivel internacional podemos también encontrar otras entre las que destacamos:

Chile**,** por ejemplo fue el primer país latinoamericano en expedir una "Ley contra los delitos informáticos" (55) el 28 de Mayo de 1993, la cual consta de cuatro artículos en los que se castigó conductas ilícitas como: la inutilización o destrucción de un sistema de tratamiento de información o sus componentes afectando el correcto funcionamiento del sistema, al igual que la interferencia, intercepción o acceso a un sistema de información con el fin de apoderarse de datos almacenados en el mismo, también sancionó el daño o destrucción de datos, así como la revelación o difusión de datos contenidos en un sistema de una manera malintencionada.

En ***Argentina,*** en Junio del 2008 se promulgó la "Ley No 26388" (56) con reformas al Código Penal modificando delitos existentes e incluyendo el alcance de los términos documento, firma, suscripción, instrumento privado y certificado, y de esta manera contemplar el uso de nuevas tecnologías. Esta reforma contempló los siguientes delitos: La pornografía infantil mediante el uso de internet u otros medios

digitales, el robo y acceso no autorizado de información almacenada digitalmente, fraude y sabotaje informático, interferencias en comunicaciones, entre otros.

En ***Colombia,*** el 5 de enero de 2009, el Congreso de la República promulgó la "Ley 1273" [(57)], la cual modificó el código penal adicionando nuevas sanciones en casos relacionados con los delitos informáticos, buscando proteger la información y preservar los sistemas de tecnologías de información y comunicaciones. Esta ley contempla dos capítulos: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", y "De los atentados informáticos y otras infracciones".

En ***Estados Unidos,*** el Acta de fraude y abuso informático [(58)] fue aprobada por el Congreso de los Estados Unidos en 1986 para castigar los delitos federales relacionados con ordenadores, también la sección 1030 "Fraude y actividad relacionadas con ordenadores" fue modificada en el 2001 por la "Ley para unir y fortalecer a América proveyendo las herramientas apropiadas requeridas para interceptar y obstaculizar el terrorismo" (USA PATRIOT Act. 2001), esta modificación castigaba:

- Al que con conocimiento de causa accede a una computadora sin autorización o excediendo el acceso autorizado y obtiene datos de seguridad nacional.
- Al que intencionalmente accede a una computadora sin autorización y obtiene datos de instituciones financieras, información de cualquier departamento o agencia de los Estados Unidos, información de computador protegido con comunicación interestatal o internacional.
- Al que intencionalmente accede a una computadora no pública sin autorización del gobierno, entre otros delitos.

En Europa también existe legislación al respecto por ejemplo, ***Alemania*** adoptó la Segunda Ley contra la Criminalidad Económica [(59)] el 15 de mayo de 1986, la cual reformó el Código Penal para contemplar los delitos de espionaje de datos, fraude informático, falsificación de evidencia, alteración de datos, sabotaje informático, etc.

En ***Austria*****,** la Ley de Reforma del Código Penal [(60)] del 22 de diciembre de 1987 sancionó la destrucción de datos que incluye datos personales, no personales y programas, y la estafa informática la cual sanciona a aquel que cause prejuicios a terceros alterando el

procesamiento automático de datos ya sea por ingreso, borrado o modificación de los mismos.

Francia, a través de la Ley No. 88-19 [(61)] de 5 de enero de 1988 sobre el fraude informático contempló: la intromisión fraudulenta para suprimir o modificar datos, la obstaculización o alteración de un sistema de procesamiento de datos automáticos, el sabotaje informático y la falsificación de documentos informáticos, como delitos penados.

España, posiblemente el país que tiene mayor experiencia en casos de delitos informáticos en Europa [(62)], a través del Código Penal, sancionó el daño, alteración o inutilización de datos, programas o documentos electrónicos ajenos, violación de secretos, espionaje informático, divulgación de datos, estafas valiéndose de manipulación informática.

3.3. CONVENIOS INTERNACIONALES

Debido a que muchos países del mundo optaron por la informática para el continuo desarrollo de sus actividades, existen convenios internacionales que tratan de regular y evitar que se lleven a cabo delitos informáticos.

El ***Tratado De Libre Comercio*** [(63)]**,** que propugna la existencia de "condiciones de justa competencia" entre las naciones participantes y ofrece no sólo proteger sino también velar por el cumplimiento de los derechos de propiedad intelectual. Esto guarda relación con los delitos informáticos, ya que afectan a la propiedad intelectual como en el robo de información y quienes violan este derecho deben ser sancionados.

El ***Convenio De Budapest*** [(64)]**,** que es el único acuerdo internacional que cubre todas las áreas importantes de la legislación relacionadas con la ciberdelincuencia, el derecho penal, el derecho procesal y la cooperación internacional. Fue adoptado por el Comité de Ministros del Consejo de Europa en su sesión Nº 109 del 8 de noviembre de 2001, se presentó a firma en Budapest, el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004.

3.4. ORGANIZACIONES INTERNACIONALES

Además de la legislación y convenios internacionales, existen organizaciones que buscan limitar y proteger contra este tipo de delitos como:

Business Software Alliance (BSA) [(65)]**,** que es una asociación que actúa legalmente en contra de la piratería informática en el mundo,

actúa para proteger los derechos de propiedad intelectual de los miembros proveedores de software, hacer cumplir la legislación acerca del derecho de autor y fomentar su cumplimiento, además utiliza lo último en tecnología para rastrear las descargas ilegales de software y la distribución de software pirata en Internet a través de sitios de subastas.

Organización de Naciones Unidas (ONU) **[(66)],** que es una asociación de gobierno global que facilita la cooperación en asuntos como el Derecho Internacional, la paz y seguridad internacional, el desarrollo económico y social, los asuntos humanitarios y los derechos humanos. Reconoce varios tipos de delitos informáticos los cuales son mencionados en el capítulo 2.2.

Organización de los Estados Americanos (OEA) **[(67)],** que está comprometida con el desarrollo e implementación de la estrategia Interamericana para combatir las amenazas a la seguridad cibernética. Esta estrategia reconoce la necesidad de que todas las personas involucradas en las redes y sistemas de información sean conscientes de sus funciones y responsabilidades con respecto a la seguridad, con el fin de crear una cultura de seguridad cibernética.

4. ESTUDIO DE LA CIENCIA FORENSE DIGITAL

Para iniciar en la investigación de casos de delitos informáticos se requiere conocer el concepto de ciencia forense digital, las fases del análisis forense digital que se presentan en la escena del crimen y en el laboratorio, así como también conocer los objetivos que se deben alcanzar con el análisis, todos estos puntos se detallan en este capítulo.

4.1. CONCEPTO DE CIENCIAS FORENSES

El Dr. Santiago Acurio del Pino, Director Nacional de Tecnología de la Información define a las ciencias forenses como “la utilización de procedimientos y conocimientos científicos para encontrar, adquirir, preservar y analizar las evidencias de un delito y presentarlas apropiadamente a una corte de Justicia” [(68)]. También se podría definir a las ciencias forenses como los métodos, técnicas y

conocimientos aplicados para el análisis y tratamiento de la evidencia encontrada con el fin de darle la validez necesaria ante un proceso legal.

4.2. CONCEPTO DE CIENCIA FORENSE DIGITAL

Basándonos en las definiciones anteriores de Ciencias Forenses, podemos extrapolar una definición de Ciencia Forense Digital como: Una investigación minuciosa de medios digitales, datos procesados electrónicamente, de toda evidencia digital encontrada con el fin de que pueda ser utilizada en un proceso legal. Así mismo, en la publicación "Introducción a la Informática Forense" [(69)] se define Ciencia Forense Digital como la forma de aplicar conceptos, estrategias y procedimientos de la criminalística tradicional en medios informáticos especializados, con el objetivo de esclarecer hechos que puedan catalogarse como incidentes, fraudes o uso indebido de los mismos ya sea en el ámbito de la justicia especializada o en materia de administración de la seguridad informática de las organizaciones.

4.3. FASES DEL ANÁLISIS FORENSE DIGITAL

El análisis forense digital se compone de fases, que debido a la naturaleza de los crímenes y conductas que investigan se pueden

presentar en dos lugares: Escena del crimen y Laboratorio Forense (70) (71).

En la ***escena del crimen*** se encuentran normalmente las fases que tienen como objetivo proteger el estado de la escena de tal manera que no afecte la identificación y recolección de evidencias. Se debe asegurar la escena del crimen, ya que se encuentran las pruebas que podrían ser tomadas como evidencia digital, y por lo tanto se deben tomar las precauciones necesarias para preservarlas y así evitar la modificación o destrucción de las mismas. También es necesario identificar los sistemas de información que posiblemente contengan información relevante, todo tipo de dispositivo electrónico como un computador, celulares, agendas electrónicas, dispositivos externos de almacenamiento como memorias USB, discos duros, CDs y DVDs. Para la recolección de pruebas se debe tratar en lo posible, minimizar el impacto en la prueba original, realizando copias exactas de las evidencias para que estas sean utilizadas en los análisis forenses y la evidencia original no sea alterada.

En el ***Laboratorio Forense*** se encuentran las etapas que realizan los expertos en Ciencias Forenses Digitales, empezando por preservar las evidencias realizando la documentación de cada actividad y

procedimiento, realizando el análisis siguiendo la metodología forense especializada para obtener resultados y presentando de manera adecuada para que sean válidas en un proceso judicial.

La recuperación de las pruebas está basada en el ***Principio de Intercambio de Locard,*** criminalista francés, pionero en esta ciencia, fundador del Instituto de Criminalística de la Universidad de Lion, que establece en esencia, que "siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto" (72).

Ilustración 4. 1 - Principio de intercambio de Locard

4.4. OBJETIVOS DEL ANÁLISIS FORENSE DIGITAL

En un análisis forense se busca descubrir si se produjo el delito, los pasos que se llevaron a cabo para esclarecer cómo se produjo el delito, además se busca conocer cuando y donde se originó el ataque, el o los bancos de ataque, así como también los activos de información que se vieron afectados y la gravedad en que fueron afectados. Con todos los rastros encontrados se pretende poder identificar quien cometió el delito.

5. EVIDENCIA DIGITAL

La clave en un análisis forense digital es la evidencia digital por lo cual debemos conocer su definición y clasificación, así como también principios básicos, legales y constitucionales que se deben cumplir para asegurar su admisibilidad en la investigación y juzgamiento de un caso.

5.1. CONCEPTO DE EVIDENCIA DIGITAL

Según el “Guidelines for the Management of IT Evidence” [73], la evidencia digital es "cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático". Basándonos en este concepto, la evidencia digital es cualquier información que ha sido generada, almacenada o enviada en un sistema de información que se encuentre comprometida con el cometimiento de un delito, sea directa o

indirectamente, y que una vez obtenida, esta información se encuentra entendible para las personas o es capaz de ser interpretada por personas expertas con la ayuda de programas adicionales.

5.2. CLASIFICACIÓN

Todo investigador tiene que recordar que todo lo que se transmite, procesa o almacena en un dispositivo digital como computadora, celular, palm, queda registrado y pueden ser recuperados con la ayuda de técnicas y herramientas específicas, al ser manipulada por personal experto en el trato de evidencia digital, respetando normas y regulaciones legales esta información puede ser usada como evidencia válida dentro de un proceso judicial y es por ello que según "HB: 171 Guidelines for the Management of IT Evidence" [(73)], la evidencia digital puede ser dividida en tres categorías:

En ***registros almacenados en el equipo de tecnología informática,*** como por ejemplo correos electrónicos, archivos de aplicaciones de ofimática, imágenes. También los ***Registros generados por los equipos de tecnología informática,*** como por ejemplo registros de auditoría, registros de transacciones,

registros de eventos. Finalmente, los ***registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática,*** como por ejemplo hojas de cálculo financieras, consultas especializadas en bases de datos, vistas parciales de datos.

5.3. CRITERIOS DE ADMISIBILIDAD

En Ecuador, el Dr. Santiago Acurio, Director Nacional de Tecnología de la Información, indica que la admisibilidad de la evidencia digital está dada por varios factores como: (74)

Establecer un procedimiento de operaciones estándar como se describe en el capítulo 7, además de esto, cumplir con los principios básicos reconocidos internacionalmente en el manejo de evidencia digital, los cuales se mencionan a continuación (74):

- El funcionario de la Fiscalía o de la Policía Judicial nunca debe acudir solo al lugar de los hechos, es recomendable que asistan un mínimo de dos funcionarios. El segundo funcionario aporta con más seguridad y ayuda a captar detalles.

- Ninguna acción debe tomarse por parte de la Policía Judicial, la Fiscalía o por sus agentes y funcionarios ya que podrían alterar la información almacenada en sistemas informáticos y medios magnéticos, y perder validez ante un tribunal. En casos excepcionales una persona capacitada puede tener acceso a la información digital pero se debe describir la manera en que se realizó dicho acceso, justificar la razón y detallar las consecuencias de dicho acceso, se debe llevar una bitácora de todos los procesos con antelación que se le aplicaron a la evidencia digital.

- El fiscal del caso y/o el oficial encargado de la investigación son los responsables de garantizar el cumplimiento de la Ley y de estos principios, los mismos que se aplican a la posesión y acceso a la información almacenada en sistemas informáticos. De la misma manera, cualquier persona que acceda o copie información deberá cumplir con la ley y estos principios.

Otro criterio es el cumplimiento de los principios constitucionales y legales establecidos en Ecuador. ***Doctrina del árbol envenenado*** **(75),** la cual hace referencia a una metáfora para referirse a la

evidencia recolectada con ayuda de información obtenida ilegalmente. Es decir si la fuente de la evidencia (el árbol) se corrompe entonces la evidencia que se obtiene de la misma (el fruto) también lo está, por lo tanto esta evidencia por lo general no tiene validez ante tribunales. ***Secreto de la correspondencia*** **(76)**, expresado en el artículo 23 de la Constitución Política de la República del Ecuador, el cual garantiza la inviolabilidad y el secreto de la correspondencia, estableciendo que la correspondencia sólo podrá ser retenida, abierta y examinada en los casos previstos en la ley. ***Secreto de las telecomunicaciones*** **(77)** expresado en la Ley 184 de Telecomunicaciones (Registro Oficial No. 996) en el artículo 14, que garantiza el derecho al secreto y a la privacidad de las telecomunicaciones, prohibiendo a terceras personas interceptar, interferir, publicar o divulgar sin consentimiento de las partes la información cursada mediante los servicios de telecomunicaciones.

Finalmente, el personal encargado de la evidencia debe regirse al procedimiento determinado en la Ley de Comercio Electrónico y el Código de Procedimiento Penal.

6. PERITOS INFORMÁTICOS

Las investigaciones realizadas para esclarecer un delito informático son llevadas a cabo por técnicos expertos en el área de tecnología informática, a los cuales se denomina peritos informáticos, quienes obtienen la evidencia digital de las pruebas recolectadas en una escena del crimen y quienes deben cumplir con requerimientos legales para ser reconocidos como tales.

6.1. CONCEPTO DE PERITAJE INFORMATICO

Se puede definir al peritaje informático como el estudio o investigación, que tiene como fin la obtención de evidencias digitales relevantes para que puedan ser usadas dentro de un proceso judicial o extrajudicial y determinar la inocencia o culpabilidad de un sospechoso autor de un delito [(78)].

El peritaje informático debe ser usado en cualquier caso en el cual se incluyan equipos o medios digitales como parte del delito, ya sea como medio o fin, debe ser usado en casos civiles, en los delitos contra la propiedad privada e intelectual, espionaje industrial, protección de datos personales, fraudes, sabotajes, entre otros.

6.2. PERFIL DE UN PERITO INFORMÁTICO

El Código de Procedimiento Penal en el artículo 94 señala: “Son peritos los profesionales especializados en diferentes materias que hayan sido acreditados como tales, previo proceso de calificación del Ministerio Público” [(54)]. Así mismo Jeimy Cano, examinador Certificado de Fraude (CFE) por la ACFE (Asociación de Examinadores de Fraude Certificados), miembro de la Red Iberoamericana de Criptología y Seguridad de la Información (CriptoRED) y de la Red Latinoamericana de Especialistas en Derecho Informático, define a los peritos informáticos como “profesionales que contando con un conocimiento de los fenómenos técnicos en informática, son personas preparadas para aplicar procedimientos legales y técnicamente válidos para establecer evidencias en situaciones donde se vulneran o comprometen sistemas, utilizando métodos y procedimientos científicamente probados y claros que permitan establecer posibles hipótesis sobre el

hecho y contar con la evidencia requerida que sustente dichas hipótesis" a los cuales también los llama "investigadores en informática" [79].

De todo lo anterior, se desprende que el perito deberá estar capacitado en las técnicas y el uso de herramientas de recuperación de información, debido a que muchas veces las pruebas no están en condiciones óptimas y deben ser tratadas de tal forma que se pueda obtener la mayor cantidad de información útil para emitir criterios dentro de un proceso judicial. El perito debe también poseer conocimiento acerca de la legislación nacional, internacional, procedimientos y metodologías legales, tecnologías de información, fundamentos de criminología y criminalística, o estar bien asesorado en estos campos para que pueda presentar un informe válido en un proceso judicial. Las áreas principales que debe cubrir para llegar a ser un perito informático integral son las siguientes.

Área de tecnologías de información y electrónica. Debe conocer lenguajes de programación, teoría de sistemas operacionales y sistemas de archivo, protocolos e infraestructuras de comunicación, fundamentos de circuitos eléctricos y electrónicos y arquitectura de

computadores. Estos conocimientos son necesarios al momento de realizar el análisis y saber dónde buscar información.

Fundamento de bases de datos área de seguridad de la información. Los conocimientos principales en esta área son los principios de seguridad de la información, las políticas estándares y procedimientos en seguridad de la información, el análisis de vulnerabilidades de seguridad informática, el análisis y administración de riesgos informáticos, la recuperación y continuidad de negocio, y la clasificación de la información.

Con respecto a los conocimientos sobre ataques informáticos, el perito debe conocer acerca de técnicas de Hacking y vulneración de sistemas de información, mecanismos y tecnologías de seguridad informática, y concientización en seguridad informática.

Área jurídica. Debe tener conocimientos en teoría general del derecho, formación básica en análisis forense digital, protección de datos y derechos de autor, convergencia tecnológica, evidencias digitales y pruebas electrónicas, el análisis comparado de legislaciones e iniciativas internacionales.

Área de criminalística y ciencias forenses. El perito debe tener noción de conductas criminales, perfiles técnicos, procedimientos de análisis y valoración de pruebas, cadena de custodia y control de evidencias, fundamentos de derecho penal y procesal, ética y responsabilidades del perito, metodologías de análisis de datos y presentación de informes.

Área de informática forense. El perito debe conocer sobre esterilización de medios de almacenamiento magnético y óptico, selección y entrenamiento en software de recuperación y análisis de datos, análisis de registros de auditoría y control, correlación y análisis de evidencias digitales, procedimientos de control y aseguramiento de evidencias digitales, y sobre verificación y validación de procedimientos aplicados en la pericia forense.

Cabe resaltar que de no encontrar peritos avalados por la fiscalía en el área específica en que se llevara a cabo la investigación, el código de procedimiento penal en su Art. 95 establece que el Fiscal deberá nombrar a personas mayores de edad, de honradez reconocida y que posea conocimientos sobre el tema que deban informar.

6.3. FUNCIONES DE UN PERITO

Un perito puede cumplir una lista larga de funciones [80] [81] como son:

- Preservar la evidencia.
- Identificación y recolección de evidencias en medios digitales.
- Recuperación y análisis de datos.
- Presentación de evidencia de una manera clara y entendible
- Agente auxiliar del juez en aclaración de conceptos para que se pueda dictar sentencia.

6.4. ACREDITACIÓN PARA PERITOS

El consejo de la judicatura es el organismo encargado de organizar y controlar la asignación de peritos en territorio Ecuatoriano, de acuerdo al Código Orgánico de la Función Judicial que en su Art. 264 numeral 14 establece que a éste órgano le corresponde “Fijar el monto de las tasas y establecer las tablas respectivas por informes periciales, experticias y demás instrumentos similares necesarios en la tramitación de causas, así como sistematizar un registro de los peritos autorizados y reconocidos por el Consejo de la Judicatura como idóneos, cuidando que éstos sean debidamente calificados y acrediten experiencia y profesionalización suficiente” [82].

Para obtener la acreditación como perito, el Consejo de la Judicatura en su normativa que rige Las Actuaciones y Tabla de Honorarios de los peritos en lo civil, penal y afines, dentro de la función judicial [(82)], en su Art. 2 resolvió, que los interesados deben de cumplir con los requisitos de ser mayor de edad, la cual en Ecuador se define al cumplir 18 años, una correcta ética profesional, seriedad e imparcialidad para cumplir con las tareas asignadas y desvincularse inmediatamente al concluir su trabajo, y presentar la documentación general solicitada por el organismo la cual consiste en :

- Solicitud dirigida al Director Provincial del Consejo de la Judicatura, respectiva, especificando la especialidad pericial.
- Hoja de vida.
- Cédula de identidad y papeleta de votación, en original y copia.
- Record policial actualizado.
- Documentos que acreditan capacitación y experiencias en las materias.
- Comprobante de pago de servicios administrativos.

Además de lo anteriormente enumerado, en caso de ser peritos profesionales se requiere que el título haya sido registrado en el CONESUP, en original y copia que acredite la formación académica en la especialidad que postula.

6.5. CERTIFICACIONES PROFESIONALES

Actualmente existen organizaciones con programas estructurados para la formación de profesionales en Ciencia Forense Digital, con el fin de que los forenses que tengan esta certificación cuenten con conocimientos de metodologías aplicadas internacionalmente, a continuación detallamos certificaciones que ofrecen estas organizaciones [83] [84] [85]:

Tabla 6. 1 - Certificaciones profesionales

Certificación	Organización	Detalle
Certified Computer Examiner - CCE	ACFE Asociación de Examinadores de Fraude Certificados	Examinador digital certificado, profesional que utiliza las técnicas de investigación y análisis para poder proporcionar pruebas digitales
CFEC –Computer Forensic External Certification	IACIS Asociación Internacional para Sistemas de Computadoras de Información	Organización no lucrativa que ofrece reconocimiento y una certificación a profesionales del análisis forense en medios digitales
CCCI – Certified Computer Crime Investigator	HTCN High Technology Crime Network	Investigador de crímenes informáticos certificado
CHFI – Computer Hacking Forensic Investigator	EC-Council Consejo Internacional de Consultores de Comercio Electrónico	Prepara al personal para llevar a cabo investigaciones usando tecnología de Forensia digital innovadora
CFE – Certified Fraud Examiners	ACFE Asociación de Examinadores de Fraude Certificados	La ACFE provee capacitación y entrenamiento anti fraude

7. DEFINICIÓN DE LA METODOLOGÍA FORENSE DIGITAL

La aplicación de la metodología orientada al análisis de evidencia digital en sus diferentes fases, procura mantener la integridad de la evidencia original, de la misma manera que los resultados presentados al final sean íntegros, confiables y precisos. Para esto se deben cumplir principios o normas de carácter general al realizar el análisis y búsqueda de evidencias digitales, los cuales son: Evitar la contaminación de la evidencia, aplicar metodologías o procedimientos definidos como estándares y controlar la cadena de evidencia [(86)].

7.1. CADENA DE CUSTODIA

La cadena de custodia es “el procedimiento de control documentado que se aplica a la evidencia física, para garantizar y demostrar la identidad, integridad, preservación, seguridad, almacenamiento, continuidad y registro de la misma” [87]. La cadena de custodia comienza en el lugar donde se encuentra, obtenga o recolecta la evidencia física y solo finaliza cuando la autoridad competente lo ordene, durante este proceso se siguen varias etapas que presentamos a continuación: [88] [89]

7.1.1. Recolección, clasificación y embalaje de la prueba.

La cadena de custodia empieza en la escena del delito por lo cual es fundamental el aseguramiento de la misma con el fin de evitar la contaminación de la evidencia.

El personal encargado de la recolección de las pruebas en la escena, no siempre es personal técnico capacitado, sino personal del departamento de policía quienes son los primeros en llegar al lugar de los hechos, por esto se debe definir una serie de procedimientos a seguir para evitar que la evidencia digital se vea afectada en su integridad y/o admisibilidad, tales como:

- Aislar a los equipos informáticos inmediatamente de todo contacto con las personas que se encuentren en el lugar de los hechos, impidiendo que estos equipos sean utilizados nuevamente. Se debe de identificar y dejar registrado en un acta la(s) personas que trabajen en los equipos informáticos disponibles o el dueño del equipo. Si es posible, obtener en el lugar las contraseñas de las aplicaciones y dejarlas registradas en un acta de allanamiento.

- Registrar todos los elementos y fotografiarlos antes de moverlos o desconectarlos. Fotografiar las pantallas de cada uno de los equipos, si se encuentran encendidas, que se encuentren en el lugar, así como una toma del lugar completo.

- Evitar el contacto directo de la piel con el material informático presente en el lugar, es necesario el uso de guantes de látex para realizar la recolección, ya que puede existir muestras de ADN, huellas dactilares, etc., en las partes y dispositivos informáticos, como teclado, mouse, DVD, etc.

- Si se encuentran equipos encendidos no se procede a apagarlos inmediatamente, se procede como se indica en el capítulo 7.2.1 para poder obtener la evidencia y trasladarla al laboratorio. Se debe documentar la hora y la fecha del sistema antes de apagar el computador, ya que puede ser de utilidad al momento de presentar evidencias.

  En el caso de encontrar equipos apagados se procede únicamente a desconectarlos desde la toma del equipo ya que al encontrarse en este estado no incurren en el riesgo de pérdida de información. Si se tratase de una laptop se procede a quitarle la batería.

- Identificar y clasificar la evidencia encontrada de acuerdo a su naturaleza, al hacer la clasificación se debe rotular cada uno de los equipos y componentes que se van a trasladar como evidencia, y llenar el acta definida en el Anexo F.

  Usar bolsas y/o envases especiales antiestáticos etiquetados o etiquetables, para el almacenamiento de

dispositivos susceptibles a la estática tales como discos duros, CDs, DVDs, y dispositivos de almacenamiento con características electromagnéticas, ya que la mínima descarga de electricidad estática puede llegar a dañar los dispositivos.

7.1.2. Embalaje de la evidencia

Se debe de registrar el nombre del oficial encargado del embalaje, etiquetado y clasificación de la evidencia encontrada ya que él será el encargado de su traslado hasta los almacenes de custodia. En esta etapa se recomienda etiquetado y rotulación que permitan una fácil ubicación e identificación de la evidencia.

7.1.3. Custodia y traslado de la evidencia.

El oficial que realizó el embalaje, clasificación y etiquetado de la evidencia será el encargado de trasladarla al almacén del laboratorio, y este permanecerá en el lugar hasta que la evidencia sea aceptada e ingresada por la persona encargada de la custodia de la misma. En caso contrario, se documentará el cambio de custodia.

Una vez ingresada al Laboratorio de Ciencias Forenses Digitales, se procede a realizar el registro de entrada de la evidencia digital completando el formulario Ingreso de Evidencia mostrado en el Anexo B. Debe de quedar registrado el número del caso al cual pertenece la evidencia, el estado en que llego al laboratorio, el nombre de la persona que entrega la prueba en el laboratorio.

Posteriormente se procederá a almacenar la evidencia en recipientes especiales, con aislamiento y protegidos contra la estática que se puede generar en el medio, esta será almacenada en una habitación con seguridades físicas, a la cual solo podrá acceder personal del laboratorio que cuente con la debida autorización.

Para las evidencias almacenadas en el laboratorio se debe llevar un inventario llenando el formulario de Inventario mostrado en el Anexo C, con el fin de controlar las evidencias almacenadas.

Todo traslado de la evidencia dentro y fuera del laboratorio será registrado indicando el nombre de la persona encargada del

traslado de la evidencia, fecha y hora de entrega de la evidencia, y se llevará un registro de la ubicación de la evidencia durante su transporte, para así no perder nunca el rastro de la evidencia, este formulario de Entrada y Salida de Evidencia se detalla en el Anexo D.

7.1.4. Análisis de la evidencia

Para realizar el o los análisis el perito encargado debe de solicitar al almacén del laboratorio la prueba a la cual le va a efectuar los análisis, procediendo al llenado de las actas respectivas de entrega de evidencia que se encuentran en el almacén, y en las cuales se registrará el nombre de cualquier elemento del laboratorio que tenga contacto directo con la evidencia y el procedimiento y/o análisis que va a realizar.

Así mismo para evitar corromper y afectar la integridad de la evidencia al momento de realizar el análisis, es obligación del perito obtener el número de copias idénticas de la muestra, necesarias para realizar los análisis respectivos.

Toda persona que reciba una evidencia física por parte del almacén debe de revisar el recipiente que la contiene antes de

registrar el recibido de la evidencia, y registrará las condiciones en que encuentra la evidencia en el formato que maneja el laboratorio. Esta evidencia podrá ser sacada de su almacenaje y podrá ser abierta únicamente por el perito designado para su análisis.

El perito encargado del análisis de la evidencia digital tiene la obligación de llevar una bitácora de análisis como lo muestra el Anexo E, en la cual se registrará cada uno de los procedimientos que se realizan sobre la evidencia, así como la justificación del análisis, las observaciones o inconvenientes que se presenten durante el análisis.

Posterior a la finalización del análisis, toda evidencia debe ser devuelta al almacén del laboratorio para su almacenaje, el encargado del almacén debe de registrar el ingreso de la evidencia y debe de etiquetarlas con una codificación para que sea posible su ubicación para nuevos análisis o para su destrucción.

7.1.5. Custodia y preservación final hasta que se realice el debate.

La evidencia tendrá que ser recibida por el personal encargado del almacén del laboratorio, el cual debe de registrar la fecha y hora de recepción del material así como el nombre del perito que hace entrega de la misma y verificar el estado en que fue recibida y almacenarla siguiendo códigos que faciliten la localización para futuros análisis y/o destrucción según sea el caso.

7.2. PROCEDIMIENTOS TÉCNICOS

Los procedimientos técnicos aplicados a las evidencias digitales deben ser implementados guardando la integridad y confiabilidad de las evidencias digitales.

7.2.1. Recolección de evidencia digital

Se deben tomar decisiones y precauciones para mantener la evidencia intacta y libre de contaminación externa, una de las primeras decisiones que se debe tomar es con respecto a un computador encontrado en la escena de los hechos, ya que se debe de tomar en cuenta que si es apagado inmediatamente

puede existir pérdida de memoria RAM y si no se apaga existiría la posibilidad de que se ejecute una bomba lógica.

Para apagar el computador, que es evidencia se recomienda seguir los siguientes pasos:

- No apagar el equipo desde el botón que cumple esta función.
- Si el computador no se encuentra bloqueado, se debe poner el computador en modo suspensión. En caso contrario, desconectar el cable de alimentación eléctrica desde la fuente del poder del computador, de esta manera los datos pasan al disco duro.

Al finalizar el allanamiento, para el traslado de las pruebas se procede como se indica en la sección 7.1.1 de la cadena de custodia para que una vez que las pruebas se encuentren en el laboratorio se pueda proceder al análisis.

Realizar copias de la prueba original.

De los elementos donde se espera encontrar pruebas, se debe realizar por lo menos una copia del original sobre la que se trabajará.

La copia de las evidencias digitales como información en archivos de texto, imágenes, entre otros que están almacenadas en discos duros debe ser realizada mediante software especializado que no altere la evidencia y esta pueda ser aceptada en un proceso judicial [90] [91].

La copia del contenido original incluye archivos ocultos, registros, archivos corruptos, archivos borrados y que aún no hayan sido sobrescritos. Se utiliza el método CRC para validar que es fiel copia del original.

Para realizar la copia del contenido original del computador, se debe extraer el disco duro siempre tomando las medidas de seguridad adecuadas para proteger la evidencia. Si no es posible extraer el disco duro, se debe modificar la secuencia de arranque en el BIOS del sistema y arrancar con un sistema operativo desde un CD, sin instalar nada en el sistema.

Para realizar la imagen del disco original se pueden tomar varias alternativas, dependiendo del equipamiento del laboratorio.

Opción 1: Se puede usar un cable convertidor (IDE o SATA) a USB, enclosure, conexión de red, conexión Ethernet, cable cruzado, USB, etc., para transferir el contenido del disco mediante software como el Encase (capítulo 8.3).

Opción 2: Se hace uso de la herramienta duplicador Forensic Talon kit (capítulo 8.2), que facilitara la obtención de la imagen del disco duro.

Desconectar el disco duro original y almacenarlo adecuadamente, con las seguridades antiestáticas.

Copia de información de dispositivos de mano como celulares, PDAs y PocketPCs [91]***.*** Para crear una imagen de estos dispositivos se utiliza software especializado que realiza copias completas de la información almacenada en la memoria de estos dispositivos, incluyendo aplicaciones, datos del usuario, calendario y tareas.

De la misma manera se obtiene información del equipo, como versión del sistema operativo, modelos del dispositivo, tipo de tecnología que utiliza y el fabricante.

Retención de tiempos y fechas [91]***.*** Durante el análisis, siempre que sea posible se debe trabajar con zonas de tiempo GMT o cualquier otro estandarizado. El delito puede involucrar varias zonas de tiempo y usando una estandarizada puede ser un punto de referencia que haga el análisis de las evidencias más sencillo.

Generar los procesos de suma de verificación criptográfico de la evidencia digital (copia y original) [91]***.*** Se genera un proceso de suma de verificación de la evidencia original y de las copias para garantizar que esta no ha sido alterada durante el análisis, para esto usamos el algoritmo de suma de verificación MD5.

7.2.2. Identificación de las evidencias digitales

Debido a que en los sistemas de información es posible encontrar evidencia digital heterogénea, lo mejor es realizar una clasificación de las evidencias digitales en evidencias digitales en medios volátiles y en medios no volátiles.

Las evidencias digitales en medios volátiles desaparecen ante la falla de alimentación eléctrica o falla de conexión y es posible

obtenerlas en diferentes lugares (Anexo U). Para obtener esta información disponemos de software como por ejemplo Deft Extra (Anexo O), que es una colección de herramientas con las cuales podemos obtener registros de las actividades del computador, tiempos en los que ha estado encendido y que usuario lo hizo, etc.

Ya que es información volátil, se deben realizar los pasos para preservación de evidencia, de esta manera los datos pasan al disco duro y la evidencia pasa a ser tratada como información en un medio no volátil. Las evidencias no volátiles perduran aún con la interrupción de alimentación eléctrica y es posible obtenerlas en diferentes lugares como se detalla en el Anexo U [92].

7.2.3. Análisis de las evidencias digitales

La evidencia digital normalmente se forma por el contenido de los ficheros o datos y la información sobre los ficheros (metadatos). Basándose en estas evidencias el investigador debe tratar de contestar las preguntas de: [91]

- ¿Qué?: Determinar la naturaleza de los eventos ocurridos.

- ¿Cuándo?: Reconstruir la secuencia temporal de los hechos.
- ¿Cómo?: Descubrir que herramientas o piezas de software se han usado para cometer el delito.
- ¿Quién?: Reunir información sobre los involucrados en el hecho.

Durante el análisis se extrae información relevante del caso para recrear la cadena de eventos sucedidos, por lo tanto se requiere noción de lo que se está buscando y como obtenerlo.

Categorías de datos.

Los datos se dividen en varias categorías para facilitar la búsqueda de la evidencia, ya que existen grupos clasificados [91].

Datos lógicamente accesibles: Los cuales son almacenados en dispositivos de almacenamiento internos, externos y extraíbles. En estos datos pueden existir algunas dificultades en estos datos como una gran cantidad de información a analizar, la posibilidad que los datos estén cifrados o que existan datos corruptos o que incluyan alguna trampa como código hostil, que

al producirse cierta situación puede hacer que se formatee el disco duro.

Datos que han sido eliminados: Mientras los datos no hayan sido completamente sobrescritos se pueden recuperar. Para recuperar los datos que han sido eliminados se utilizan herramientas de software (capítulo 8.3) que permiten recuperar archivos incluso después de haber formateado el disco duro.

Datos en "ambient data": Datos en espacio no asignado, archivos de intercambio, espacio entre sectores, entre particiones, flujos alternativos de datos, etc. Para recuperarlos se necesita software especial (capítulo 8.3).

Datos ocultos: Los forenses informáticos pueden usar técnicas esteganográficas para buscar y detectar información oculta en los sistemas o ficheros (Anexo J).

Elementos a analizar según el tipo de sistema (Anexo K).

Se deben analizar los elementos según el tipo de sistema, ya que contienen información distribuida de diferente manera. En los sistemas operativos como MS Windows o Unix/Linux,

existen diferentes tipos de ficheros y registros que proporcionan información descriptiva importante.

Existen diferentes tipos de redes inalámbricas, conexiones, de donde se obtiene información de tarjetas, logs, módems, etc. Para determinar información de las comunicaciones existentes que se realizan desde el ordenador.

En el caso de los dispositivos móviles se pueden obtener memorias, chips, tarjetas SIM donde se almacena la información personal que contiene y las actividades realizadas mediante este dispositivo.

7.2.4. Análisis de dispositivos móviles

El dispositivo debe ser totalmente cargado previo al examen, se debe considerar tener una fuente de alimentación de energía fija o portátil. El análisis se debe empezar con una copia de la información que se extrae del dispositivo, el tipo de información que puede encontrarse y los pasos para encontrarla se detallan en el Anexo P.

Los dispositivos móviles cuentan con tres tipos de almacenamiento [93]: Tarjeta SIM, memoria externa y memoria interna.

En las tarjetas desmontables SIM de los teléfonos móviles podemos encontrar evidencia registrada en la información del servicio, el listado de llamadas, directorio telefónico y los mensajes de texto o multimedia.

En la memoria interna de estos dispositivos se almacena información como la identidad del teléfono, mensajes de texto, configuración del teléfono, grabaciones de audio, calendario, imágenes, archivos, programas, e-mail e historial web.

Existen dispositivos móviles de última generación que tienen una tarjeta de memoria externa que posee capacidad de almacenamiento para archivos personales tales como imágenes, música, video, documentos, etc.

Con la información obtenida se puede realizar una relación entre los datos encontrados y los resultados que se espera

obtener, esto lo podemos representar en una matriz de referencia.

Tabla 7. 1 - Matriz de referencia

Fuente de evidencia	¿Quién?	¿Qué?	¿Dónde?	¿Cuándo?	¿Por qué?	¿Cómo?
Identificadores de dispositivo / suscriptor	X					
Registro de llamadas	X			X		
Directorio telefónico	X					
Calendario	X	X	X	X	X	X
Mensajes	X	X	X	X	X	X
Ubicación			X	X		
Contenido de URL de web	X	X	X	X	X	X
Imágenes / video	X	X	X	X		X
Otro contenido de archivo	X	X	X	X	X	X

7.2.5. Presentación de resultados

La elaboración del reporte de los resultados detalla las evidencias encontradas durante el análisis, presenta cada procedimiento realizado a cada una de ellas, justificándolos para darle validez a la evidencia digital, replantea los hechos y determina las conclusiones.

El objetivo de presentar los resultados de las evidencias encontradas ante la corte es probar el delito que se ha

realizado, el qué, como, cuando y quien fue el autor del mismo. El éxito del caso depende en su gran mayoría de la efectividad de la presentación de los resultados.

Los informes deben presentar la información relevante de la evidencia evitando la terminología técnica, de manera clara, concisa, estructurada y sin ambigüedad para hacer su interpretación lo más sencilla posible, el lenguaje natural utilizado en la presentación facilita a que las personas en la audiencia que no necesariamente tengan conocimientos técnicos comprendan los resultados.

8. DISEÑO DEL LABORATORIO DE CIENCIAS FORENSES DIGITALES

Analizaremos las condiciones físicas, ambientales e infraestructura para la adecuación del Laboratorio de Ciencia Forense Digital, así como también las opciones de hardware y software necesarios para el proceso de análisis forense digital. Luego de analizar las opciones se seleccionará una de ellas para la implementación del laboratorio basándonos en factores prioritarios como ubicación, seguridad, entre otras.

8.1. INSTALACIONES

El Laboratorio de Ciencia Forense Digital requiere de instalaciones que cumplan con las características y acondicionamiento descritos a continuación:

8.1.1. Seguridad física de las instalaciones

Las instalaciones deben de garantizar la integridad y la seguridad de la evidencia, es por esto que contará con medidas de seguridad que permitan el acceso solo a personal autorizado, para definir las medidas de seguridad que se detallan a continuación nos ayudaremos de algunas fuentes [94] [95].

Acceso mediante sistema biométrico, y cerradura, previamente se debe haber realizado la identificación de la persona que desea ingresar. También, contará con un sistema de video de circuito cerrado, que grabará todos los acontecimientos dentro del laboratorio, todas las áreas contarán con cámaras y estas grabarán durante las 24 horas incluso si el laboratorio no se encuentra operando y solo podrán acceder a las grabaciones la persona encargada de la seguridad del laboratorio y el supervisor. Finalmente, se instalará un sistema de alarma con sensor de movimientos que se encontrará intercomunicado con la estación de policía más cercana y con un equipo de guardianía privada, los cuales atenderán cualquier alerta del laboratorio.

Todo el personal que labore dentro de las instalaciones del laboratorio deberá de portar la credencial otorgada por el laboratorio en todo momento y en un lugar visible. Por lo general no se aceptan visitas al laboratorio, pero en el caso de que alguna persona requiera comunicarse con personal del laboratorio, deberá presentar una identificación y será anunciado con esa persona para luego ser atendido en el área anexa de Control de Acceso y Entrada, ninguna persona que no labore en el laboratorio podrá ingresar a las áreas de análisis, en casos especiales se deberá solicitar una autorización del supervisor del laboratorio. Además, se llevará un registro de las personas que ingresan al laboratorio mediante el llenado de un documento de registro (Anexo H), toda persona que ingrese al área de Control de Acceso y Entrada del laboratorio quedará registrada junto con el nombre de la persona con quien se comunicó, el motivo y firmará su salida.

8.1.2. Condiciones ambientales

El laboratorio debe poseer las condiciones ambientales ideales, las cuales detallamos más adelante, como energía eléctrica, buena iluminación, ventilación, temperatura y humedad apropiados para la realización de las investigaciones,

asegurándose en todo momento que estas condiciones no invaliden el resultado de los análisis ni la calidad requerida, así mismo el estado de las evidencias digitales originales [94] [96] [97].

Un laboratorio de Ciencias Forenses Digitales debe estar preparado para el peor de los casos, puesto que se manejan dispositivos eléctricos y electrónicos susceptibles a problemas eléctricos, por ello, es primordial tomar en cuenta las siguientes condiciones para evitar que influyan en la calidad de los resultados:

- Esterilidad biológica.- Se desinfectará la superficie de trabajo, se recomienda lejía al 2%.
- Interferencia electromagnética.- Se utiliza la jaula de Faraday para blindaje contra radiofrecuencia e interferencia electromagnética.
- Suministro eléctrico.- Instalación de UPS y generador eléctrico
- Ruido y vibración.- Instalación de materiales aislantes para evitar la propagación de ruido y vibraciones dentro del laboratorio.

El sistema de climatización e instalación de filtros evita el paso de polvo, la humedad, y el sobrecalentamiento y deterioro de los equipos de cómputo que se usarán en las diferentes etapas del proceso de análisis de la evidencia, es recomendable manejar un correcto sistema de refrigeración con temperaturas que vayan de 18°C a 30°C, aunque se recomienda que se mantenga en una temperatura estable de 22°C y mantener un límite de humedad máximo del 65% dentro de las instalaciones.

Sistema de extinción de incendios que este adecuado al material eléctrico y magnético, que se va a manejar dentro de las instalaciones, para tratar de causar el menor impacto en caso de su uso, tales como polvo químico seco o bióxido de carbono , espuma, INERGEN, entre otras.

Una valoración de los costos de estos sistemas se detallan en el Anexo L de presupuesto inicial, la distribución de estos sistemas se detallan a continuación.

8.1.3. Despliegue de infraestructura en el interior de laboratorio

Las instalaciones deberán contar con elementos esenciales, tales como [98] [99]:

- Cableado de red, con puntos de red en todas las áreas del laboratorio, esta será una intranet sin acceso a internet, en la mayoría de las áreas.
- Conexión a red exterior (internet), la cual va a ser destinada para cualquier consulta, investigación, transmisión de información, que tenga que realizar el personal del laboratorio entorno a un caso en análisis o a analizar.
- Cableado telefónico para uso tanto externo como interno, uso de las líneas externas mediante la digitación de un código de seguridad, y el uso interno mediante la digitación del número de la extensión.
- Generador eléctrico propio o UPS, en caso de que falle el suministro de energía eléctrica, el generador se encontraría ubicado en un área externa al laboratorio.
- Habitaciones en lo posible sin ventanas a la parte externa del laboratorio y con divisiones para las distintas áreas son ideales para este tipo de instalaciones. Si el techo tiene cielo raso asegurarse que no existan aperturas por el cual puede caer algún tipo de contaminante o elemento que contamine la evidencia.

Las instalaciones estarán divididas en tres áreas: almacenamiento, mecánica y análisis; a continuación presentamos tres opciones de diseño, en cuanto a la distribución de las áreas mencionadas:

Diseño 1.

En el diseño uno, las divisiones son realizadas con paneles móviles, se muestra un área de control de acceso y entrada, donde se recibirán visitantes en caso de existir, se tiene una puerta que permitirá el ingreso al laboratorio. Existirá un área de almacenamiento abierta, la cual tendrá varios armarios y un mostrador donde se receptará la evidencia.

En el área mecánica estarán ubicados dos puestos de trabajo utilizados por el personal del laboratorio para el ensamblaje y desmonte de equipos. En el área de análisis también existirán dos puestos de trabajo, uno tendrá acceso a internet y el otro no.

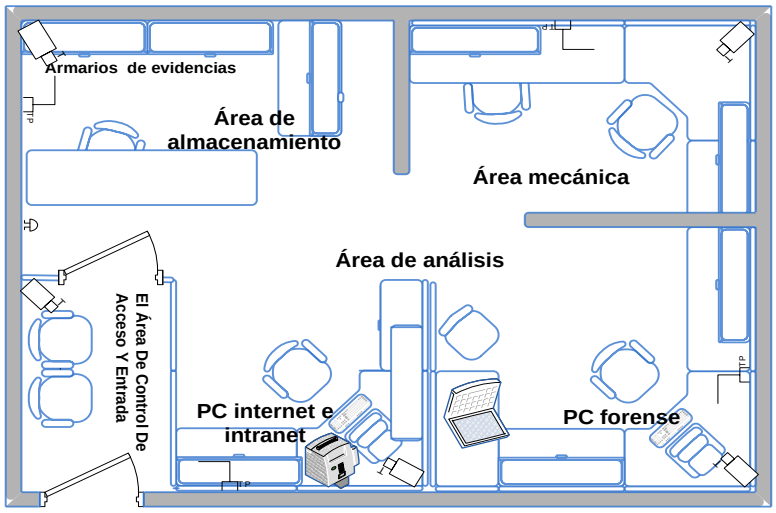


Ilustración 8. 1 - Diseño del Laboratorio de Ciencias Forenses Digitales, opción 1

Diseño 2.

En el diseño dos, se muestra un área de almacenamiento más segura, ya que previo a esta área se acondicionará un cubículo con una puerta de acceso a la ubicación de los armarios de evidencia.

Se cuenta con mayor amplitud en el área de análisis, aquí se ubicarán tres puestos de trabajo cada uno con un armario respectivo, y serán divididos con paneles móviles. Todas las áreas son de libre acceso, solo se cuenta con una puerta de entrada principal a las instalaciones del laboratorio.

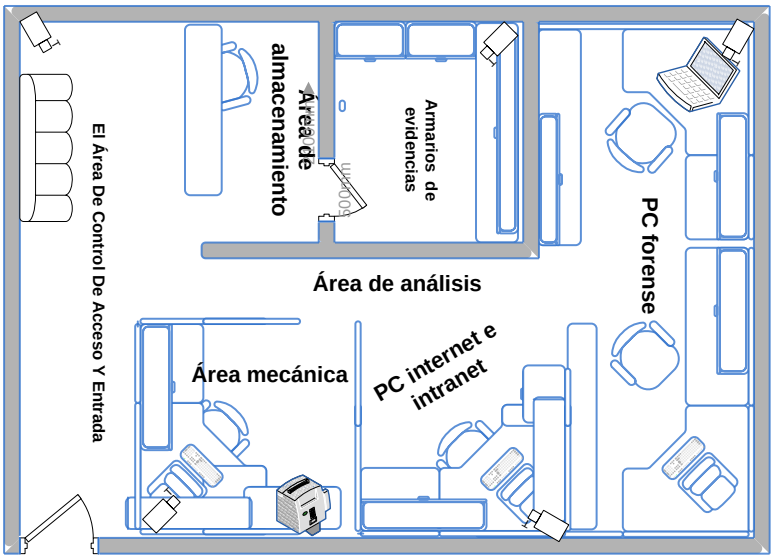


Ilustración 8. 2 - Diseño del Laboratorio de Ciencias Forenses Digitales, opción 2

Diseño 3.

En el diseño tres, se muestra un área de análisis en la que se ubicarán cuatro puestos de trabajo, con una puerta de acceso a esta área haciéndola más segura. El área mecánica contará con tres puestos de trabajo de mayor amplitud, y con una puerta individual de acceso restringiendo la entrada. El área de almacenamiento es de mayor seguridad ya que para poder ingresar a los armarios se debe de ingresar por dos puertas previas con seguridades.

En esta opción las divisiones serán hechas con paredes fijas de cemento, haciendo a esta la opción más segura, sin embargo

se convierte en la opción que genera un mayor consumo de recursos económicos, y limitaría el crecimiento futuro del laboratorio.

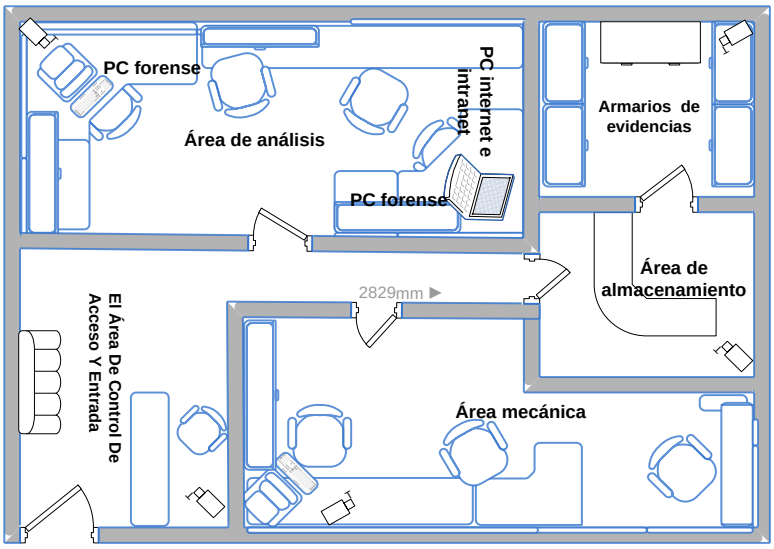


Ilustración 8. 3 - Diseño del Laboratorio de Ciencias Forenses Digitales, opción 3

Se selecciona el diseño número dos como el que mejor se adapta a las necesidades del laboratorio, ya que cuenta con seguridades en el área más crítica como es el área de almacenamiento con respecto a la opción uno, y con respecto a la opción tres supondría una menor inversión económica y facilidad de reubicación de las áreas de acuerdo a las necesidades o crecimiento del laboratorio.

8.1.4. Especificaciones generales de las opciones de instalaciones físicas para la implementación del laboratorio

Para el ***diseño del área de almacenamiento,*** tomaremos como referencia el documento “Forensic Laboratories: Handbook for Facility Planning, Design, Construction, and Moving” [(95)], del Departamento de Justicia de los Estados Unidos.

Esta área contará con seguridades físicas desde su ingreso debido a la importancia que representa el almacenamiento de la evidencia para garantizar su integridad. Además, contará con un Área de Control de Acceso y Entrada, que será el lugar donde se atenderá a las personas que soliciten alguna prueba para su análisis, ningún personal sin autorización podrá acceder más allá del Área de Control de Acceso y Entrada.

También tendrá armarios en donde se almacenará la evidencia que llegan a las instalaciones del laboratorio para el proceso de investigación y para su almacenaje posterior a los análisis, esta área tendrá acceso restringido al igual que todas las instalaciones y se registrará la hora y el nombre de la persona que acceda a ella (Anexo G).

Para evitar daños en la evidencia por condiciones ambientales se tomarán precauciones para el correcto almacenamiento de la evidencia dependiendo de la naturaleza de la misma, usando contenedores antiestáticos y/o esponja antiestática, lo que ayudará a aislar de fuentes eléctricas y de campos magnéticos, que puedan corromper la información contenida en los dispositivos digitales durante su almacenamiento y transporte.

Las puertas de acceso al almacén poseerá cerraduras tipo multilock para mantener una mayor seguridad de las pruebas, lo que garantizará que solo personal autorizado podrá ingresar y tener contacto con los contenedores de las evidencias, además se instalarán cámaras de seguridad que se encuentren registrando quienes entran y salen del almacén.

Así mismo los armarios tendrán cerraduras o candados tipo multilock como medida de seguridad, y un control escrito de acceso a los armarios, la integración de estas medidas permitirá mantener un registro de quienes acceden a los armarios para la manipulación del sistema, el acceso a estos armarios solo lo tendrá la persona encargada del almacén de la evidencia, y solo

se podrá acceder a estos armarios cuando sea necesario, almacenar nueva evidencia, extraer evidencias para los análisis, para almacenar la evidencia después del análisis, o para extraer la evidencia para su destrucción o su traslado a otras instalaciones según ordene la autoridad competente a cargo del caso.

Toda persona que ingrese a la recepción y almacén, tendrá que registrar sus datos y el motivo por el cual entra al área de almacenamiento, así mismo serán grabadas durante toda su permanencia en esta área.

En el área mecánica, se realizará el desmontaje, ensamblaje y manipulación física de un computador, en caso de que se necesite analizar un computador completo, esto es para que sus partes puedan ser analizadas por separado si las circunstancias lo ameritan. Usaremos como referencia [99], para ayudarnos al diseño de esta área.

Para llevar a cabo la tarea de desmontaje, se dispondrán de herramientas necesarias, así como de equipos especializados, entre las herramientas que se dispondrán están:

- Juego destornilladores (Estrella. hexagonal o torx, de pala, de copa y Y, entre otros)
- Pulsera Antiestática
- Soplador
- Limpia contactos en aerosol

En esta área se realizará la extracción de ciertos elementos del computador como disco duros, tarjetas de memorias, para posteriormente pasen al área de análisis.

En el área de análisis del laboratorio, se llevará a cabo el proceso de respaldo de información, copias de la evidencia original, etc. Para proceder al análisis y búsqueda de evidencia.

Para llevar a cabo todas las tareas que están incluidas en el análisis de la evidencia, esta área contará con las herramientas de análisis forenses que se dispongan tanto hardware como software. Existirán dos zonas, una de la cuales tendrá acceso a internet en la cual se podrán realizar investigaciones, que se necesiten dentro del proceso de análisis, y la otra zona no tendrá acceso a internet para evitar cualquier intervención externa en el análisis de la evidencia.

En todas las áreas, se dispondrá de cámaras de seguridad, que registrarán en video todo lo que suceda en el interior.

8.2. EQUIPOS INFORMÁTICOS

El conjunto de equipos de trabajo en el laboratorio de Ciencia Forense Digital, integra herramientas especializadas, computadores de escritorio y portátiles para llevar a cabo el proceso de análisis forense.

Herramientas de duplicación de discos con alta velocidad de copiado, conectividad con las diferentes interfaces de discos duros, adaptadores, portabilidad, esto permitirá realizar copias de discos duros los cuales se usarán para los análisis de las pruebas de una manera fácil y rápida. En el punto uno del Anexo V de Hardware, se muestra una comparación entre varias herramientas de este tipo y que nos servirá para la elaboración de las opciones de implementación mostradas en el capítulo 8.7

Además se contará con dos tipos de equipo en las instalaciones el equipo base que será una desktop y un equipo portátil que será una laptop con similares características que el equipo base. Las

características de los equipos se mostrarán a continuación, se usó como referencia para decidir las características la fuente [99]:

Equipo base forense.

Este equipo servirá para el almacenamiento de evidencia digital, reportes técnicos, para creación y ejecución de máquinas virtuales, y para operaciones que requieran una alta capacidad de procesamiento. Entre las caracteristicas que debe poseer este equipo estan: Procesador con una alta capacidad para tener una mayor velocidad de procesamiento en especial para el trabajo con audio y video, con un sistema operativo estable y capaz de ser compatible con el software forense que se va a utilizar, disco duro con gran capacidad de almacenamiento, en configuración RAID-1+0 que serán utilizados como almacen de información de casos trabajados, Y 500 GB en configuración RAID-0 que serán usados para almacenamiento de trabajo temporal o tareas especificas, memoria RAM 8 GB DDR3, puertos USB, fireware, red 100/1000, Monitor 22''.

Equipo Portatil.

Este equipo servirá para realizar trabajo de campo en caso de que se amerite, con alta capacidad de procesamiento para poder realizar las

tareas. Entre las características de este equipo tenemos: Sistema operativo estable y capaz de ser compatible con el software forense que se va a utilizar, procesador con alto poder de procesamiento para tener un tiempo de respuesta alto, disco duro con gran capacidad de almacenamiento, memoria RAM de alta velocidad, puertos USB, fireware, red 100/1000.

Accesorios adicionales.

Adicionalmente a los equipos especializados dentro del laboratorio, se deberá de contar con una serie de herramientas y suministros, que ayudarán a llevar a cabo la labor del perito, estas herramientas servirán entre otras cosas para sacar respaldos de la información relevante, la presentación de informes, imágenes de discos duros. Entre esos accesorios tenemos [(99)]: discos duro externos, grabadores de CD/DVD, adaptadores, dispositivos de almacenamiento, podemos ver una lista más detallada en el punto dos de Anexo V hardware.

8.3. SOFTWARE UTILIZADO

Existen varias herramientas de software usadas en el análisis forense digital de las cuales presentamos las características principales de algunas de ellas en la tabla que se presenta a continuación:

Tabla 8. 1 - Tabla comparativa de software

	Encase	Deft Extra	Caine	Digital Forensics Framework	Forensics Toolkit	Easy Recovery Professional	Fox Analysis	Chrome Analysis
Clonación de discos	X	X			X			
Comprobar integridad criptográfica	X	X		X	X			
Información del sistema	X	X	X		X			
Adquisición en vivo	X	X	X		X			
Recuperación de contraseñas	X	X	X		X			
Recuperación de archivos borrados	X			X	X	X		
Recuperación de emails borrados	X				X			
Análisis forense en redes	X	X	X					
Análisis forense en navegadores	X	X	X		X		X	X
Análisis de dispositivos móviles	X			X				
Análisis de firmas de archivos	X							
Búsqueda de archivos	X	X			X			
Utilitarios extras		X	X					
Reporte manual		X						
Reporte automático	X				X			
Volcado de memoria RAM			X					
Adquisición de evidencia RAM	X							
Herramientas de automatización	X							

En base a la evaluación y comparación de los software indicados en la tabla 8.1, se puede observar que existen dos herramientas de software que son los más completos en cuanto a tareas se puedan realizar, estos son el Encase y el Deft-extra, y que se puede hacer

uso de software complementario si fuese necesario para las tareas que no puedan desempeñar estas dos herramientas. La descripción y características detalladas de estos tipos de software se encuentran en el Anexo M.

Para la elección final del software que se va a usar en el laboratorio de Ciencias Forenses Digitales se basará además de las características en el costo de la licencias y la capacidad adquisitiva del laboratorio al momento de implementación, es por esto que mostramos tres opciones de implementación (Anexo N).

8.4. MATERIALES DE REFERENCIA.

Una biblioteca con libros y revistas referentes al tema de seguridad informática, análisis forense, y temas relacionados a la actividad del laboratorio [94] [95] [99].

También se contará con una base de archivos digitales con papers, mejores prácticas, normas y manuales de procedimientos en el campo Forense Digital. Este material será una buena fuente de referencia al alcance de los miembros del laboratorio, la cual se mantendrá actualizada conforme a los avances tecnológicos y disponibilidad de recursos.

8.5. MANTENIMIENTO DE EQUIPO E INSTALACIONES.

El laboratorio de Ciencia Forense Digital debe estar siempre en óptimas condiciones para asegurar la confiabilidad e integridad de los resultados que se obtengan en el análisis forense.

Para eso se deberá efectuar mantenimiento tanto en los equipos como en las instalaciones, para evitar que estos se deterioren y favorecer la vida útil, hay dos tipos de mantenimiento, preventivo y correctivo:

El mantenimiento preventivo de los equipos consiste en crear un ambiente favorable para el sistema, y prolongar la vida útil del equipo, economizando el gasto de reparaciones en los equipos así como el mantener el equipo con las protecciones ante los ataques de virus informáticos, entre las tareas del mantenimiento preventivo, están: limpieza del dispositivo, actualización del sistema operativo, parches, seguridad, antivirus, licencias y versiones, verificación de licencias activas, verificar que cumplan con las necesidades actuales de los análisis.

El mantenimiento correctivo de los equipos consiste en la reparación de los componentes de la computadora, esto va desde una pequeña soldadura, al cambio total de una tarjeta o dispositivo, ya que en muchos casos es más barato cambiar un dispositivo que repararlo.

Mantenimiento de las instalaciones

Al igual que los equipos computacionales, las instalaciones físicas del laboratorio también necesitan un mantenimiento preventivo y correctivo cuando sea el caso.

Mantenimiento preventivo de las instalaciones**,** el cual podría tomar en cuenta pintura, limpieza de pisos, paredes y/o techo, mantenimiento a los muebles de las oficinas, mantenimiento de los equipos de ventilación, tareas de reorganización del mobiliario.

Mantenimiento correctivo de las instalaciones, en el cual se podría realizar el cambio de alguna de las piezas en el laboratorio, puertas, piezas eléctricas, focos, reubicación de áreas, entre otras.

Es recomendable realizar estos mantenimientos con una periodicidad de una vez por semestre y establecerlo como política del laboratorio,

para evitar la contaminación de la evidencia durante y después del análisis forense. Se debe registrar el último mantenimiento realizado.

8.6. POSIBLES UBICACIONES EN LA ESPOL

Dentro de las instalaciones de la ESPOL se encuentran áreas disponibles que podrían ser utilizadas para la implementación del laboratorio, de las cuales mencionaremos tres áreas donde podría ser implementado el laboratorio, de estas escogeremos una como posible ubicación del laboratorio forense digital.

Una posible ubicación se encuentra en las instalaciones del CSI, en el aula que actualmente es utilizada como sala de capacitaciones, pero en caso de implementar el laboratorio el lugar podría ser ocupado para este fin, el aula está ubicada frente a la entrada principal y junto a la sala de servidores del CSI.

Dentro de las ventajas de esta opción esta el acondicionamiento, esta aula cuenta con un sistema de aire acondicionado ideal para el desempeño de las actividades a desarrollarse, además cuenta con sistema de alarma con sensores de movimiento y sistema contra incendio automático, lo cual supondría un ahorro en la inversión inicial del laboratorio. También cuenta con una habitación que se la

puede acondicionar como el almacén de evidencia, su tamaño mediano (aproximadamente 40mts^2).

Como desventajas esta la ubicación ya que hace que sea un poco complicado de llegar, para personas que no conocen la ESPOL, Cuenta con una pared completamente de vidrio que une a la sala de servidores del CSI lo cual supondría una inversión en su cambio por una pared de cemento, habría que realizar una impermeabilización de su techo ya que hay alguna filtración en época de lluvia.

La sala de ayudantes ubicada en el edificio de Gobierno de la FIEC (Edif. 15-A), en el segundo piso, que en caso de ser solicitado podría reubicarse en otra área del edificio y este salón ser asignado en su totalidad o parcialmente asignado al laboratorio de Ciencias Forenses Digitales, es otra opción de ubicación dentro del área de ingenierías.

Como ventajas, esta instalación cuenta con un sistema de aire acondicionado con alta capacidad de enfriamiento lo cual permite tener un clima ideal para el trabajo a realizar en el laboratorio, además cuenta con sistema de alarma con sensor de movimiento distribuido por toda el aula. Esta área es la más grande

(aproximadamente 90mts^2) de entre las tres mencionadas cabe recalcar que como esta área se encuentra en el segundo piso se adaptaría muy bien a las necesidades del laboratorio.

Como desventajas podríamos determinar que al encontrarse en el edificio de gobierno, es de libre acceso a los estudiantes, lo cual puede causar problemas de ruido e interrupciones en el desarrollo normal de actividades. Además esta área no cuenta con ningún tipo de divisiones por lo cual habría que hacer un acondicionamiento completo en divisiones y mobiliario. También se debe de realizar el cambio de una pared de vidrio que se encuentra en el frente de esta aula por una pared de cemento y poner las seguridades necesarias en el ingreso al lugar

La oficina del VLIR en el edificio 16C de la FIEC, actualmente es utilizada ocasionalmente y según los encargados del área, esta oficina podría ser solicitada al decanato para la implementación del laboratorio.

Como ventajas, esta área cuenta con un sistema de aire acondicionado instalado, lo cual disminuiría el presupuesto inicial, así mismo cuenta con un sistema de alarma con sensores de

movimiento lo cual reducirá el costo de la inversión inicial, además el acceso previo a las instalaciones cuenta con cerradura eléctrica y solo pueden acceder con llave o si alguien de adentro lo permite.

Algunas características que podríamos considerar como desventajas son el ruido en su exterior y que se filtra al interior del aula, ya que se encuentra en una ubicación de alta concurrencia de estudiantes puede interferir en la concentración de los peritos. Además, cuenta con una división de vidrio que separa el salón con el exterior, la cual debe ser cambiada con una pared de cemento. De las tres áreas mencionadas esta opción es la más pequeña y se necesitaría acondicionar el lugar completamente.

Evaluando las ventajas y desventajas de cada una de las tres opciones planteadas, la que más se adapta a las necesidades y requerimientos del laboratorio es el aula del CSI ya que cuenta con mayor acondicionamiento sobre las demás áreas, además el ambiente tiene poca contaminación de ruido y no existe un acceso masivo de personal que no labora en estas instalaciones.

8.7. OPCIONES DE IMPLEMENTACIÓN DEL LABORATORIO FORENSE DIGITAL EN LA ESPOL

Tomando en cuenta todas las características de diseño del laboratorio mencionadas al inicio de este capítulo, las necesidades actuales con respecto a solución de casos de delitos informáticos y los recursos con los que podríamos contar, planteamos tres opciones para la implementación de un laboratorio de Ciencias Forenses Digitales.

Se indican los precios de los elementos básicos necesarios para la implementación se detallan en el Anexo N de Opciones de Implementación, el lugar óptimo para el funcionamiento del laboratorio debe cumplir con el acondicionamiento descrito en el capitulo 8.1.2, Diseño de laboratorio de Ciencias Forenses Digitales.

Alternativa Uno: hardware especializado y software comercial.

Esta alternativa se compone de hardware forense, y software forense comercial. Por lo tanto, se requiere de una mayor inversión económica. Para esta alternativa se seleccionó al Encase como el software principal para el proceso de análisis de la evidencia ya que es la herramienta más completa y utilizada en el campo forense digital.

La alternativa uno incluye los costos de la inversión inicial, y del hardware y software que se va a utilizar en el laboratorio, lo cual da un costo total de 54.319,14 dólares.

Alternativa Dos: Hardware especializado y software libre.

Esta alternativa combina herramientas de hardware forense especializado, software forense libre y software complementario comercial y libre, esta opción requiere un poco menos de inversión ya que no sería necesaria la compra de licencias de software para su uso. Para esta alternativa se ha seleccionado como software forense el Deft-Extra ya que es una herramienta que presta una integración de varias utilidades forenses que son de gran ayuda en el momento del análisis.

La alternativa dos incluye los costos de la inversión inicial, y del hardware y software que se va a utilizar en el laboratorio, lo cual da un costo total de 45.840,64 dólares.

Alternativa Tres: Hardware básico y software libre.

Para esta alternativa escogemos solo herramientas de software libre, así como hardware básico computacional de uso diario que lo ajustaremos a las necesidades del laboratorio, no haremos uso de

equipos especializados. Esto permitirá tener un laboratorio con una inversión inferior a las otras dos opciones.

La alternativa tres incluye los costos de la inversión inicial, y del hardware y software que se va a utilizar en el laboratorio, lo cual da un costo total de 15.890,40 dólares.

De estas tres alternativas seleccionamos la primera ya que al contar con hardware y software especializado el trabajo realizado por los peritos cuenta con mayor respaldo ya que se realizará con mayor precisión y confiabilidad que genera el uso de software comercial.

9. EJEMPLOS DE ESCENARIOS DE APLICACIÓN DE LA METODOLOGÍA

Existen varios tipos de delitos informáticos como hemos descrito anteriormente, a continuación presentamos varios ejemplos basados en situaciones reales y posibles resoluciones de estos delitos aplicando la metodología descrita en el capítulo 7.

9.1. CASO PORNOGRAFÍA INFANTIL CIFRADA

La policía se encuentra en proceso de investigación de un caso de pornografía infantil, durante el allanamiento del domicilio del sospechoso se encontró un celular Nokia modelo 5310 y una PC de escritorio. Esta evidencia es entregada al Laboratorio de Ciencias Forenses Digitales para su análisis.

Definimos a continuación varios pasos a seguir para el análisis de la evidencia digital.

Análisis de celular (Anexo P)

- Se recibe la evidencia proveniente de la persona que lleva el caso llenando el formato Ingreso de evidencia del Anexo B.
- Se ingresa la evidencia al inventario del laboratorio llenando el formato del Anexo C.
- Se procede a obtener una imagen del contenido del celular para conservar la integridad de la evidencia original cumpliendo los criterios de admisibilidad detallados en el capítulo 5.3.
- Se procede a realizar el análisis sobre la imagen obtenida como se detalla en el Anexo P.
- La herramienta que usamos en este análisis nos presenta la información del dispositivo móvil clasificada de la siguiente manera:
    - Mensajes de texto
    - Directorio telefónico
    - Llamadas realizadas
    - Llamadas recibidas

- Llamadas perdidas
- Fotos
- Videos
- Audio
- Calendario
- Notas
- Tareas
- Registro de navegación web

- Determinar la información relevante con respecto al caso investigado.
- Realizar el informe de la evidencia encontrada y adjuntar el informe generado por el programa.

Análisis de PC de escritorio

- Se recibe la evidencia proveniente de la persona que lleva el caso llenando el formato Ingreso de evidencia del Anexo B.
- Se ingresa la evidencia al inventario del laboratorio llenando el formato del Anexo C.
- Obtener una imagen del disco duro del computador como se indica en el capítulo 7.2.1 y cumpliendo los criterios de admisibilidad mencionados en el Capitulo 5.3.

- Determinar información almacenada en el disco duro.
- Recuperar información que haya sido eliminada del disco duro con la ayuda de las herramientas descritas en el capítulo 8.3.
- De la información recuperada, determinar la información relevante con respecto al caso vigente.
- Con ayuda de la herramienta forense mencionada en el Anexo O se determina:
    - PC On/Off time, el tiempo en que la PC ha estado encendida, registros de horas y fechas de esta acción.
    - Obtener el registro de los logs.
    - Registro de navegación web.
    - Registro de dispositivos USB conectados.
    - Recuperación de contraseñas almacenadas en memoria.
    - Registro de puertos usados.
    - Obtención de imágenes.
- Clasificación de la información almacenada en el disco duro.

  Dentro de la información almacenada en el disco duro, se encontraron archivos encriptados. Se determinó que la encriptación era de tipo AES-256, (Anexo Q.)

Se aplican técnicas para obtener la información cifrada y se selecciona la información que sea relevante para el caso (Anexo J).

- Realizar el informe de la evidencia.

9.2. CASO RASTREO DE CORREOS OFENSIVOS

El gerente de la empresa ha recibido un correo muy ofensivo de un empleado de la empresa que se encuentra de vacaciones, resulta que en la empresa no se puede enviar correos si no se está conectado a la red interna, he conversado con este empleado quien confirma no haber enviado ningún correo de ningún lado.

Pasos a seguir:

Rastreo de correos (excepto Gmail) (Anexo R)

- Recolectar evidencia para poner la denuncia
- Ver cabecera del correo para determinar IP de origen.
- Rastrear IP con la ayuda de herramientas.
- Determinar si el correo fue enviado en el país.
- Se pueden tomar dos opciones, realizar una investigación privada o acudir a la fiscalía.
- En caso de poner la denuncia en la fiscalía, se deben presentar las evidencias encontradas que demuestren el hecho

que se va a denunciar, en este caso que se han enviado correos ofensivos desde cierta IP.

- Una vez presentada la denuncia y la evidencia, el agente fiscal emite una orden judicial para poder acudir al ISP y obtener la información necesaria.
- El ISP proporciona la información necesaria para obtener la zona de origen.
- Localizar e ir al lugar donde se encuentra el equipo al que se asignó la IP. Existe la posibilidad de que esa IP haya sido asignada a un cyber o una residencia.

    - En el caso de que esté asignada a un cyber se debe establecer los posibles escenarios del envío del correo.

      Escenario 1: Que la máquina esté comprometida dentro de una botnet (Anexo S). En este caso se debe proceder a realizar un escaneo de vulnerabilidades para determinar cuál de ellas pudo ser explotada.

      Escenario 2: El correo fue enviado directamente desde el equipo.

Debido a que el correo fue enviado desde el equipo, se puede insertar un script en el servidor de correos para obtener la cabecera del correo en caso de que otro correo sea enviado desde la misma IP.

- En el caso de que esté asignada a una residencia se debe establecer los posibles escenarios del envío del correo.

  Escenario 1: Que la máquina esté comprometida dentro de una botnet (Anexo S).

  Escenario 2: El correo fue enviado directamente desde el equipo.

  En el caso de ser una residencia se da el caso de que las IP son asignadas dinámicamente lo cual dificulta un poco más el rastreo, ya que una misma IP puede ser usada en varias ocasiones por diferentes personas, para lo cual hay que solicitar al ISP el registro de las asignaciones de esa IP con usuario y fecha.

Ya que el correo fue enviado desde el equipo, se puede insertar un script en el servidor de correos para obtener la cabecera del correo en caso de que otro correo sea enviado desde la misma IP.

9.3. CASO DESARROLLO DE RETO FORENSE DIGITAL DE LA COMUNIDAD DRAGONJAR.

Este caso es un escenario planteado por la comunidad Dragonjar como un reto de Análisis Forense Digital. DragonJAR.org [(100)] es una comunidad de investigadores, estudiantes, profesionales y entusiastas de la Seguridad Informática.

“Gracias a una denuncia por CiberBullying a la Unidad de Delitos Informáticos Lunix, se pretende llevar a cabo un Análisis Forense a un sistema propiedad de un sospechoso que tiene contacto con la víctima. Este análisis se realizará bajo la sospecha que desde éste equipo se están realizando actos delictivos y judicializables.”

“Se sospecha que éste distribuye contenido pedófilo por medio de internet”.

Este reto fue resuelto por nosotros utilizando herramientas de software libre y una máquina virtual para montar la imagen del disco, referenciamos nuestra solución al caso (Anexo T).

CONCLUSIONES

1) Según la entrevista realizada a la Fiscal Dra. Sandra Morejón, las personas consideran una pérdida de tiempo y dinero denunciar casos de delitos informáticos, motivo por el cual muchos de estos casos no son denunciados ante las autoridades competentes.

2) Se determinó que en la actualidad existe un déficit de personal capacitado y certificado como peritos informáticos que trabajen para la fiscalía, debido a esto no se aplica la metodología apropiada en el análisis de la evidencia digital lo cual se refleja en la presentación de los resultados.

3) Todo el personal que está involucrado en la investigación de un delito, el personal de la policía que realiza el allanamiento en el lugar de los hechos, y los agentes fiscales, no cuentan con la capacitación adecuada para el tratamiento de evidencia digital, esto tiene como consecuencia el retraso de la investigación, la alteración de la evidencia y de los resultados que se podrían obtener.

4) En el diseño del Laboratorio Ciencias Forenses Digitales se consideraron varios aspectos, entre ellos el hardware y el software forense, la seguridad de las instalaciones del laboratorio, la custodia de la evidencia, la calidad y confiabilidad de los resultados del análisis, por este motivo hemos basado los elementos que integran el laboratorio forense, descritos anteriormente, en la norma ISO / IEC 17025:2005 [(101)], la cual también es conocida como “Requisitos generales para la competencia de los laboratorios de ensayo y de calibración” y con la ayuda de la norma ISO 17799 [(101)] para llevar a cabo los inventarios de la evidencia y activos del laboratorio.

5) Este proyecto planteó opciones de implementación de un laboratorio de Ciencias Forenses Digitales que incluyen herramientas de software libre, software propietario, hardware básico y hardware especializado. Al momento de elegir una opción se tomaron en cuenta los costos y las características de estas herramientas.

Para la implementación del laboratorio de Ciencia Forense Digital se necesita una inversión de la cual el mayor porcentaje sería destinado a la adquisición de hardware y software, el porcentaje restante se utilizará en seguridad y adecuación del laboratorio como sistemas de alarma, sistema de climatización, entre otros.

6) La legislación Ecuatoriana actualmente cuenta con una Ley de Comercio Electrónico y Firmas Digitales con reformas al Código Penal la cual contempla los delitos que se detallan en el anexo I, para poder penalizar las conductas ilícitas que están relacionadas con la informática e información digital del afectado, se opta por buscar un artículo acorde, que tenga similitud con el fin del delito cometido. Estos ítems por lo general se tratan de incluir en conceptos de propiedad intelectual, plagio, hurto y/o integridad física, por lo tanto la penalización que se aplica no está acorde a la gravedad del delito.

RECOMENDACIONES

1) Para el control de los delitos informáticos participan diferentes entidades, las cuales trabajan en conjunto con el fin de mitigar estos actos ilícitos, descubrir y penalizar a los autores, las mismas deberían capacitar a todos los miembros involucrados en el control de la cadena de custodia, desde el personal de la policía que realiza el allanamiento hasta los agentes fiscales que llevan el caso, deben ser capacitados en el tratamiento de evidencia, para no contaminarla o alterar la integridad de la misma y que tenga validez en un proceso penal ante un juez.

2) Se recomienda el uso de firmas digitales para la emisión de órdenes judiciales, esto sería de gran utilidad para agilizar el proceso de obtención de evidencia en la escena del crimen y en el caso de los ISP podrían entregar información con la certeza de que la orden judicial es original. El proceso se llevaría a cabo de la siguiente manera: el Juez de Garantía Penales emitiría la orden con su firma digital y la enviará por correo electrónico y ésta podrá ser recibida y

verificada por el Fiscal que solicitó la orden quedando así aprobado el allanamiento y el secuestro de evidencia.

3) Recomendamos la implementación de un Laboratorio de Ciencias Forenses Digitales en la ESPOL, planteando un referente en investigación Forense Digital, el mismo que prestaría sus servicios a entidades públicas y privadas. Para la realización de este proyecto se propuso la alternativa número dos detallada en el capítulo 8.

ANEXO A: ENTREVISTA CON LA DRA. SANDRA MOREJÓN

Extracto de la entrevista con la Dra. Sandra Morejón, fiscal de la Unidad de Delitos Informáticos y Telecomunicaciones

Día: 13 de julio del 2010

Hora: 9:30 am

Entrevistado: Dra. Sandra Morejón, fiscal de la Unidad de Delitos Informáticos y Telecomunicaciones

Antecedentes y datos de la administración de los delitos informáticos en la Fiscalía del Guayas

Anteriormente, en la Fiscalía General del Guayas la Unidad de Misceláneos se encargaba de recibir todas las denuncias con respecto a los delitos informáticos y actualmente aún tienen algunos datos y documentos que lo evidencian.

Hasta hace algunos años no había gran cantidad de denuncias de este tipo de delitos y no eran considerados en una clasificación específica, conforme a pasado el tiempo y la tecnología avanza, los delitos informáticos aumentaron en cantidad, se hacían más evidentes y más complicada la tarea de rastrear al autor o autores del delito.

Cambios que se han realizado en la estructura de la fiscalía con respecto a los delitos informáticos

Se realizaron varias reuniones con el Fiscal del Guayas Antonio Gagliardo acerca de este tema, surgieron carias ideas. Ahora contamos con leyes específicas acerca de los delitos informáticos y estos han aumentado en proporción y complejidad, era necesario reorganizarnos y se decidió crear una unidad que maneje las denuncias de delitos informáticos y telecomunicaciones específicamente.

Por esto en el año 2010 se creó la Unidad de Delitos Informáticos y Telecomunicaciones de la cual estoy encargada. En esta unidad nos encargamos de todas las denuncias de delitos informáticos, trabajamos con un perito informático que no es parte del personal interno de la Fiscalía pero trabaja con nosotros en estos casos.

El Dr. Santiago Acurio, quien es el Director Nacional de Tecnología de la Información, creo un “Manual de Manejo de Evidencias Digitales y Entornos Informáticos”, que tiene como objetivo ser una guía para el personal involucrado en los procesos de obtención de evidencia y en el proceso judicial, cuando en una escena del delito se encuentren dispositivos Informáticos o electrónicos.

Esta no es una guía oficial y no todos los miembros de la fiscalía y personal que trabaja con nosotros externamente como los peritos informáticos tienen el conocimiento de esta guía, se basan en su formación profesional y la experiencia adquirida.

Tipos de delitos informáticos más denunciados

Dentro de las denuncias que recibimos, las más comunes son por clonaciones de tarjetas de crédito o débito de esta manera realizan muchos robos en cajeros automáticos, robo de identidad por medio de redes sociales y estafas por correo electrónico.

Las personas muchas veces no hacen la denuncia de los delitos de los cuales son víctimas porque posiblemente gastarían mucho dinero en abogados y demás procedimientos y terminaría costándoles más de lo que les fue robado. Además consideran que es un proceso muy lento y se pierde mucho tiempo.

Su opinión acerca de la implementación de un laboratorio de ciencias forenses digitales

Me parece una muy buena idea, actualmente no hay un laboratorio que se especialice en Ciencias Forenses Digitales, sería muy bueno implementarlo para centralizar el análisis y recolección de evidencia en un lugar adecuado para esto.

En nuestro caso podríamos tener personal que trabaje exclusivamente para los casos que se den en la fiscalía.

Opiniones personales además de los temas tratados anteriormente

En Ecuador necesitamos ser parte de convenios internacionales como el de Budapest, porque ¿Qué pasaría si encontramos al autor de una estafa y se encuentra en un país extranjero?, ¿Cómo se puede enjuiciar a esa persona?

Cuando se es parte de un Tratado o convenio internacional, un estado está obligado a conceder la extradición del autor de un delito extranjero, si el país de donde proviene también es parte de este tratado.

ANEXO B: INGRESO DE EVIDENCIA

AL LABORATORIO

INGRESO DE EVIDENCIA	
Número de caso:	
Fecha de ingreso:	
Hora de ingreso:	
Entregada por:	
Fiscal asignado:	
Objeto de la investigación:	
Descripción de la evidencia:	
Observaciones:	
Recibida por:	

X _____

Entregada por

X _____

Recibida por

ANEXO C: INVENTARIO DE EVIDENCIA

INVENTARIO				
N. de caso	**Cód. Evidencia**	**Fecha Ingreso**	**Tipo de evidencia**	**Detalle**

ANEXO D: ENTRADA Y SALIDA DE EVIDENCIA ALMACENADA

ENTRADA Y SALIDA DE EVIDENCIA			
Número de caso:			
Código de evidencia:			
Ingreso:	☐	Salida:	☐
Fecha:			
Hora:			
Justificación:			
Responsable:			

X _____

Responsable

ANEXO E: FORMULARIO ANÁLISIS DE EVIDENCIA

ANÁLISIS DE LA EVIDENCIA	
Número de caso:	
Código de evidencia:	
Tipo de análisis:	
Responsable:	
Fecha:	
Hora inicio:	
Duración:	
Detalle de análisis:	
Resultado:	

X _____

Responsable

ANEXO F: ACTA DE RECOLECCION DE PRUEBAS

ACTA DE RECOLECCION DE PRUEBAS

NÚMERO DE PRUEBA:_____
FECHA ____/____/_____ (dd/mm/aaaa)
HORA ____:____ 0-24HORAS (hh:mm)

LUGAR DE RECOLECCION_____
_____

CANTIDAD _____
MARCA _____

MODELO _____

FABRICANTE _____

NÚMERO SERIE _____

DESCRIPCION DE LA PRUEBA_____
_____
_____
_____
_____

NOTA DE ESTADO DE LA PRUEBA_____
_____
_____
_____
_____

AGENTE ENCARGADO DE RECOLECCION
ID _____

NOMBRES Y APELLIDOS_____

CARGO_____

FIRMA_____

ANEXO G: INGRESO Y SALIDA DEL PERSONAL AL ALMACEN DEL LABORATORIO

Control de ingreso y salida

Fecha	Nombre	Hora entrada	Hora salida	Firma

X

Responsable

ANEXO H: INGRESO DE VISITANTES AL LABORATORIO

REGISTRO DE INGRESO DE VISITANTES

FECHA:
TURNO:

	APELLIDOS Y NOMBRE	HORA DE INGRESO	HORA SALIDA	FIRMA	ASUNTO
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					
30					

Firma y Sello
Supervisor

ANEXO I: PENALIDADES PARA INFRACCIONES INFORMÁTICAS

Tabla I.1 - Código Penal Ecuatoriano

Infracciones informáticas		Represión	Multa
Art. no numerado Delitos contra la confidencialidad	Acceso a información violentando claves y sistemas de seguridad.	6 meses a 1 año	$500 a $1000
	Obtención de información de seguridad nacional, secretos comerciales e industriales.	1 a 3 años	$1000 a $1500
	Divulgación o utilización fraudulenta de la información.	3 a 6 años	$2000 a $10000
	Divulgación o utilización fraudulenta de la información por parte de la misma persona o custodios.	6 a 9 años	$2000 a $10000
Art. no numerado Daños informáticos	Programas, datos, base de datos o mensajes de datos de un sistema de información o red electrónica.	6 meses a 3 años	$60 a $150

Infracciones informáticas		Represión	Multa
	Programas, datos, base de datos o mensajes de datos de un sistema de información o red electrónica de un servicio público o de defensa nacional.	3 a 5 años	$200 a $600
	Si no se trataré de un delito mayor.	8 meses a 4 años	$200 a $600
Art. no numerado Apropiación ilícita	Utilización fraudulenta de sistemas informáticos y redes electrónicas.	6 meses a 5 años	$500 a $1000
	Uso de claves, tarjetas, seguridades.	1 año a 5 años	$1000 a $2000
Art. 262 Destrucción maliciosa Empleado público o persona encargada de un servicio público		3 años a 6 años	
Art. no numerado Falsificación electrónica, alteración o modificación de mensajes de datos e información contenida en cualquier sistema de información o telemático		3 a 6 años	
Art. 563 Estafa Apropiación de cosas utilizando medios electrónicos y telemáticos.		3 a 6 años	$500 a $1000

ANEXO J: CRIPTOGRAFÍA

Por **cifrado o encriptación**, nos referimos al proceso de ocultar información o hacerla ilegible a primera vista, para que dicha información pueda ser leída naturalmente otra vez debe pasar por un proceso llamado descifrado.

Utilizando fuertes técnicas de cifrado, la información valiosa puede ser protegida contra personas que no se encuentren autorizadas a acceder a ella. Sin embargo, al movernos dentro de la sociedad de la información, el valor de la criptografía se hace evidente en todos los días de la vida en determinadas áreas como la privacidad, confianza, pagos electrónicos y control de acceso. Por lo tanto el campo de la criptografía es cada vez más amplio, aplicando desde las técnicas de cifrado clásicas hasta áreas como la autenticación, integridad de datos, y el no-repudio de la transferencia de datos [(1)].

Algoritmo criptográfico

Es una función matemática usada en los procesos de cifrado y descifrado. Un algoritmo criptográfico trabaja en combinación con una clave (un número, palabra, frase, o contraseña) para cifrar y descifrar datos [(2)].

(1) “Criptografía de la AZ”. 2009. SEGU-INFO. 1 de Mayo 2011. <http://www.segu-info.com.ar/proyectos/p1_criptografia.htm>
(2) “Seguridad y algoritmos de encriptación”. 2011. Cripto-forge. 1 de Mayo 2011. <http://www.cryptoforge.com.ar/seguridad.htm>

Para cifrar, el algoritmo combina matemáticamente la información a proteger con una clave provista. El resultado de este cálculo son los datos cifrados.

Para descifrar, el algoritmo hace un cálculo combinando los datos cifrados con una clave provista, siendo el resultado de esta combinación los datos descifrados (exactamente igual a como estaban antes de ser cifrados si se usó la misma clave). Si la clave o los datos son modificados el algoritmo produce un resultado diferente. El objetivo de un algoritmo criptográfico es hacer tan difícil como sea posible descifrar los datos sin utilizar la clave.

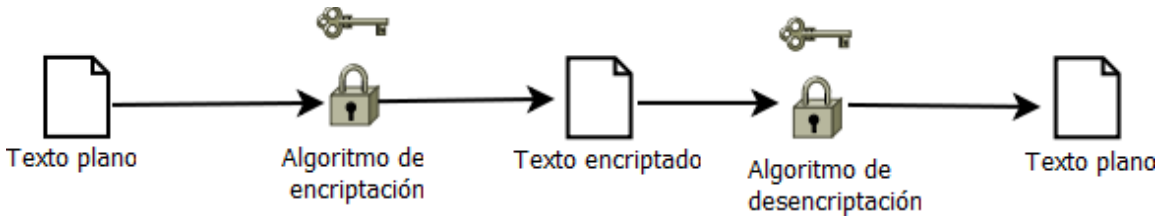


Ilustración J. 1 - Cifrado de información

Tipos de algoritmos de cifrado

Se pueden realizar al menos tres tipos de cifrado:

Tabla J. 1 - Tipos de algoritmo de cifrado

Tipos de algoritmos	Cifrado	Descifrado	Ventajas	Desventajas	Algoritmos más usados
Simétrico	Clave a (privada)	Clave a (privada)	Rápido y permiten cifrar y descifrar eficientemente con claves relativamente grandes	El receptor debe conocer la clave, ¿cómo se transmite sin comprometer su seguridad? No permite autenticar al emisor ya que una misma	**DES** con tamaño de clave de 56 bits **Triple-Des** con tamaño de clave de 128 bits a 256 bits **Blowfish** con tamaño de clave

Tipos de algoritmos	Cifrado	Descifrado	Ventajas	Desventajas	Algoritmos más usados
				clave la utilizan dos personas.	de 128 bits a 256 bits **AES** con tamaños de clave de 128, 192 o 256 bits
Asimétrico	Clave publica	Clave privada	Número de claves reducido, cada individuo necesitará únicamente un par de claves. Dificultad para encontrar la clave privada a partir de la pública. No es necesario transmitir la clave privada entre emisor y receptor. Permite autenticar a quien utilice la clave privada.	La necesidad de un tercero (Autoridad de Certificación) en el proceso Se precisa mayor tiempo de proceso y claves más grandes	**RSA** con tamaño de clave mayor o igual a 1024 bits **DSA** con tamaño de clave de 512 bits a 1024 bits **El Gamal** con tamaño de clave comprendida entre los 1024 bits y los 2048 bits

Algoritmo Simétrico

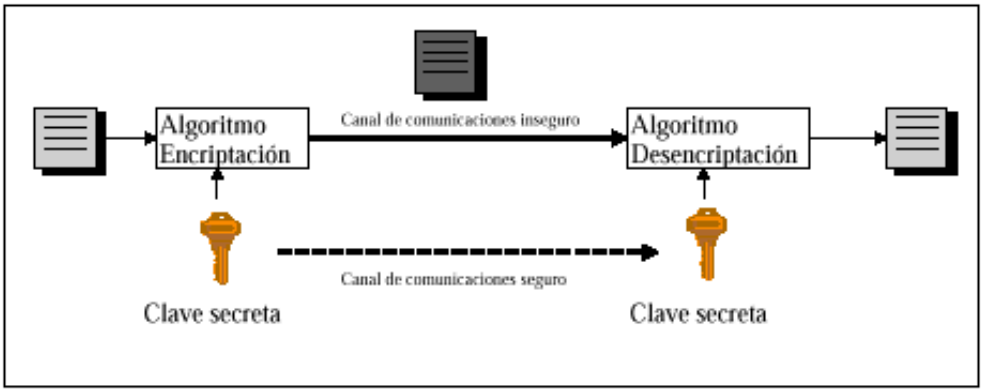


Ilustración J. 2 - Algoritmo Simétrico [3]

(3) “Introducción - algoritmo simétrico”. Eurologic. 1 de Mayo 2011. <http://www.eurologic.es/cifrado/simetric.htm>

Algoritmo Asimétrico

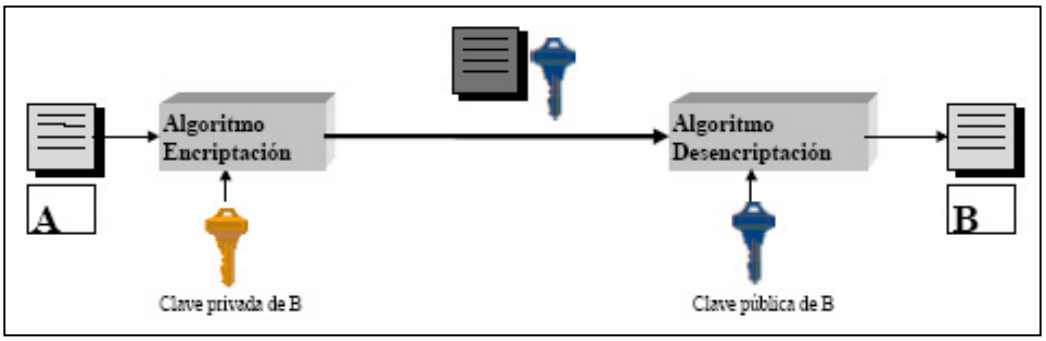


Ilustración J. 3 - Algoritmo Asimétrico [4]

Cifrado híbrido

Por lo general, las conexiones seguras de Internet utilizan una mezcla de los dos tipos de cifrado: simétricos y asimétricos. Aprovechan la rapidez de uno y la fortaleza del otro [5].

Lo que suelen hacer protocolos de comunicación seguros como HTTPS, es cifrar los mensajes usando un algoritmo simétrico, de forma que se hace un cifrado y descifrado rápido de los mismos, además de que los mensajes cifrados tengan menos volumen. Como hay que transmitir la clave del cifrado de alguna manera, ésta se cifra con un algoritmo asimétrico. Con esto se consigue que la parte más voluminosa de la información, que es el mensaje,

---

(4) “Control de accesos de usuarios”. 8 de Agosto 2005. Wikilearning. 1 de Mayo 2011. <http://www.wikilearning.com/tutorial/control_de_accesos-control_de_accesos_de_usuario/3394-3>

(5) “Cifrado de datos”. 11 de Junio 2009. Ekontsulta. 1 de Mayo 2011. <http://www.ekontsulta.net/test/wiki/index.php/Cifrado_de_datos>

vaya cifrada con un algoritmo seguro pero ligero, y la parte menos voluminosa, que es la clave, vaya cifrada con el algoritmo más pesado, y que garantiza que sólo podrá ser descifrada en el destino. De esta manera, en el destino primero ha de descifrar la clave del cifrado simétrico, con su clave privada, y una vez tenida esta clave, descifrar el mensaje. Esto garantiza una conexión segura.

Aplicaciones del cifrado

El cifrado de datos se usa en numerosas aplicaciones cotidianas. Algunas de las más habituales tomando como referencia [5], son:

- **SSL (Secure Socket Layer)**

  Protocolo criptográfico que proporciona comunicaciones seguras en Internet. Esta seguridad es en forma de privacidad y autenticación:

  - Por un lado autentica el servidor de la comunicación (mediante certificados), y por otra parte selecciona un algoritmo de cifrado.
  - Permite el intercambio de claves de forma segura entre cliente y servidor, y cifra la información con cifrado simétrico.

  Esta capa de seguridad se puede aplicar en diversos ámbitos:

  - HTTPS: Protocolo http seguro

- FTP: protocolo de intercambio de ficheros. Puede utilizar SSL para ser seguro.
- SMTP: protocolo de correo. Puede utilizar SSL para ser seguro.

- **Firma digital**

  La firma digital es el método criptográfico que permite asociar la identidad de una persona o máquina a un documento como autor del mismo.

  Para incorporar las firmas digitales:

  - Primero se calculan los datos de la firma, que se obtienen de aplicar cierto algoritmo matemático.
  - Esos datos se cifran con alguno de los algoritmos descritos anteriormente
  - Finalmente la firma cifrada es incorporada al documento.

  El receptor del documento deberá tener medios tecnológicos tanto para extraer la firma cifrada como para descifrarla, por lo que también deberá tener la clave.

- **VPN (Virtual Private Network)**

  Es una red con las características de una LAN, pero está extendida sobre una red pública como Internet; esto es, tiene el control y la

seguridad que ofrece una red LAN pero topológicamente tiene un ámbito descontrolado e inseguro como es Internet. Para que estas redes sean seguras se usan técnicas de Tunneling que consisten en crear un “túnel” seguro dentro de la red insegura, por el que circulan los datos de la VPN cifrados. Es por esto que las redes privadas virtuales es uno de los usos más frecuentes de cifrado.

Para garantizar la seguridad de la red VPN y las características que debe cumplir, se usan protocolos de comunicación segura como IPSec (Internet Protocol Security), que es el estándar de facto, aunque también se usan otros como SSL o PPTP.

Cifrado de archivos

También existen aplicaciones que permiten el cifrado de archivos completos, que pueden ser utilizados para enviarlos o simplemente se quiera guardar cifrado para que sólo pueda ser accedido por quienes tengan la clave de cifrado. Esto también es útil para almacenar información confidencial de una organización. En caso de sustracción de la información no servirá de nada si no se tiene una clave para descifrarla.

Cifrado de disco duro

Tener todo el sistema de archivos cifrado permite que cada vez que se guarde un archivo ya lo haga cifrado por defecto y que todo lo contenido en

el disco duro esté cifrado. Esto hace que haya procesos ligeramente más lentos, ya que cada vez que se guarda, por ejemplo ha de cifrarlo [5].

Métodos para obtener la clave de descifrado

Existen varios métodos para obtener la clave que se necesita para descifrar información, entre las cuales definimos [6]:

1. **Fuerza bruta**

   En este procedimiento se pretende intentar todas las combinaciones de bits posibles hasta encontrar la más adecuada y encontrar la clave. Se trata de prueba y error. Para hash simple o algoritmos, la fuerza bruta funciona bastante bien. A medida que aumenta la longitud de la clave también aumenta el número de posibilidades. Como se puede notar en la siguiente tabla, una clave de 512 bits tiene más de 154 ceros detrás de él.

Tabla J. 2 - Fuerza bruta

Key Length in Bits	Number of Possible Combinations
8	256
40	1,099,511,627,776
128	18,446,744,073,709,600,000
256	$1.15792 * 10^{77}$
512	$1.3408 * 10^{154}$

(6) Linda Volonino - Reynaldo Andaluza. Computer Forensics For Dummies. año 2008.

Con los avances en los algoritmos de criptografía y de larga longitud de las claves, encontrar una llave por la fuerza bruta suele ser poco práctico. Es el último recurso para la obtención ilegal de una contraseña.

2. **Ataque de diccionario**

   Este método utiliza un diccionario de contraseñas o hashes que son comparados con el valor hash almacenado en el archivo de contraseñas del sospechoso.

   Los diccionarios no contienen sólo las palabras estándar, sino también los nombres de celebridades, equipos deportivos, programas de televisión, etc.

3. **Tablas arco iris**

   Es una extensión de los diccionarios que poseen bases de datos mucho más extensas. Por lo cual Las tablas del arco iris permiten utilizar una base de datos con mayor posibilidades de comparación y que podrían ser almacenados en un equipo forense.

4. **Keystroke logger**

   Se utiliza keylogger para capturar las pulsaciones de teclado cuando un usuario lo pulse en el teclado. Este método funciona bien cuando

se sabe que la persona a quien se está vigilando está usando algún tipo de encriptación. Las características de Keylogger varían, pero todos registran las pulsaciones de teclado.

Se puede instalar el manual de keyloggers o usar software Troya (software para un propósito, como jugar un juego, pero en realidad se inserta otro programa en el ordenador).

5. **Snooper software**

   Este tipo de software se utiliza de la misma manera que los keyloggers, excepto que el software espía registra no sólo las pulsaciones de teclado, sino también cualquier actividad que se produce en el equipo. Archiva desde las capturas de pantalla hasta sesiones de chat, mensajes de correo electrónico, e incluso las veces que se enciende el ordenador.

6. **Aplicación específica de circuito integrado ASIC**

   Este tipo de chip está específicamente programado para realizar una tarea. El único propósito de programación de un sistema de descifrado ASIC es resolver un tipo específico de cifrado. La mayoría de los investigadores en informática forense no tienen acceso a equipos de

este tipo, pero las agencias de gobierno si, y que puede descifrar una clave de cifrado de 40 bits en cuestión de segundos.

7. **Cache checking**

   Algunas aplicaciones y sistemas operativos pueden poner contraseñas en una memoria caché temporal. Los usuarios que permiten que sus sistemas almacenen sus contraseñas, por lo general son almacenadas en texto plano en un área de la memoria cache.

Encriptación AES – 256

AES conocida como Estándar de Encriptación Avanzada (Advanced Encryption Standard). AES es una técnica de cifrado de clave simétrica que remplazará el Estándar de Encriptación de Datos (DES) utilizado habitualmente [(7) (8)].

AES proporciona una encriptación segura, utiliza una de las tres fortalezas de clave de cifrado: Una clave de encriptación de 128-, 192-, o 256- bits. Cada tamaño de la clave de cifrado hace que el algoritmo se comporte ligeramente

(7) AES Encryption – data security. 2011. Bitzipper. 1 de Mayo 2011. <http://www.bitzipper.com/es/aes-encryption.html>

(8) Cáceres Sosa – Arnold Ylla - Jhony Cruz. “Encriptación de datos una vista general”. 2008. Slideshare. 1 de Mayo 2011. <http://www.slideshare.net/christianikolai/encriptacion-de-datos-una-vista-general>

diferente, por lo que el aumento de tamaño de clave no sólo ofrece un mayor número de bits con el que se pueden cifrar los datos, sino también aumentar la complejidad del algoritmo de cifrado.

Tiempos de ejecución de algoritmos asimétricos

Diffie-hellman. Intercambio de clave

Pruebas realizada para tamaños de clave de 64, 256, 1024 bits variando el tamaño del número primo. Se ha cifrado la palabra “hola” para cada uno de los casos.

Tabla J.3 – Clave de 64 bits

N. Primo	Clave 1, 2	Máx.	Mín.	Media
2^{64}	2^{64}	11.6719	11.6406	11.6564
2^{256}	2^{64}	11.9219	11.6406	11.7500
2^{512}	2^{64}	12.7656	12.6094	12.694
2^{1024}	2^{64}	14.2500	14.0469	14.1500

Tabla J. 4 - Clave 256 bits

N. Primo	Clave 1, 2	Máx.	Mín.	Media
2^{64}	2^{64}	11.8438	11.7031	11.6564
2^{256}	2^{64}	12.0000	11.6406	11.8344
2^{512}	2^{64}	12.8750	12.6094	12.7219
2^{1024}	2^{64}	14.1094	14.0625	14.0775

Tabla J. 5 - Clave 1024 bits

N. Primo	Clave 1, 2	Máx.	Mín.	Media
2^{64}	2^{1024}	11.7500	11.6875	11.7219
2^{256}	2^{1024}	12.4531	11.6562	11.9156
2^{512}	2^{1024}	12.8750	12.6406	12.7065
2^{1024}	2^{1024}	14.3438	14.1562	14.2219

El Gamal, Cifrado de información

Pruebas realizada para tamaños de clave de 64, 256, 1024 bits variando el tamaño del número primo. Se ha cifrado la palabra “hola” para cada uno de los casos.

Tabla J. 6 - Clave 64 bits

N. Primo	Clave privada	Máx.	Mín.	Media
2^{64}	2^{64}	4.2975	4.1375	4.1533
2^{256}	2^{64}	4.3125	4.1875	4.2615
2^{512}	2^{64}	6.0625	5.4535	5.7785
2^{1024}	2^{64}	22.1925	21.3825	21.742

Tabla J. 7 - Clave de 256 bits

N. Primo	Clave privada	Máx.	Mín.	Media
2^{64}	2^{256}	4.1250	4.0156	4.0437
2^{256}	2^{256}	4.2656	4.0973	4.1412
2^{512}	2^{256}	6.0625	6.3281	6.4481
2^{1024}	2^{256}	6.7656	21.5313	22.275

Tabla J. 8 - Clave de 1024

N. Primo	Clave privada	Máx.	Mín.	Media
2^{64}	2^{1024}	4.1318	4.0625	4.0826
2^{256}	2^{1024}	4.2187	4.1406	4.1636
2^{512}	2^{1024}	5.7218	5.0625	5.2537
2^{1024}	2^{1024}	17.1500	15.1062	15.6906

RSA, Cifrado de información

Pruebas realizada para tamaños de clave de 64, 256, 1024 bits variando el tamaño del número primo. Se ha cifrado la palabra “hola” para cada uno de los casos.

Tabla J. 9 - Clave de 64 bits

N. Primo	Clave privada	Máx.	Mín.	Media
2^{64}	2^{64}	0.5938	0.4375	0.4750
2^{256}	2^{64}	0.9219	0.8031	0.8813
2^{512}	2^{64}	2.1094	1.9813	2.0688
2^{1024}	2^{64}	18.1406	15.8063	17.1946

Tabla J. 10 - Clave 256 bits

N. Primo	Clave privada	Máx.	Mín.	Media
2^{64}	2^{256}	0.6406	0.5556	0.6050
2^{256}	2^{256}	1.1406	1.0781	1.1063
2^{512}	2^{256}	3.7813	3.4219	3.6109
2^{1024}	2^{256}	28.9688	25.2500	27.1946

Tabla J. 11 - Clave de 1024 bits

N. Primo	Clave privada	Máx.	Mín.	Media
2^{64}	2^{1024}	8.6875	8.3438	8.5438
2^{256}	2^{1024}	11.6406	10.7969	11.3969
2^{512}	2^{1024}	18.3594	15.7500	17.0688
2^{1024}	2^{1024}	33.9531	30.1250	32.9531

Herramientas para cifrado y descifrado

Tabla J. 12 - Herramientas cifrado

Nombre	Algoritmos usados
Steganos Security Suite	ASD 256
True Crypt	AES, Serpent, Twofish, algoritmos de hash
Invisible Secret 4	AES - Rijndael, Twofish, RC 4, Cast128, GOST, Diamante 2, Zafiro II, Blowfish
AF Neo Cryptor	AES
Encryption and Decryption - - free	AES
EnCryption Gadget	Blowfish, AES
KriptoDrive	AES 256
CryptoLab 1.02	AES – Rijndael
TextEncrypt	Blowfish
SecuBox for Smartphone 1.3	AES 256

ANEXO K: ELEMENTOS A ANALIZAR SEGÚN EL TIPO DE SISTEMA

Elementos a analizar según el tipo de sistema [(1)]

1. **Sistemas Informáticos**

Plataforma Windows

- Registro del sistema
- Contenido de Sistema de Fichero Cifrados (EFS)
- FAT o MTF (Tablas de Metadatos de sistemas de ficheros Windows)
- Archivo BITMAP (Fichero creado durante el formateo de volúmenes NTFS para Windows NT y superiores)
- Papelera de reciclaje
- Ficheros de acceso directo
- Directorio Activo (Active Directory) (Windows 2000 y superiores)
- Log de visor de eventos

Plataforma Unix/Linux

- Listado descriptores de ficheros
- Ficheros SUID/SGID
- Trabajos planificados (Schedule jobs)
- Ficheros del historial de la Shell

---

(1) "Herramientas para el análisis y recolección de evidencias en el sabotaje informático en los centros de datos". 2011. Slideshare. 1 de Mayo 2011. <http://www.slideshare.net/UCACUE/herramientas-para-el-anlisis-y-recoleccin-de-evidencias-en-el-sabotaje-informtico-en-los-centros-de-datos>

Las ubicaciones comunes de evidencia en varias plataformas son:

- Mensajes de correo electrónico.
- Ficheros de trabajo de impresión.
- Archivos temporales de los navegadores web.
- Cache de los navegadores web.
- Historiales de los navegadores web.
- Favoritos de los navegadores web.
- Ficheros de cookies de los navegadores web.
- Logs del sistema operativo.
- Logs de aplicaciones.
- Logs de clientes de chat.
- Documentos de texto (doc, wpd, wps, rtf, txt, etc.).
- Hojas de cálculo (xls, wgl, wkl, etc.).
- Ficheros gráficos (jpg, gif, tif, bmp, etc.).

2. Redes

- Información proporcionada por la tarjeta de red (dirección MAC, dirección IP, etc.).
- Tabla de direcciones IP asignadas por el servidor DHCP (Protocolo de Configuración de Host Dinámico).
- Cache de ARP (Protocolo de Resolución de Direcciones).

- Logs del IDS (Sistema de detección de intrusos).
- Memoria del IDS.
- Logs del Cortafuego.
- Memoria del Cortafuego.
- Logs de servidores (Web, FTP, de correo electrónico).
- Mensajes de correo electrónico almacenados en el servidor.
- Logs de módems.
- Información de routers.
- RAM con información de configuración.
- Cache ARP.
- Logs del router.
- Datagramas almacenados cuando el tráfico es alto.
- Información de servidores DIAL-UP (Servidores ISP).
- Logs del servidor DIAL-UP.
- Memoria del servidor DIAL-UP.
- Logs del servidor de autentificación.
- Memoria del servidor de autentificación.
- Logs del servidor VPN.
- Memoria del servidor VPN.

2.1. Redes inalámbricas

Debemos identificar dos tipos de redes inalámbricas

Redes LAN inalámbricas (wireless LAN)

- Información proporcionada por las tarjetas inalámbricas de red (direcciones MAC, IP, etc.)
- Puntos de acceso
- Logs de módems wireless

Redes inalámbricas basadas en conmutación de circuitos

- Registros de facturación CDR (Charging Detail Records).

  Registros que contienen información para cada llamada realizada, como número que se llamó, el día de la llamada, duración, entre otros, organizados por clientes para efectos de facturación. Estos registros son archivados y están disponibles en un periodo aproximado de varios años, dependiendo de las políticas de la operadora.

- HLR (Home Location Register)

  Contiene información del subscriptor, referente a sus capacidades móviles contratadas (clase de servicio), la identificación de la unidad móvil, la ubicación actual de la misma ya sea en el área de cubrimiento de la red

proveedora o de otras redes celulares (roaming), la información de autenticación, el nombre de la cuenta y la dirección de facturación.

- VLR (Visitor Location Register)

  Almacena información física, electrónica y de radio, acerca de todos los usuarios que están actualmente autenticados dentro de una red particular del MSC (Mobile Switching Center o centro de conmutación móvil). Dicha información incluye la localización actual del dispositivo móvil y el estado del mismo (activo, en espera, etc.).

- OMC (Operation and Maintenance Center o Centro de operación y administración).

  Realiza tareas administrativas como obtener datos de la MSC para propósitos de facturación y administra los datos de la HLR.

  Además, proporciona una visión del estatus de operación de la red, la actividad de red y las alarmas. A través de éste, es posible examinar una o rastrear una llamada móvil particular en progreso (Mobile trace).

3. Dispositivos móviles

Teléfonos móviles

Ficheros con distinta información almacenada en la tarjeta del móvil (SIM: Subscriber Identity Module, código PIN, código PUK).

- Chips de memoria Flash (contienen información sobre el teléfono así como software interno del mismo).
- Números de teléfonos almacenados
- Mensajes de texto
- Configuraciones (lenguaje, día/hora, tono/volumen, etc.).
- Grabaciones de audio almacenadas.
- Programas ejecutables almacenados.
- Configuraciones de Internet, GPRS, WAP.
- Log de llamadas (llamadas realizadas, recibidas, perdidas).
- Datos (logs de sesiones, números marcados, etc.) contenidos en dispositivos a los que se haya conectado el teléfono móvil (computadoras de sobremesa, ordenadores portátiles, etc.).

Organizadores de mano

- RAM.
- ROM. Memoria en la que se encuentra el sistema operativo y las aplicaciones base.

- FLASH-ROM. Memoria en la que podemos guardar aplicaciones y datos que no queremos perder por resetear el dispositivo o porque no tenga batería.
- Datos (de sincronización, contactos, tareas, etc.) contenidos en dispositivos a los que se en dispositivos a los que se haya conectado el teléfono móvil (ordenadores de sobremesa, ordenadores portátiles, teléfonos móviles, etc.)

4. Sistemas embebidos

Tarjetas de memoria

Básicamente su recolección de datos es igual que la de un disco duro puesto que se basan en sistemas de ficheros tipo FAT (normalmente).

Las estructuras de datos en las que se pueden analizar evidencias son:

- CIS (Card Information System), área oculta que contiene información del fabricante.
- MBR (Master Boot Record), en las tarjetas este sector está presente por razones de compatibilidad y raramente se usará como arranque de un disco duro (aunque los delincuentes, podría ocultar aquí información).

- Sector de arranque. Se usa junto al MBR para establecer la geometría del dispositivo.
- FAT. Contiene la lista que describe los clúster ocupados por los ficheros.
- El área de datos que contiene los datos de los ficheros actuales.

ANEXO L: PRESUPUESTO INICIAL ADECUACIONES

Presupuesto Inicial			
	Cantidad	**Precio Unitario**	**Global**
Sistema Circuito Cerrado			$ 1,255.0
Sistema de Alarma			$ 190.0
Sistema contra incendios (extintores)	1		$ 500.00
Aire acondicionado 48000btu	1		$ 1,000.00
Enrutador			$ 300.00
Conmutador			$ 200.00
Cable de red		$ 0.70	$ 50.00
Cable telefónico		$ 0.50	$ 50.00
UPS 1000 VA	4	$ 62.00	$ 248.00
Generador de Energía a diesel			$ 1,000.00
Disco duro externo 2TB ETHERNET			$ 338.39
Cerraduras biométricas			$ 400.00
Cerraduras tipo multilock			$ 160.00
Copiadora e impresora			$ 600.00
Herramienta varias (destornilladores, pinzas, entre otras)			$ 500.0
Mobiliario			$ 1,500.00
Adecuaciones (divisiones, pintura, entre otra)			$ 3,000.00
TOTAL			**$ 11,291.4**

SISTEMA CIRCUITO CERRADO	**Cantidad**	**Precio unitario**	**Global**
Cámaras con visión nocturna	5	$ 90.0	$ 450.0
Instalación	5	$ 25.0	$ 125.0
CPU	1	$ 300.0	$ 300.0
Tarjeta que captura 8 canales	1	$ 380.0	$ 380.0
TOTAL			**$ 1,255.0**

SISTEMA DE ALARMA	**Cantidad**	**Precio unitario**	**Global**
Permite 8 zonas de detección			
incluye:			
Sensores de movimiento	8	$ 15.00	$ 120.00
Sirena	1	$ 35.00	$ 35.00
instalación		$ 35.00	$ 35.00
TOTAL			**$ 190.00**

ANEXO M: SOFTWARE FORENSE

En este anexo describiremos las características principales de los software forenses que se analizaron para llevar a cabo la selección y utilización en el laboratorio como herramienta principal me el análisis de la evidencia. Entre las cuales tenemos:

Encase

Es un software de investigación forense informática, que tiene la capacidad de realizar análisis complejo de evidencia digital [1].

- Entre sus principales características tenemos:
- Amplia compatibilidad de formatos disponibles.
- Amplia compatibilidad de correos electrónicos disponibles.
- Amplia compatibilidad con navegadores disponibles.
- Análisis y generación de informes de manera detallada.
- Recopilación inteligente de evidencia digital.
- Validado por los tribunales de justicia.

(1) "Encase Forensic". 2011. Digital Intelligence. 10 de Mayo 2011. <http://www.digitalintelligence.com/software/guidancesoftware/encase/>

Deft-Extra

Es una interfaz Gráfica de Computo Forense que asiste en el análisis forense de discos, redes y navegadores [(2)].

Esta herramienta está dividida en seis secciones que incluyen diversas herramientas forenses las cuales se detallan a continuación:

- Información del Sistema(SysInfo)
- Adquisición Viva(Live Adquisition)
- Forense(Forensics)
- Búsqueda(Search)
- Utilidad(Utility)
- Reporte(Report)

CAINE (Computer Aided Investigative Environment)

El Entorno de Investigación Asistido por Computadora es una distribución italiana de GNU/Linux que ofrece herramientas forenses como módulos de software [(3)].

(2) Deft Linux. 2010. 10 de Mayo 2011. <http://www.deftlinux.net/>

(3) C.A.IN.E (Computer Aided Investigative Environment). 2011. 10 de Mayo 2011. <http://www.caine-live.net/>

Ha sido diseñado de manera que garantice las siguientes características:

- Entorno que sirva de apoyo al investigador en las cuatro fases Forenses Digitales.
- Interfaz gráfica amigable.
- Generación semiautomática de un informe final.

Digital Forensics Framework

Es una herramienta basada en Python con un módulo de sistema flexible para investigación forense digital de memorias USB, PDA, tarjetas de memoria y celulares [(4)].

Entre sus principales características tenemos:

- Recuperación potente de archivos borrados.
- Análisis del sistema de archivos de teléfonos móviles.
- Descifrar contenido y metadatos de SMS para mostrarlos como en un teléfono móvil.

(4) Open Source Digital Investigation Framework. 2011. 10 de Mayo 2011. <http://www.digital-forensic.org/>

Forensics Toolkit

Es un estándar de tecnología de investigación informática forense [(5)].

Entre sus características principales tenemos:

- Análisis de vanguardia.
- Descifrado y craqueo de contraseñas.
- Interfaz intuitiva.
- Es personalizable y fácil de usar.
- Potente velocidad de procesamiento.

Easy Recovery Professional

Es una solución para recuperar datos, reparar archivos, correo electrónico y realizar diagnóstico de discos [(6)].

Posee soporte para:

- Discos duros IDE/ATA/EIDE/SATA/SCSI
- Discos extraíbles.
- Disquetes.
- Soportes periféricos.
- Soportes digitales.

---

(5)Forensics Toolkit. 10 de Mayo 2011. <http://www.forensics.ie/software/product/forensic-toolkit-ftk/>

(6) "Recuperación de datos y reparador de archives". 2011. Kroll Ontrack Inc. 10 de Mayo 2011. <http://www.ontrackdatarecovery.es/software-recuperacion-ficheros/>

Fox Analysis

Es una herramienta que permite el análisis de los datos generados por el uso de Mozilla Firefox fue desarrollada con el fin de ayudar en investigación forense digital [(7)].

Sus funcionalidades principales son:

- Extracción de marcadores, cookies, descargas, inicios de sesión.
- Analizar datos con opciones de filtrado:
    - Por palabras claves
    - Rangos de fechas.
    - Estado de la descarga.
    - Por selección.
- Informe de actividad de exportación.

Chrome Analysis

Es una herramienta que permite el análisis de los datos generados por el uso de Google Chrome fue desarrollada con el fin de ayudar en investigación forense digital [(8)].

Sus funcionalidades principales son:

---

(7) "FoxAnalysis". 2010. Forensic-Software. 10 de Mayo 2011. <http://forensic-software.co.uk/foxanalysis.aspx>

(8) "Chrome Analysis". 2010. Forensic-Software. 10 de Mayo 2011. <http://forensic-software.co.uk/chromeanalysis.aspx>

- Extracción de marcadores, cookies, descargas, inicios de sesión.
- Analizar datos con opciones de filtrado:
    - Por palabras claves
    - Rangos de fechas.
    - Estado de la descarga.
    - Por selección.
- Informe de actividad de exportación.

Para la elección de las herramientas de software más adecuadas hemos tomado en cuenta varios criterios de selección, de acuerdo al laboratorio que deseamos plantear que cumpla con las necesidades actuales y sea factible de implementar.

Tabla M. 1 - Criterios de selección de software

	Encase	**Deft Extra**	**Caine**	**Digital Forensics Framework**	**Forensics Toolkit**	**Easy Recovery Professional**	**Fox Analysis**	**Chrome Analysis**
Tipo	Comercial	Libre	Libre	Libre	Libre	Comercial	Libre	Libre
Estándar de la industria	Si	No	No	No	Si	No	No	No
Multiplataforma	Si	Si	Si	Si	No	Si	No	No

SOFTWARE PARA ANÁLISIS DE DISPOSITIVOS MÓVILES

MOBILedit Forensic

Es una herramienta confiable de análisis forense en celulares utilizada en más de 70 países y reconocida por el Instituto Nacional de Estándares y Tecnología página oficial [(9)].

Permite extraer todo el contenido del teléfono y genera un reporte (en cualquier idioma) listo para su presentación en una audiencia.

Entre sus principales características se puede mencionar:

- Análisis de teléfonos vía cable USB, Bluetooth e Infrarrojo.
- Compatibilidad con una gran cantidad de teléfonos.
- Recuperación de mensajes borrados de tarjetas SIM.
- Exportación a Word, Excel / XLS, navegador, XML / XSL.

(9) “MOBILedit! Forensic Overview”. 2011. MOBILedit. 10 de Mayo 2011. <http://www.mobiledit.com/mef-overview.htm>

ART – Mobile

Es un software desarrollado para asistir en la captura de imágenes (vía cámara) de dispositivos móviles para producir un documento en Microsoft Word, página oficial [(10)].

Provee las siguientes funciones:

- Reduce el tiempo que se expende en reportes manuales.
- Captura imágenes de una cámara conectada vía USB.
- Almacena imágenes en una carpeta de estructura lógica.
- Crea un reporte personalizable con las imágenes capturadas.

BitPIM

Es un programa que permite ver y manipular datos en teléfonos CDMA como LG, Samsung, Sanyo, etc. pudiendo obtener datos que incluyen Contactos, calendario, fondos de pantalla, tonos musicales y archivos del sistema, página oficial [**(11)**].

(10) "ART (Automatic Reporting Tool)". 2010. IntaForensics. 10 de Mayo 2011. <http://www.intaforensics.com/Software/ART.aspx>

(11) BitPIM. 2010. 10 de Mayo 2011. <http://www.bitpim.org/>

Oxygen Forensic Suite

Es un software forense móvil para análisis estándar de teléfonos celulares, teléfonos inteligentes y PDA's, utilizando protocolos avanzados para extraer más cantidad de datos de los que generalmente se puede extraer con herramientas forenses, especialmente en teléfonos inteligentes, página oficial [(12)].

Permite extraer datos de:

- Información general del teléfono y de la tarjeta SIM.
- Contactos
- Calendario.
- Historial de llamadas.
- Notas.
- Caché de navegación web.
- Entre otros.

UndeleteSMS

Permite recuperar mensajes SMS borrados de tarjetas SIM GSM, página oficial [(13)].

(12) Oxygen Forensic Suite 2011. 2011. 10 de Mayo 2011. http://www.oxygen-forensic.com/en/

(13) "UndeleteSMS". 2007. BaxWare. 10 de Mayo 2011. <http://www.baxware.com/undelete-sms.htm>

Cell Seizure

Es un software que permite la recolección y análisis de datos extraídos de diversos tipos de celulares, teniendo como principal objetivo organizar los distintos tipos de archivos y generar un informe HTLM a partir de los mismos, página oficial [(14)].

Entre sus características tenemos:

- Soporta GSM, TDMA, CDMA.
- Adquiere información completa de la tarjeta SIM.
- Recupera datos borrados y descargas flash.
- Soporta múltiples idiomas.
- Diferentes formatos de informe disponibles.
- Búsqueda avanzada de texto y valores hexadecimales.

Tabla M. 2 - Software dispositivos móviles

Software	Tipo
MOBILedit! Forensic	Comercial con versión gratuita reducida
ART-Mobile	Comercial
BitPIM	Comercial
Oxygen Forensic Suite	Comercial con versión gratuita reducida
UndeleteSMS	Libre
Cell Seizure	Comercial

(14) “Device Seizure”. 2011. Digital Intelligence. 10 de Mayo 2011. <http://www.digitalintelligence.com/software/parabenforensictools/deviceseizure/>

ANEXO N: OPCIONES DE IMPLEMENTACION

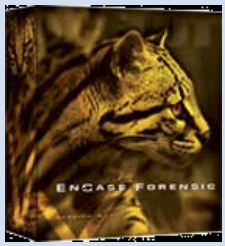
Presentamos a continuación tres alternativas de implementación con diferente tipo de software y hardware para el funcionamiento del Laboratorio Forense Digital

ALTERNATIVA DE IMPLEMENTACION 1

Tabla N. 1 - Alternativa de implementación uno

Equipo	Características	Precio
Equipo Base 	• Sistema operativo: window 7 • Procesador Intel Core I7 • Tarjeta de video Geforce • Disco duro de 4TB • Memoria RAM 8 Gb DDR3 • Puertos: Usb, fireware, red 100/1000 • Quemador CD/DVD • Blu-ray • Lector de tarjetas • Puerto Firewire • Puerto e-sata • Monitor 19''	1,900
Equipo portatil 	• Sistema operativo: Windows 7 • Procesador Intel Core I5 • Disco duro de 1TB • Memoria RAM 4 Gb DDR3	1,200
Duplicador **Forensic talon kit**	• Sistema para el clonado de discos duros. • Analiza los dispositivos IDE/UDMA/SCSI/SATA.	6,130.74

Equipo	Características	Precio
		
Bloqueador de escritura Ultra Kit III + FireWire + TD1 	• Contiene hardware UltraBlock, bloqueador de escritura. • Adaptadores y conectores	2,699
FRED **Forensic Recovery of Evidence Device** 	• Posee bandejas extraíbles para instalar los discos duros. • Posee dos unidades de disco duro, Una para sistema operativo (s), la adquisición forense, herramientas de tratamiento y el otro disco como una unidad de trabajo para la restauración y el procesamiento de la evidencia digital. • Intel i7 920 CPU , 2,66 GHz, caché de 8M • 6 GB DDR3-1333	5,999
CellDEK	• Obtiene información de dispositivos PDA, Blackberry de Windows y Garmin y dispositivos Tom Tom de navegación satelital. • Adquiere llamadas perdidas, salientes, recibidas, agenda, SMS, SMS eliminados de la SIM, MMS (mensajes multimedia), calendarios, citas recordatorios, imágenes, video, audio.	20,000

Equipo	Características	Precio
		
Encase 	• Permite visualizar previamente los datos mientras se obtienen imágenes de unidades o de otros medios. • Compatibilidad con diversos sistemas de archivos • Compatibilidad con RAID avanzada	3,600
Oxygen Forensic Suite	• Software forense móvil para análisis estándar de teléfonos celulares, teléfonos inteligentes y PDA's	Versión profesional 1,499
	Total	**43,027.74**

ALTERNATIVA DE IMPLEMENTACION 2

Tabla N. 2 - Alternativa de implementación dos

Equipo	Características	Precio
Equipo Base 	• Sistema operativo: Windows server 2008 • Procesador Intel Core I7 • Tarjeta de video Geforce • Disco duro de 4TB • Memoria RAM 8 Gb DDR3 • Puertos: Usb, fireware, red 100/1000 • Quemador cd/dvd • Blu-ray • Lector de tarjetas • Puerto Firewire • Puerto e-sata • Monitor 19"	1,900
Equipo portatil 	• Sistema operativo: Windows 7 • Procesador Intel Core I5 • Disco duro de 1TB • Memoria RAM 4 Gb DDR3	1200
Duplicador **Forensic talon kit** 	• Sistema para el clonado de discos duros. • Analiza los dispositivos IDE/UDMA/SCSI/SATA.	6,130.74

Equipo	Características	Precio
Bloqueador de escritura Ultra Kit III + FireWire + TD1 	• Contiene hardware UltraBlock, bloqueador de escritura. • Adaptadores y conectores	2,699
FRED **Forensic Recovery of Evidence Device** 	• Posee bandejas extraíbles para instalar los discos duros. • Posee dos unidades de disco duro, Una para sistema operativo (s), la adquisición forense, herramientas de tratamiento y el otro disco como una unidad de trabajo para la restauración y el procesamiento de la evidencia digital. • Intel i7 920 CPU , 2,66 GHz, caché de 8M • 6 GB DDR3-1333	5,999
Celldesk Tek	• Obtiene información de dispositivos PDA, Blackberry de Windows y Garmin y dispositivos Tom Tom de navegación satelital. • Adquiere llamadas perdidas, salientes, recibidas, agenda,	15,121.5

Equipo	Características	Precio
	SMS, SMS eliminados de la SIM, MMS (mensajes multimedia), calendarios, citas recordatorios, imágenes, video, audio.	
DefExtra	▪ Software Forense que asiste en el análisis de discos, redes y navegadores. ▪ Esta herramienta está dividida en seis secciones que incluyen diversas herramientas forenses las cuales se detallan a continuación: 1. Información del Sistema. 2. Adquisición en Vivo. 3. Forense. 4. Búsqueda. 5. Utilidades. 6. Reporte.	0,0
Oxygen Forensic Suite	• Software forense móvil para análisis estándar de teléfonos celulares, teléfonos inteligentes y PDA's	Versión profesional 1,499
	Total	**34,549.24**

ALTERNATIVA DE IMPLEMENTACION 3

Tabla N. 3 - Alternativa de implementación tres

Equipo	Características	Precio
Equipo Base 	• Sistema operativo: Windows 7 • Procesador Intel Core I7 • Tarjeta de video Geforce • Disco duro de 4TB • Memoria RAM 8 Gb DDR3 • Puertos: Usb, fireware, red 100/1000 • Quemador cd/dvd • Blu-ray • Monitor 19''	1,900
Equipo portatil 	• Sistema operativo: Windows 7 • Procesador Intel Core I5 • Disco duro de 1TB • Memoria RAM 4 Gb DDR3	1200
FTK Imager 	• Software orientado a la adquisición y tratamiento de imágenes de dispositivos de almacenamiento. • Herramienta Windows • Interfaz gráfica.	Libre
Deft-extra	▪ Software Forense que asiste en el análisis de discos, redes y navegadores. ▪ Esta herramienta está dividida en seis secciones que incluyen diversas herramientas forenses: 1. Información del Sistema. 2. Adquisición en Vivo. 3. Forense. 4. Búsqueda. 5. Utilidades. 6. Reporte.	libre

Equipo	Características	Precio
Oxygen Forensic Suite	• Software forense móvil para análisis estándar de teléfonos celulares, teléfonos inteligentes y PDA's	Versión profesional 1,499
Restoration	• Recuperar archivos borrados.	Libre
	Total	**4,599**

ANEXO O: DETALLE SOFTWARE DEFT-EXTRA

Análisis de la herramienta Deft-Extra (Digital Evidence & Forensic Toolkit)

Ilustración O. 1 - Pantalla principal Deft Extra

Es un kit de herramientas de análisis forense adaptado a Windows pero basado en la distribución Linux Xubuntu.

Características

- Posee una interfaz gráfica amigable.
- Orientado tanto para administradores de sistemas, policía, investigadores y peritos especializados en el área informática.
- Disponible en los idiomas inglés e italiano.

Funcionalidades

Deft-Extra cuenta con varios módulos para clasificar sus funcionalidades.

Módulo SysInfo

Dentro de este módulo encontramos varias funcionalidades explicadas en la siguiente tabla.

Tabla O. 1 - Características módulo SysInfo

Funcionalidad	Descripción
System Information	Muestra información básica del sistema: Sistema operativo Procesador RAM Usuario Host Dirección IP Unidades de disco
Running Process	Información de los procesos que se están ejecutando.
System Information Utilities	Provee las siguientes herramientas Drive Manager WinAudit USB Deview User Profile View WRR MSI My Event View CurrProcess

System Information

Ilustración O. 2 - Pantalla System Information

En esta pantalla encontramos datos importantes como la ip, el nombre del equipo en la red, el usuario y unidades de disco.

Running Process

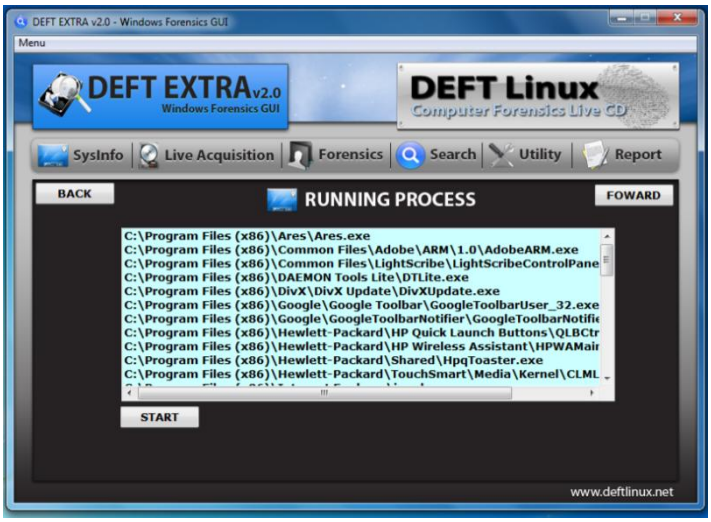


Ilustración O. 3 - Pantalla Running Process

Este es el listado de procesos ejecutándose actualmente así como su id.

System Information Utilities

Ilustración O. 4 - Pantalla System information Utilities

Con estas herramientas podemos recolectar toda la información del sistema.

Drive manager

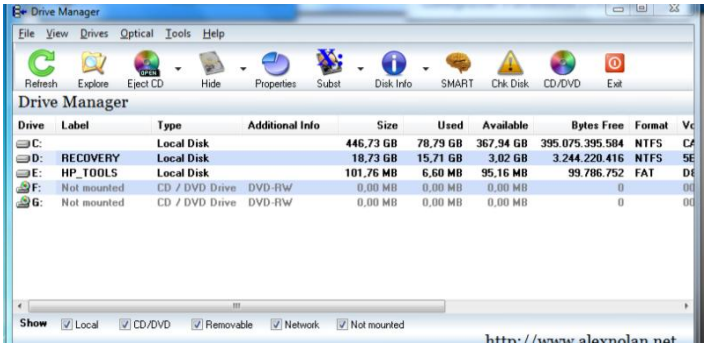


Ilustración O. 5 - Sección drive Manager

Provee información sobre las unidades de disco del sistema.

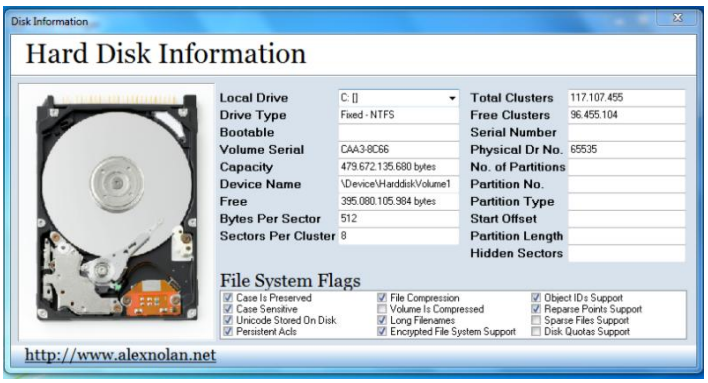


Ilustración O. 6 - Información de disco duro

En la información de cada unidad podemos encontrar información más precisa para nuestra investigación.

WinAudit

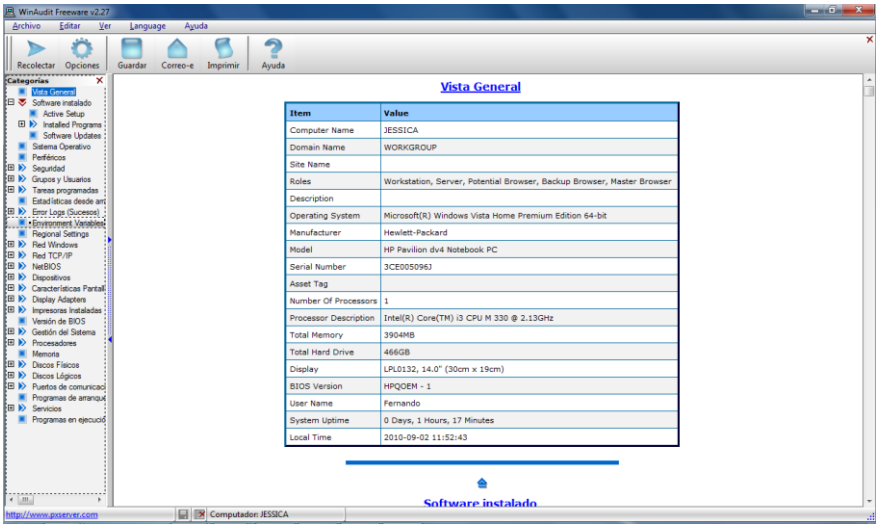


Ilustración O. 7 - Sección WinAudit

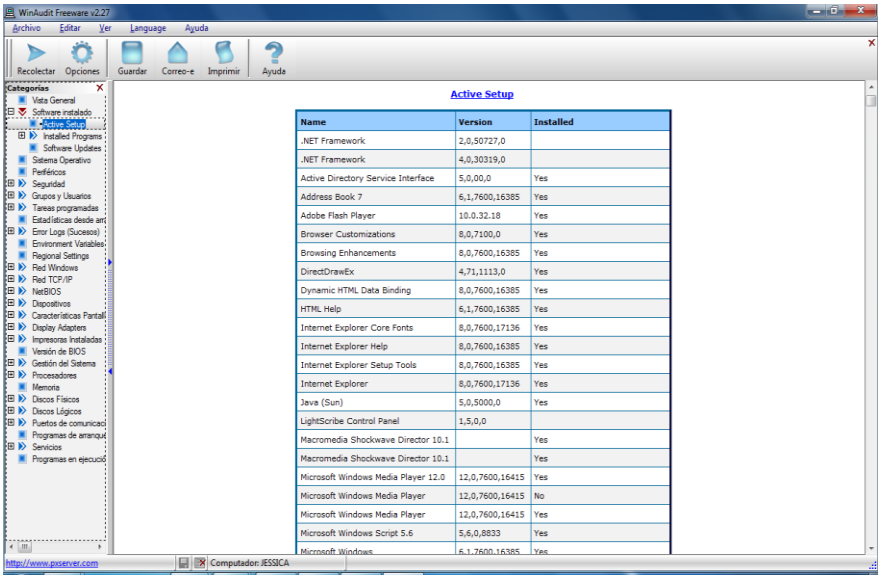


Ilustración O. 8 - Active Setup

Nos permite inventariar el sistema, de esta manera podemos tener acceso datos tales como:

- Software instalado.
- Seguridad.
- Grupos y usuarios.
- Tareas programadas.
- Logs de errores.
- Discos físicos.
- Discos lógicos.
- Servicios, entre otros.

USB Deview

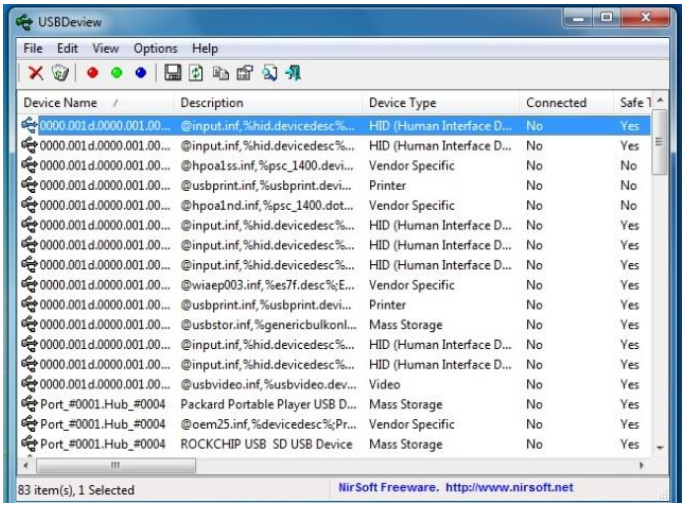


Ilustración O. 9 - Sección USB deview

Muestra información de los últimos dispositivos conectados al sistema.

Modulo Live Acquisition

Dentro de este módulo encontramos varias funcionalidades explicadas en la siguiente tabla.

Tabla O. 2 - Características módulo Live Acquisition

Funcionalidad	Descripción
FTK Imager v 2.6.1 WFT – Windows Forensics ToolChest	Herramientas para obtener imágenes de las unidades de almacenamiento del sistema.
WINEN MDD	Herramientas para obtener una copia de la memoria RAM del sistema.

WTF - Windows Forensics ToolChest

FTK Imager v 2.6.1

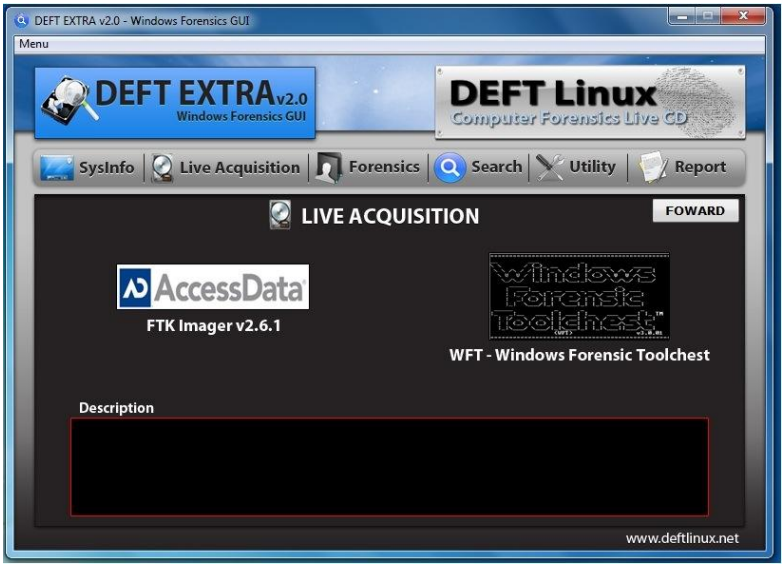


Ilustración O. 10 - Sección live acquisition

WINEN

MDD

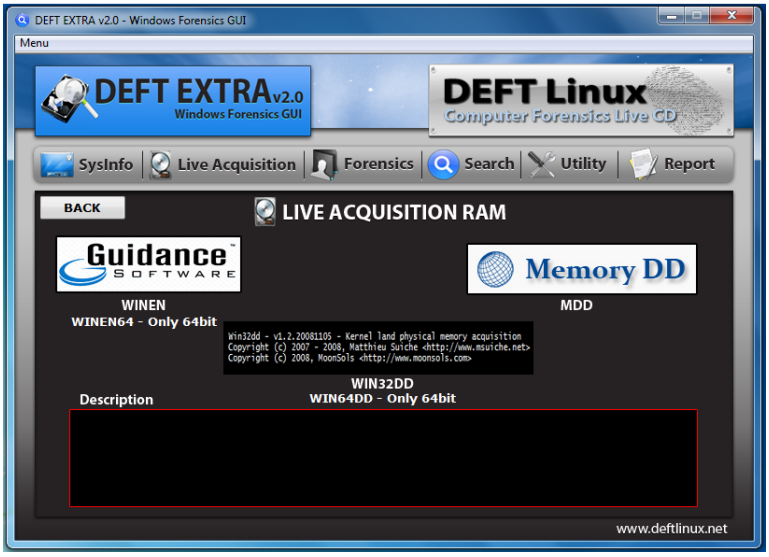


Ilustración O. 11 - Sección live acquisition RAM

Módulo Forensics

Dentro de este módulo encontramos varias funcionalidades explicadas en la siguiente tabla.

Tabla O. 3 - Características Módulo Forensics

Funcionalidad	Descripción
Forensics Tools	Herramientas extras para el análisis forense digital: Recuva Zero View WFA FileAlyzer PC ON/OFF TIME Terminal NIGILANT 32
Password Recovery	Permite recuperar contraseñas que hayan sido almacenadas en el sistema con las siguientes herramientas: MessenPass Asterix Logger Password Fox ChromePass IePass View Wireless Key View Mail Pass View
Networking	Permiten el análisis forense de redes mostrando información de puertos abiertos, conexiones inalámbricas, adaptadores de red para ello cuenta con las herramientas: CurrPorts AdapterWatch SniffPass

	Bluetooth View WirelessNet View
Web Browser	Herramientas para el análisis forense de navegadores web IECookie View IEHistory View Mozilla Cookie View Mozilla History View Historian Mozilla Cache View Opera Cache View Chrome Cache View FoxAnalysis Index.Dat 2.0

Forensics Tools

Ilustración O. 12 - Sección forensics tool

Password Recovery

Ilustración O. 13 - Sección Password recovery

Networking

Ilustración O. 14 - Sección Forensics Networking

Wirelessnet view

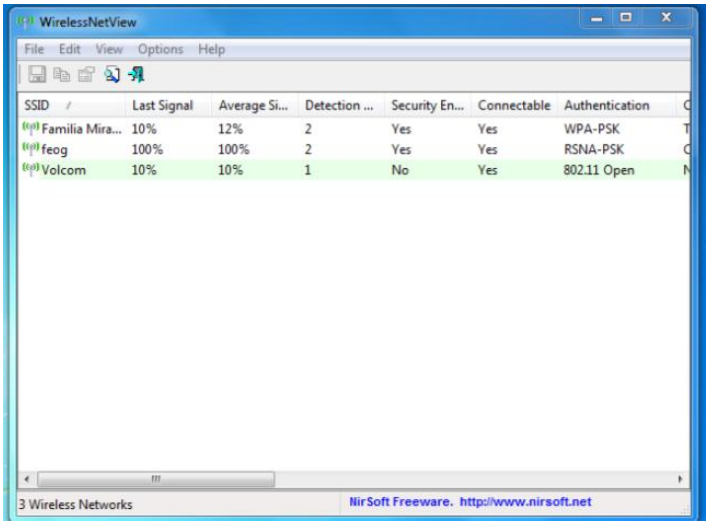


Ilustración O. 15 - Sección WirelessNet

Web Browser

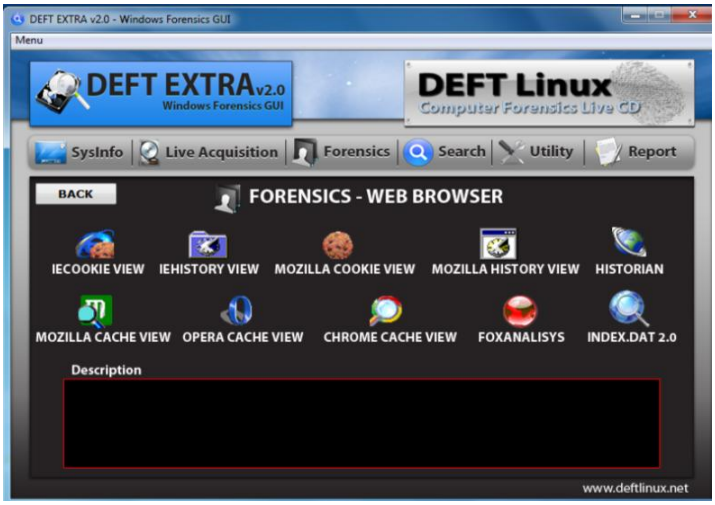


Ilustración O. 16 - Pantalla Web Browser

Proporciona información de navegación tales como: historial, cache, contraseñas guardadas.

History view

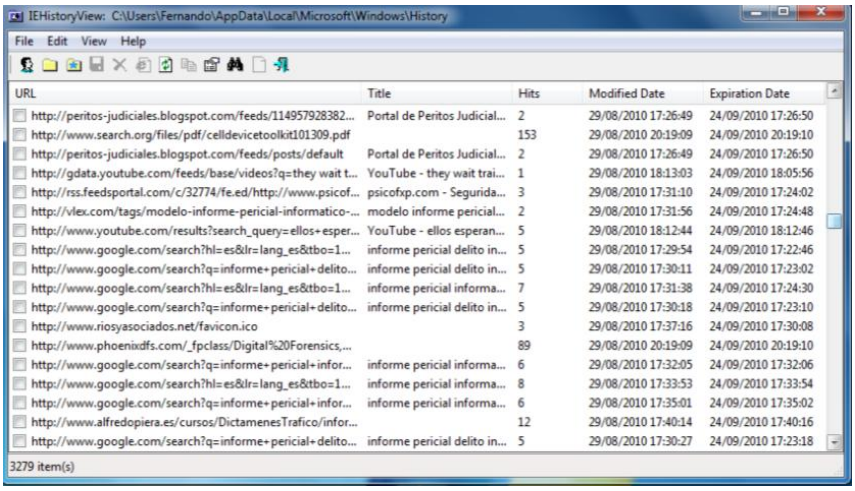


Ilustración O. 17 - Sección History view

Módulo Search

Dentro de este módulo encontramos varias funcionalidades explicadas en la siguiente tabla.

Tabla O. 4 - Características Módulo Search

Funcionalidad	Descripción
Search	Permite la búsqueda de archivos en los dispositivos conectados al equipo mediante criterios, además permita la visualización de miniaturas de los archivos encontrados.

Ilustración O. 18 - Pantalla Módulo search

Herramienta de búsqueda archivos, incluye la funcionalidad MD5 para evitar la alteración de archivos.

Módulo Utility

Dentro de este módulo encontramos varias funcionalidades explicadas en la siguiente tabla.

Tabla O. 5 - Características Módulo Utility

Funcionalidad	Descripción
Utility	Herramientas de apoyo en el análisis forense digital IncrediMail Me TestDisk SumatraPDF SkipeLog View Pre-Search RootKit Revealer Putty Photorec

Funcionalidad	Descripción
	HoverSnap HashCalc Hexedit AviScreen IpNetInfo LtfViewer Notepad++ VncViewer AbiWord KeyLog

Ilustración O. 19 - Pantalla Módulo Utility

Proporciona una colección de herramientas extras para análisis forense.

Módulo Report

Tabla O. 6 - Características módulo Report

Funcionalidad	Descripción
Report	En esta sección el investigador forense puede realizar anotaciones de los hallazgos de su investigación.

Este apartado del software permite hacer anotaciones de datos claves que nos ayudaran en la elaboración del informe pericial.

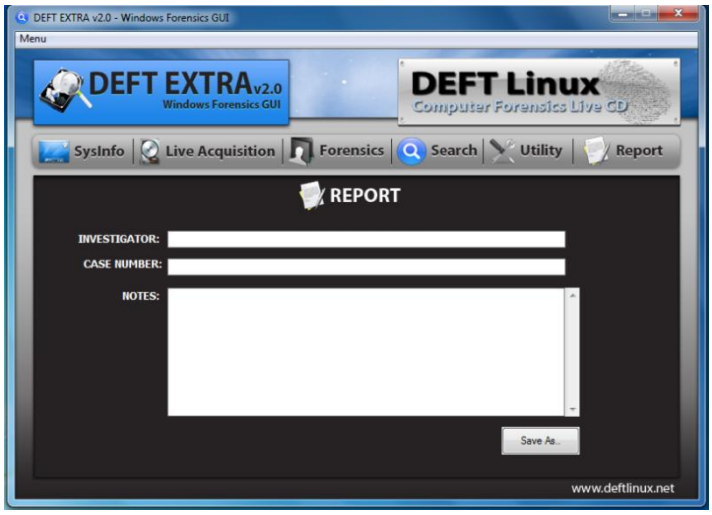


Ilustración O. 20 - Pantalla Módulo Report

ANEXO P: ANÁLISIS DE CELULARES

Análisis con Oxygen Forensic Suite 2010

Con esta herramienta podemos obtener principalmente una imagen de la memoria del celular y obtener la información relevante dentro de las memorias del dispositivo para proceder a clasificarla y analizar la evidencia. Dentro de la información principal que se puede obtener del dispositivo móvil se encuentra:

- Registros internos de los dispositivos
- Memoria física
- Memoria cache
- Registro estado de la red
- Registros de procesos en ejecución
- Contenido del portapapeles
- Archivos abiertos
- Servicios activos y drivers
- Registro de comandos ejecutados
- Usuarios conectados y autenticados
- Hora y fecha

Los siguientes pasos indican desde la detección del teléfono celular hasta obtener la información que se encuentra dentro de la memoria.

1. Ejecutar **Oxygen**.
2. Dar clic en **Connect a new device** y aparece la siguiente ventana:

Ilustración P. 1 - Oxygen Welcome

3. Clic en Next.
4. Conectar un dispositivo **vía USB** (el programa también permite conectarse vía **Bluetooth** y **puerto infrarrojo**)

Ilustración P. 2 - Oxygen tipos de conexión

5. Dar clic en el tipo de conexión según sea el caso.

6. El programa comienza la búsqueda de dispositivos conectados.

Ilustración P. 3 - Oxygen búsqueda de dispositivos

7. Una vez encontrado nos muestra el tipo del teléfono encontrado.

Ilustración P. 4 - Oxygen dispositivo encontrado

8. Dar clic en Next por dos ocasiones y aparece una pantalla donde se indica que el proceso de extracción de datos está a punto de empezar.

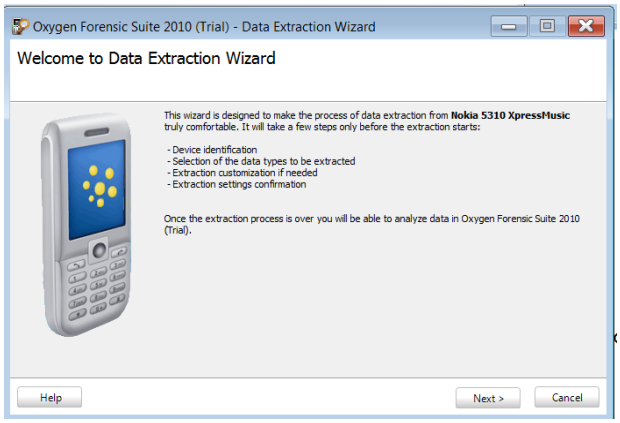


Ilustración P. 5 - Oxygen proceso de extracción de datos

9. Dar clic en Next aparece una pantalla para almacenar datos del caso.

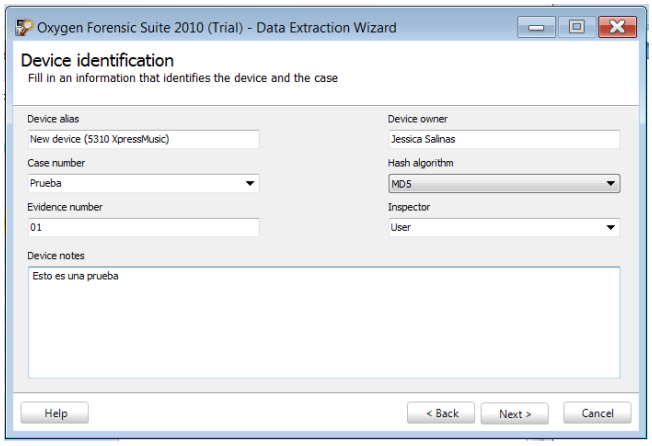


Ilustración P. 6 - Oxygen almacenar datos

10. A continuación podemos incluir el número del propietario:

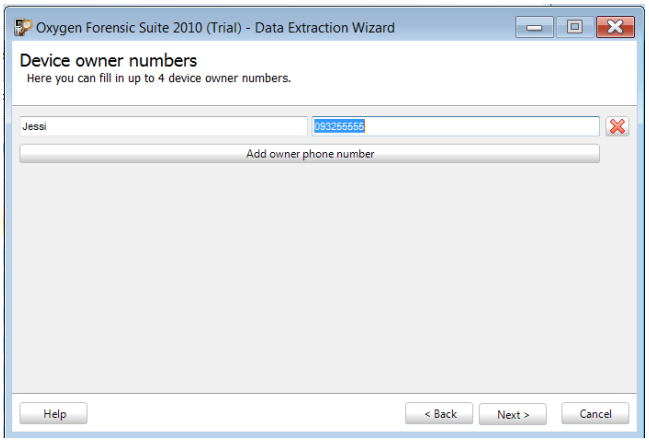


Ilustración P. 7 - Oxygen número del propietario

11. Al dar clic en Next nos muestra los datos que se van a extraer, podemos seleccionar los que sean útiles para nuestra investigación.

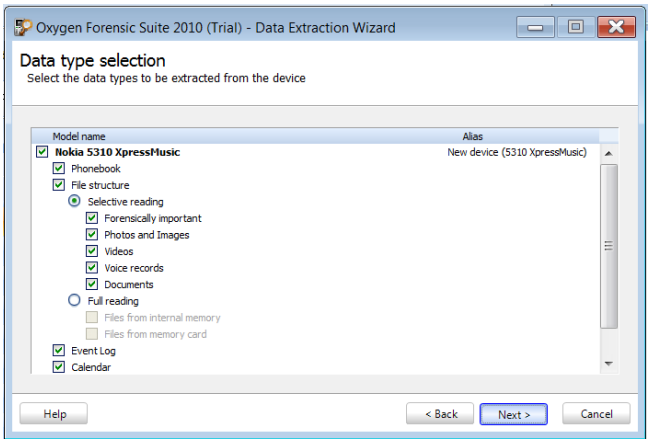


Ilustración P. 8 - Oxygen seleccionar datos

12. Al dar clic en Next nos muestra un informe detallado de lo que se va a extraer y detalles del caso.

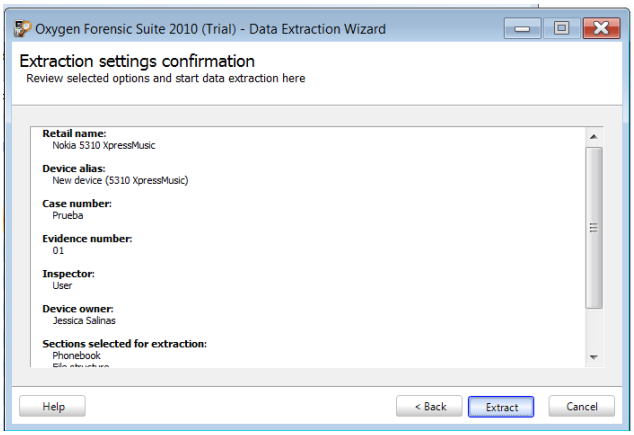


Ilustración P. 9 - Oxygen extracción de datos

13. Al dar clic en **Extract** empieza el proceso.

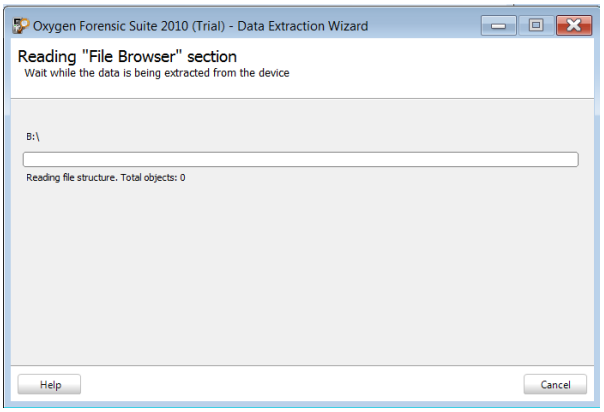


Ilustración P. 10 - Oxygen extrayendo datos

14. Al concluir el proceso nos da las opciones de exportar o empezar el análisis directamente.

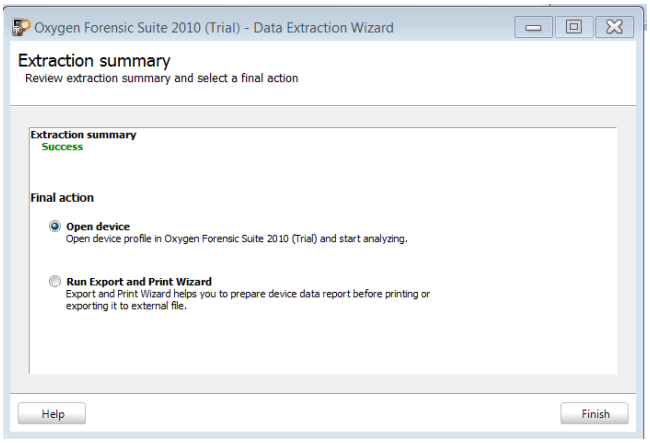


Ilustración P. 11 - Oxygen empezar análisis

15. Escogemos **Open device**. Se muestra la información del dispositivo, podemos explorar cada una de las opciones.

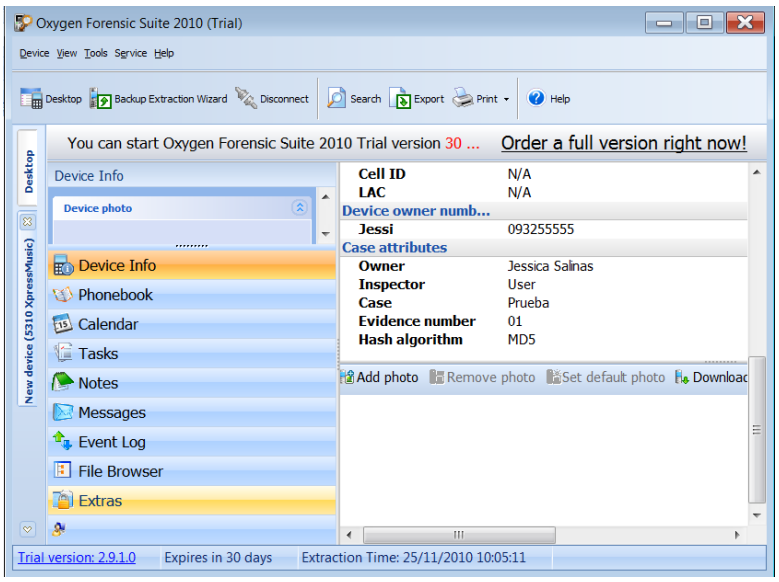


Ilustración P. 12 - Oxygen Información de dispositivo

16. **Phonebook**: Nos muestra un listado de los números telefónicos almacenados en el celular.

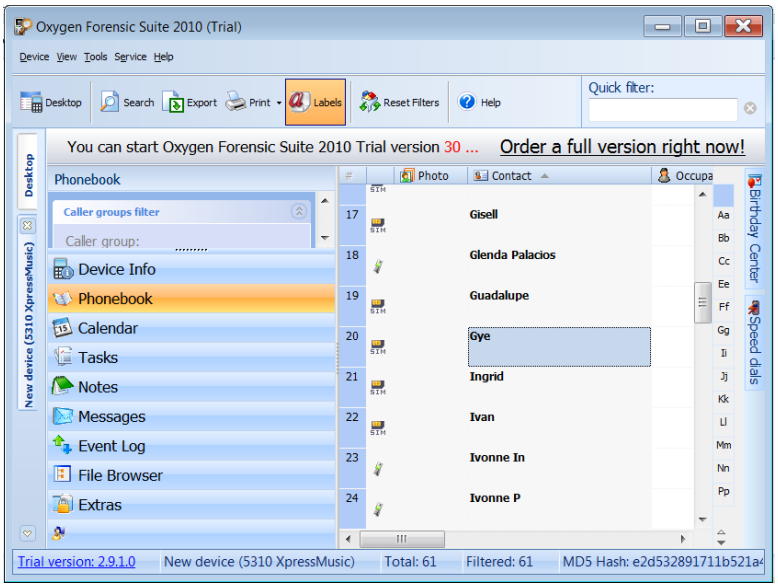


Ilustración P. 13 - Oxygen phonebook

17. **Calendar**: Anotaciones de eventos almacenados en el calendario.

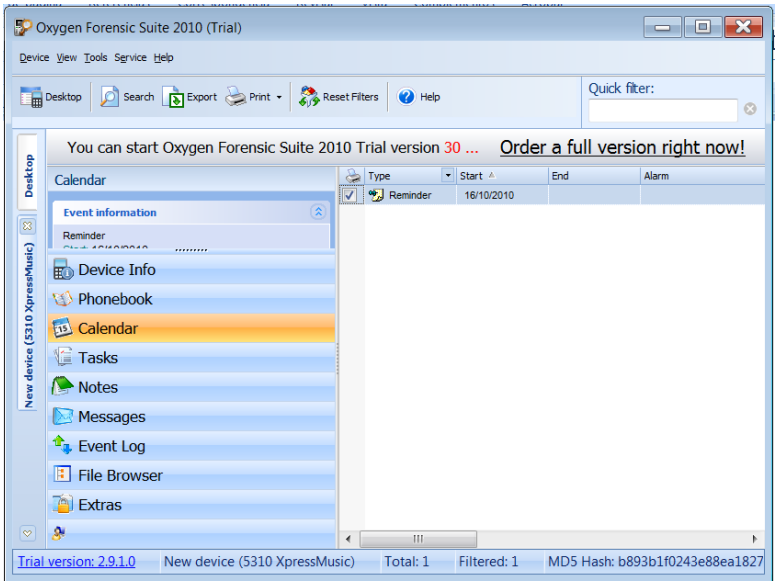


Ilustración P. 14 - Oxygen calendar

18. **Messages**: Detalles de mensajes enviados y recibidos.

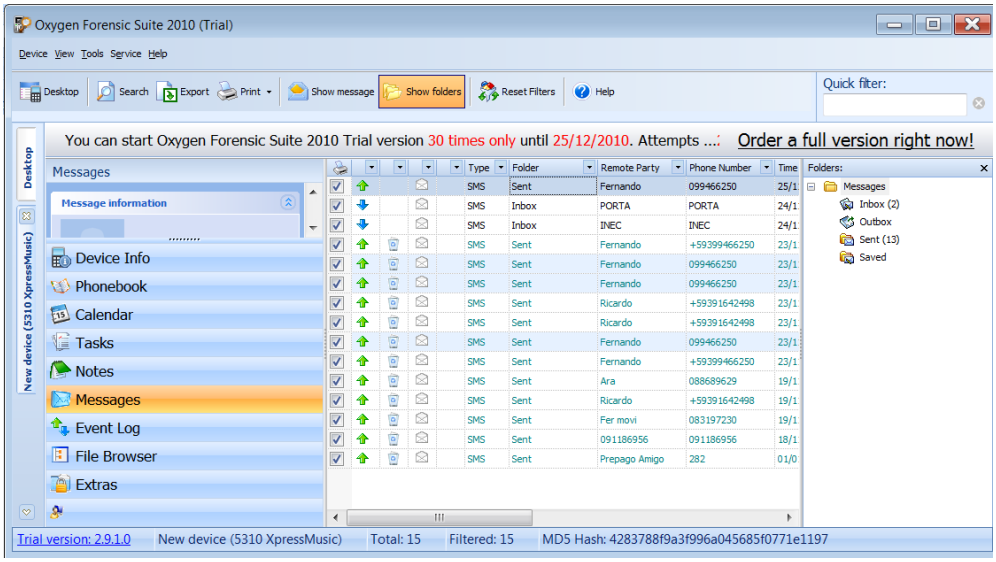


Ilustración P. 15 - Oxygen messages

19. **Event Log:** Detalle de eventos en el dispositivo tales como: mensajes, llamadas y navegación web.

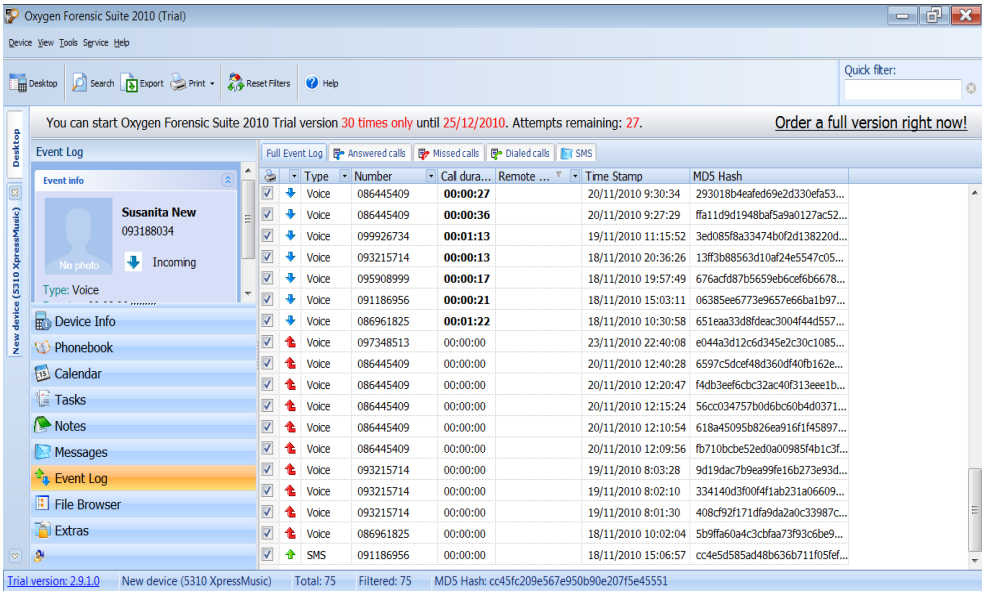


Ilustración P. 16 - Oxygen log

20. **File Browser:** Listado de todos los archivos encontrados en el teléfono, tanto en la memoria externa e interna.

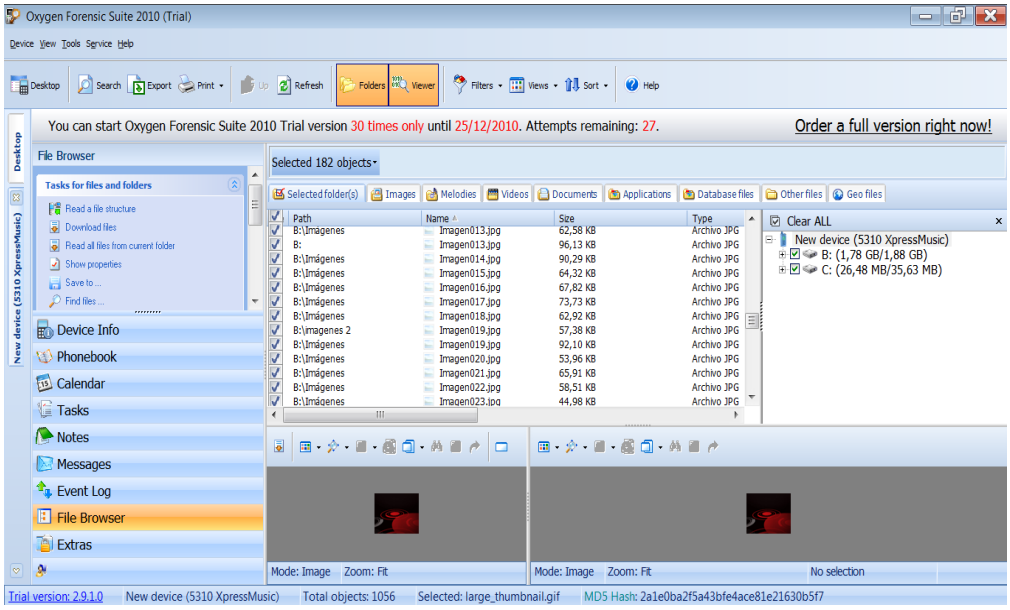


Ilustración P. 17 - Oxygen buscador de archivos

21. **Extras**

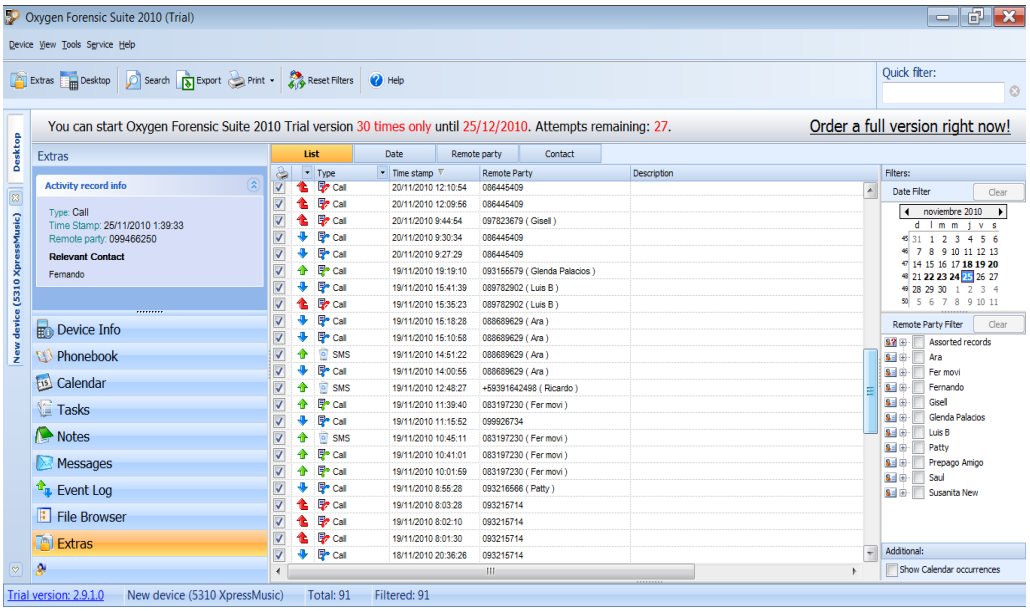


Ilustración P. 18 - Oxygen extras

22. Para realizar el **informe** procedemos a exportar los datos encontrados.

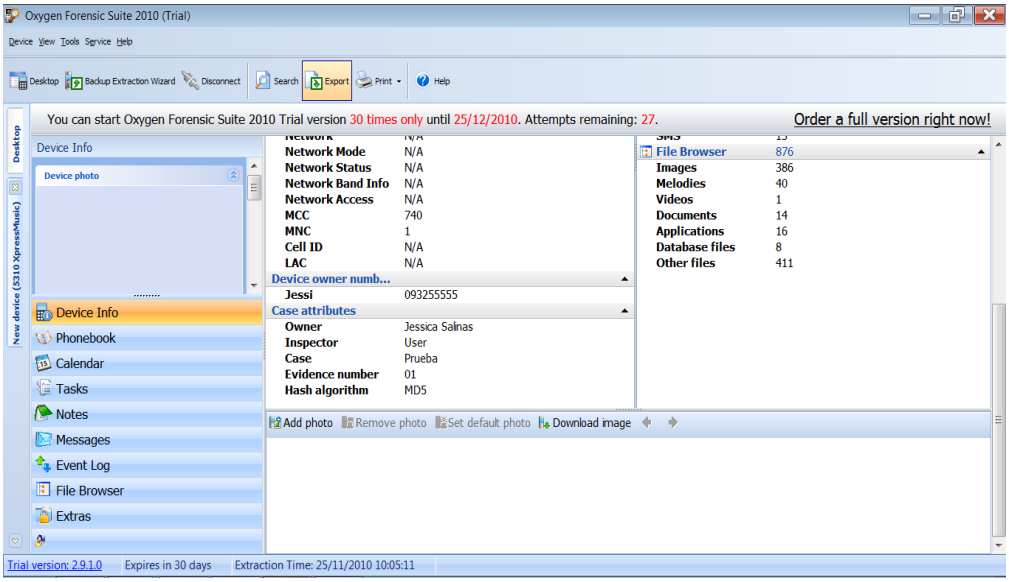


Ilustración P. 19 - Oxygen exportar datos

23. Y se genera un reporte en **formato PDF.**

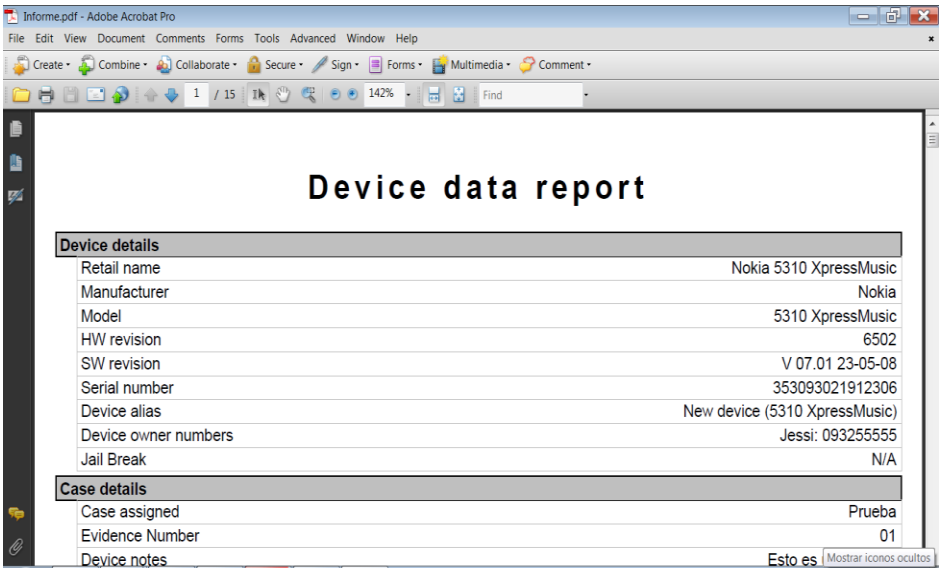


Ilustración P. 20 - Oxygen reporte

Análisis de SIM con Data Doctor Recovery - SIM Card

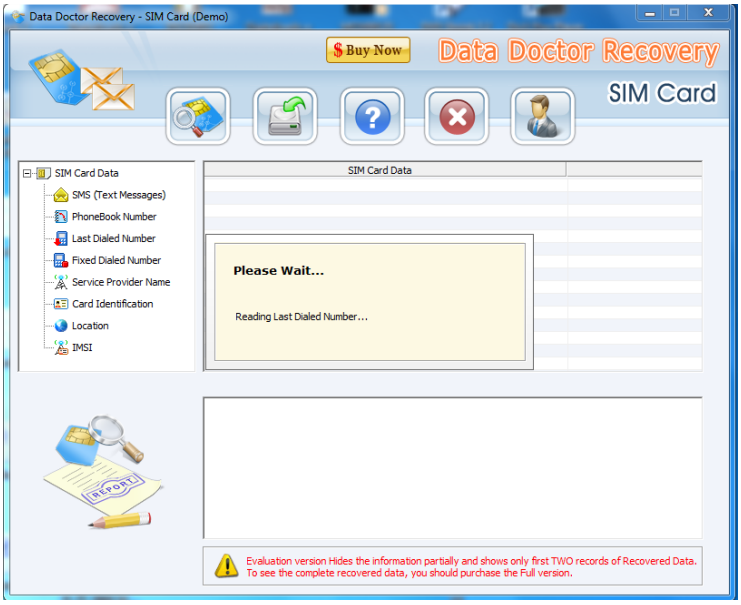


Ilustración P. 21 - Oxygen data doctor recovery

Permite la recuperación de números y mensajes de la tarjeta SIM. Para utilizar este programa se requiere un lector USB de tarjetas SIM.

Barra de herramientas

Tabla P. 1 - Barra de herramientas Data Doctor Recovery

Icono	Nombre	Descripción
	Search SIM Card	Explora los datos de la tarjeta
	Save Recovered Data	Permite guardar los datos recuperados.
	Help	Ayuda
	Exit	Salir

ANEXO Q: ARCHIVO CIFRADO

Podemos darnos cuenta de que un archivo está cifrado de varias maneras:

- La extensión del archivo es desconocida.
- Al abrir el documento encontrar la información de manera ilegible, con símbolos y caracteres extraños, etc.

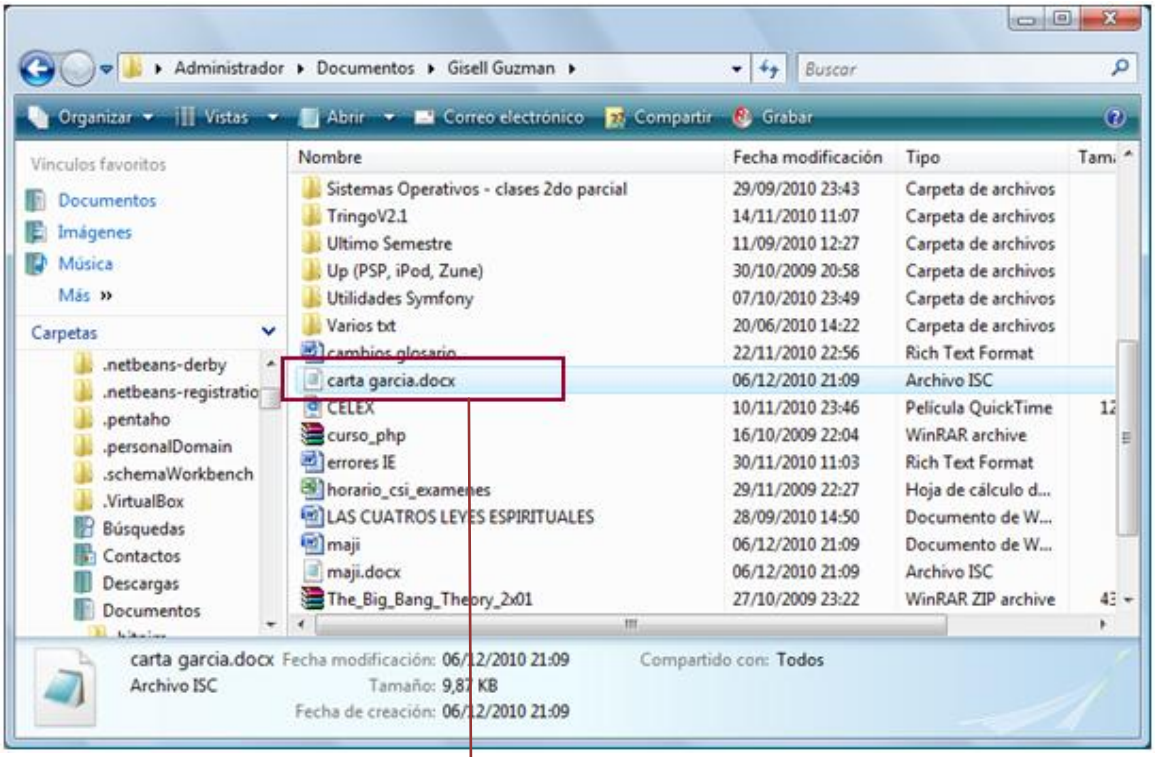


Ilustración Q. 1 - Archivo cifrado

Archivo cifrado

Este archivo, carta garcia.docx está cifrado y al abrirlo encontramos caracteres ilegibles que forman el contenido de este archivo.

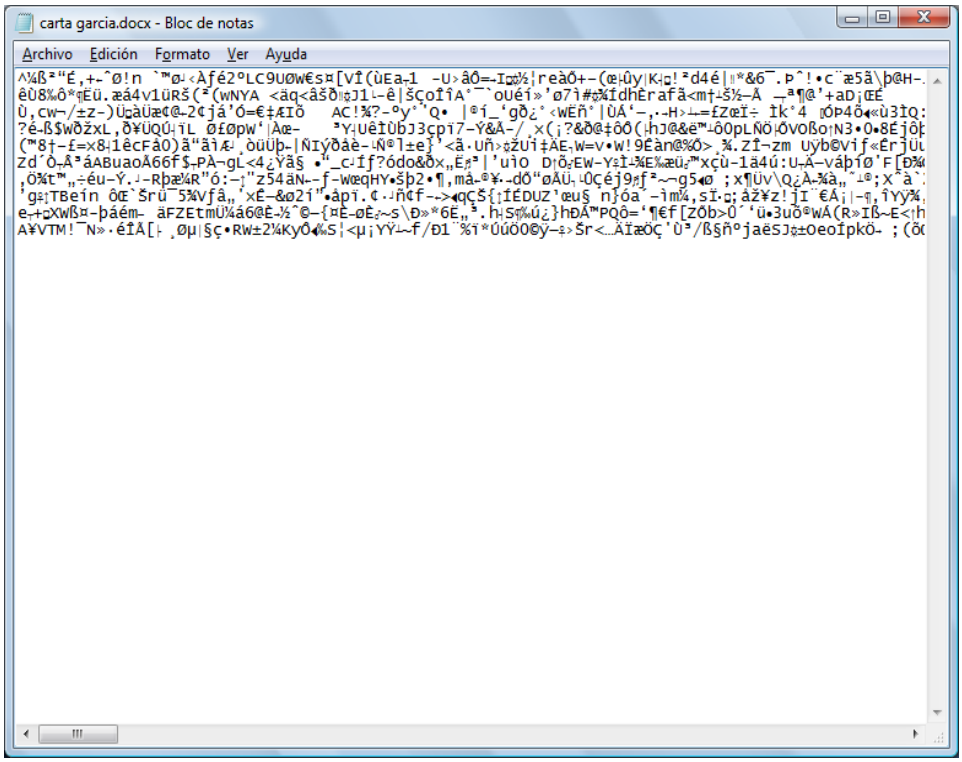


Ilustración Q. 2 - Contenido de archivo cifrado

ANEXO R: RASTREO DE CORREO ELECTRÓNICO

Para realizar el rastreo se necesita conocer la cabecera del correo electrónico que fue recibido.

Con esta cabecera se pueden utilizar herramientas para obtener la ip de origen de donde fue enviado el correo electrónico. En este caso utilizamos el sitio web http://whatismyipaddress.com/trace-email que nos ayuda en esta tarea.

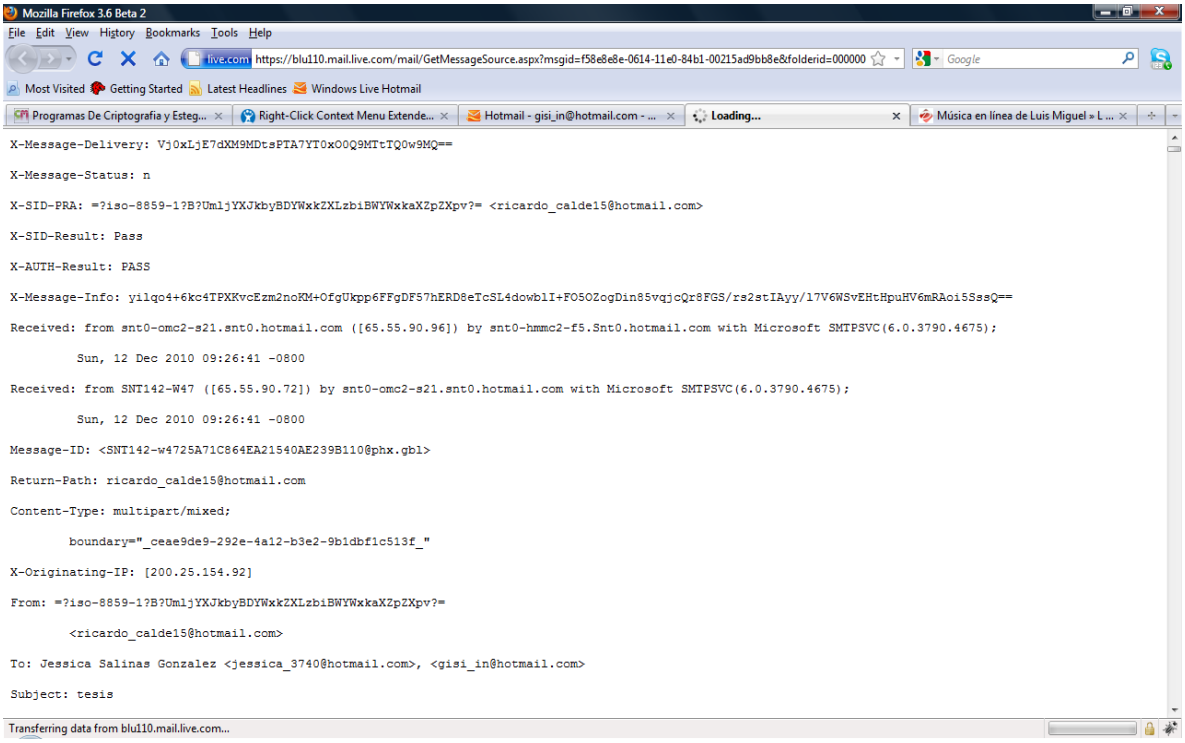


Ilustración R. 1 - Cabecera correo electrónico

Es necesario copiar la cabecera en el sitio web para obtener la ip de origen

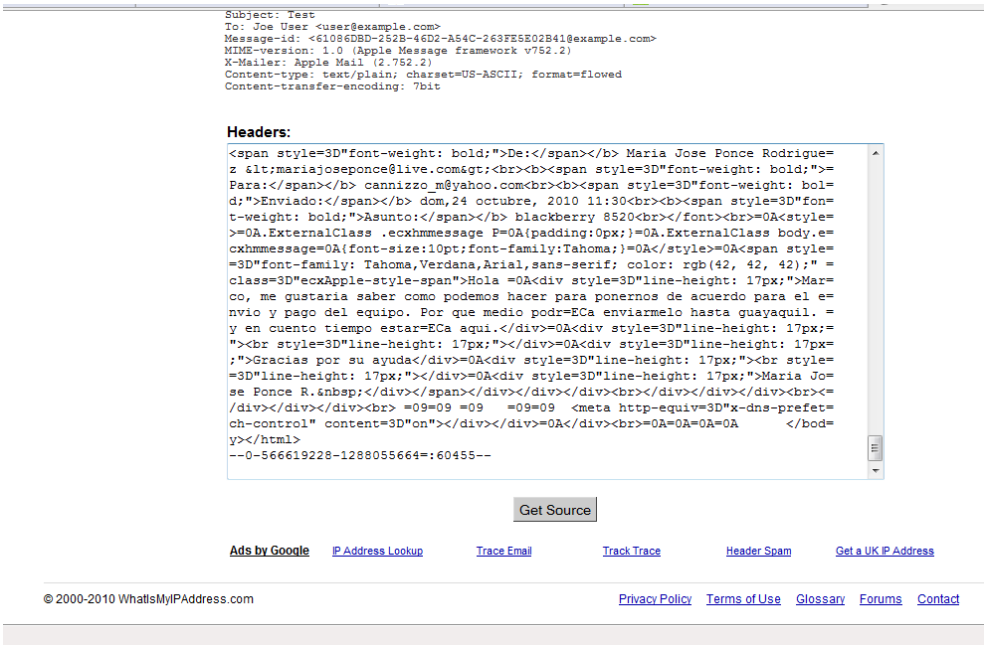


Ilustración R. 2 - Headers sitio What's my ip address

Se obtiene como resultado la dirección IP origen

Source:

The source IP address is 190.111.64.8.

Geo-Location Information

Country	Ecuador
State/Region	08
City	Arenillas
Latitude	-3.55
Longitude	-80.0667
Area Code	

Otra información necesaria es el ISP, para obtenerla accedimos a la siguiente dirección:

http://lacnic.net/cgi-bin/lacnic/whois?lg=EN&query=190.111.64.8, en la cual obtuvimos la siguiente información.

```
% Joint Whois - whois.lacnic.net
%  This server accepts single ASN, IPv4 or IPv6 queries

% LACNIC resource: whois.lacnic.net


% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2010-12-16 02:15:15 (BRST -02:00)

inetnum:     190.111.64/20
status:      allocated
owner:       CONECEL
ownerid:     EC-CONE-LACNIC
responsible: Robert Ordóñez Dueñas
address:     Edif. Centrum, Av. Fco de Orellana y Alberto Borge, 1,
3er Piso
address:     5934 - Guayaquil -
country:     EC
phone:       +593 4 2693693
begin_of_the_skype_highlighting              +593 4
2693693      end_of_the_skype_highlighting [2801]
owner-c:     ROD
tech-c:      ROD
abuse-c:     ROD
created:     20100106
changed:     20100106
nic-hdl:     ROD
person:      Anibal Gamboa
e-mail:      RedDaNac@CONECEL.COM
address:     Edif. Centrum; Av.Fco. Orellana y Alberto Borges, 1, 1
address:     5934 - Guayaquil -
country:     EC
phone:       +593 4 2693693
begin_of_the_skype_highlighting              +593 4
2693693      end_of_the_skype_highlighting [2020]
created:     20041208
changed:     20100105
```

ANEXO S: MÁQUINA COMPROMETIDA

Botnet

Los botnets (*o* software robots) representan en la actualidad una de las mayores amenazas en la web, detrás de estos *robots* se encuentran la mayoría de los fraudes que se cometen en internet.

Un botnet es un término que hace referencia a una colección de *software robots*, bots *o* zombies, que se ejecutan de manera autónoma. El dueño del botnet o bot master puede controlar todos los ordenadores/servidores infectados de forma remota. Para la creación de este tipo de *software* malicioso normalmente se utilizan lenguajes Orientados a Objetos para construir debido a que resultan mucho más cómodos.

La mayor parte del tiempo ni siquiera nos damos cuenta que nuestro ordenador es un software robot a disposición de alguna persona o mafia.

Como Se Puede Convertir El Computador En Un Robot (Botnet)?.

Para que un computador se infecte y forme parte de una botnet requiere que el usuario realice una acción como, instalación de programas de dudosa procedencia, ejecución de *cracks* y generadores de seriales (keygens), entre otros, son las principales maneras que pueden ocasionar que un ordenador se convierta en un botnet.

Como Podemos Identificar Una Botnet?

Para detectar que nuestro computador está siendo usado en una botnet podemos tomar en cuenta los siguientes aspectos: el equipo tarda mucho tiempo para apagarse, o no lo hace correctamente, con frecuencia el malware posee errores que pueden causar una variedad de síntomas, incluyendo que el apagado del sistema sea muy largo o directamente falle, Las aplicaciones andan muy lento**,** esto puede ocurrir porque programas ocultos estén utilizando una gran cantidad de recursos del equipo.

Además no se pueden descargar las actualizaciones del sistema operativo, del antivirus o visitar sitios web de los proveedores**:** este es un síntoma que no se puede ignorar.

El acceso a internet es muy lento: si un bot está en ejecución en el sistema para, por ejemplo, enviar grandes cantidades de spam, realizar un ataque contra otros equipos, puede causar que el acceso a internet sea muy lento. Para confirmarlo, se debe de deja de navegar completamente, acceder al administrador de tareas (CTRL+ALT+SUPR), selecciona Funciones de Red y observa si tu ordenador está usando Internet, en caso afirmativo esta sería una prueba bastante evidente de que eres parte de una red zombie.

Recomendaciones

Las recomendaciones son básicamente las mismas que se utilizan cuando se cuenta con un virus, escanear con un buen antivirus (actualizado) y como se mencionó, monitorear la actividad en la red.

Si al hacer la prueba anterior confirmamos que ya somos un Bot es lógico pensar que nuestro actual antivirus no está dando los resultados que esperábamos, Algunas de las herramientas gratuitas creadas para detectar la intrusión son RuBotted de Trend Micro, Bot Hunter de SRI International, y el escaneo de Windows Live OneCare.

En el caso de Eset Nod32 Antivirus, las detecciones Win32/Spy.Zbot, IRC/SdBot y Win32/AutoRun.IRCBot, entre otras, indican la presencia de malware del tipo bot.

ANEXO T: RETO ANÁLISIS FORENSE DIGITAL

Objetivos

Realizar un análisis forense sobre una imagen de disco perteneciente al principal sospechoso involucrado en un caso acoso a menores de edad así como la distribución de pornografía infantil a través de internet.

Recolectar pruebas suficientes y válidas para incriminar al sospechoso en el caso señalado, y demostrar que este equipo fue utilizado para llevar a cabo actividades ilícitas.

1. Descripción de la Evidencia

Para llevar a cabo el análisis se facilita un snapshot del sistema objetivo en formato ".wmdk" (Virtual Machine Disk).

La imagen a analizar podrá ser descargada desde los siguientes enlaces:

Cada imagen posee el valor hash MD5, CRC32 y SHA-1 para comprobar su integridad por medio de checksum, es decir que no haya sido manipulada desde la obtención de la misma.

Parte 1 del Reto Forense Comunidad DragonJAR

CRC32: 76B78AE4

MD5: D542187FF2C9D651BAF40FF488C367FE

SHA-1: A51BA56118F094C910F9BF428ACF27FBD935679A

Parte 2 del Reto Forense Comunidad DragonJAR

CRC32: 2F55CB1E

MD5: C33FA1AF1EBA82EB07182106E1A1B060

SHA-1: 63052A87F323BD729ACDB8AEF4FD311080E2D9C8

Parte 3 del Reto Forense Comunidad DragonJAR

CRC32: 59CD3705

MD5: 08FF1B6A0E8CBD1DF1724B40B20228E2

SHA-1: D228E81F5FDC20F561967C8EBF15CD49B7EB6F96

Parte 4 del Reto Forense Comunidad DragonJAR

CRC32: 125309ED

MD5: 6F0D583A6560D49004B9FD52065CDBC2

SHA-1: 29E52CD2A28CA65007CD16FD95418B566B1F0980

Parte 5 del Reto Forense Comunidad DragonJAR

CRC32: 731CF2D6

MD5: 4FD27F4415BE756B0C47BD04C54D586C

SHA-1: FB6B31CD8A4D2ED5E6D9EF96B974485826F2399D

2. Entorno de trabajo

Para el estudio de la imagen adquirida vamos a utilizar el software VMware Workstation, en el cual se carga la imagen del sistema operativo y se conectaran los dispositivos necesarios con las herramientas forenses para realizar el análisis, en estos mismo dispositivos se almacenaran los datos recolectados y fundamentales para la investigación.

3. Herramientas utilizadas

Para llevar a cabo el análisis nos ayudamos de varias herramientas forenses.

Tabla T. 1 - Herramientas forenses reto DrajonJar

Herramienta	Descripción
VMware	Software de emulación de máquinas virtuales.
Deft extra	Kit de herramientas y utilidades forenses
Imager Lite	Adquisición y tratamiento de imágenes para ser posteriormente usadas y tratadas como de evidencias forenses.
Lads	Búsqueda de Alternate data Stream. (ADS)
LAGADS	Lista y extrae Alternate Data Stream

4. Recolección De Datos

Se procederá a recoger datos o rastros de los mismos existentes en:

- Procesos en ejecución
- Servicios Activos

- Programas Instalados
- Temporales de Internet
- Historial y Carpetas de Mensajería instantánea (MSN)
- Clúster no asignados del HD
- Archivos borrados

5. Análisis

5.1. Integridad de la evidencia

Descargada la imagen del disco es necesario verificar el checksum MD5 facilitado, para garantizar que la evidencia no haya sido alterada luego de haber sido publicada.

Para obtener el valor MD5 realizamos los siguientes pasos:

1. Descomprime el MD5.ZIP, el cual se puede descargar de http://www.mundoprogramacion.com/colabora/md5.zip
2. Copiar el fichero MD5.exe en una carpeta que esté en PATH.
3. Abre una ventana de MS-DOS
4. En la ventana de comandos, escribir **MD5** seguido de un espacio y la ruta donde se encuentra el ZIP al que se quiere obtener el valor de comprobación.
5. Al dar ENTER se presenta una lista de números hexadecimales.

6. Esta lista de letras y números es la que tienes que usar para comparar con el valor MD5 facilitado inicialmente.

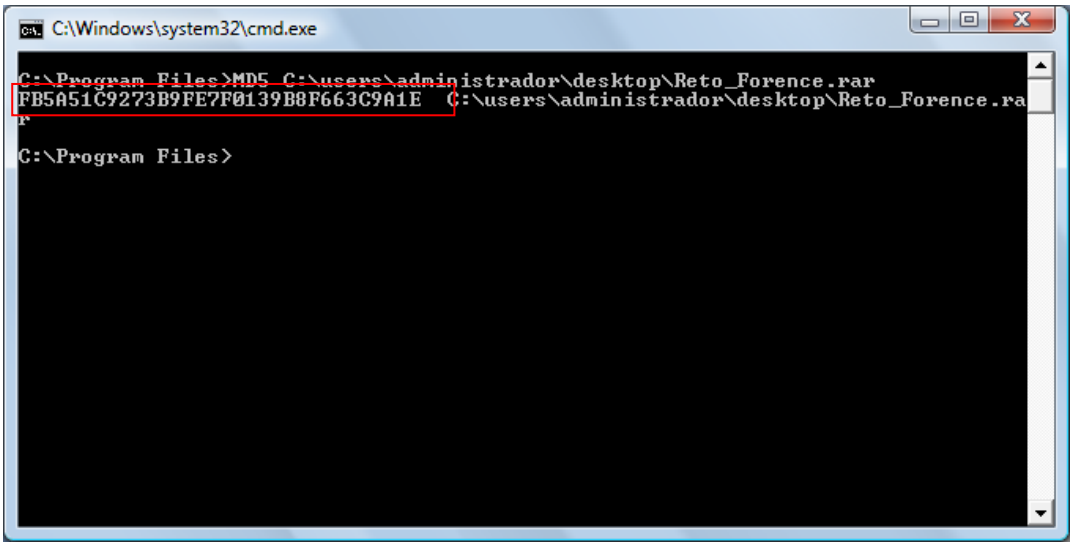


Ilustración T. 1 - MD5

5.2. Identificación de la Evidencia

Una vez que cargamos la imagen con el Software VMWare Workstation, al entrar a las propiedades del sistema podemos determinar:

- El Sistema Operativo cargado es Windows XP corriendo con el Service Pack 3.
- Como usuario propietario tenemos el nombre de "**Scarface**"
- La fecha de instalación del S.O. fue el 15-12-2009

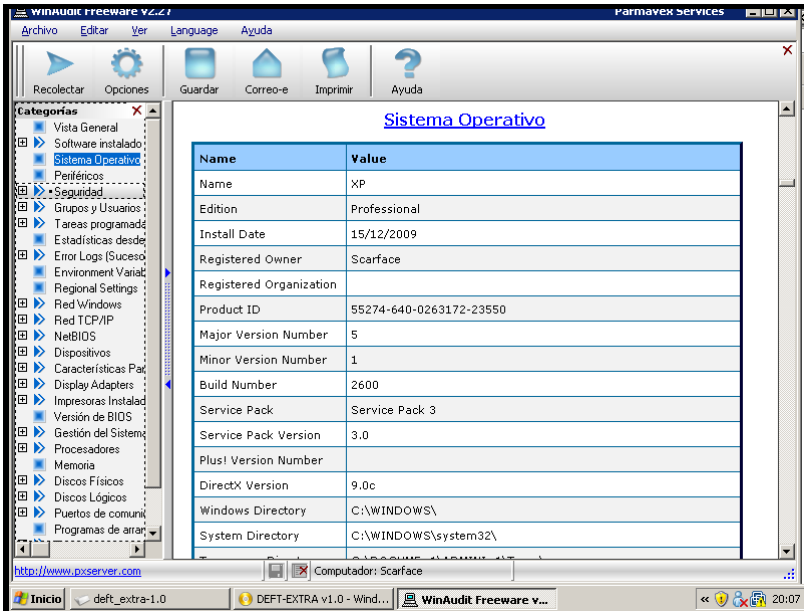


Ilustración T. 2 – Detalles Sistema Operativo

Para obtener los datos principales del sitema operativo utilizamos la herramienta WinAudit.

El uso horario configurado es el de EE.UU. y Canadá. Existe solo un acuenta de usuario Admnistrador, la cual no tiene contraseña para ingresar.

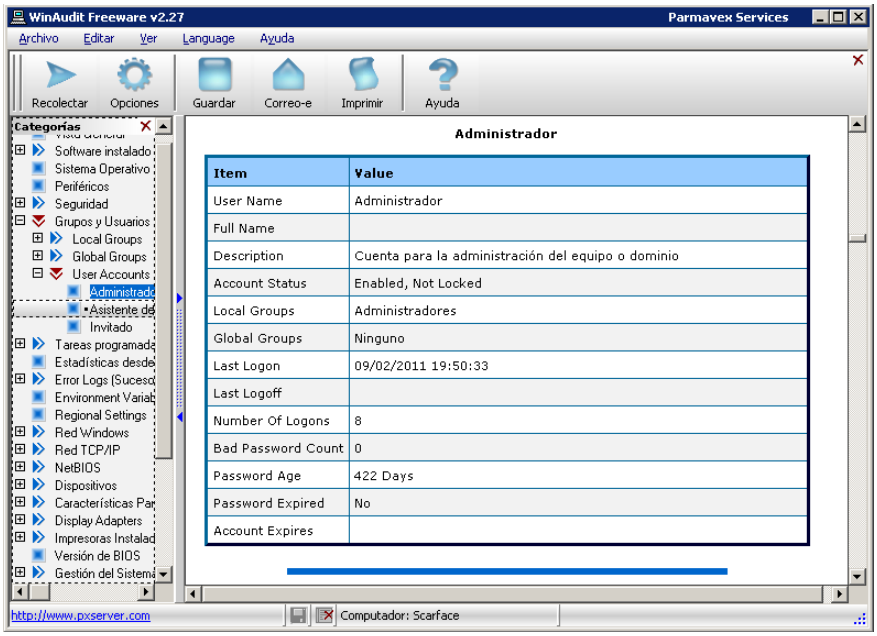


Ilustración T. 3 - Detalles usuario administrador

5.3. Software instalado

Se determina el software instalado en el sistema.

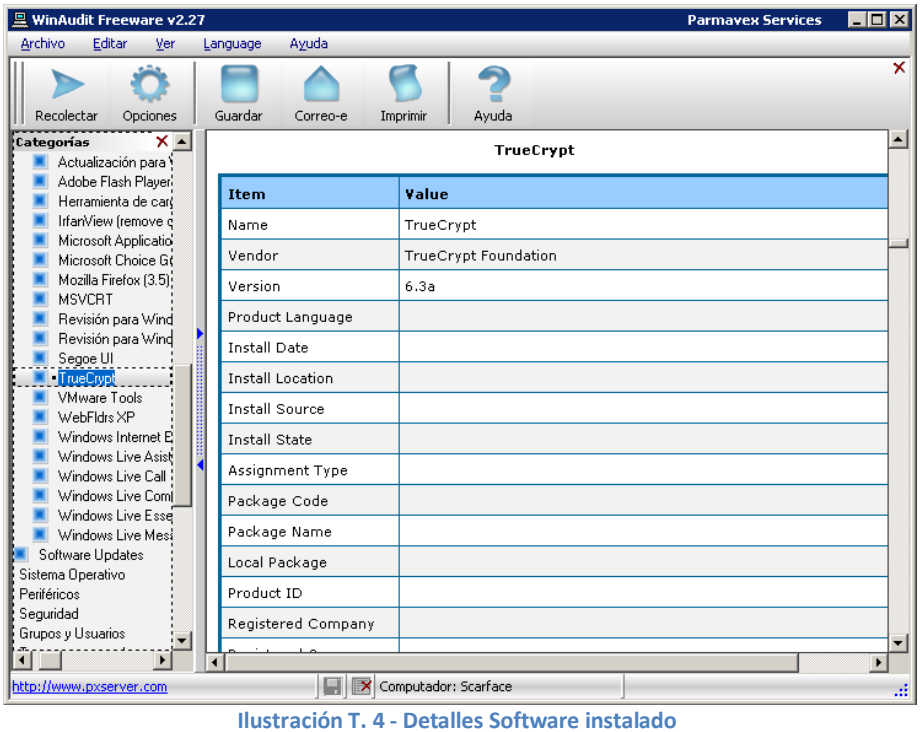


Ilustración T. 4 - Detalles Software instalado

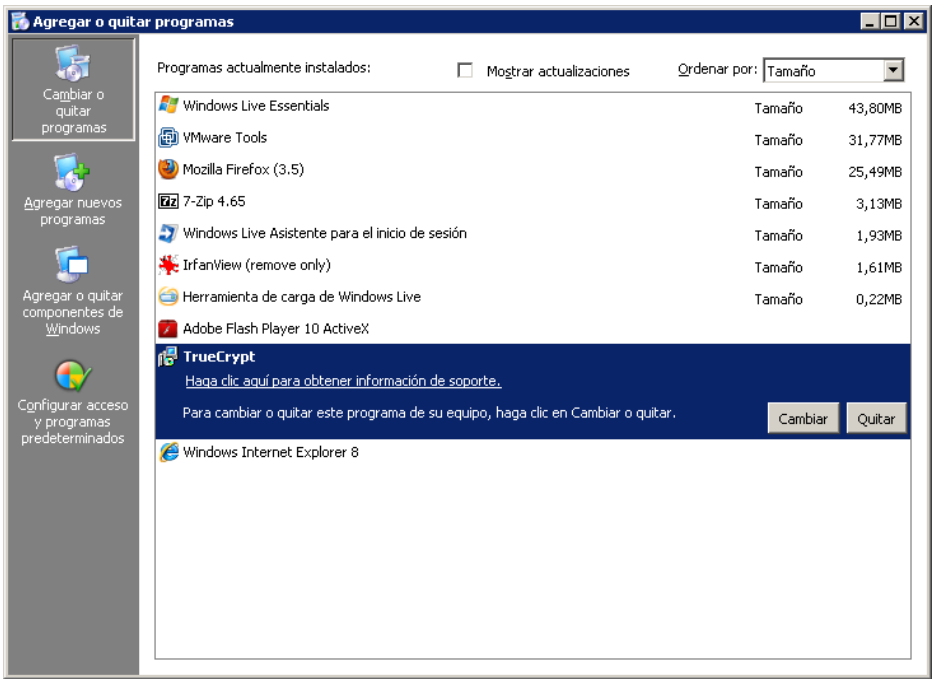


Ilustración T. 5 - Programas instalados

Determinamos los programas instalados en el equipo, dentro de los cuales encontramos el software **TrueCrypt**, por lo que podríamos esperar encontrar ficheros o volúmenes de discos duros encriptados.

5.4. Servicios y procesos en ejecución

Determinamos los servicios y procesos que están corriendo en el sistema, de los cuales el que más llama la atención es el servicio de TrueCrypt ejecutándose a nivel de Kernel y fue iniciado por el sistema, de lo cual concluimos que el software que llama a este servicio se utiliza normalmente.

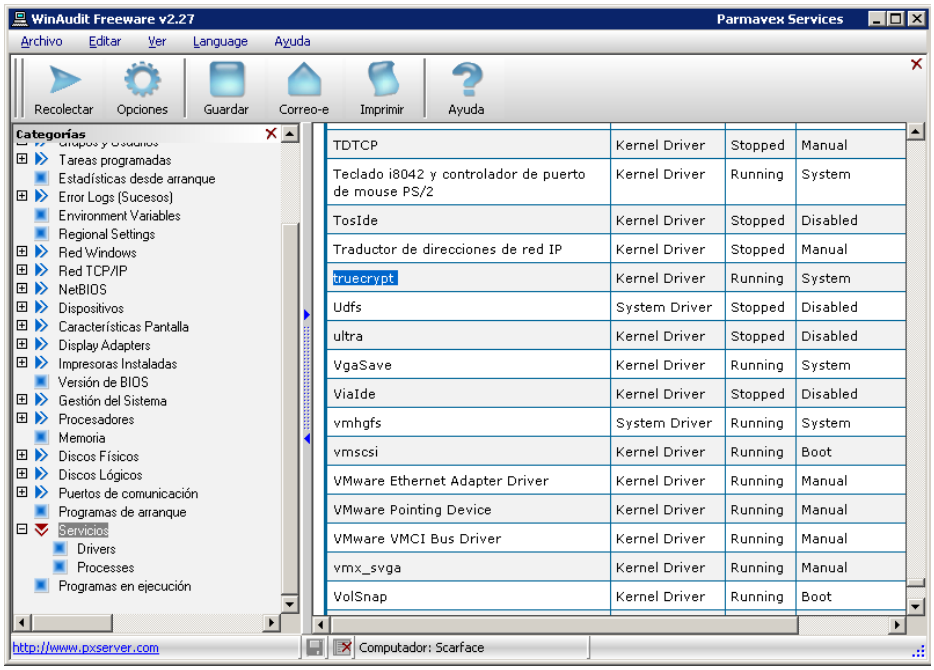


Ilustración T. 6 - Detalle WinAudit

5.5. Programas y servicios de inicio

Revisamos el software y los servicios que se ejecutan al iniciar el sistema operativo, pero no encontramos algún software sospechoso.

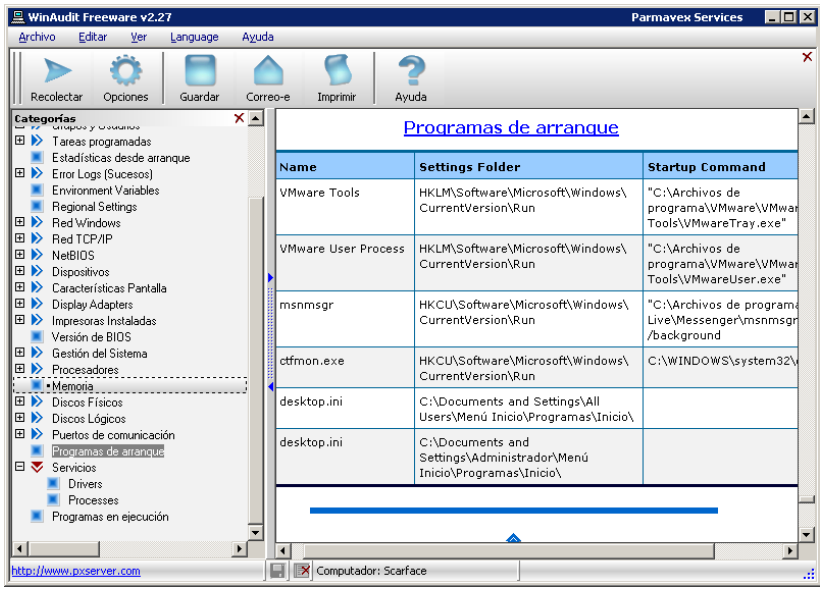


Ilustración T. 7 - Programas de arranque

5.6. Programas ejecutados en el sistema

Nuevamente vemos que el software TrueCrypt se ha ejecutado varias veces. Le damos importancia a este software ya que sirve para cifrar y ocultar datos en el ordenador usando diferentes algoritmos de cifrado.

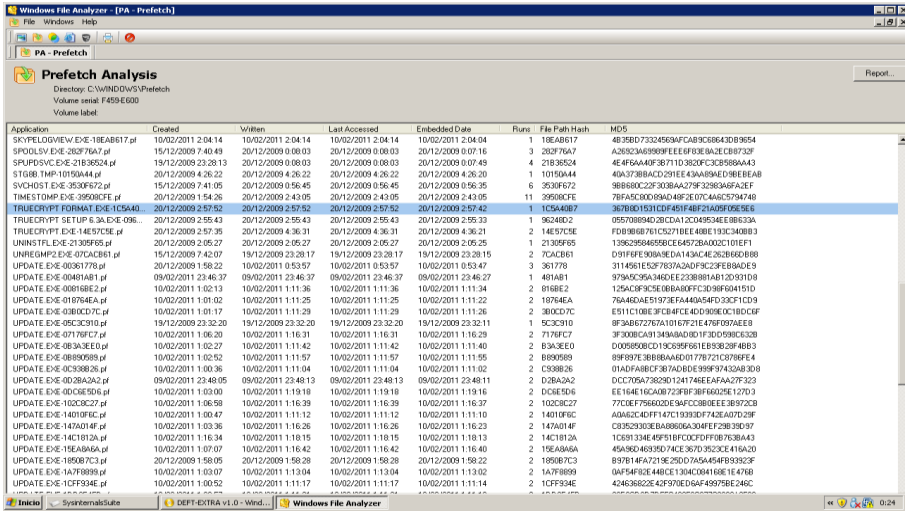


Ilustración T. 8 – File Analyzer

6. Metodología

6.1. Búsqueda de “Alternate Data Stream”

Utilizando la herramienta LADS encontramos Metainformación oculta dentro del fichero **Scarface.jpg.**

Alternate Data Stream es una característica de los archivos NTFS en los que s oculta un fichero dentro de otro.

Ilustración T. 9 - Búsqueda ADS

Al ejecutar este comando se realiza una búsqueda en el disco C, luego se obtienen los resultados en el archivo resultado.txt

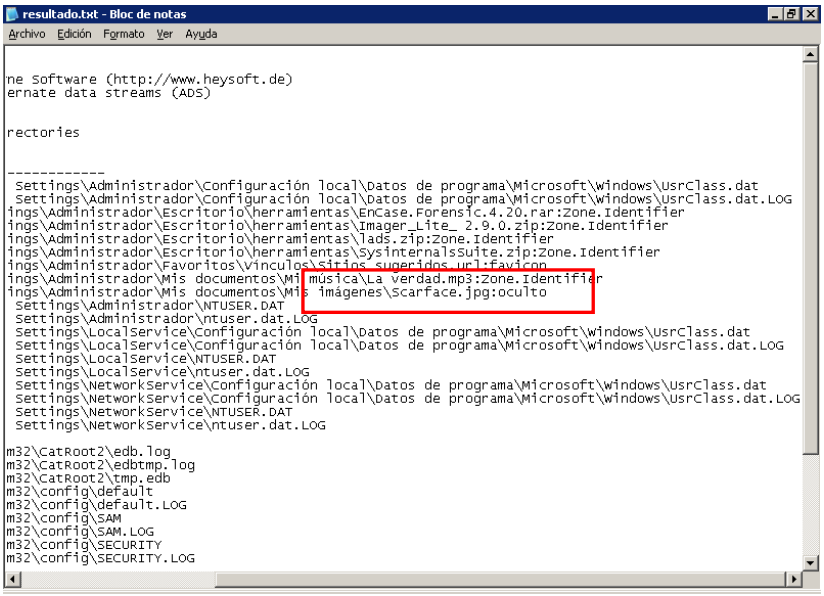


Ilustración T. 10 – ADS encontrado

Necesitamos ubicar la imagen en la que se encuentran los metadatos ocultos, para esto usamos la herramienta FTK Imager

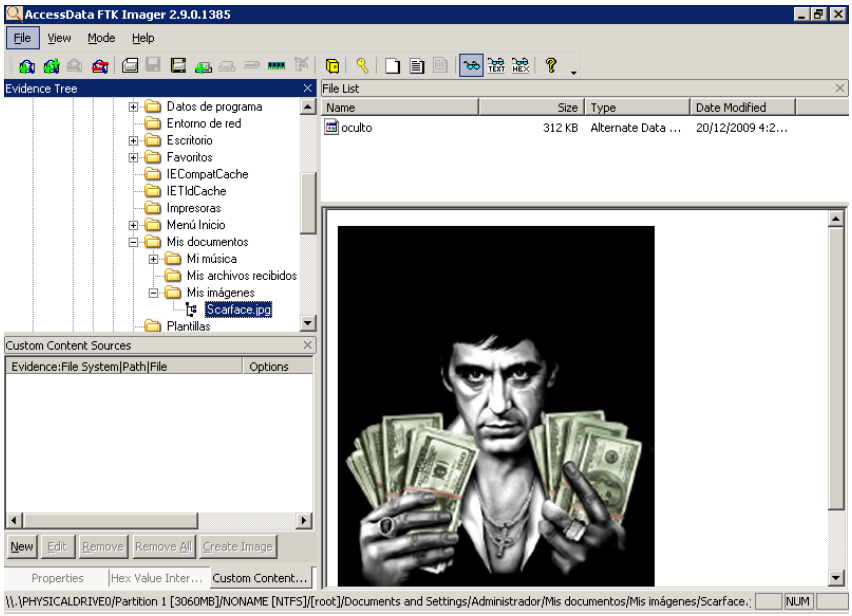


Ilustración T. 11 - Tipo de fichero oculto

Necesitamos determinar qué tipo de fichero se encuentra oculto en la imagen, para esto ejecutamos el comando more en la consola.

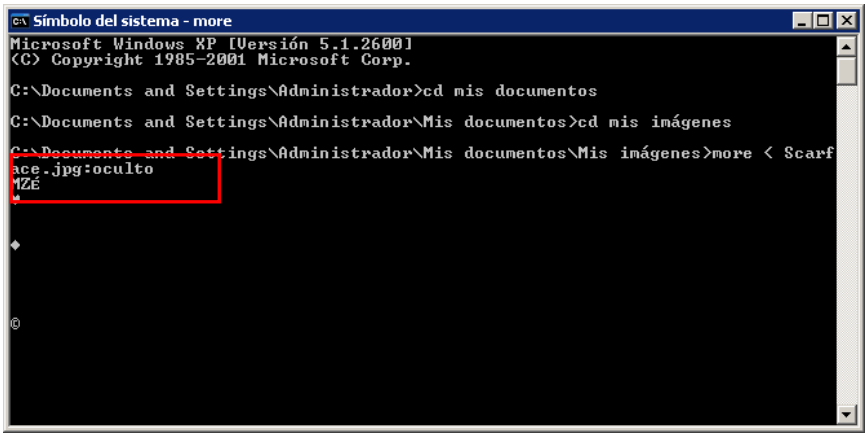


Ilustración T. 12 – Comando more

El resultado presenta que el fichero es un ejecutable.

Ya que tenemos la información del fichero, es decir donde está oculto y que extensión tiene, procedemos a extraer el fichero oculto dentro de Scarface.jpg. Para esto utilizaremos la herramienta LAGADS.

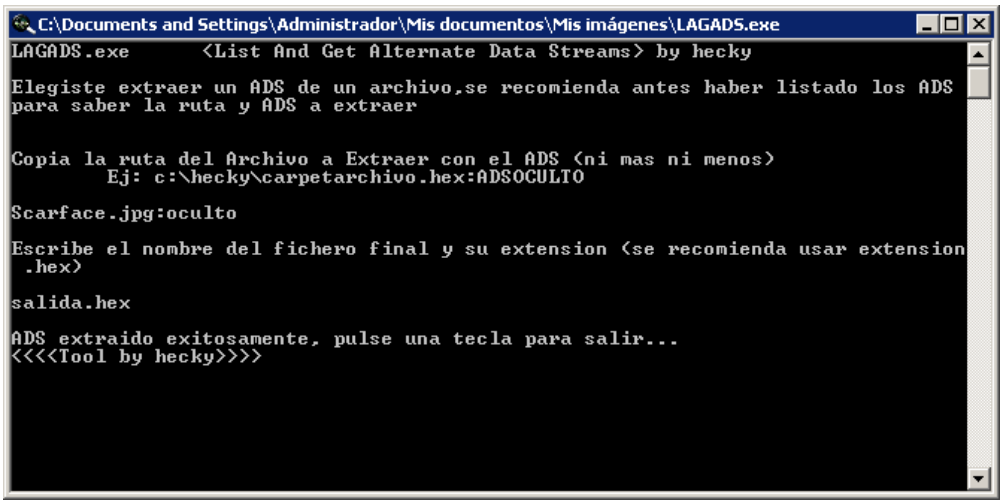


Ilustración T. 13 - Extraer ADS

Como resultado se obtuvo un archivo hexadecimal “salida.hex”

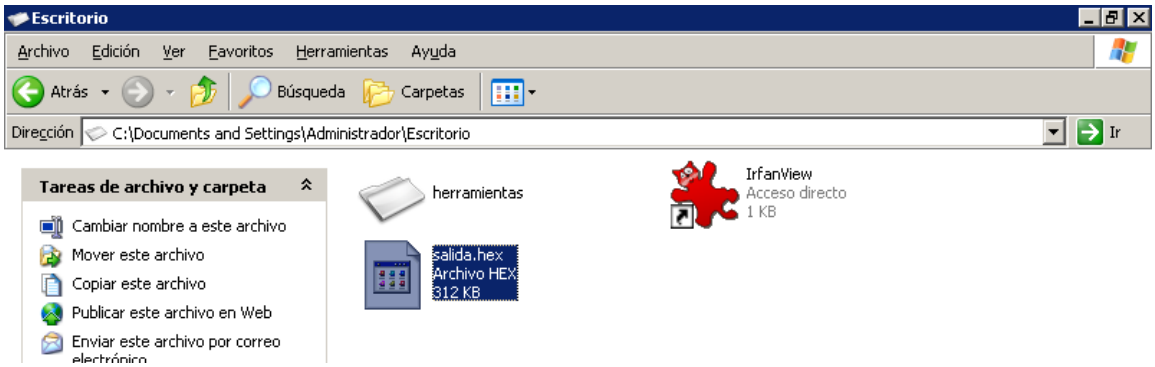


Ilustración T. 14 - Archivo oculto obtenido

Como ya conocemos la extensión del fichero oculto vamos a cambiar la extensión .hex por .exe para determinar el programa que se ejecuta.

El software que se ejecuto es la herramienta que contiene datos cifrados “Steganos LockNote”, el cual es una herramienta que permite codificar nuestros textos de una forma sencilla y fiable, utiliza el algoritmo AES de 256 bits.

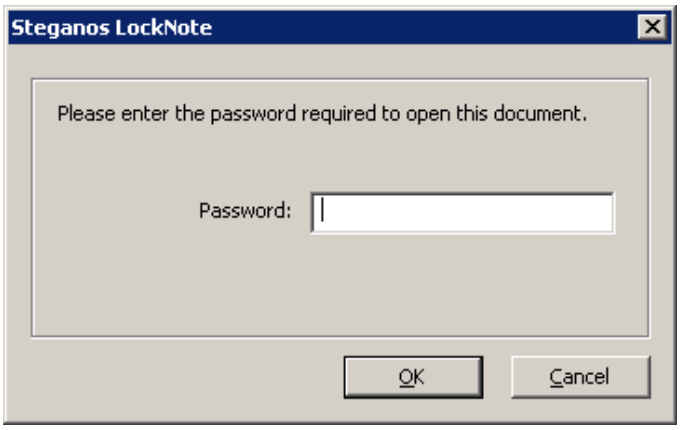


Ilustración T. 15 – password Locknote

Esta herramienta nos pide una contraseña para poder acceder. Para obtener la contraseña requerido vamos a buscar rastros dejados en el equipo de esta información.

6.2. Búsqueda de volúmenes de datos cifrados con TrueCrypt

Como primera estrategia vamos a realizar una búsqueda en el disco duro, utilizando como parámetros archivos mayores a 1000 Kb y que no posean extensión para poder compararlos con los del sistema que cumplan estas condiciones y poder analizar los determinados como sospechosos.

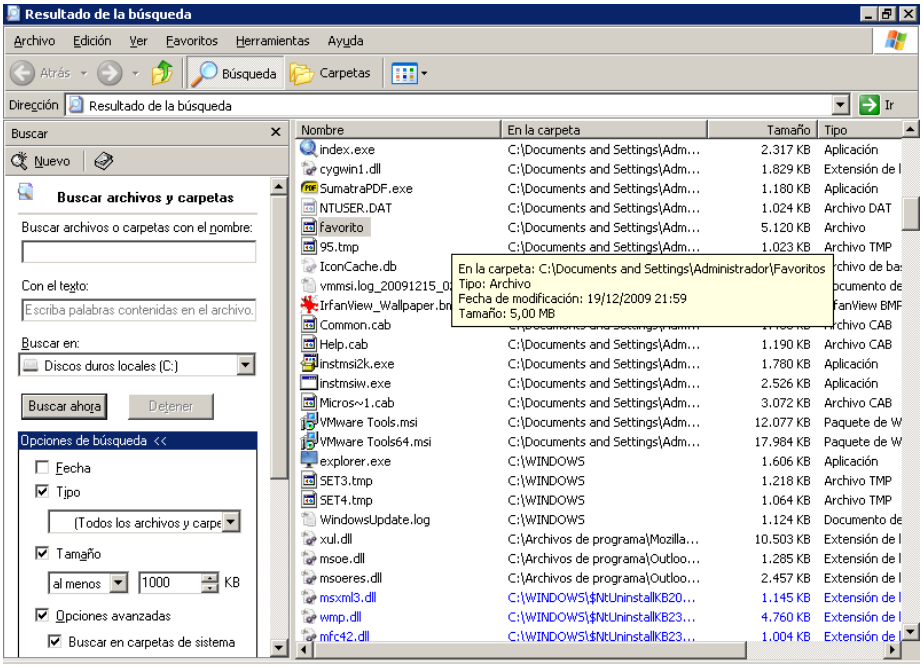


Ilustración T. 16 - Fichero sospechoso

El fichero que más se destaca es el llamado “favorito” localizado en la carpeta Favoritos, pesa 5.120 KB y no posee extensión, por lo tanto podemos sospechar que es un volumen cifrado de datos.

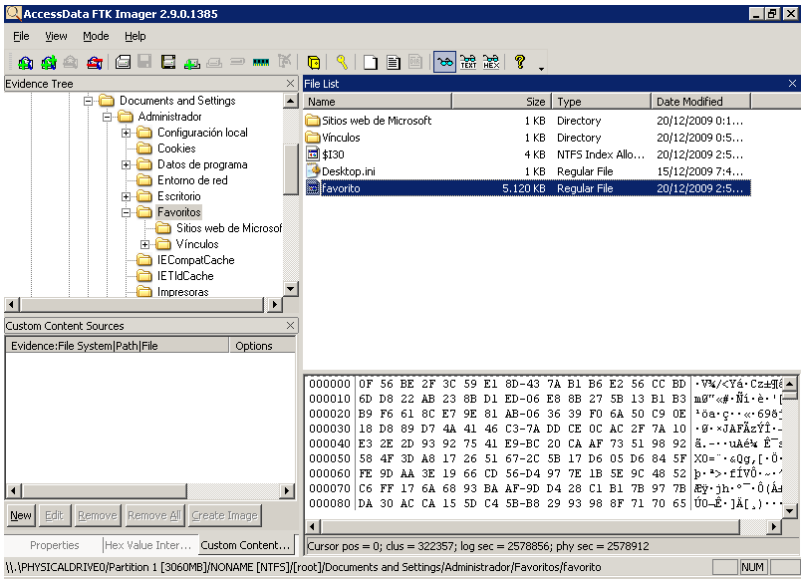


Ilustración T. 17 - Archivo sospechoso visto con FTK Imager

6.3. Localización de la aplicación TrueCrypt

Necesitamos encontrar la aplicación TrueCrypt para comprobar que el fichero encontrado “favoritos” se trata de un volumen cifrado con esta herramienta.

Como ya lo hemos determinado esta herramienta se encuentra instalada en el equipo y corriendo en el sistema pero no es encontrada en los archivos de programa o en su localización predefinida de instalación.

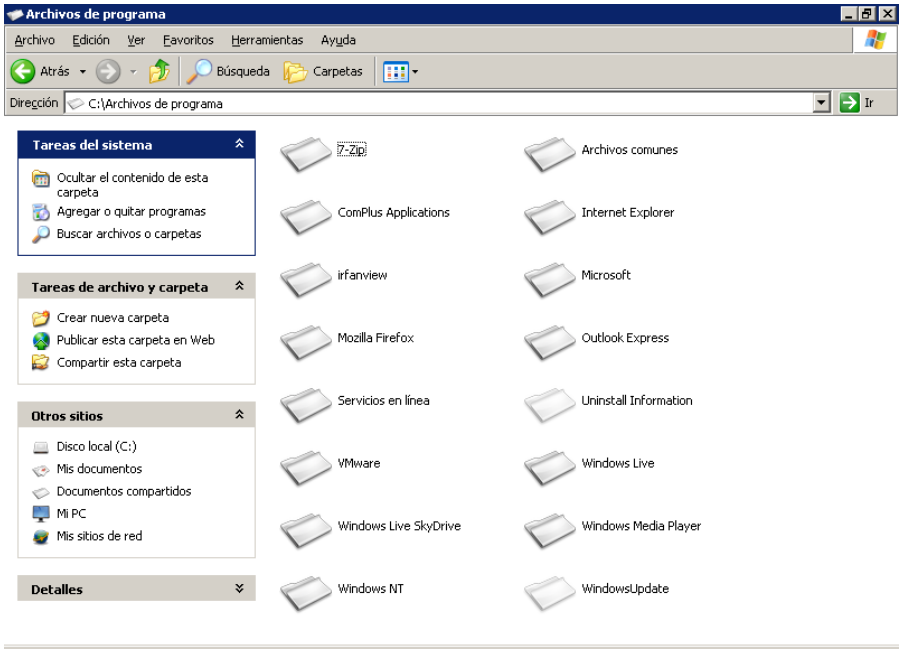


Ilustración T. 18 - Archivos de programas

Ilustración T. 19 – Listado de programas

Verificamos la opción de configuración para mostrar carpetas y archivos ocultos para proceder a realizar una búsqueda de la aplicación TrueCrypt por el motor del sistema operativo.

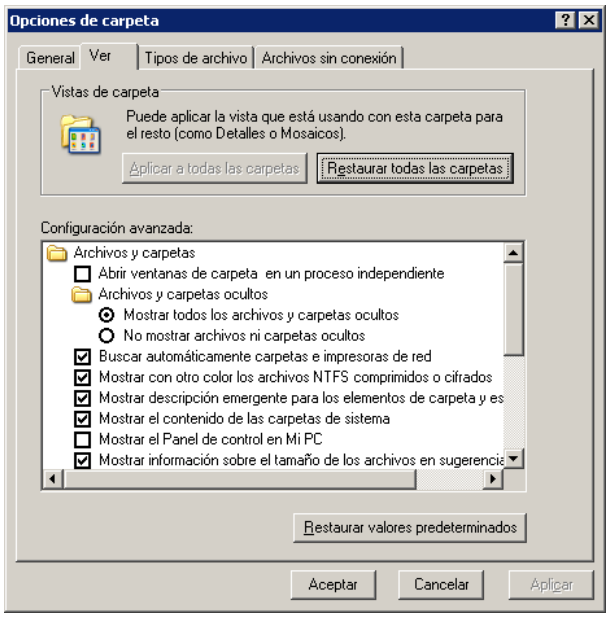


Ilustración T. 20 - Mostrar archivos ocultos

Luego de realizar la búsqueda del ejecutable TrueCrypt no se encontraron resultados.

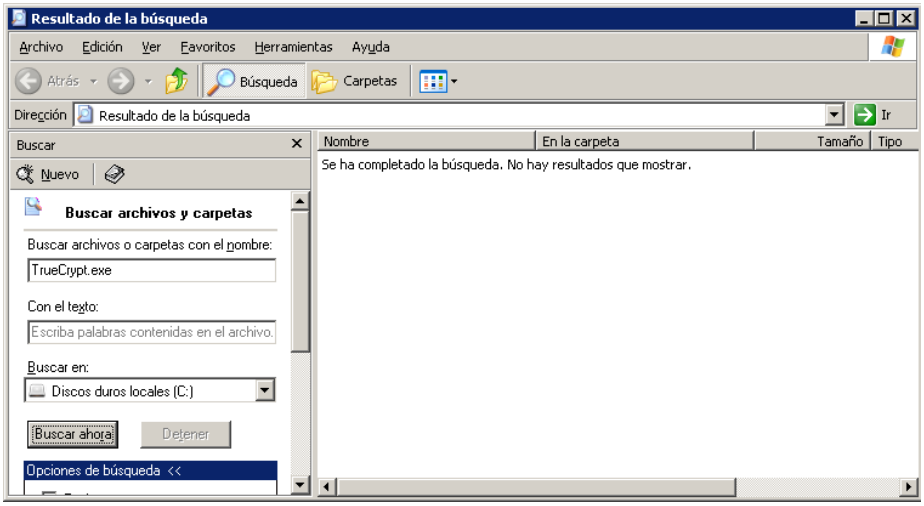


Ilustración T. 21 - Búsqueda de archivos

Sin embargo, al realizar la búsqueda por el nombre de TrueCrypt se encuentran dos carpetas con este nombre, una con un archivo de configuración “Configuration.xml” y la otra sin contenido.

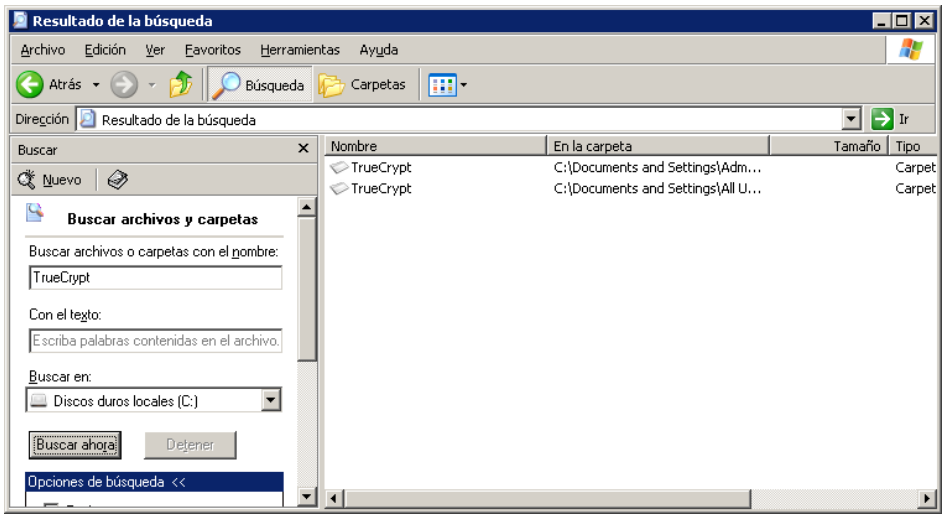


Ilustración T. 22 – Resultado de la búsqueda

Para continuar en la búsqueda de esta aplicación vamos a acceder a los registros del sistema operativo con Regedit.exe

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

Y encontramos una ruta modificada de TrueCrypt

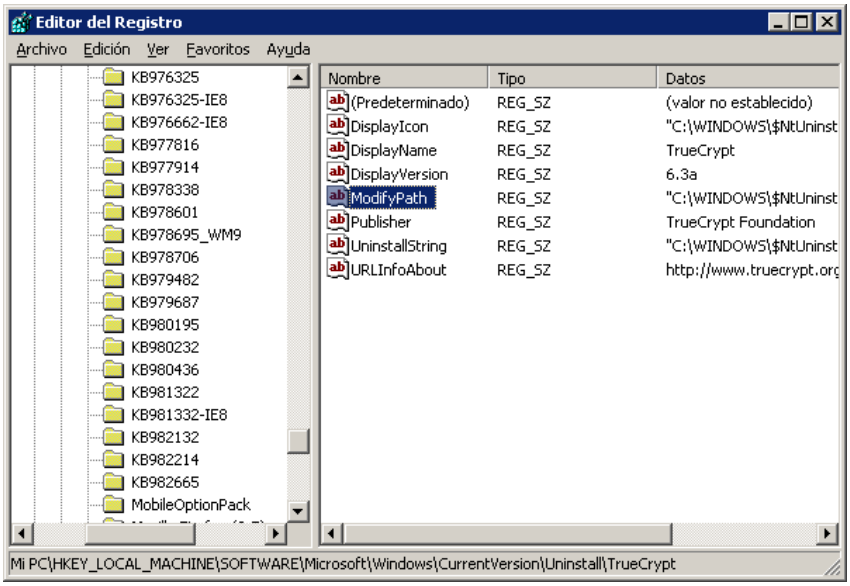


Ilustración T. 23 - Editor del Registro

Accedemos a la ruta que se nos indica para encontrar la aplicación

C:\WINDOWS\$NtUninstallKB954155_WM9$\spuninst

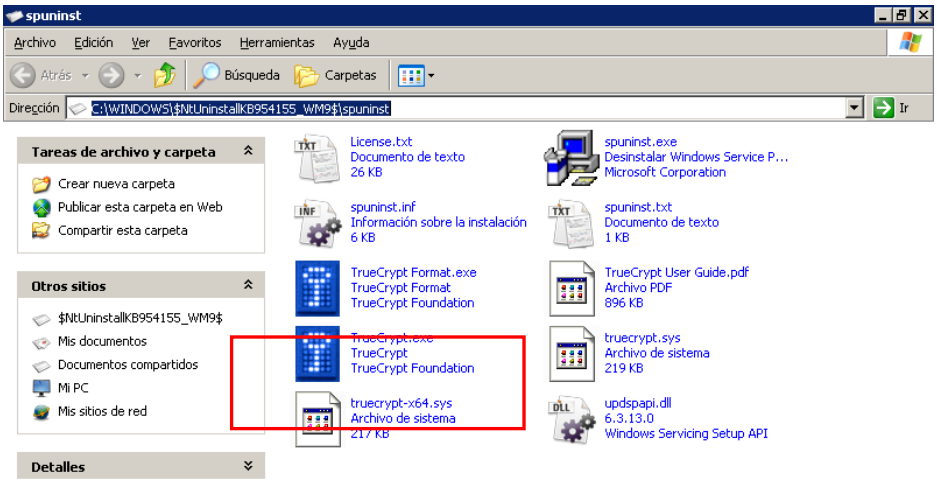


Ilustración T. 24 - TrueCrypt.exe

Podemos ejecutar la aplicación.

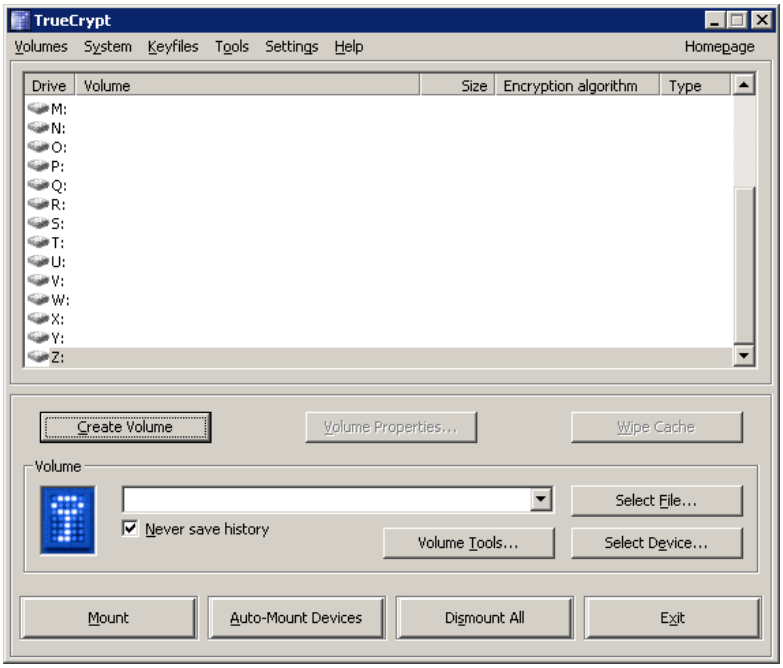


Ilustración T. 25 - Dispositivos montados

6.4. Archivos temporales de internet

Se van a realizar dos búsquedas principales: imágenes en cache y url's visitadas.

Podemos hacer uso de las herramientas forenses y además accesar al los datos de la ruta "Documents and Settings\Administrador\Configuración local\Archivos temporales de Internet\Content.IE5"

6.5. Imágenes de carácter pedófilo

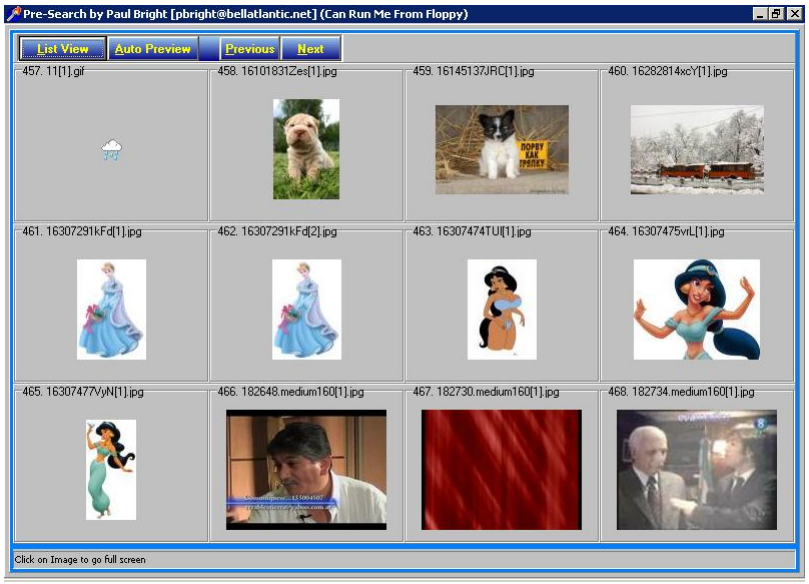


Ilustración T. 26 - Imágenes encontradas de contenido pedófilo

A primera vista con la herramienta **Pre-Search** podemos observar varias imágenes de contenido pedófilo**.**

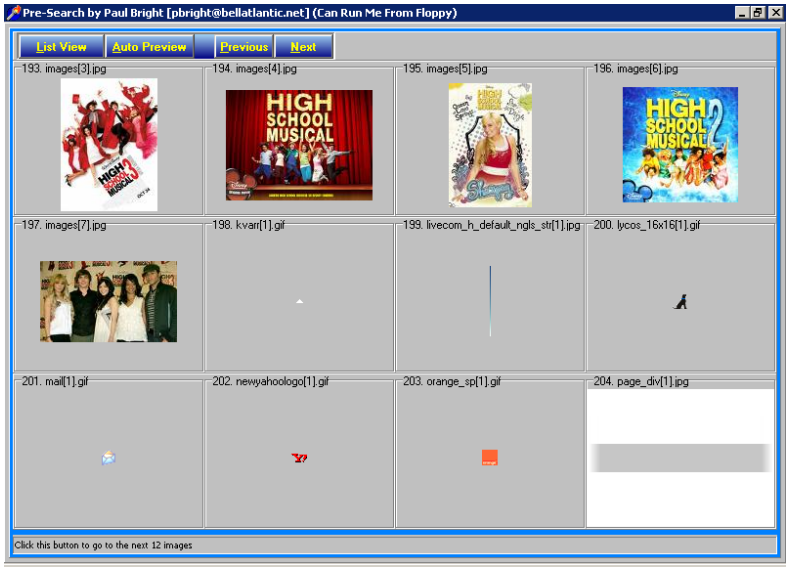


Ilustración T. 27 - Imágenes encontradas de contenido pedófilo

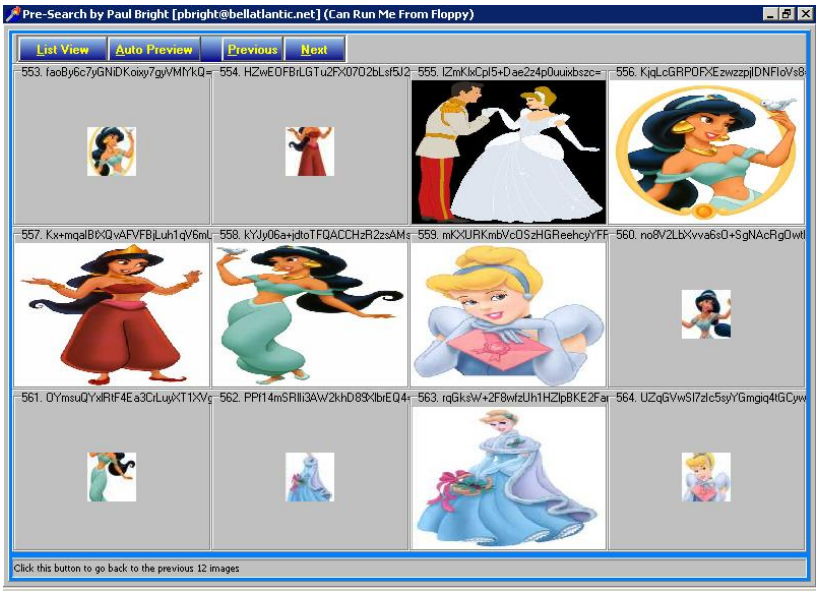


Ilustración T. 28 - Imágenes encontradas de contenido pedófilo

Se han encontrado varias imágenes que pueden ser clasificadas como para niños y/o adolescentes. Muchas de estas corresponden a películas de Disney para niños o adolescentes como “High School Musical”, las cuales pueden ser utilizadas normalmente como una excusa para entablar conversaciones con los mismos.

6.6. Búsqueda de URL’s y archivos de interés

Utilizamos la herramienta **Index.dat Analizer** para obtener información de URL’s visitadas.

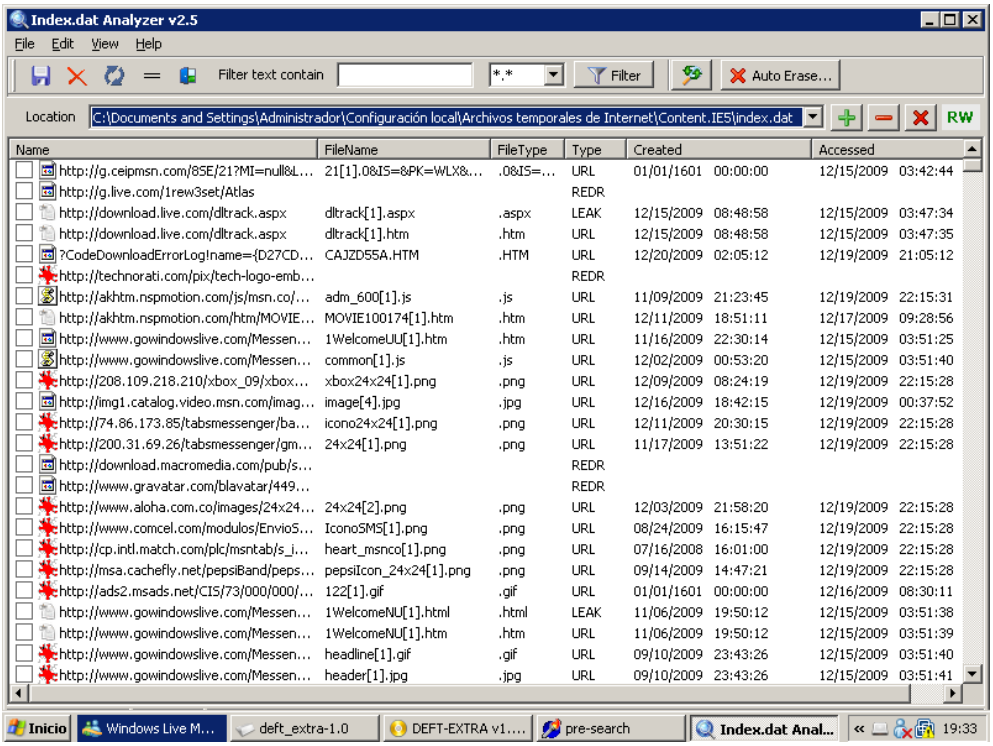


Ilustración T. 29 – Búsqueda de URLs visitadas

Nos encontramos con información de interés, un registro en el portal "ImgSrc.ru" con los siguientes datos:

E-mail de registro: "scarface1fisica@hotmail.com"

Usuario: scarface123

Fecha: 19-12-2009 - 21:27:47

ImgSrc.ur según la descripción que aparece es un hosting de álbumes de fotos.

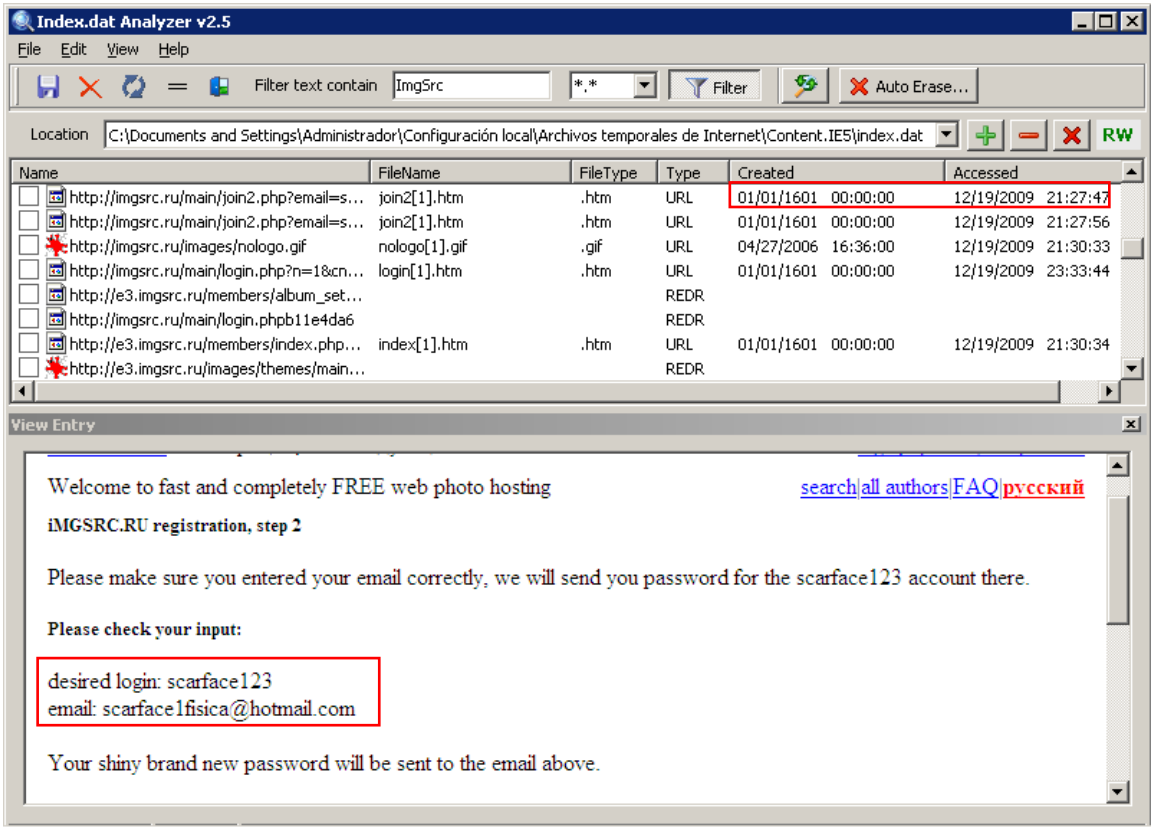


Ilustración T. 30 - Información de registro en el portal

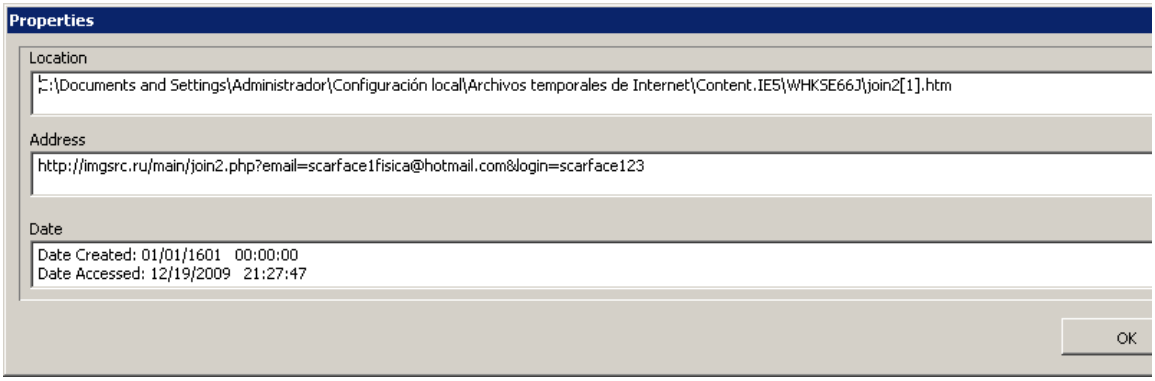


Ilustración T. 31 - Propiedades de archivos temporales

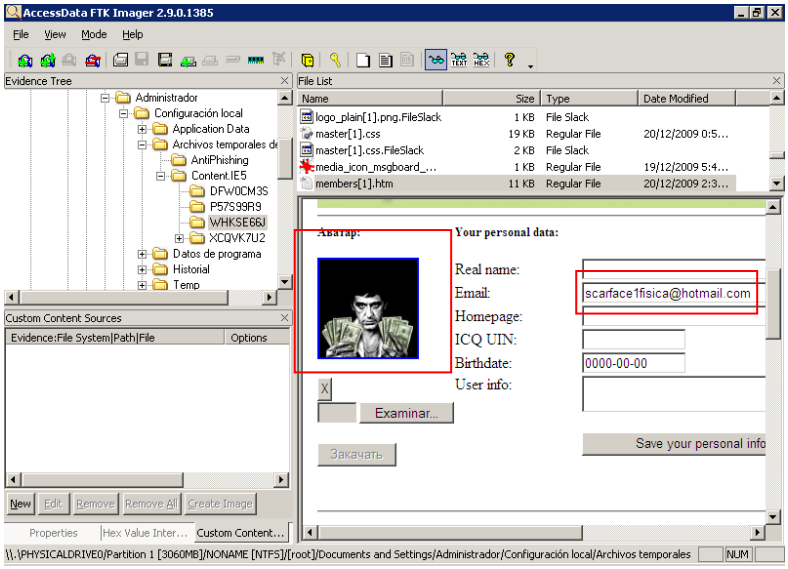


Ilustración T. 32 - Información obtenida con FTK Imager

Existen rastros de acceso a la cuenta y dominio antes descrito, en el que se puede apreciar el contenido de un álbum llamado "**Otra Pendeja"** y que contiene fotografías de tipo pedófilo.

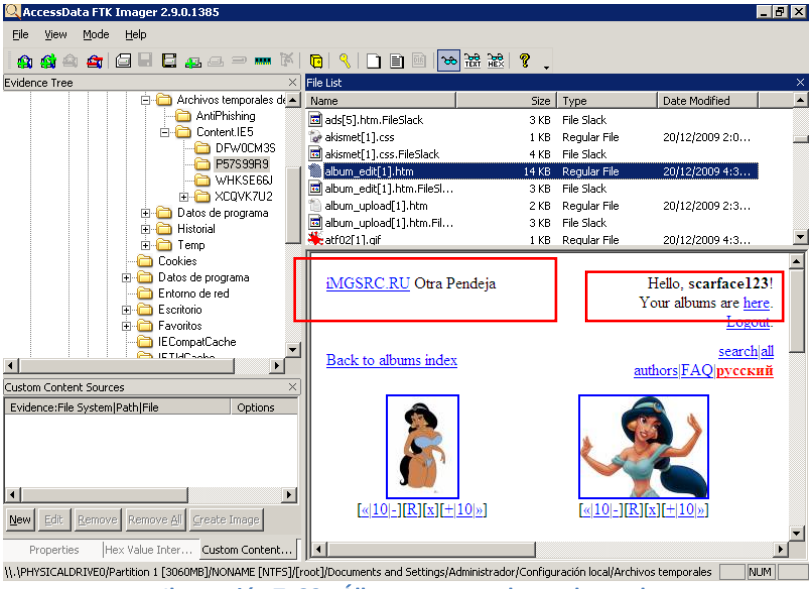


Ilustración T. 33 - Álbum encontrado en el portal

Se encontró que a este álbum **“otra pendeja”** se subió una imagen con el nombre de **“sexy(1).jpg”**

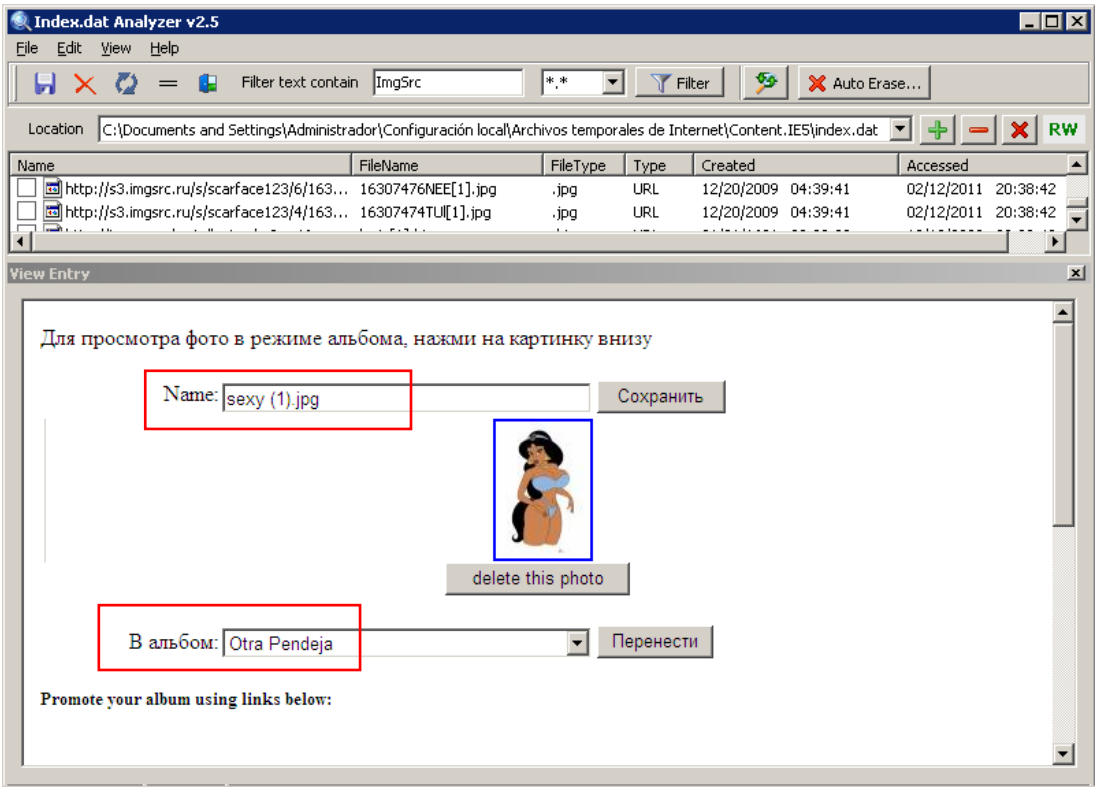


Ilustración T. 34 - Foto subida al álbum

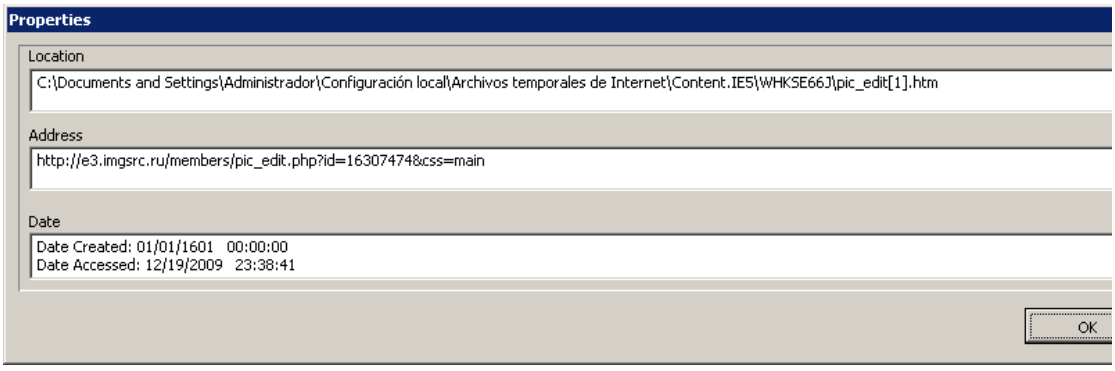


Ilustración T. 35 - Propiedades de la foto

Otra entrada muestra otra imagen de Disney subida al mismo álbum con el nombre de **“lunar.jpg”.**

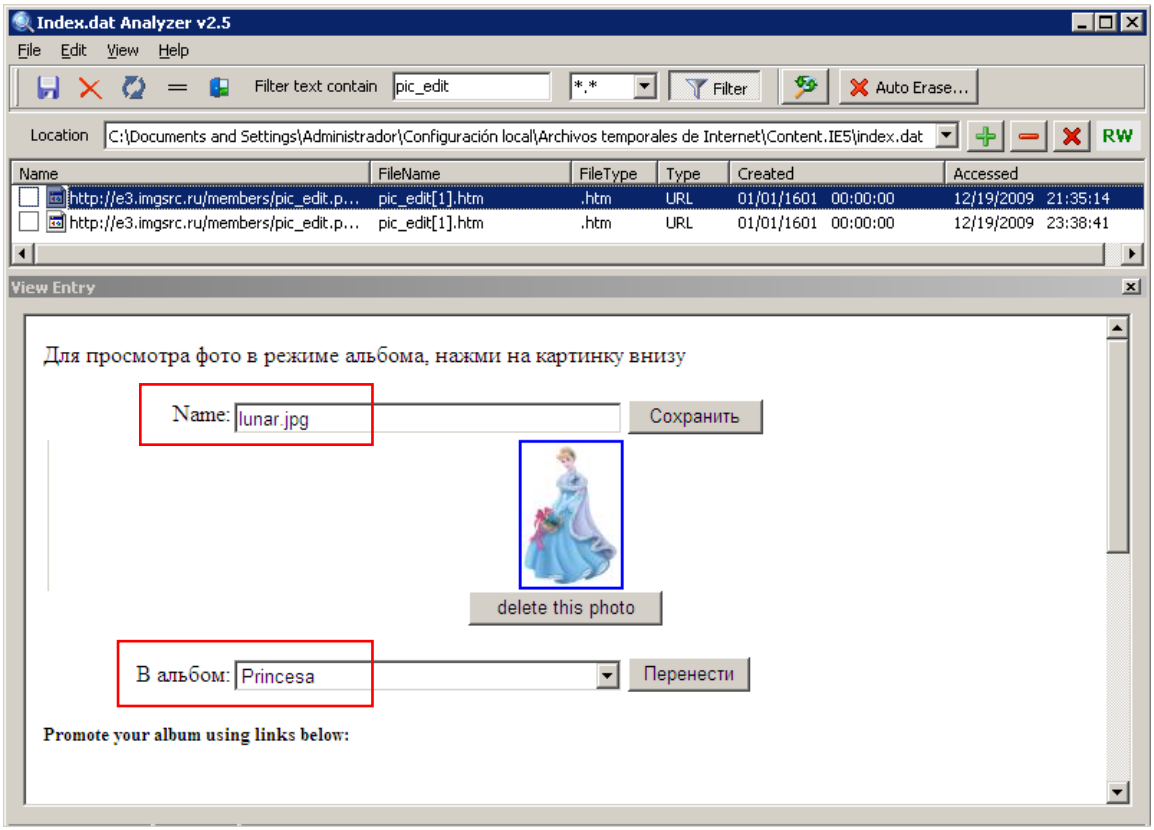


Ilustración T. 36 -Ilustración R. 37 Foto subida a un álbum

Con la herramienta FTKImager buscamos más información que fue enviada al subir la imagen **“lunar.jpg”**

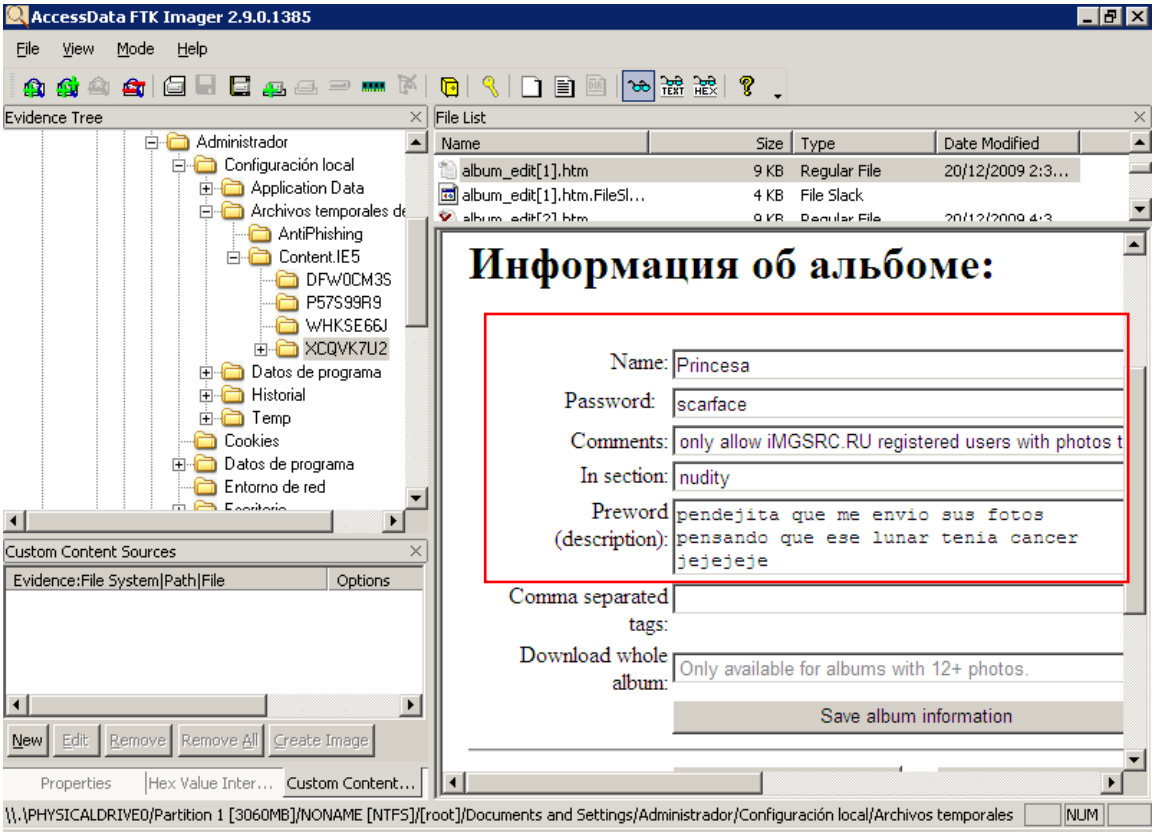


Ilustración T. 38 - Datos del álbum subido al portal

Uno de los principales datos que encontramos es un password **“scarface”** que puede ser utilizado para acceder a los álbumes, de la misma manera obtenemos el nombre de un álbum **“Princesa”**.

En la descripción del álbum se encuentra un texto sospechoso de interés para la investigación, se puede leer que alguien envió fotos bajo el engaño de una enfermedad.

Podemos ver que el usuario **“Scarface”** ha tenido acceso a su cuenta de Hotmail **“scarface1fisica@hotmail.com”,** podemos observar que tiene un contacto **“preciosa.natalia@hotmail.com”,** en el cual podemos notar cambios en su estado referenciando su afinidad con la película High School Musical, recordando que el usuario “Scarface” posee varias fotos de esta película en su ordenador.

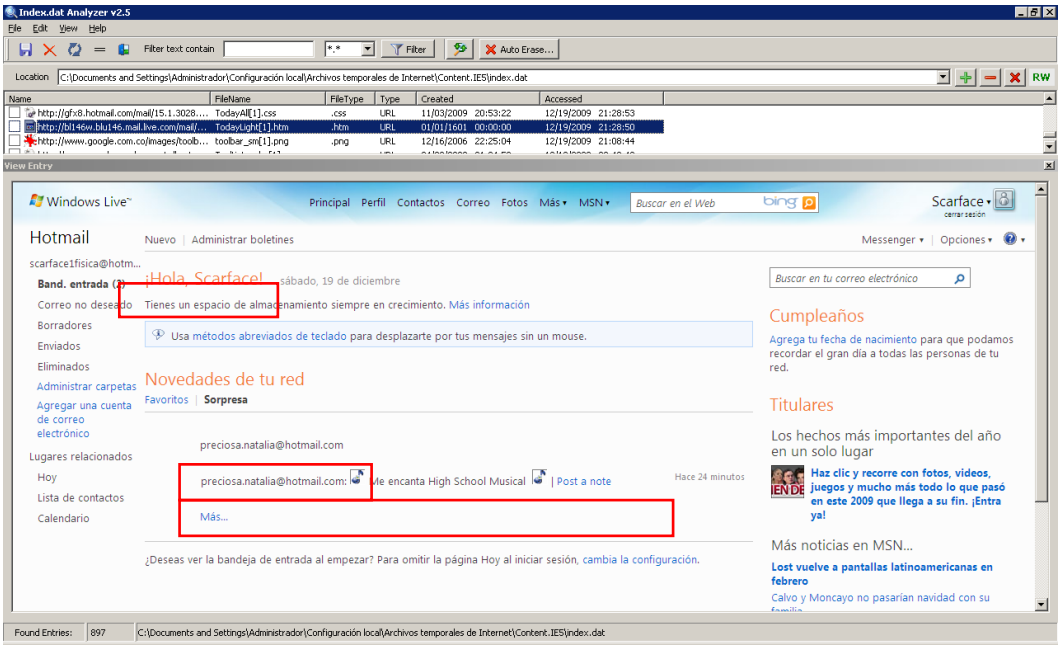


Ilustración T. 39 - Datos encontrados en cuenta de correo hotmail

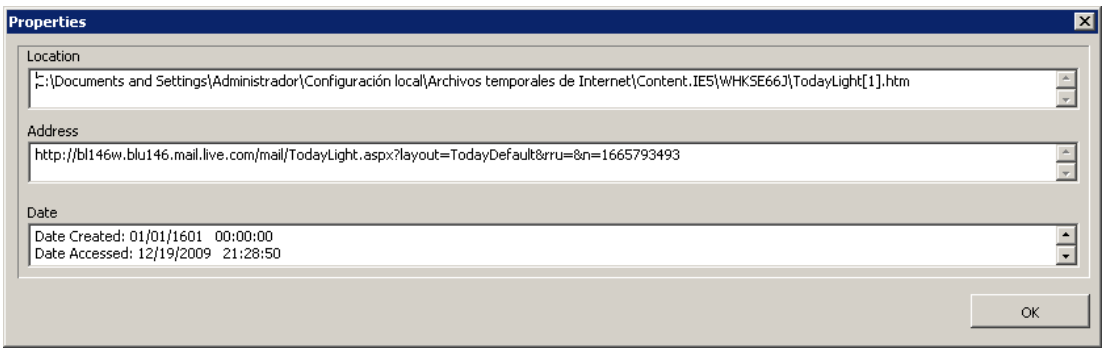


Ilustración T. 40 - Propiedades del archivo temporal

Podemos determinar que con la cuenta de Hotmail y el usuario **“Scarface”** se realizó el registro en el portal **ImgSrc.ru**

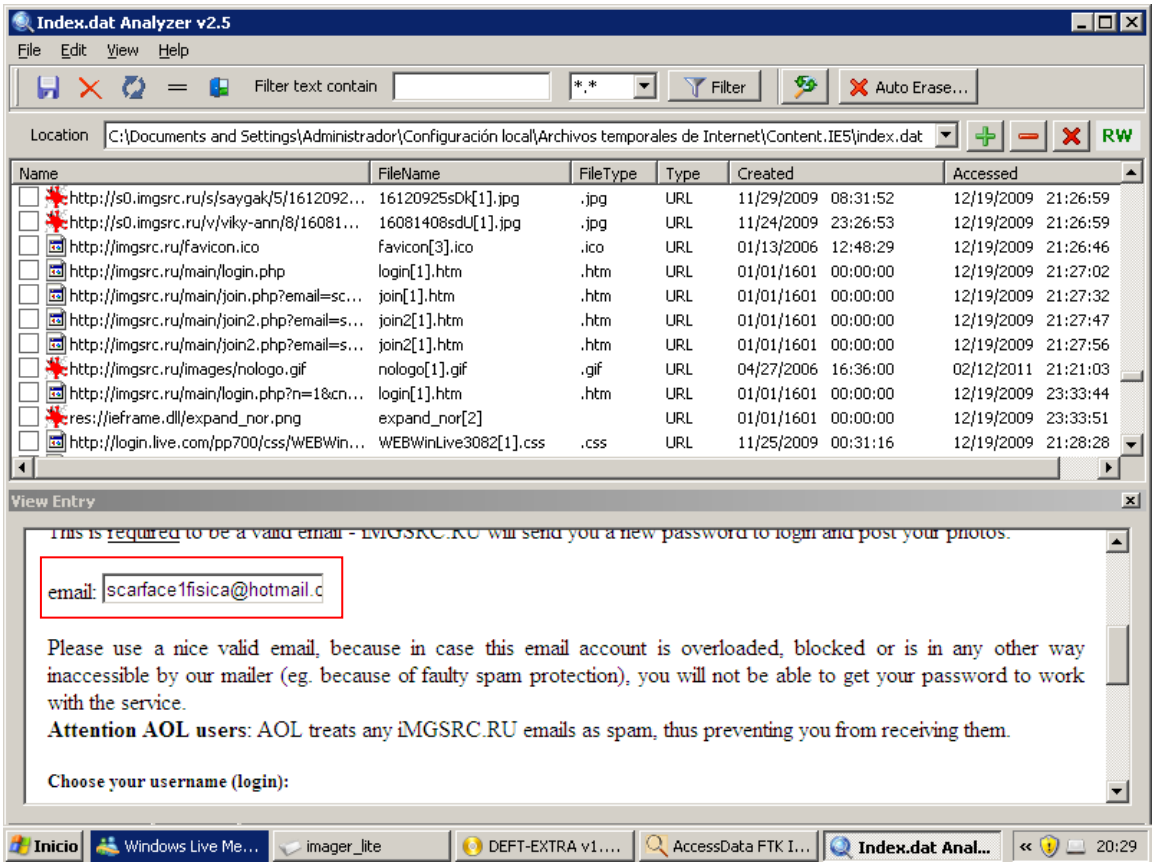


Ilustración T. 41 - Index data analyzer, registro en el portal

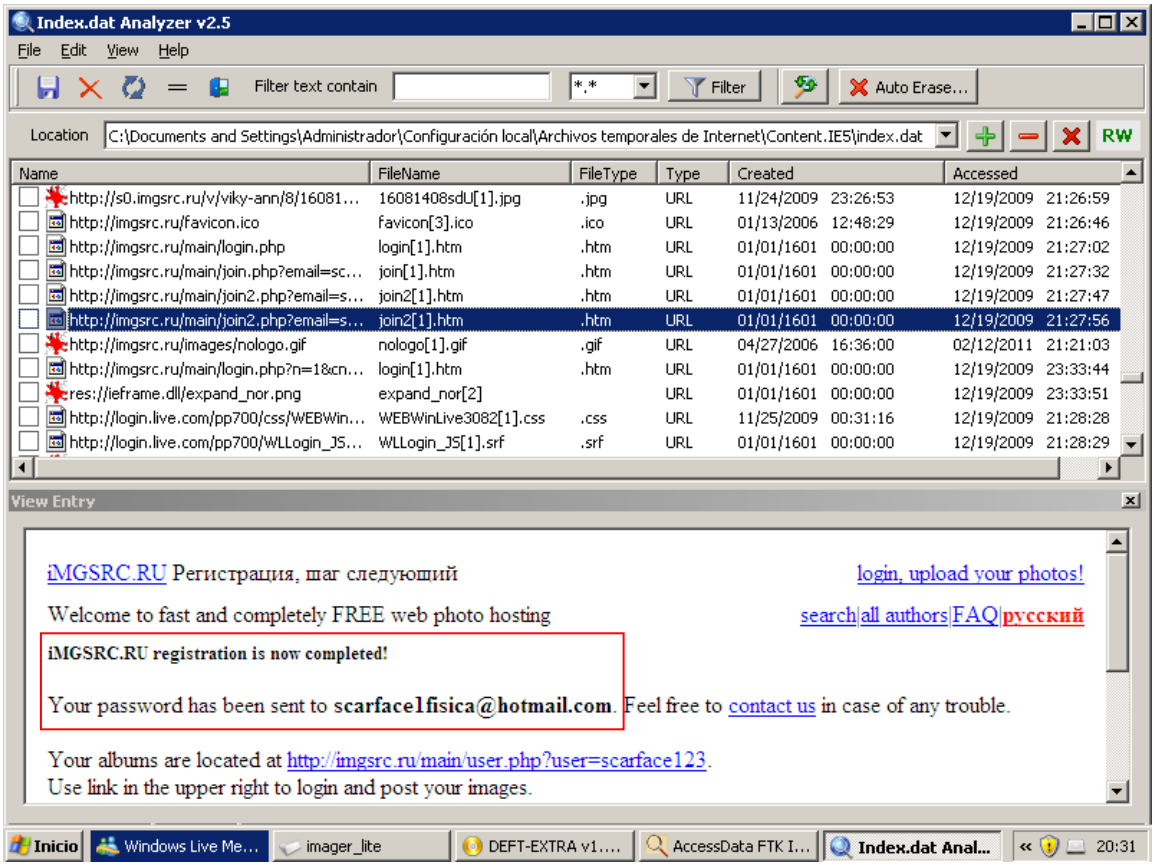


Ilustración T. 42 – Index Data Analyzer, detalles de imágenes

Al momento de registrarse en ese portal se envió un correo con el usuario y contraseña, las cuales obtuvimos del correo de confirmación de registro.

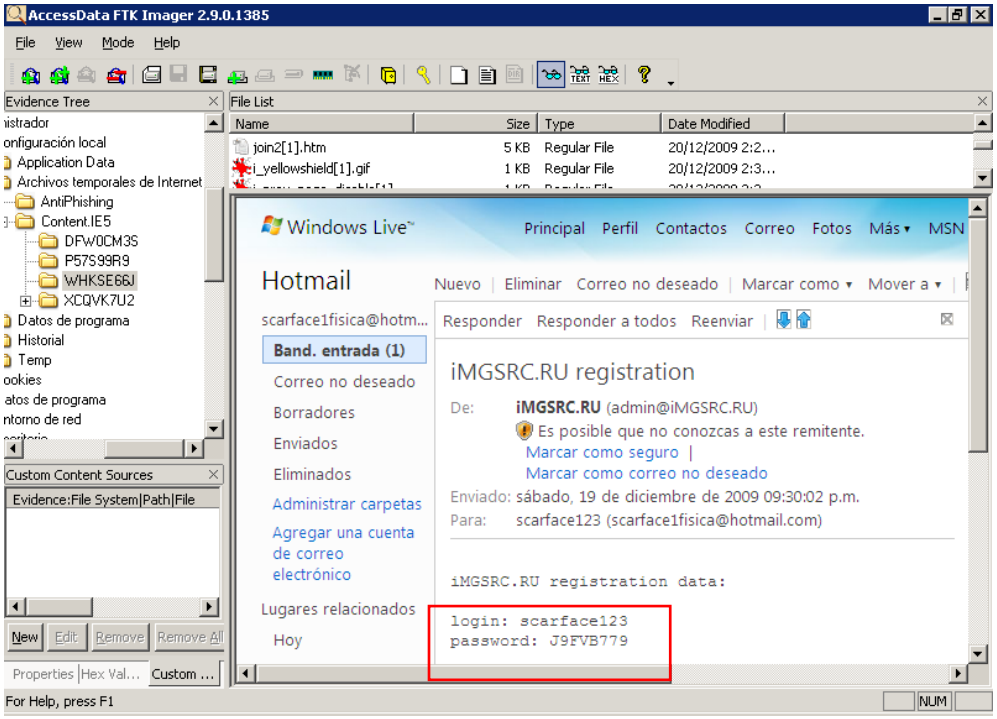


Ilustración T. 43 - Datos en correo de hotmail

Referenciamos que el usuario recolecta mucha información y fotografías de artistas juveniles y caricaturas infantiles.

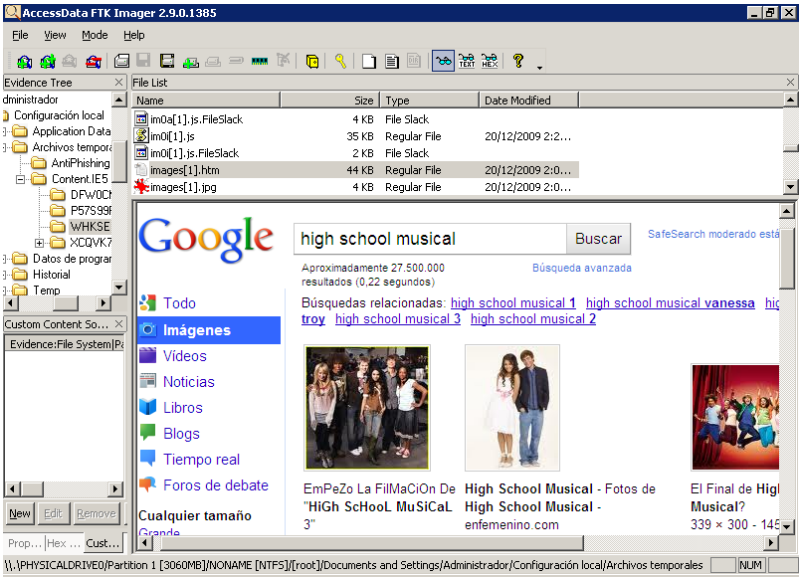


Ilustración T. 44 - Búsqueda de imágenes

Ha realizado búsquedas de imágenes de la película “High School Musical”, noticias, videos y demás información sobre esta y otras series infantiles y juveniles.

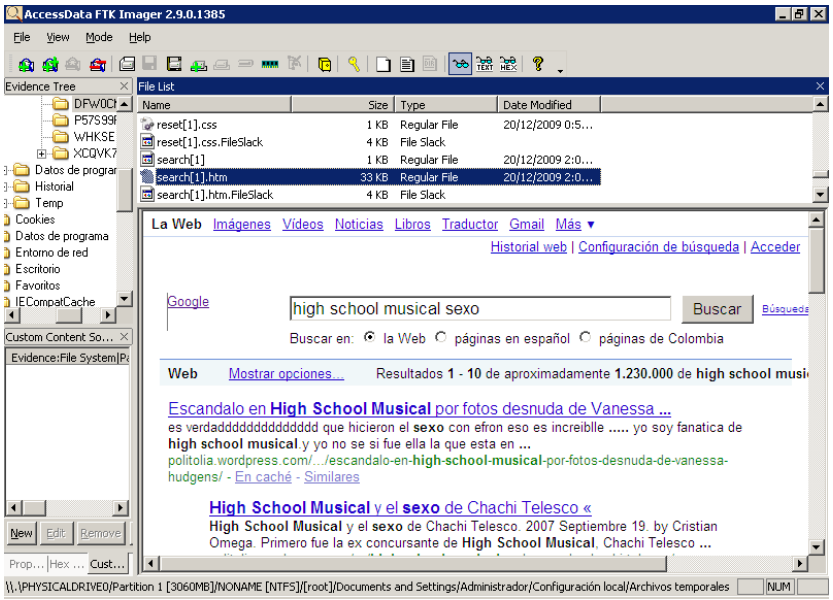


Ilustración T. 45 - Búsqueda en la web contenido infantil

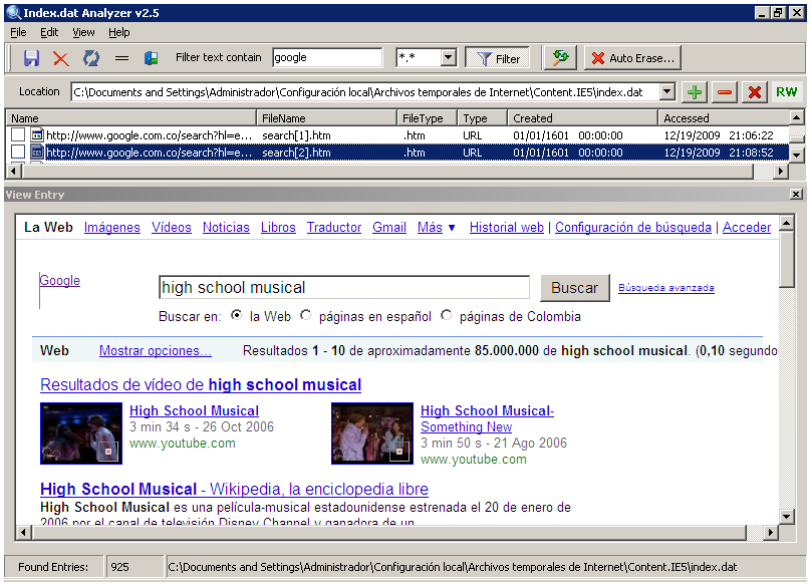


Ilustración T. 46 - Búsqueda en la web contenido infantil

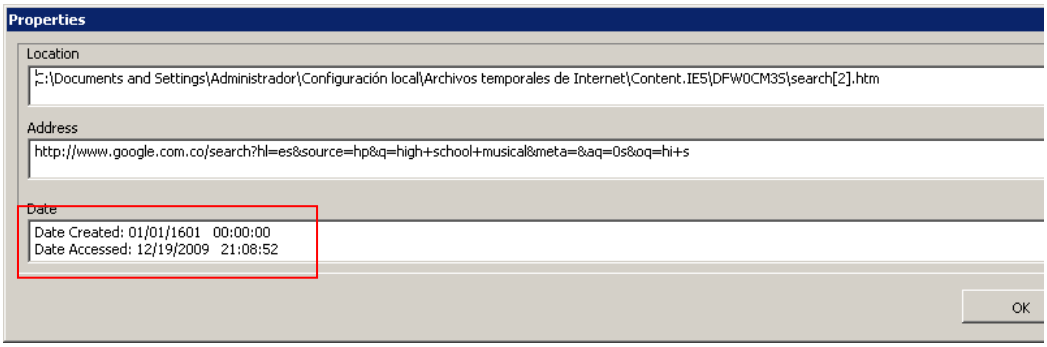


Ilustración T. 47 – Fechas de creación archivos tempporales

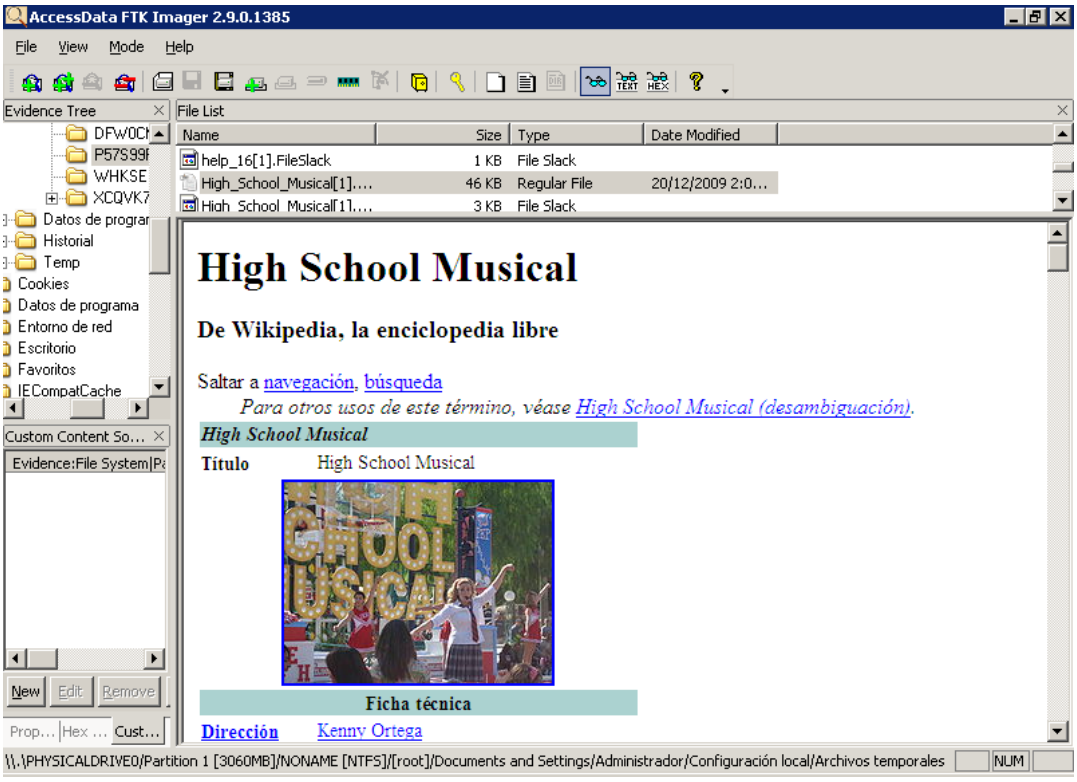
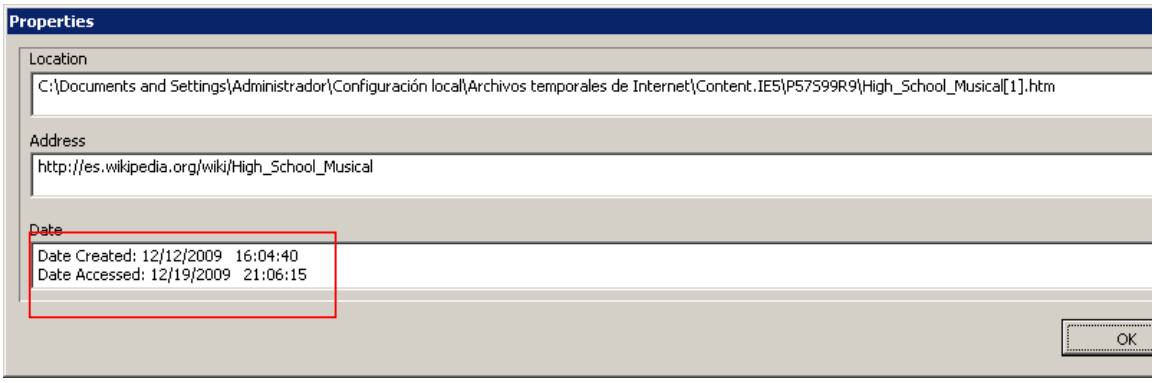
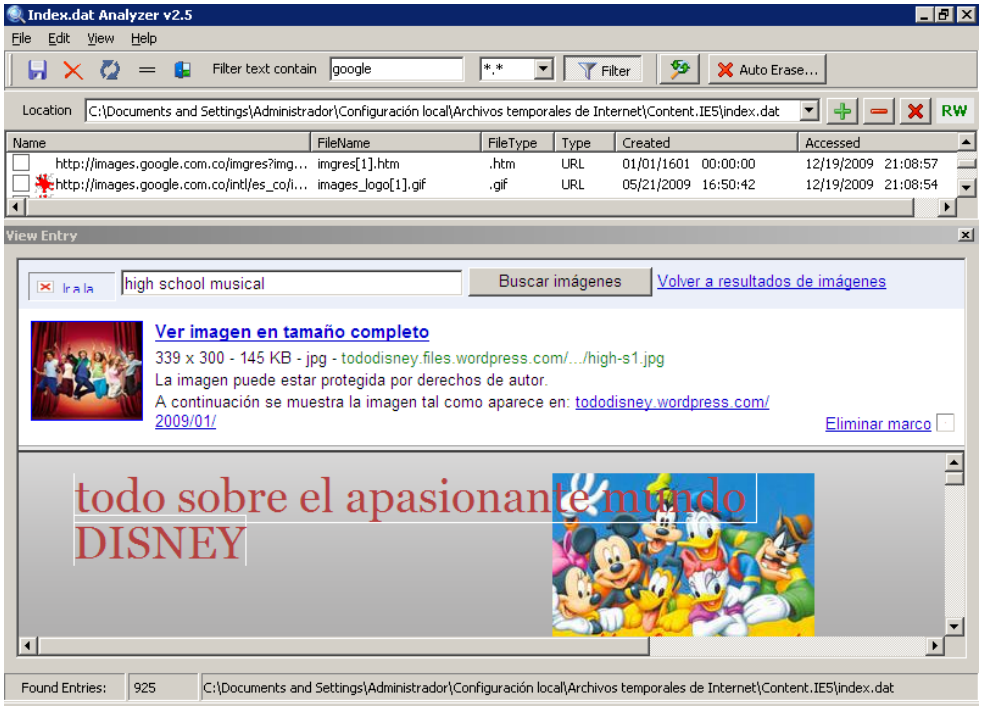


Ilustración T. 48 - Búsqueda en la web contenido infantil


Properties
Location
C:\Documents and Settings\Administrador\Configuración local\Archivos temporales de Internet\Content.IE5\P57S99R9\High_School_Musical[1].htm
Address
http://es.wikipedia.org/wiki/High_School_Musical
Date
Date Created: 12/12/2009 16:04:40
Date Accessed: 12/19/2009 21:06:15
OK


Index.dat Analyzer v2.5
File Edit View Help
Filter text contain
.
Filter
Auto Erase...
Location
C:\Documents and Settings\Administrador\Configuración local\Archivos temporales de Internet\Content.IE5\index.dat
RW
Name
FileName
FileType
Type
Created
Accessed
http://politolia.files.wordpress.com/200...
vanesa[1].jpg
.jpg
URL
09/06/2007 00:51:29
12/19/2009 21:06:27
View Entry
Politolia
Politica Noticias Tecnologia y Otras Yerbas
Inicio About Cambiar Idioma
Escandalo en High School Musical por fotos desnuda de Vanessa Hudgens
ULTIMO MOMENTO
2007 SEPTIEMBRE 6
Found Entries:
925
C:\Documents and Settings\Administrador\Configuración local\Archivos temporales de Internet\Content.IE5\index.dat

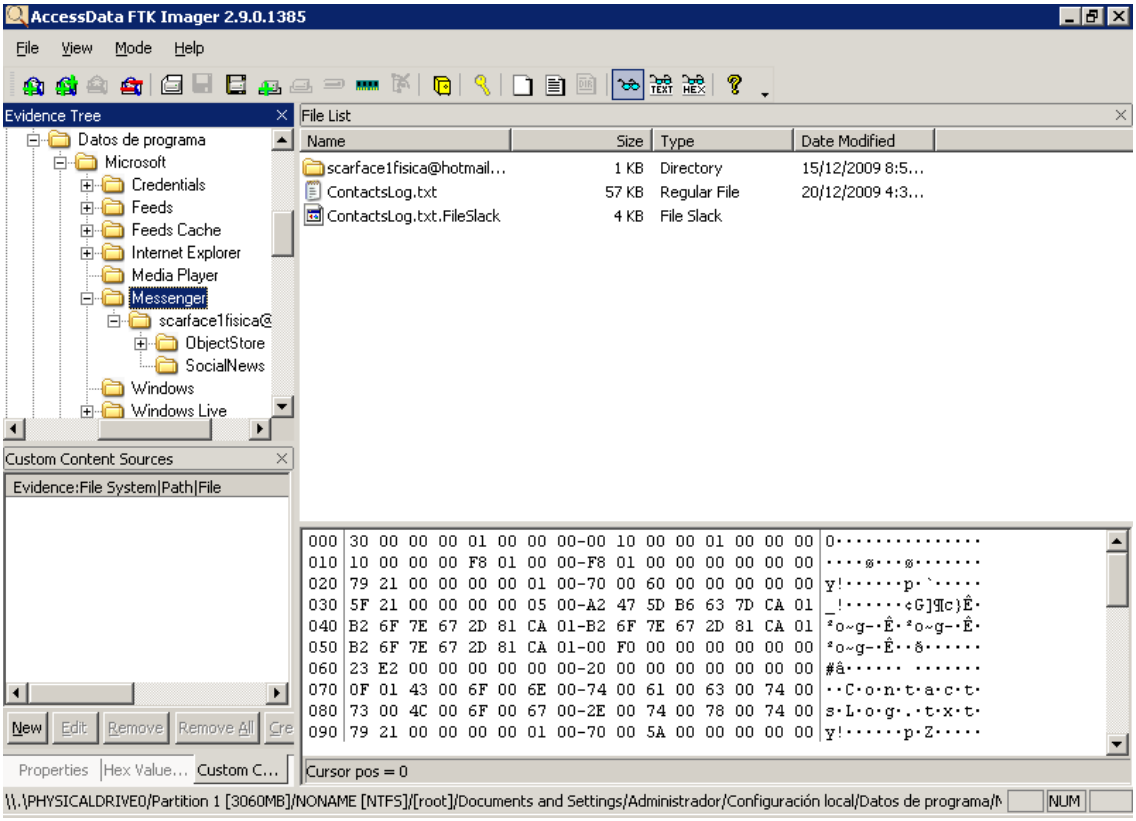


6.7. Historial de mensajería instantánea MSN

Se busca información y rastros dejados de conversaciones con la aplicación de mensajería instantánea MSN.

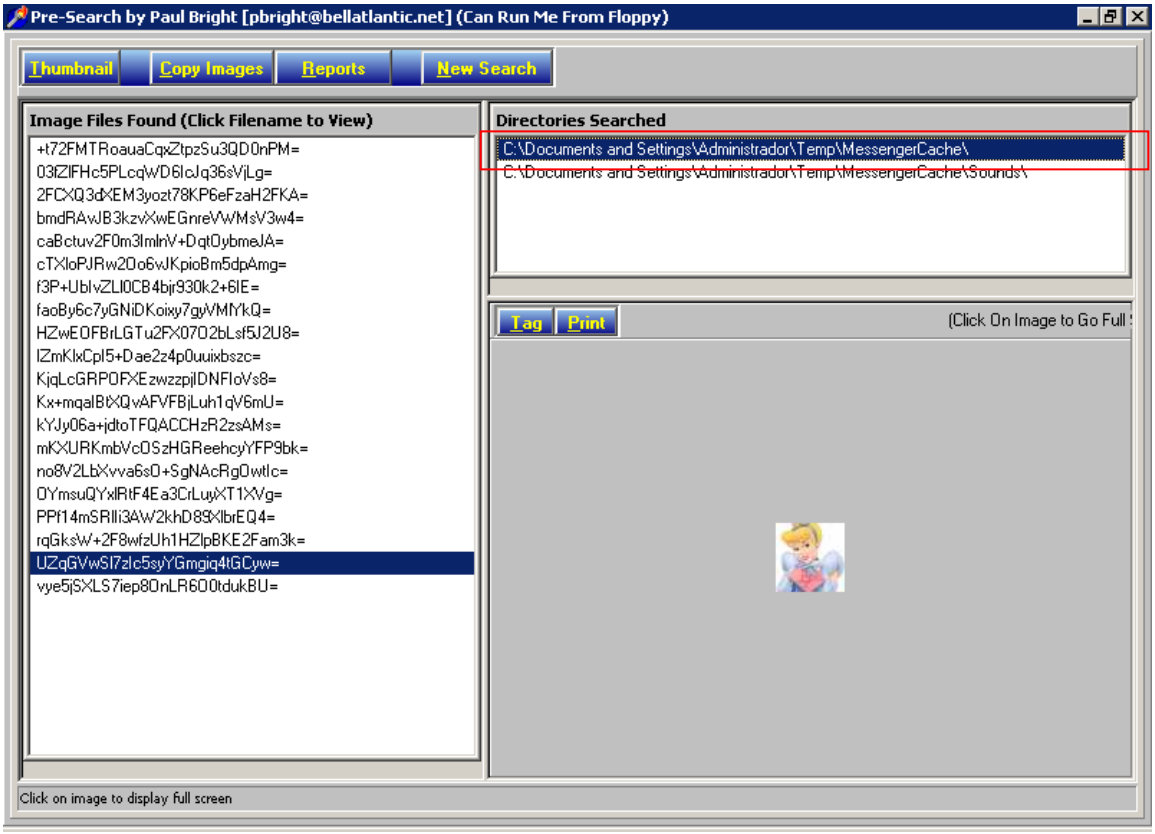
6.8. Archivos físicos en el disco duro

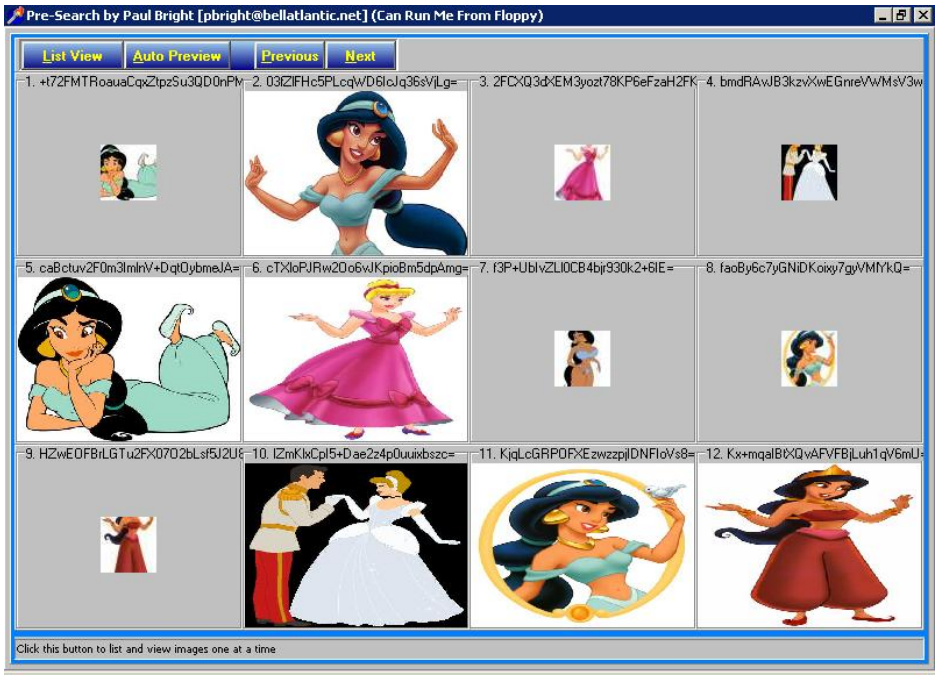
La cuenta “**scarface1fisica@hotmail.com”** se encuentra en la carpeta por defecto de Microsoft Messenger. No se encuentran ningún log de conversaciones guardadas ni archivos recibidos durante las mismas.

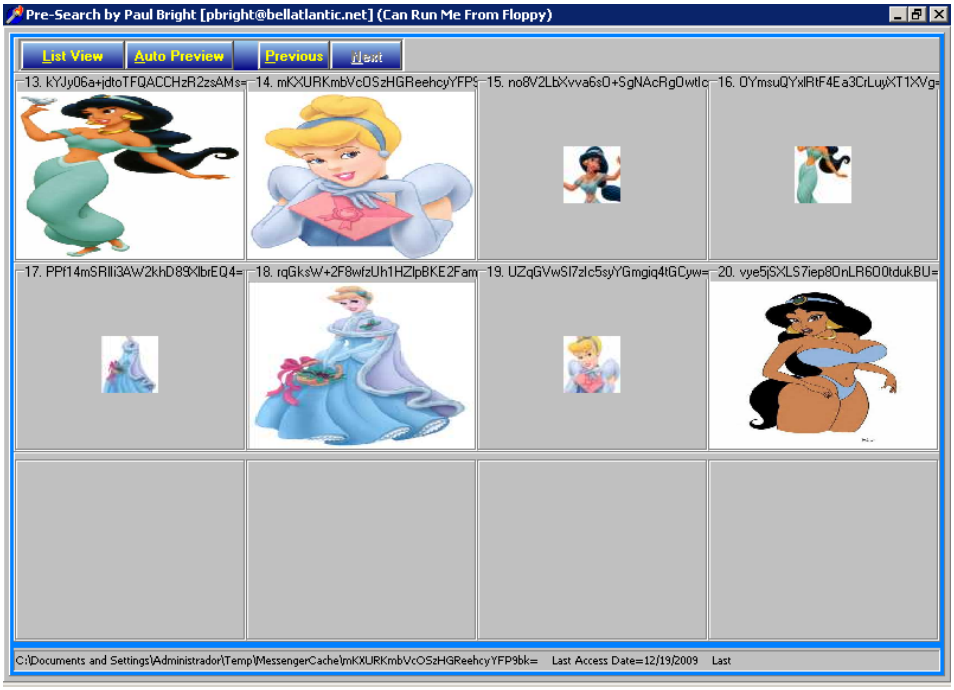


En la ruta:

“**DocumentsandSettings\Administrador\Temp\MessengerCache”,** que es la carpeta donde se almacenan archivos temporales de la aplicación MSN, se encontraron imágenes de contenido pedófilo que son recibidas a través de esta aplicación.

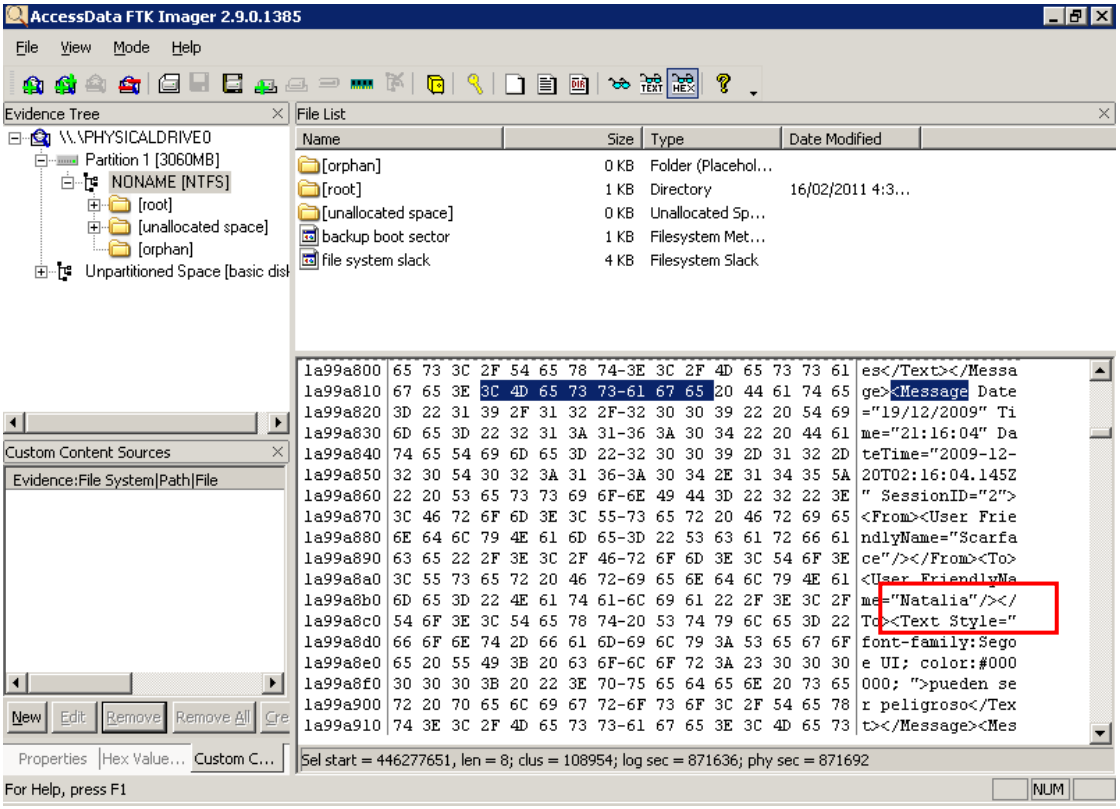

Pre-Search by Paul Bright [pbright@bellatlantic.net] (Can Run Me From Floppy)
Thumbnail
Copy Images
Reports
New Search
Image Files Found (Click Filename to View)
+t72FMTRoauaCqxZtpzSu3QD0nPM=
03lZlFHc5PLcqWD6lcJq36sVjLg=
2FCXQ3dXEM3yozt78KP6eFzaH2FKA=
bmdRAvJB3kzvXwEGnreVWMsV3w4=
caBctuv2F0m3lmlnV+DqtOybmeJA=
cTXloPJRw2Oo6vJKpioBm5dpAmg=
f3P+UblvZLl0CB4bjr930k2+6lE=
faoBy6c7yGNiDKoixy7gVMfYkQ=
HZwEOFBrLGTu2FX07O2bLsf5J2U8=
lZmKlxCpl5+Dae2z4p0uuixbszc=
KjqLcGRPOFXEzwzzpjlDNFloVs8=
Kx+mqalBtXQvAFVFBjLuh1qV6mU=
kYJy06a+jdtoTFQACCHzR2zsAMs=
mKXURKmbVcOSzHGReehcyYFP9bk=
no8V2LbXvva6sO+SgNAcRgOwtlc=
0YmsuQYxlRtF4Ea3CrLuyXT1XVg=
PPf14mSRIli3AW2khD89XlbrEQ4=
rqGksW+2F8wfzUh1HZlpBKE2Fam3k=
UZqGVwSI7zlc5syYGmgiq4tGCyw=
vye5jSXLS7iep8OnLR6O0tdukBU=
Directories Searched
C:\Documents and Settings\Administrador\Temp\MessengerCache\
C:\Documents and Settings\Administrador\Temp\MessengerCache\Sounds\
Tag
Print
(Click On Image to Go Full
Click on image to display full screen


Pre-Search by Paul Bright [pbright@bellatlantic.net] (Can Run Me From Floppy)
List View
Auto Preview
Previous
Next
1. +t72FMTRoauaCqxZtpzSu3QD0nPM=
2. 03lZlFHc5PLcqWD6lcJq36sVjLg=
3. 2FCXQ3dXEM3yozt78KP6eFzaH2FK
4. bmdRAvJB3kzvXwEGnreVWMsV3w
5. caBctuv2F0m3lmlnV+DqtOybmeJA=
6. cTXloPJRw2Oo6vJKpioBm5dpAmg=
7. f3P+UblvZLl0CB4bjr930k2+6lE=
8. faoBy6c7yGNiDKoixy7gVMfYkQ=
9. HZwEOFBrLGTu2FX07O2bLsf5J2U8
10. lZmKlxCpl5+Dae2z4p0uuixbszc=
11. KjqLcGRPOFXEzwzzpjlDNFloVs8=
12. Kx+mqalBtXQvAFVFBjLuh1qV6mU=
Click this button to list and view images one at a time

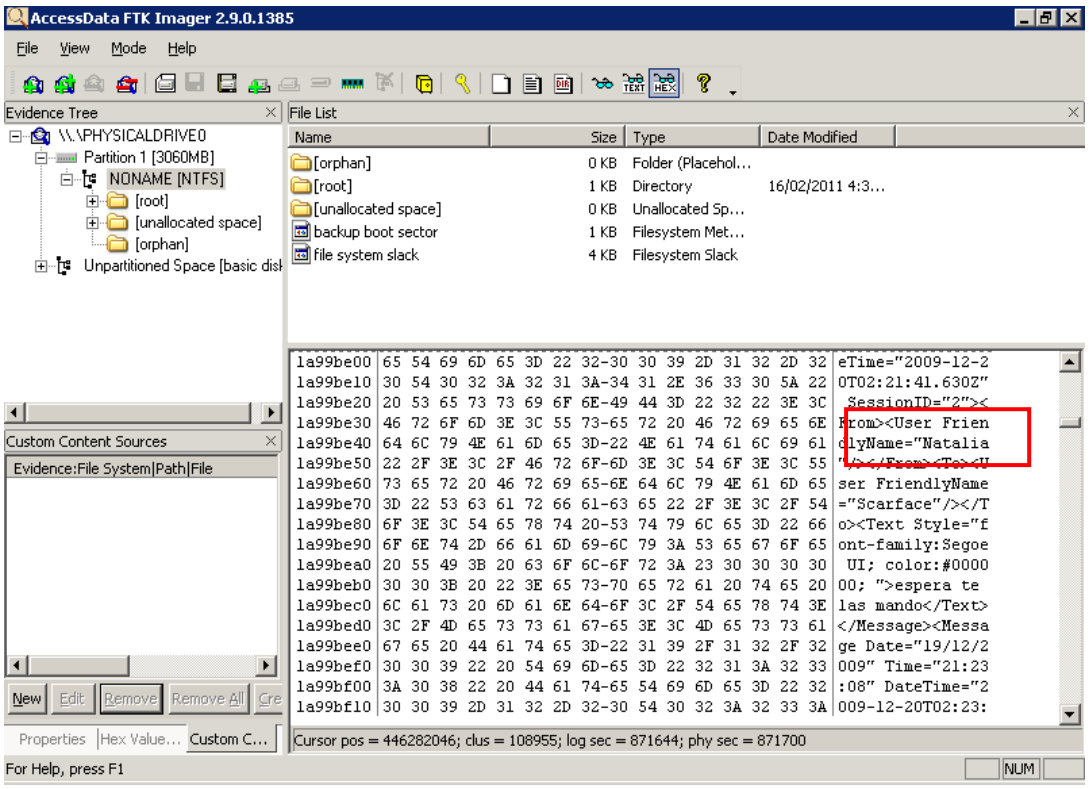


6.9. Rastros en Cluster no Asignados

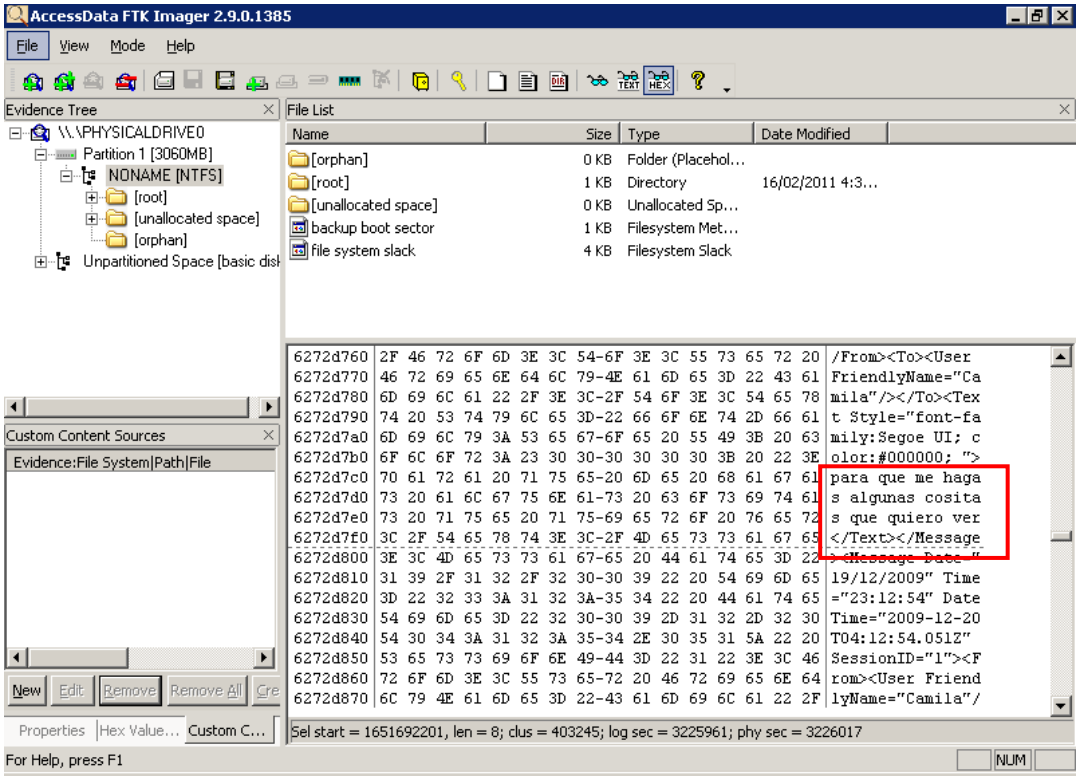
Ahora que determinamos que se han mantenido conversaciones por la aplicación Messenger y ya que no existen logs de estas, vamos a profundizar en la búsqueda por los clúster del disco duro filtrando la búsqueda con la palabra clave **"<message"** porque es el formato utilizado en la estructura de las conversaciones del MSN.

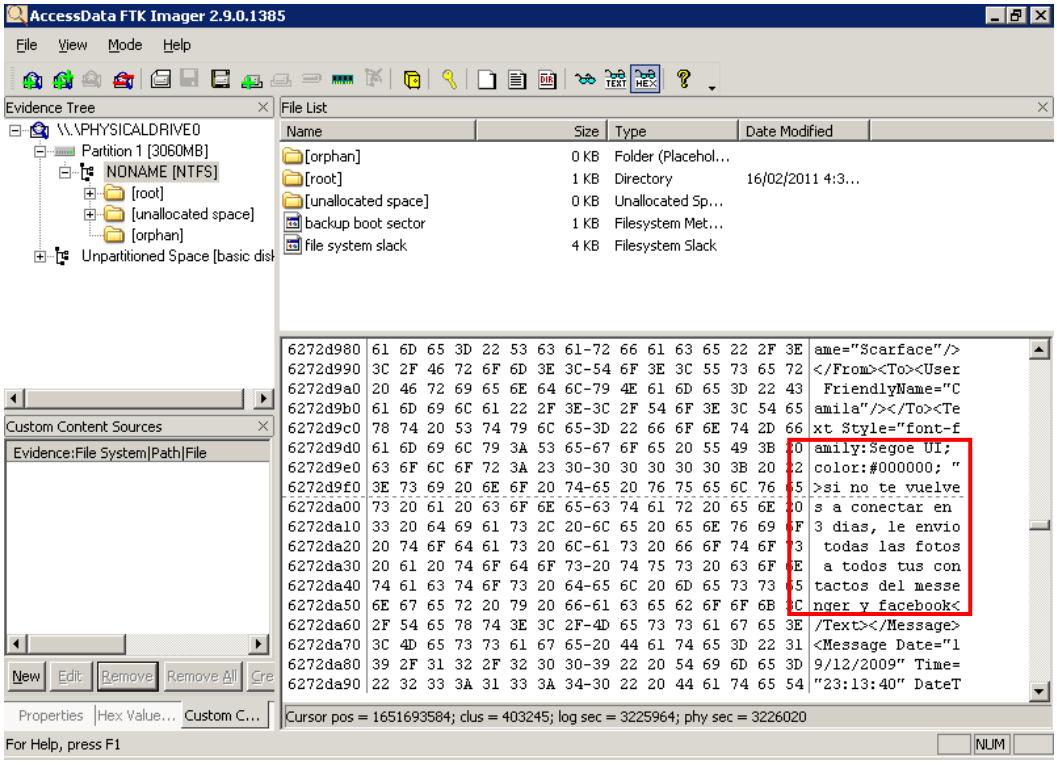


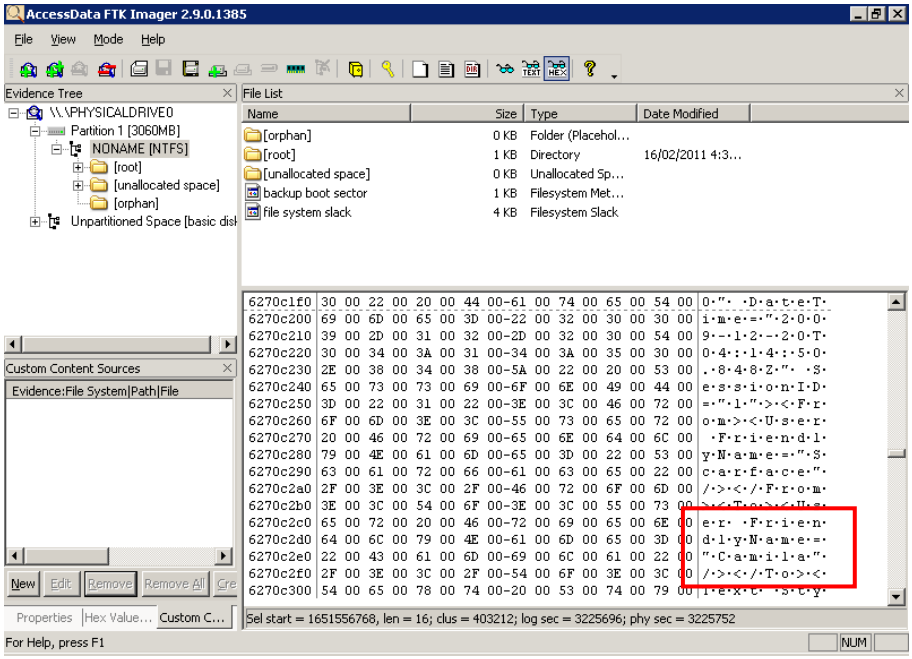
Conversaciones entre usuario “Scarface” y “Natalia”: Se le piden fotografías de ella con la excusa de que tiene lunares que podrían ser cancerígeno, según la apreciación del usuario Scarface. “Natalia” responde con temor y envía las fotos solicitadas.



Conversaciones entre usuario “Scarface” y “Camila”: mantienen conversaciones inapropiadas por parte del usuario “Scarface” a las que “Camila” responde con desagrado, se producen amenazas hacia “Camila” si no vuelve a conectarse “Scarface” publicara fotos de ella. “Scarface” ha averiguado información de “Camila” como facebook, correo, etc.

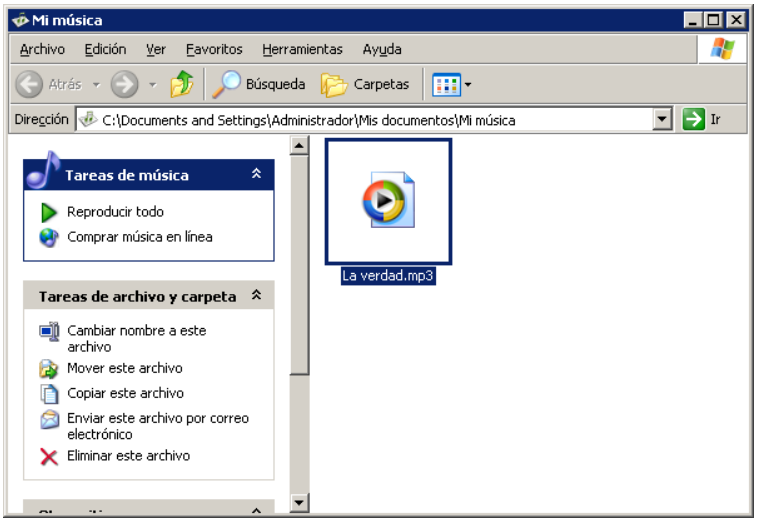

AccessData FTK Imager 2.9.0.1385
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE0
Partition 1 [3060MB]
NONAME [NTFS]
[root]
[unallocated space]
[orphan]
Unpartitioned Space [basic disk
File List
Name Size Type Date Modified
[orphan] 0 KB Folder (Placehol...
[root] 1 KB Directory 16/02/2011 4:3...
[unallocated space] 0 KB Unallocated Sp...
backup boot sector 1 KB Filesystem Met...
file system slack 4 KB Filesystem Slack
6272d760 2F 46 72 6F 6D 3E 3C 54-6F 3E 3C 55 73 65 72 20 /From><To><User
6272d770 46 72 69 65 6E 64 6C 79-4E 61 6D 65 3D 22 43 61 FriendlyName="Ca
6272d780 6D 69 6C 61 22 2F 3E 3C-2F 54 6F 3E 3C 54 65 78 mila"/></To><Tex
6272d790 74 20 53 74 79 6C 65 3D-22 66 6F 6E 74 2D 66 61 t Style="font-fa
6272d7a0 6D 69 6C 79 3A 53 65 67-6F 65 20 55 49 3B 20 63 mily:Segoe UI; c
6272d7b0 6F 6C 6F 72 3A 23 30 30-30 30 30 30 3B 20 22 3E olor:#000000; ">
6272d7c0 70 61 72 61 20 71 75 65-20 6D 65 20 68 61 67 61 para que me haga
6272d7d0 73 20 61 6C 67 75 6E 61-73 20 63 6F 73 69 74 61 s algunas cosita
6272d7e0 73 20 71 75 65 20 71 75-69 65 72 6F 20 76 65 72 s que quiero ver
6272d7f0 3C 2F 54 65 78 74 3E 3C-2F 4D 65 73 73 61 67 65 </Text></Message
6272d800 3E 3C 4D 65 73 73 61 67-65 20 44 61 74 65 3D 22 ><Message Date="
6272d810 31 39 2F 31 32 2F 32 30-30 39 22 20 54 69 6D 65 19/12/2009" Time
6272d820 3D 22 32 33 3A 31 32 3A-35 34 22 20 44 61 74 65 ="23:12:54" Date
6272d830 54 69 6D 65 3D 22 32 30-30 39 2D 31 32 2D 32 30 Time="2009-12-20
6272d840 54 30 34 3A 31 32 3A 35-34 2E 30 35 31 5A 22 20 T04:12:54.051Z"
6272d850 53 65 73 73 69 6F 6E 49-44 3D 22 31 22 3E 3C 46 SessionID="1"><F
6272d860 72 6F 6D 3E 3C 55 73 65-72 20 46 72 69 65 6E 64 rom><User Friend
6272d870 6C 79 4E 61 6D 65 3D 22-43 61 6D 69 6C 61 22 2F lyName="Camila"/
Custom Content Sources
Evidence:File System|Path|File
New Edit Remove Remove All Cre
Properties Hex Value... Custom C...
Sel start = 1651692201, len = 8; clus = 403245; log sec = 3225961; phy sec = 3226017
For Help, press F1
NUM


AccessData FTK Imager 2.9.0.1385
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE0
Partition 1 [3060MB]
NONAME [NTFS]
[root]
[unallocated space]
[orphan]
Unpartitioned Space [basic disk
File List
Name Size Type Date Modified
[orphan] 0 KB Folder (Placehol...
[root] 1 KB Directory 16/02/2011 4:3...
[unallocated space] 0 KB Unallocated Sp...
backup boot sector 1 KB Filesystem Met...
file system slack 4 KB Filesystem Slack
6272d980 61 6D 65 3D 22 53 63 61-72 66 61 63 65 22 2F 3E ame="Scarface"/>
6272d990 3C 2F 46 72 6F 6D 3E 3C-54 6F 3E 3C 55 73 65 72 </From><To><User
6272d9a0 20 46 72 69 65 6E 64 6C-79 4E 61 6D 65 3D 22 43 FriendlyName="C
6272d9b0 61 6D 69 6C 61 22 2F 3E-3C 2F 54 6F 3E 3C 54 65 amila"/></To><Te
6272d9c0 78 74 20 53 74 79 6C 65-3D 22 66 6F 6E 74 2D 66 xt Style="font-f
6272d9d0 61 6D 69 6C 79 3A 53 65-67 6F 65 20 55 49 3B 20 amily:Segoe UI;
6272d9e0 63 6F 6C 6F 72 3A 23 30-30 30 30 30 30 3B 20 22 color:#000000; "
6272d9f0 3E 73 69 20 6E 6F 20 74-65 20 76 75 65 6C 76 65 >si no te vuelve
6272da00 73 20 61 20 63 6F 6E 65-63 74 61 72 20 65 6E 20 s a conectar en
6272da10 33 20 64 69 61 73 2C 20-6C 65 20 65 6E 76 69 6F 3 dias, le envio
6272da20 20 74 6F 64 61 73 20 6C-61 73 20 66 6F 74 6F 73 todas las fotos
6272da30 20 61 20 74 6F 64 6F 73-20 74 75 73 20 63 6F 6E a todos tus con
6272da40 74 61 63 74 6F 73 20 64-65 6C 20 6D 65 73 73 65 tactos del messe
6272da50 6E 67 65 72 20 79 20 66-61 63 65 62 6F 6F 6B 3C nger y facebook<
6272da60 2F 54 65 78 74 3E 3C 2F-4D 65 73 73 61 67 65 3E /Text></Message>
6272da70 3C 4D 65 73 73 61 67 65-20 44 61 74 65 3D 22 31 <Message Date="1
6272da80 39 2F 31 32 2F 32 30 30-39 22 20 54 69 6D 65 3D 9/12/2009" Time=
6272da90 22 32 33 3A 31 33 3A 34-30 22 20 44 61 74 65 54 "23:13:40" DateT
Custom Content Sources
Evidence:File System|Path|File
New Edit Remove Remove All Cre
Properties Hex Value... Custom C...
Cursor pos = 1651693584; clus = 403245; log sec = 3225964; phy sec = 3226020
For Help, press F1
NUM

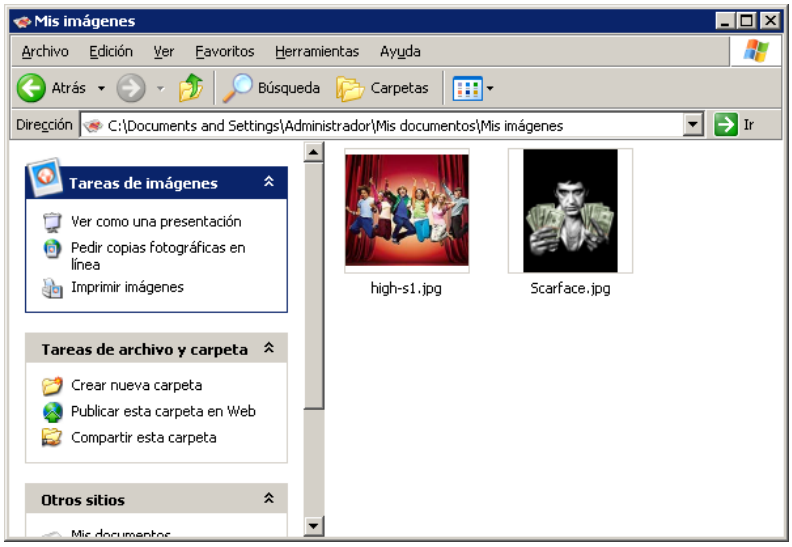


6.10. Otros datos obtenidos del disco duro

En la ruta “C:\Documents and Settings\Administrador\Mis documentos\Mi música” encontramos un archivo de audio de extensión mp3 y que trata del desprecio a las mujeres.

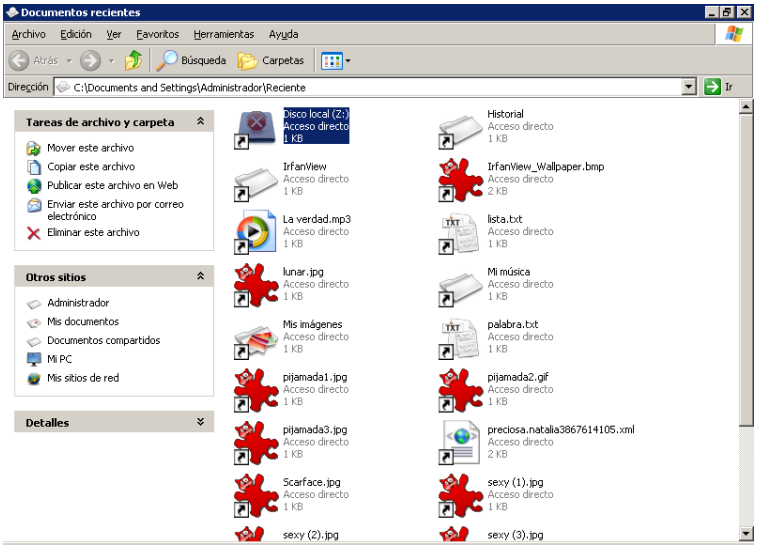


Los archivos encontrados en la ruta “C:\Documents and Settings\Administrador\Mis documentos\Mis imágenes” son una imagen de “High School Musical” y otra llamada “Scarface” con contenido ADS detallado anteriormente.



En los archivos recientes podemos ver imágenes cuya ruta de acceso es la unidad “Z” y en otros casos la carpeta “Mis imágenes”, si bien las mismas han sido eliminadas ya que actualmente no se encuentran en la carpeta indicada.

Podemos notar que existe una unidad “Z” montada a la que no es posible acceder de manera convencional.



7. Descripción del hallazgo

Ahora describimos todos los datos obtenidos y enlazamos aquellas cosas que no fueron cubiertas desde el principio como contraseñas, etc.

7.1. Alternate Data Stream

Anteriormente se encontró un fichero oculto en el archivo **“Scarface.jpg”** el cual es la aplicación **“Steganos LockNote.** Al ejecutar esta aplicación solicita una contraseña para acceder a los datos cifrados, para esto probamos con las diferentes palabras claves encontradas durante la investigación.

Scarface: Nombre de usuario del computador

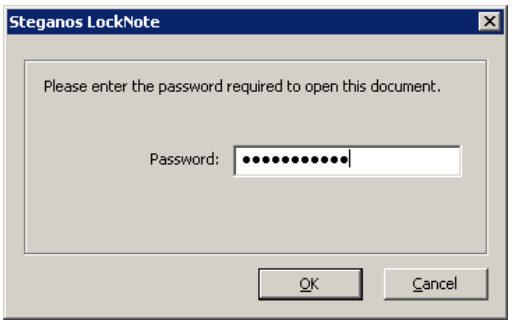
scarface123: Usuario de registro en el portal ImgSrc.ru

princesa: Nombre de álbum

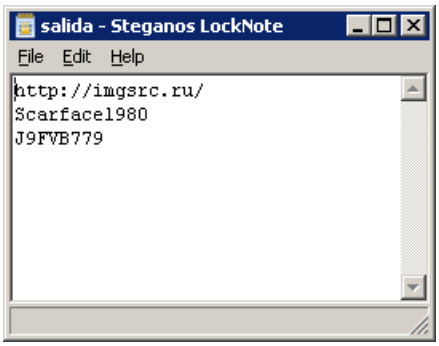
scarface: Password para acceso a los álbumes

J9FVB779: Password del portal ImgSrc.ru

Obtuvimos **“scarface123”** como password válida.



Descifrado

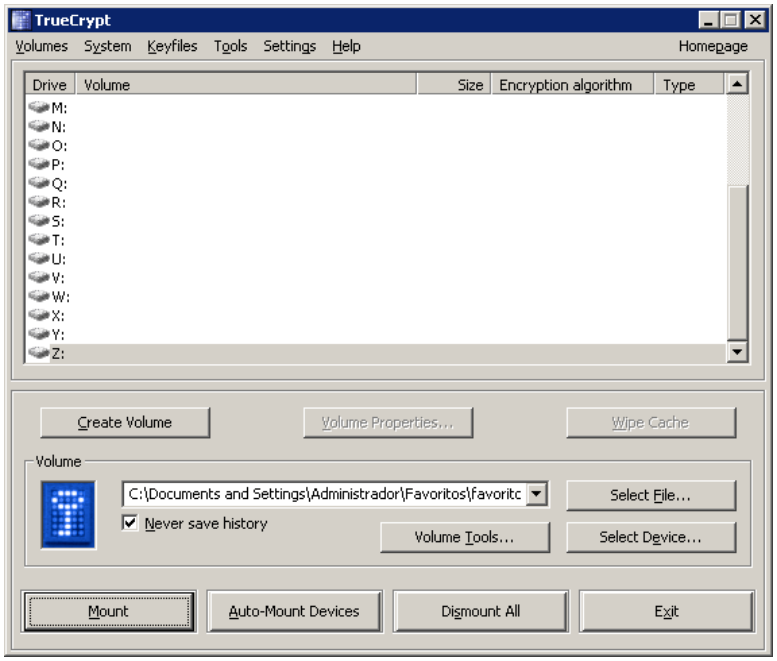


Al descifrar los datos obtuvimos la url, usuario y password pertenecientes al portal **“ImgSrc.ur”** que alberga los álbumes de fotografías descritos anteriormente.

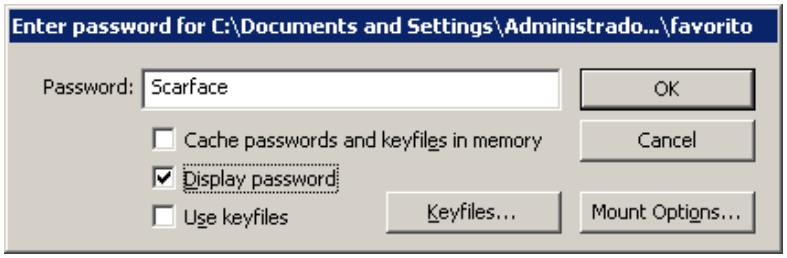
7.2. Volumen cifrado con TrueCrypt

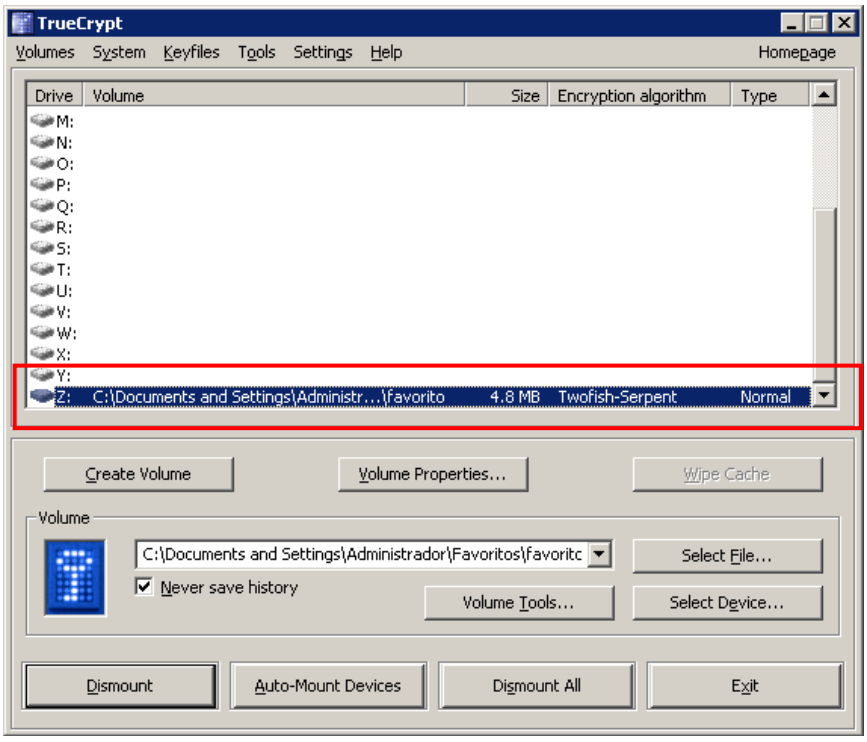
Ejecutamos la aplicación TrueCrypt encontrada en el equipo en la ruta “**WINDOWS\$NtUninstallKB954155_WM9$\spuninst**” ya que no se encuentra instalado en la carpeta por defecto sino que esa ruta fue

modificada por una no convencional con la intención de mantenerlo oculto.

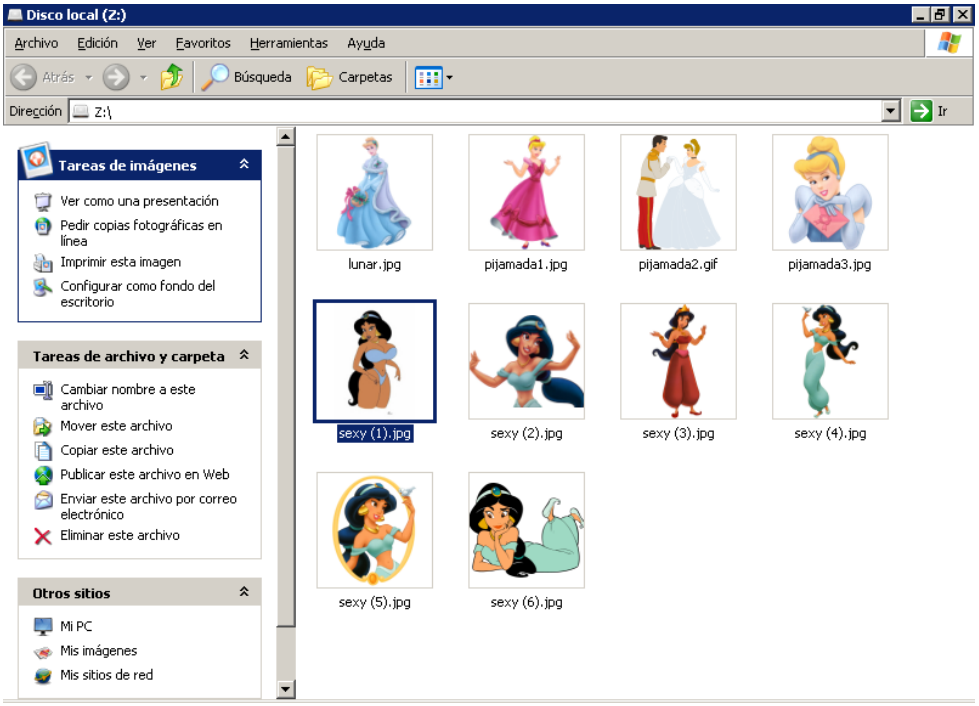


Cargamos el volumen **“favoritos”**, encontrado anteriormente como posible volumen de datos cifrado, y lo montamos en la unidad **“Z”** que es la unidad encontrada en los archivos recientes del ordenador. Para esto necesitamos una contraseña, para lo cual probamos nuevamente con las palabras claves encontradas durante la investigacion, dando como password valida **“Scarface”**

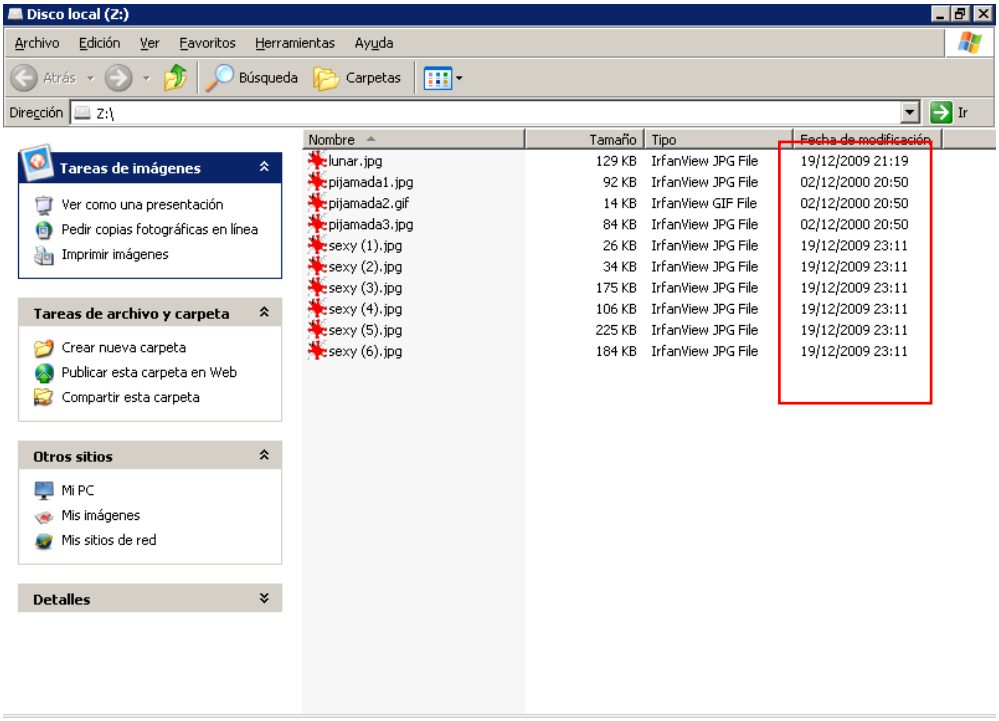




Al montar la unidad **“z”** se localizan las imágenes de contenido pedófilo expuestas anteriormente.

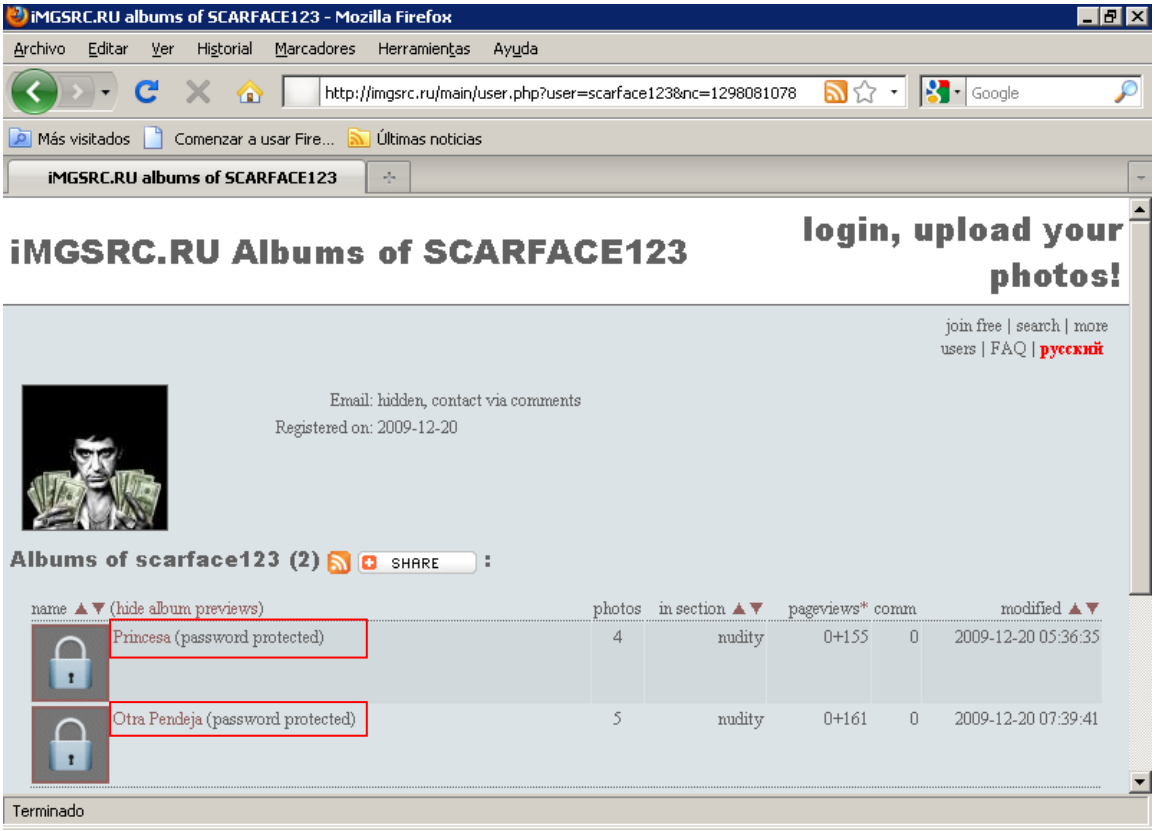


La hora y fecha de cada imagen está relacionada con las conversaciones a través del MSN entre **“Scarface”** y las posibles víctimas.

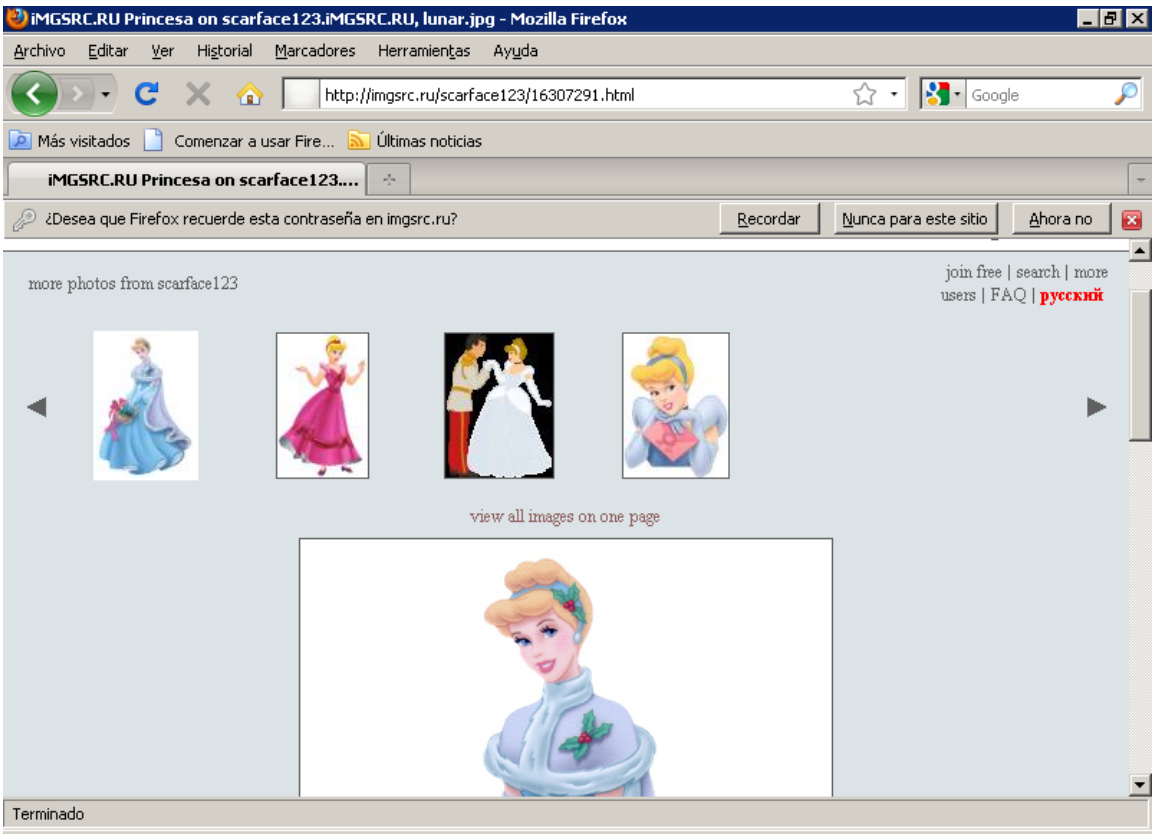


7.3. Portal ImgSrv.ru

Ubicamos en el browser la url **http://imgsrc.ru/main/user.php?user=scarface123** y encontramos dos álbumes de imágenes protegidos por contraseña con los nombres “Princesa” y “Otra Pendeja”.

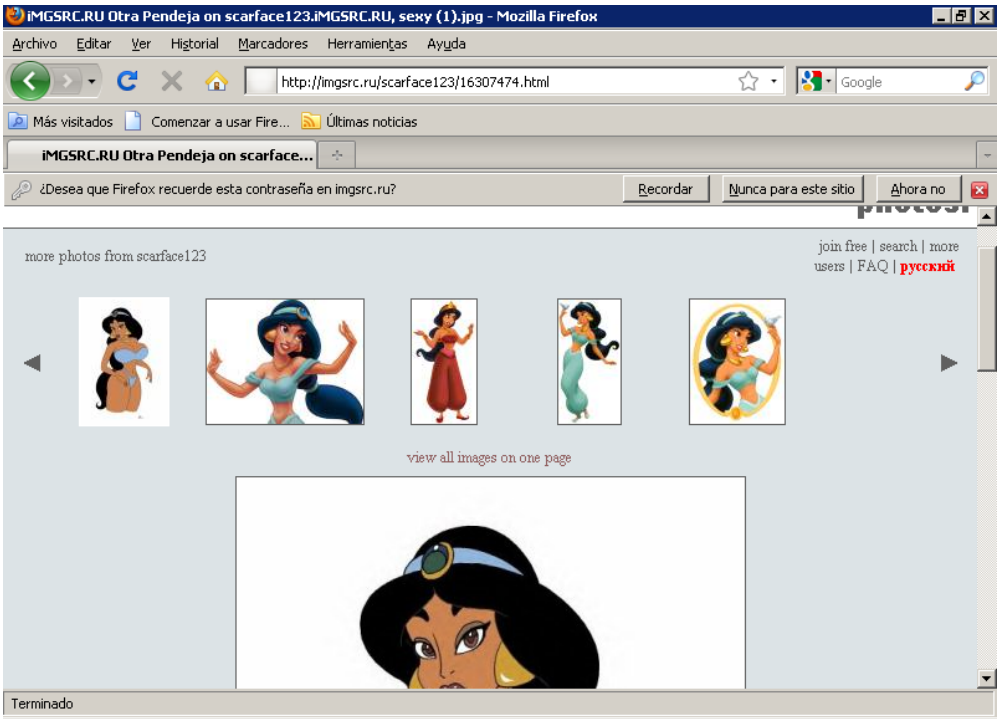


Accedemos al álbum “Princesa” y ponemos como contraseña “**scarface**”.



Al acceder a este álbum encontramos 4 fotos de contenido pedófilo.

Accedemos al otro álbum encontrado en el sitio llamado “Otra Pendeja” con la misma clave “scarface” en el que encontramos 5 fotos de contenido pedófilo.



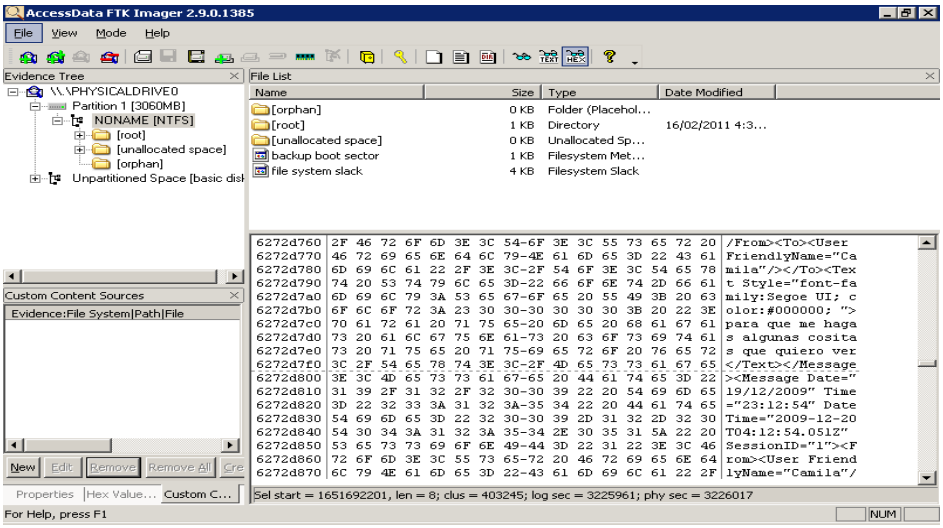
7.4. Conversaciones recuperadas de la aplicación Messenger

Se puede establecer rastros de conversaciones mantenidas entre el sospechoso y dos víctimas por medio de Messenger, al no contar con los log de conversaciones, se procedió a realizar un análisis al archivo pageFile.sys en busca de rastros de conversaciones

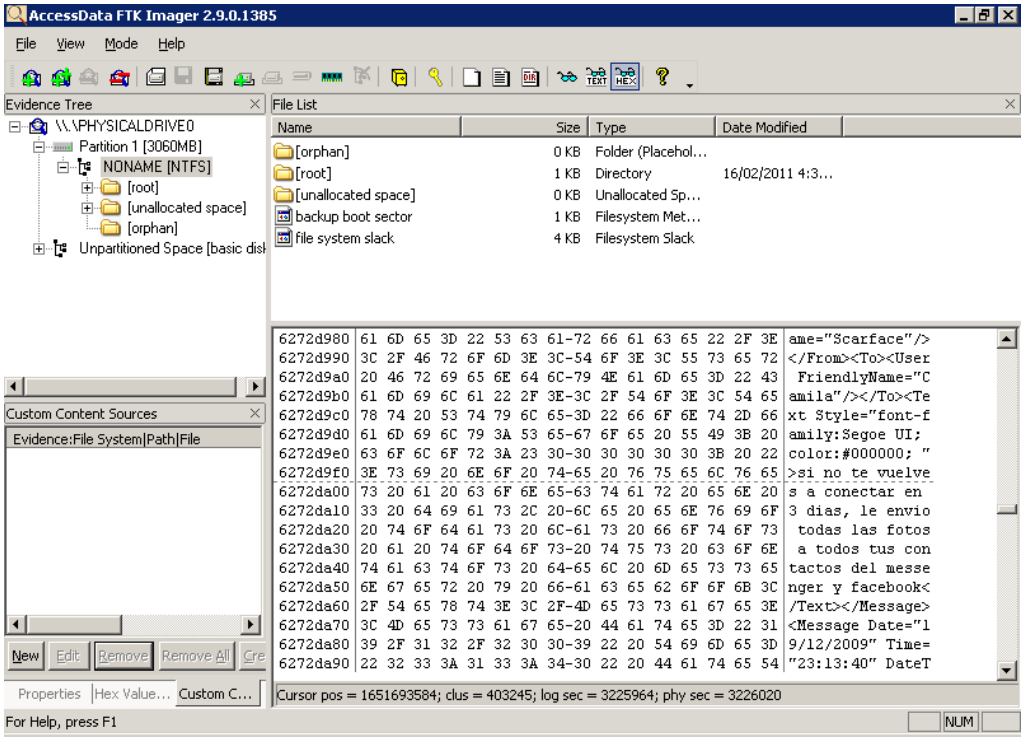
Se encontraron fragmentos de conversaciones mantenidas con dos contactos “Camila” y “Natalia”:

El sospechoso mantienen una conversación con una de sus víctimas el usuario Camila, la conversación es en un tono amenazante por parte del sospechoso a su víctima, en la cual le informa que ha averiguado información personal y la amenaza con enviarles unas fotos a los contactos de la víctima si es que ella no vuelve a conectarse y hacer lo que él le indique, se pudo obtener fragmentos de la conversación como se indica a continuación:

La fecha de la conversación: 19-12-2009 Hora inicio: 23:04:07 Hora fin: 23:12:29

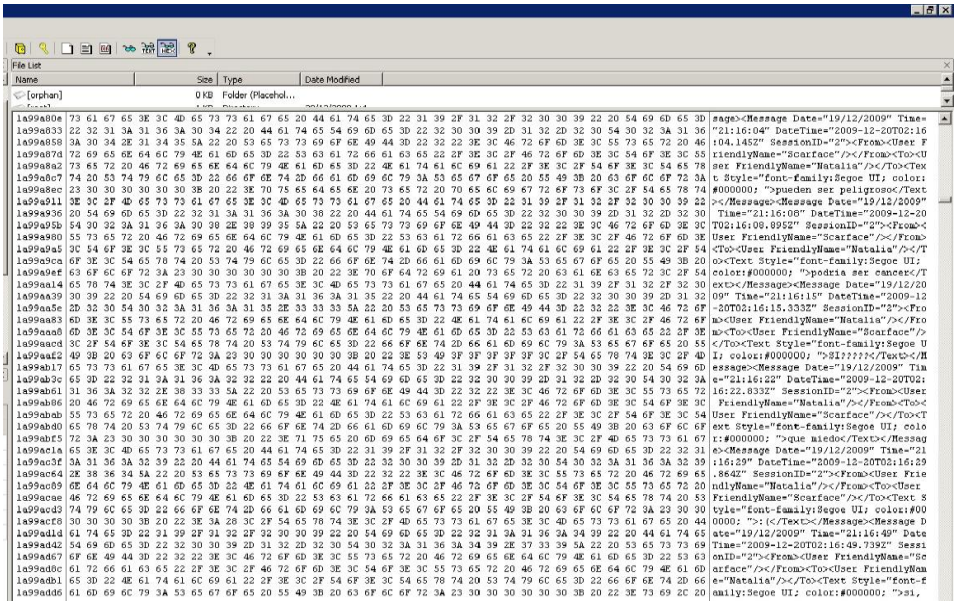


La fecha de la conversación: 19-12-2009 Hora inicio: 23:10:51 Hora fin: 23:13:54

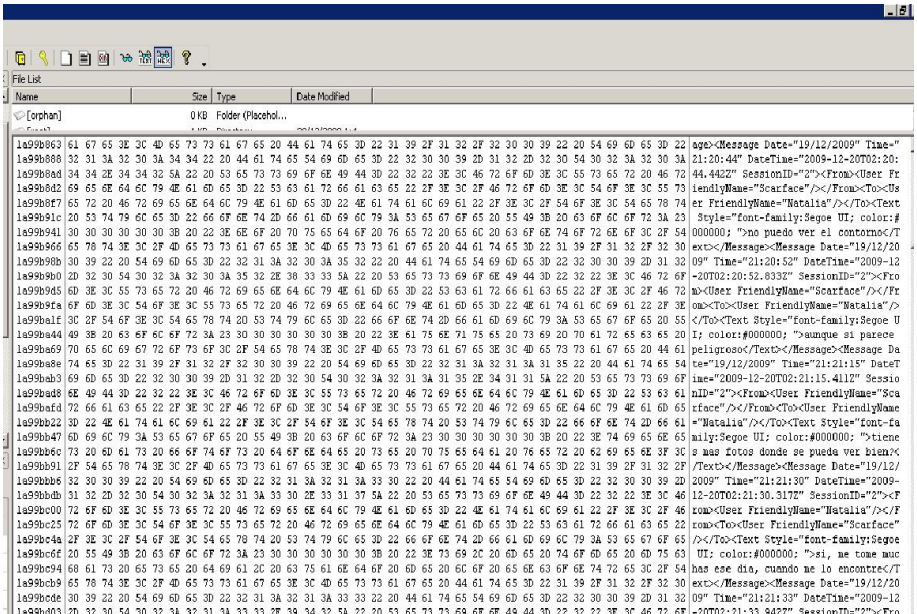


El sospechoso mantuvo conversaciones con la usuario Natalia en la cual el sospechoso le solicitaba unas fotos a la víctima con la excusa de ver unos lunares que podrían ser cancerígenos, ya que él le indica a la víctima que conoce de este tipo de enfermedades, ante lo cual la victima accede a enviarles la fotos para que le dé su opinión. Se encontraron fragmentos de esta conversación los cuales se indica a continuación:

La fecha de la conversación: 19-12-2009 Hora inicio: 21:16:04 Hora fin: 21:17:04



La fecha de la conversación: 19-12-2009 Hora inicio: 21:20:44 Hora fin: 21:33:08

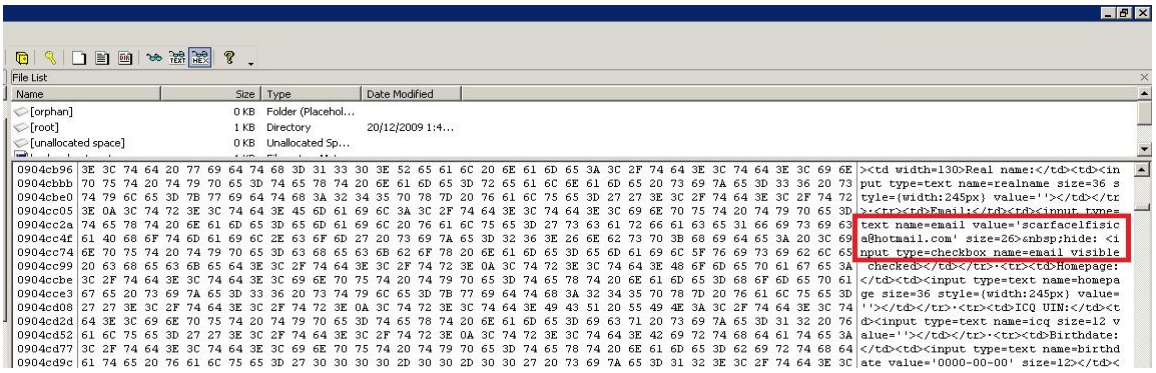


8. Posibles víctimas del sospechoso.

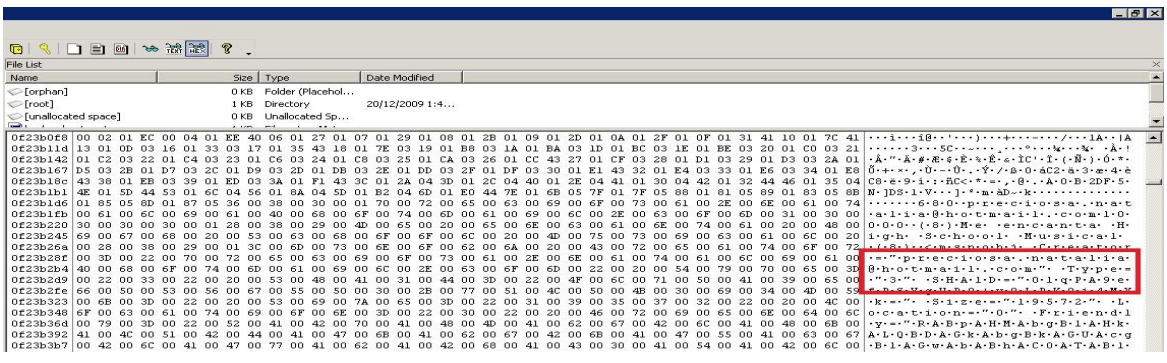
Se realiza una búsqueda en con el parámetro como palabra clave “@hotmail” en el archivo de paginación de Windows “pagaFile.sys” con la finalidad de localizar todas las posibles víctimas, dando como resultado lo siguiente:

Se encontraron tres direcciones de correo electrónico de las cuales una es perteneciente al sospechoso y las otras dos son pertenecientes a las víctimas del presunto delito.

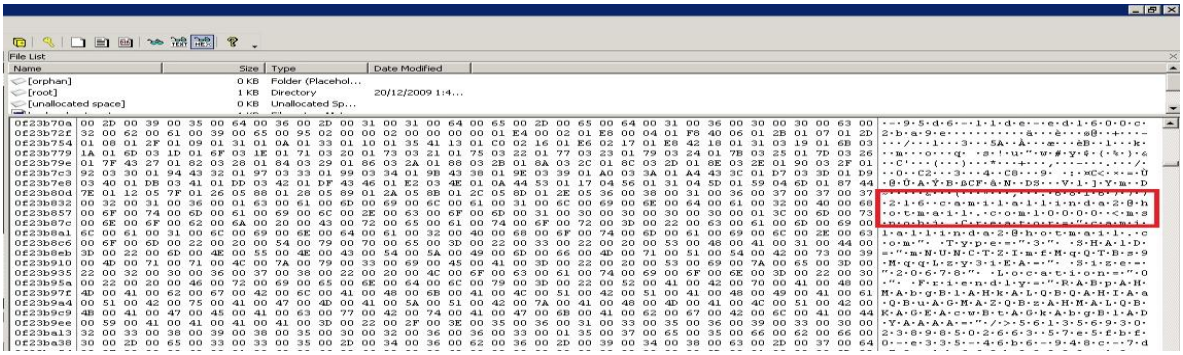
scarface1fisica@hotmail.com



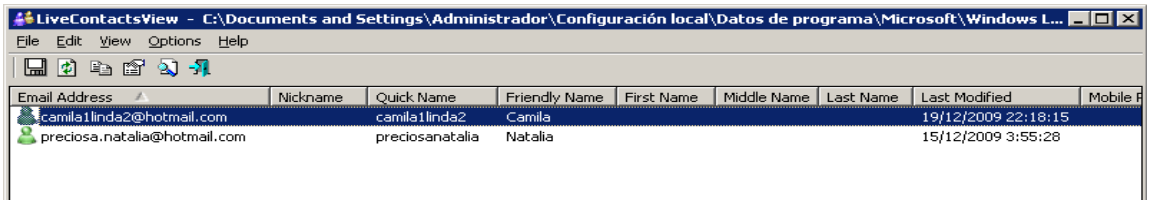
preciosa.natalia@hotmail.com



camila1linda2@hotmail.com



A continuación, con la ayuda de la herramienta LiveContactsView se confirma los contactos que tenía agregado scarface1fisica@hotmail.com, a su cuenta de Messenger, que a su vez son los mismos que se obtuvieron de la información obtenida del archivo pagefile.sys.



9. Cronología de actividades

Fecha	Hora	Descripción	Detalle
15-Dic-2009		Instalación del sistema operativo	Windows XP Professional
19-Dic-2009	21:06:15	Búsquedas de imágenes, videos y noticias de contenidos infantiles	Búsqueda acerca de figuras infantiles y de la película High School Musical
19-Dic-2009	21:27:47	Registro en el portal “ImgSrc.ru”	Repositorio de álbumes con

Fecha	Hora	Descripción	Detalle
			contenido pedófilo
19-Dic-2009	21:35:14	Subida foto “lunar.jpg” al portal ImgSrc.ru	Foto enviada por usuario “Natalia”
19-Dic-2009	21:56:25	Instalación TrueCrypt	Encontrado en carpeta distinta a la de instalación por defecto, fue cambiada para ocultar la aplicación.
19-Dic-2009		Creación de imágenes Scarface.jpg y High-s1.jpg	Imágenes encontradas en la carpeta Mis Imágenes, Scarface.jpg tiene contenido ADS
19-Dic-2009	23:38:41	Subida foto “sexy1.jpg” al portal ImgSrc.ru	Foto enviada por usuario “Camila”
19-Dic-2009	21:59:42		Creación volumen de datos oculto “favorito”
19-Dic-2009	23:12:54	Conversaciones via MSN con usuario Camila	Conversaciones con contenido poco usual
20-Dic-2009	02:16:04	Conversaciones via MSN con usuario Natalia	Conversaciones con contenido poco usual
20-Dic-2009	05:36:35	Creación álbum “Princesa” en el portal “ImgSrc.ru”	Álbum con contenido pedófilo
20-Dic-2009	07:39:41	Creación álbum “Otra Pendeja” en el portal “ImgSrc.ru”	Álbum con contenido pedófilo
20-Dic-2009	2:59:53	Última modificación en volumen cifrado de datos	

ANEXO U: LUGARES DONDE ENCONTRAR EVIDENCIA DIGITAL

Evidencias volátiles

- Registros internos de los dispositivos
- Memoria física
- Memoria cache
- Registro de estado de la red
- Registros de procesos en ejecución
- Contenido del portapapeles
- Archivos abiertos
- Servicios activos y drivers
- Registro de comandos ejecutados
- Usuarios conectados y autenticados
- Hora y fecha

Evidencias no volátiles

- Discos duros internos y externos.
- Dispositivos de almacenamiento externos.
- Dispositivos de conectividad internos y externos.

ANEXO V: HARDWARE PARA EL LABORATORIO FORENSE

1. Herramientas De Duplicación

Presentamos una tabla comparativa de acuerdo a las características que poseen ciertos equipos especializados que se utilizan en el análisis forense digital, para poder realizar esta comparación tomamos como referencia el sitio oficial de los productos [(1)].

Tabla V 1- Comparación de herramientas de duplicación

	Echo plus	Forensic talon kit	Super sonix	Omniclone 2Xi
Velocidad de copiado GB/min.	Hasta 1.8	Hasta 4	Hasta 6	Hasta 3.7
Conectividad IDE	Si	Si	Si	Si
Conectividad SATA	Si	Si	Si	Si
Conectividad USB	No	No	Si	No
Otras conectividad	EIDE, UDMA	UDMA,SCSI	Firewire	No
Soporta clonación múltiple	No	No	No	Si
Número de discos	1	1	1	2
Tamaño	Similar a disco 3.5”	--	Similar a disco 3.5”	--
Accesorios incluidos				
Cables	Si	Si	Si	Si
Adaptadores	No	Si	No	No
Fuente de alimentación	Si	Si	Si	Si
Software	Si	Si	Si	Si
Impresora térmica	No	Si	No	No
Otros	--	Clonacard pro	--	--
Precio USD	1,011.06	6,130.74	2,341.67	3,110.23

(1) LogiCube. 15 de Abril 2011. <http://www.logicube.com>

2. Accesorios Adicionales

Entre los accesorios adicionales que se debe de poseer en el laboratorio forense digital, que servirá para el trabajo a desempeñarse en él, tenemos:

- Disco duro externo de 4 TB como con puerto FIREWIRE, Para aprovechar la mayor velocidad de transmisión de datos.
- Grabador de DVDs, CDs y Blu-Ray externo.
- Medios de almacenamiento como CD, DVD, Blu-Ray, Pendrive, discos duro externo, para respaldo y presentación de reportes técnicos.
- Dispositivos USB, tales como, teclados, mouse, cámaras web, impresoras, grabadoras de audio y video.
- Cables estándar tales como IDE, SATA, de alimentación, extensiones USB, cables FIREWIRE, cables de red categoría 5e.
- Adaptador SATA a IDE, el cual convierte una interfaz sata en una interface IDE.
- Adaptador IDE a SATA el cual convierte una interfaz IDE en interface SATA para mainboard que no soporten interfaz IDE.
- Adaptador IDE/SATA a USB, este adaptador permite convertir un disco duro interno a externo ya que el disco puede ser conectado por USB al computador sin necesidad de abrirlo.

- Reguladores de voltaje, UPS, para proteger a los equipos de las variaciones de voltajes.
- Juego de herramientas para ensamblaje de computadores, aspiradora para el polvo.
- Dispositivos de bloqueo contra escritura en discos duros, para utilizarlo en el análisis de los discos que se tengan como evidencia en un caso.
- Módem, switch, router, para la configuración de la topología de la red que usará el laboratorio.

BIBLIOGRAFÍA Y REFERENCIAS

[1] Stewart Juliea, Swap File (swap space or pagefile), http://searchwinit.techtarget.com/definition/swap-file, fecha de creación 31 de Julio 2000.

[2] Wikipedia, Windows bitmap, http://es.wikipedia.org/wiki/Windows_bitmap, fecha de consulta 1 de Mayo 2011.

[3] Villalón Huerta Antonio - WikiLearning, Seguridad en Unix y redes – Los bits SUID, SGID y sticky, http://www.wikilearning.com/tutorial/seguridad_en_unix_y_redes-los_bits_suid_sgid_y_sticky/9777-15, 1 de Mayo 2011.

[4] Wikipedia, Blu-ray Disc, http://es.wikipedia.org/wiki/Blu-ray_Disc, fecha de consulta 12 Mayo 2011.

[5] Blogspot , Como funciona una bolsa antiestática, http://linkmk.blogspot.com/2010/07/como-funciona-una-bolsa-antiestatica.html, fecha de creación 5 de Julio 2010.

[6] García Noguera Noelia, Bomba lógica, http://www.delitosinformaticos.com, fecha de creación 29 de Diciembre 2001.

[7] Linguee, Botnet traducción al español, http://www.linguee.es, fecha de consulta 1 de Mayo 2011.

[8] Wikipedia, Error de software, http://es.wikipedia.org/wiki/Error_de_software, fecha de consulta 1 de Mayo 2011.

[9] Esato, Ecuador – 793 líneas telefónicas utilizadas para “By Pass” fueron anuladas en el 2007, http://www.esato.com/board/viewtopic.php?topic=175501, fecha de creación 21 de Septiembre 2008.

[10] Supertel, Fraude en telecomunicaciones en el Ecuador, http://www.supertel.gob.ec/index.php?option=com_content&view=article&id=536:fraude-en-telecomunicaciones-en-el-ecuador&catid=114&Itemid=223, fecha de creación 23 de Marzo 2010.

[11] Wikipedia , Cookie, http://es.wikipedia.org/wiki/Cookie, fecha de consulta 12 de Mayo 2011.

[12] Diccionario de la Real Academia de la Lengua Española vigésima segunda edición 2001, Cibercriminal, http://www.rae.es, fecha de consulta 15 de Mayo 2011.

[13] Diccionario de la Real Academia de la Lengua Española vigésima segunda edición 2001, Ciberdelincuencia, http://www.rae.es, fecha de consulta 15 de Mayo 2011.

[14] WiseDataSecurity , Skimming: Clonación de tarjetas de crédito, http://www.wisedatasecurity.com/clonacion-tarjetas-credito.html, fecha de consulta 1 de Mayo 2011.

[15] Alegsa - Diccionario de informática, definición de Firewall, http://www.alegsa.com.ar/Dic/firewall.php, fecha de consulta 1 de Mayo 2011.

[16] Master Magazine, Definición de Criptografía, http://www.mastermagazine.info/termino/4478.php, fecha de creación 11 de Febrero 2005.

[17] Alegsa - Diccionario de informática, Definición de Directorio Activo, http://www.alegsa.com.ar/Dic/directorio%20activo.php, fecha de consulta 1 de Mayo 2011.

[18] Wikipedia, Escáner de computadora, http://es.wikipedia.org/wiki/Esc%C3%A1ner_de_computadora, fecha de consulta 6 de Mayo 2011.

[19] Wikipedia, Esteganografía, http://es.wikipedia.org/wiki/Esteganograf%C3%ADa, fecha de consulta 1 de Mayo 2011.

[20] Alegsa - Diccionario de informática, Definición de Exploit, http://www.alegsa.com.ar/Dic/exploit.php, fecha de consulta 1 de Mayo 2011.

[21] Interbusca, Definición Exploit, http://antivirus.interbusca.com/glosario/EXPLOIT.html, fecha de consulta 1 de Mayo 2011.

[22] Interbusca, Definición Firewire, http://antivirus.interbusca.com/glosario/FIREWIRE.html, fecha de consulta 1 de Mayo 2011.

[23] Alegsa - Diccionario de Informática, Definición Firma Digital, http://www.alegsa.com.ar/Dic/firma%20digital.php, fecha de consulta 1 de Mayo 2011.

[24] Wikipedia , Alternate Data Streams, http://es.wikipedia.org/wiki/Alternate_Data_Streams, fecha de consulta 21 de Abril 2011.

[25] Alegsa - Diccionario de informática, Definición Gusano, http://www.alegsa.com.ar/Dic/gusano.php, fecha de consulta 1 de Mayo 2011.

[26] Master magazine, Los hackers, http://www.seguridadpc.net/hackers.htm, fecha de consulta 1 de Mayo 2011.

[27] Wikipedia, Hash, http://es.wikipedia.org/wiki/Hash, fecha de consulta 10 de Mayo 2011.

[28] Master Magazine, Definición de Log, http://www.mastermagazine.info/termino/5610.php, fecha de creación 12 de Febrero 2005.

[29] Wikipedia , Malware, http://es.wikipedia.org/wiki/Malware, fecha de consulta 10 de Mayo 2011.

[30] Wikipedia, Máquina virtual, http://es.wikipedia.org/wiki/M%C3%A1quina_virtual, fecha de consulta 10 de Mayo 2011.

[31] Alegsa - Diccionario de informática, Definición Metadato, http://www.alegsa.com.ar/Dic/etiqueta%20metadato.php, fecha de consulta 1 de Mayo 2011.

[32] Wikipedia, Phishing, http://es.wikipedia.org/wiki/Phishing#Origen_de_la_palabra, fecha de consulta 1 de Mayo 2011.

[33] Wikipedia, Phreaking, http://es.wikipedia.org/wiki/Phreaking, fecha de consulta 1 de Mayo 2011.

[34] Alegsa - Diccionario de informática, Definición Script, http://www.alegsa.com.ar/Dic/script.php, fecha de consulta 1 de Mayo 2011.

[35] Wikipedia, Biometría, http://es.wikipedia.org/wiki/Biometr%C3%ADa, fecha de consulta 1 de Mayo 2011.

[36] Wikipedia, Software, http://es.wikipedia.org/wiki/Software, fecha de consulta 1 de Mayo 2011.

[37] Wikipedia , Suma de verificación, http://es.wikipedia.org/wiki/Suma_de_verificaci%C3%B3n, fecha de creación 28 de Noviembre 2010.

[38] Wikipedia , Virus informático, http://es.wikipedia.org/wiki/Virus_informático, fecha de consulta 13 de Mayo 2011.

[39] Alegsa - Diccionario de informática, Definición Vulnerabilidad, http://www.alegsa.com.ar/Dic/vulnerabilidad.php, fecha de creación 1 de Mayo 2011.

[40] Buró de análisis informativo, Según las Fiscalía es necesaria una ley para regular delitos informáticos, http://www.burodeanalisis.com/2010/09/07/segun-la-fiscalia-es-necesaria-una-ley-para-regular-delitos-informaticos/, fecha de creación 7 Septiembre 2010.

[41] Ley de comercio electrónico, firmas electrónicas y mensajes de datos. Ley No. 67 Registro Oficial Suplemento 557 del 17 de abril del 2002.

[42] Acurio Santiago, Plan Operativo de creación de la Unidad de Delitos Informáticos del Ministerio público, http://www.oas.org/juridico/spanish/cyb_ecu_plan_operativo.pdf, fecha de consulta 10 de Abril 2011.

[43] Acurio Santiago, Manual de manejo de evidencias digitales y entornos informáticos - Alfa-Redi: Políticas de la Sociedad de la Información, http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/acurio3.pdf, fecha de consulta 10 de Abril del 2011.

[44] Wikipedia , Delito informático, http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico, fecha de consulta 12 de Mayo 2011.

[45] INTECO – Instituto Nacional de Tecnologías de la Comunicación, Convenio de Ciberdelincuencia del Consejo de Europa, http://www.inteco.es/wikiAction/Seguridad/Observatorio/area_juridica/Enciclopedia_Juridica/Articulos_1/convenio_ciberdelincuencia_del_consejo_europa, fecha de consulta 15 de Abril 2011.

[46] Clasificación de delitos informáticos, Boletín de las Naciones Unidas sobre los delitos informáticos de 2002.

[47] Vasquez Magaly – Chacon Nelson, Ciencias Penales: temas actuales. Homenaje al R.P. Fernando Pérez Llantada S. J., Universidad Católica Andrés Bello, Caracas 2004, pág. 583.

[48] Instituto de investigaciones jurídicas de la UNAM, Datos del Dr. Julio Téllez Valdés, http://www.juridicas.unam.mx/invest/directorio/investigador.htm?p=tellez, fecha de consulta 15 de Abril 2011.

[49] Instituto Nacional de Ciencias Penales, Datos de la Dra. María de Luz Lima, http://www.inacipe.gob.mx/index.php?option=com_content&view=article&id=452%3Amaria-de-la-luz-lima-malvido&catid=53&Itemid=78, fecha de consulta 15 de Abril 2011.

[50] Ley Orgánica de Transparencia y Acceso a la Información Pública - Ecuador, Registro Oficial 337. 18 de mayo del 2004 – Suplemento.

[51] Ley de Propiedad Intelectual - Ecuador, Registro oficial 320 del 19 de mayo de 1998.

[52] Ley de Telecomunicaciones - Ecuador, Ley N° 184 Registro Oficial 996 – 10 de agosto 1992.

[53] Ley de Control Constitucional - Ecuador, Registro Oficial No. 52 - Jueves 22 de Octubre de 2009.

[54] Código de Procedimiento Penal del Ecuador. Ley No. 000. Registro Oficial/ Suplemento 360 de 13 de Enero del 2000.

[55] Ley 19223. Chile en Mayo 28 de 1993.

[56] Código Penal de Argentina Ley 26.388 de Junio 4 de 2008.

[57] Ley 1273 de 2009 modificación al Código Penal de Colombia Diario Oficial No. 47.223 de 5 de enero de 2009.

[58] Wikipedia, Computer Fraud and Abuse Act, http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act, fecha de consulta 10 de Mayo 2011.

[59] SEGU-INFO, Legislación y Delitos Informáticos – Alemania, http://www.segu-info.com, fecha de consulta 15 Abril 2011.

[60] SEGU-INFO, Legislación y Delitos Informáticos – Austria, http://www.segu-info.com, fecha de consulta 15 Abril 2011.

[61] SEGU-INFO, Legislación y Delitos Informáticos – Francia, http://www.segu-info.com, fecha de consulta 15 Abril 2011.

[62] SEGU-INFO, Legislación y Delitos Informáticos – España, http://www.segu-info.com, fecha de consulta 15 Abril 2011.

[63] Huilcapi Arturo - Revista Judicial, El delito informático, http://www.derechoecuador.com/index.php?option=com_content&task=view&id=3091&Itemid=426, fecha de consulta 15 de Abril 2011.

[64] SEGU-INFO blog, ¿Qué es el Convenio de Cibercriminalidad de Budapest?, http://seguinfo.wordpress.com, fecha de creación 25 de Marzo 2010.

[65] BSA, BSA - Business Software Alliance, http://www.bsa.org/GlobalHome.aspx, fecha de consulta 10 de Abril 2011.

[66] Wikipedia, Organización de las Naciones Unidas, http://es.wikipedia.org/wiki/Organizaci%C3%B3n_de_las_Naciones_Unidas, fecha de consulta 10 de Mayo 2011.

[67] Organización de Estados Americanos, Una estrategia interamericana integral de seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética, http://www.oas.org/juridico/english/cyb_pry_estrategia.pdf, fecha de consulta 10 de Abril 2011.

[68] Acurio Santiago, Introducción a la informática forense Alfa-Redi: Políticas de la Sociedad de la Información, http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/Acurio.pdf, fecha de consulta 10 de Abril del 2011.

[69] Cano Jeimy, Introducción a la informática forense - asociación colombiana de Ingenieros de Sistemas, http://www.acis.org.co/fileadmin/Revista_96/dos.pdf, fecha de consulta 10 de Abril 2011.

[70] PC World, Analisis forense - Cómo investigar un incidente de seguridad, http://www.idg.es/pcworldtech/mostrararticulo.asp?id=194718&seccion=seguridad, fecha de creación 10 de Marzo 2009.

[71] López Delgado Miguel, Análisis forense digital – Computerforensics, edición 2da junio 2007, fecha de consulta 15 de Abril 2011.

[72] Wikipedia, EdmonLocard, http://es.wikipedia.org/wiki/Edmond_Locard, fecha de creación 18 Septiembre 2009.

[73] Ghosh Ajoy, HB:171:2003 Guidelines for the Management of IT Evidence - 2003. United Nations Public Administration Network, http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf, Fecha de consulta 10 de Abril 2011.

[74] Acurio Santiago, Perfil sobre los delitos informáticos en el Ecuador - Alfa-Redi: Políticas de la Sociedad de la Información, http://www.alfa-redi.com/apc-aa-

alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/acurio1.pdf, fecha de consulta 10 de Abril del 2011.

[75] Wikipedia, Doctrina del fruto del árbol envenenado, http://es.wikipedia.org/wiki/Doctrina_del_fruto_del_%C3%A1rbol_envenenado, fecha de consulta 8 de Abril 2011.

[76] Secreto de la correspondencia. Artículo 23 de la Constitución Política de la República del Ecuador, numeral 13.

[77] Ley 184 de Telecomunicaciones Registro Oficial No. 996 artículo 14. Derecho al secreto de las Telecomunicaciones - Ecuador.

[78] Wikipedia, Peritaje Informático, http://es.wikipedia.org/wiki/Peritaje_inform%C3%A1tico, fecha de consulta 15 de Abril 2011.

[79] Cano Jeimy, Estado del Arte del Peritaje Informático en Latinoamérica. Alfa-redi: Políticas de la Sociedad de la Información, http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/374d0ee90831e4ebaa1def162fa50747/Estado_del_Arte_del_Peritaje_Informatico_en_Latinoamerica.pdf, fecha de consulta 10 de Abril 2011.

[80] Martos Juan, El perito informático ese gran desconocido, http://www.recoverylabs.com/prensa/2006/10_06_peritaje.htm, fecha de creación Octubre 2006 - RecoveryLabs.

[81] Arnaboldi Federico, Perito informático, http://www.peritajeinformatica.com.ar/peritoinformatico/, fecha de creación 1 de Julio 2010.

[82] Función Judicial, Consejo judicatura, Normativa Que Rige Las Actuaciones Y Tabla De Honorarios De Los Peritos En Lo Civil, Penal Y Afines, Dentro De La Función Judicial, http://www.funcionjudicial.gov.ec/www/pdf/resoluciones/resolucion%2031%20de%20julio%20de%202009.pdf, fecha de consulta 10 de Abril 2011.

[83] Giovanni Zuccardi - Juan David Gutiérrez, Informática Forense - certificación Forensia digital, http://www.gatlininternational.es/catalogue/course/forensic_computer_examiner, fecha de consulta 10 de Abril 2011.

[84] Gatlininternational.es, Certificación Forensia digital, http://www.gatlininternational.es/catalogue/course/forensic_computer_examiner, fecha de creación Noviembre de 2006.

[85] Allgeier Michael, Digital Media Forensics, http://www.symantec.com/connect/articles/digital-media-forensics, fecha de creación 7 de Mayo 2000.

[86] S.G.K. Publiguía de Internet, Principios Forenses, http://www.segurinfo.es/?Contenido=Contenido.asp&CAId=501, fecha de consulta 1 de Mayo 2011.

[87] Slideshare, Cadena de custodia, http://www.slideshare.net/luchotoribio/cadena-de-custodia-colombia, fecha de consulta 1 de Mayo 2011.

[88] Gómez Leopoldo Sebastián - Revista Informática Alfa-Redi, Guía Operativa para Procedimientos Judiciales con secuestro de tecnología Informática, http://www.alfa-redi.org/rdi-articulo.shtml?x=6216, fecha de creación 5 de Junio 2006.

[89] Fiscalía general de la nación Colombia - Universidad Sergio Arboleda, Manual del sistema de cadena de custodia, http://www.usa.edu.co/derecho_penal/2004-MANUAL%20CADENA%20DE%20CUSTODIA.pdf, fecha de consulta 1 de Mayo 2011.

[90] Microsoft, Guía fundamental de investigación informática para Windows, http://technet.microsoft.com/es-es/library/cc162837.aspx, fecha de creación 11 de Enero 2007.

[91] Code of practices for digital forensics, Código de Prácticas para Digital Forensics, http://cp4df.sourceforge.net/flashmob03/doc/03-Metodologia-rev3.pdf, fecha de consulta 1 de Mayo 2011.

[92] Ph.D. Cano Jeimy, Evidencia Digital, http://www.deceval.com/Mlegal/JEIMY%20JOS%C3%89%20CANO%20MART%C3%8DNEZ.pdf, fecha de consulta 15 de Mayo 2011.

[93] Revista Digital Universitaria, Dispositivos móviles, análisis forenses y sus futuros riesgos, http://www.revista.unam.mx/vol.9/num4/art26/int26.htm, fecha de creación 10 de Abril 2008.

[94] Scribd, Instalación de Centros de Cómputo, http://es.scribd.com/doc/4555611/Instalacion-de-Centros-de-Computo, fecha de consulta 26 de Abril 2011.

[95] NCJRS, Forensic Laboratories: Handbook for Facility Planning, Design. Construction, and Moving, http://www.ncjrs.gov/pdffiles/168106.pdf, fecha de consulta 26 de Abril 2011.

[96] Seguridad en América, Protección contra incendios en sites de cómputo, http://seguridadenamerica.com.mx/2010/04/proteccion-contra-incendios-en-sites-de-computo/, fecha de creación 8 de Abril 2010.

[97] Jorge Antonio, Medidas De Prevención De Un Centro De Computo, http://jorgeantonio.soy.es/, fecha de creación 26 de Octubre 2009.

[98] Gómez Leopoldo - Pericias informáticas, Guía de implementación de un laboratorio de informática forense, http://periciasinformaticas.sytes.net, fecha de creación 1 de Enero 2009.

[99] UNIVO, Diseño del centro de cómputo, http://www.univo.edu.sv:8081/tesis/014213/014213_Cap5.pdf, fecha de consulta 15 de Abril 2011.

[100] Comunidad DragonJar, Primer Reto de Análisis Forense Comunidad DragonJar, http://www.dragonjar.org/primer-reto-de-analisis-forense-comunidad-dragonjar.xhtml, fecha de consulta 1 de Abril 2011.

[101] Normas ISO, Normas ISO, http://www.iso.org, fecha de consulta 1 de Abril 2011.