INSTITUTO UNIVERSITARIO AERONÁUTICO

Facultad de Ciencias de la Administración

PROYECTO DE TESIS DE GRADO

Título: “Forensia Informática aplicada a PC con sistema operativo Windows y Linux”

Autores:
Daniel Caffaratti
Lorena Holc
Director de Tesis: Ing Eduardo Casanovas

Contenido

Introducción

En los últimos años ha habido una explosión del interés sobre el estudio de evidencias digitales. Este crecimiento ha provocado acalorados debates sobre herramientas, terminología, definiciones, estándares, ética, y otros muchos aspectos de este campo en desarrollo.

La telefonía móvil, las redes wifi, los Smartphone, Tablet y los teléfonos inteligentes avanzan de manera meteórica en esta sociedad de la información, en donde los conflictos y los delitos telemáticos van en aumento, con lo que empresas, profesionales, la administración de la justicia y la Sociedad en general demandan profesionales capacitados en la extracción, análisis y estudio de las evidencia telemáticas.

Delitos tecnológicos como el robo de personalidad, datos, secretos comerciales, destrucción o mal uso de la propiedad intelectual, fraude, bases de datos, fotografías, conversaciones y la lista se hace interminable; hacen necesaria la actuación de un perito Informático capaz de extraer, estudiar, analizar, preservar y presentarlas ante quien sea requerido para esclarecer los datos importantes del litigio.

Cuando se sufre un delito tecnológico es necesario neutralizarlo, saber cómo se ha perpetrado la vulnerabilidad, el alcance del delito realizado y prevenir futuros ataques mediante el uso de técnicas, programas y herramientas forenses que determinen de manera infalible la evidencia legal.

Después de que ha ocurrido un crimen o incidente que implique una computadora, un especialista adiestrado en informática forense puede examinar la misma para encontrar pistas de lo que ha pasado. Este es el papel del examinador forense de computadoras. Este especialista podría trabajar para el estado como agente de la ley, o para una empresa privada en algunos casos, como los incidentes de seguridad en un sistema. Aunque en cada uno de los dos casos la ley es diferente, la estrategia de investigación para el especialista es más o menos la misma.

Objeto de Estudio

Haremos una breve referencia sobre el marco legal de las pericias informáticas Basados en los análisis realizados por profesionales competentes al área legal sobre la ley 26388 y el convenio internacional de Budapest, para contextualizar la situación actual en la República Argentina.

Realizaremos un análisis de las ventajas y desventajas de las posibles metodologías para la investigación en informática forense y pericial.

Tomaremos las herramientas más sobresalientes del mercado y realizaremos un análisis comparativo de ventajas y desventajas de las mismas. Teniendo en cuenta que la mayoría de las herramientas de informática forense líderes en diversas áreas de la especialidad son de alto costo y no están disponibles para testing, este análisis comparativo se limitará a software open source.

Objetivos

1- Conocer el marco legar de las pericias informáticas en la República Argentina.

2- Analizar ventajas y desventajas de las diferentes metodologías de trabajo para el análisis de datos.

2.1 Seleccionar la metodología que mejor se adecue para garantizar la cadena de custodia.

2.2 Aplicar la metodología seleccionada en un caso práctico.

2.3 Indicar conclusiones.

3- Proponer el uso de una herramienta open source que mejor se adapte al marco legal regulatorio de Argentina, para el análisis de datos

3.1 Seleccionar la herramienta con mayor cantidad de beneficios permitiendo asegurar las máximas garantías de recuperación.

3.2 Aplicar en la resolución de en un caso práctico la herramienta seleccionada.

3.3 Indicar conclusiones.

4- Comprender el uso del software elegido

4.1 Apoyarse en la herramienta para realizar la búsqueda de evidencia.

4.2 Lograr una interpretación adecuada de los resultados del análisis Forense.

4.3 Interpretar la salida de las herramientas forenses y lograr que la misma sea una evidencia confiable del proceso en curso.

Capítulo I

Informática Forense

1.1 - La informática forense

La informática forense hace su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos que implica la resolución de actos delictivos cometidos a través de medios informáticos, y también descubrir las técnicas utilizadas, se presenta así como garante de la verdad alrededor de la evidencia digital que pueda aportarse en un procedimiento.

En principio se puede definir a la informática forense o como señalan algunos autores Análisis Forense Digital, como una ciencia forense que se ocupa de la utilización de los métodos científicos aplicables a la investigación de los delitos informáticos y donde se utiliza el análisis forense de las evidencias digitales, en fin toda información o datos que se guardan en una computadora o sistema informático.

El Ing. Luis Ángel Gómez en el documento publicado en el sitio del Ministerio de Seguridad, sostiene: *""Es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permite identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal". Ampliaría diciendo que es: "Una ciencia que busca reproducir científicamente con una metodología estricta de los hechos acontecidos y su correlación para determinar el grado de impacto, y posteriormente establecer en coordinación con otros entes intervinientes, mecanismos tendientes a evitar nuevamente su ocurrencia, que van desde el marco normativo hasta la utilización de mecanismos técnicos". Es un método científico porque supone la adquisición de nuevos conocimientos, mediante el estudio de la evidencia observable y medible, aplicando un razonamiento lógico, elaborando modelos e hipótesis y corrigiendo o mejorando estas últimas según se obtiene más evidencia. Además, los resultados deben ser objetivos e imparciales, lo que implica un alto grado de profesionalidad para con la tarea por realizar. La metodología aplicada debe ser conocida, sabida y practicada, de forma que otros investigadores, utilizando los mismos métodos, puedan llegar a las mismas conclusiones. Si esto no se logra, la posibilidad de la pérdida de la evidencia con valor probatorio es inminente y todo lo que con esto conlleva."* (Gómez, http://www.minseg.gob.ar/node/1050)

Por otra parte el doctor Miguel López Delgado, se refiere a al Análisis Forense Digital como *"…un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial"*. (Delgado, 2007)

Según WIKIPEDIA el *"Análisis Forense Digital o exanimación forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal".* Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Los autores en cuanto se refiere a la definición de Análisis Forense Digital coinciden al señalar que se utilizan, o son un conjunto de técnicas que consisten en algunos procedimientos que permiten obtener información que sea válida en un proceso legal.

En conclusión la informática forense por tanto será la ciencia forense formal que se encarga del estudio de los métodos y técnicas de identificar, extraer, analizar, preservar y presentar a través de técnicas y herramientas la información, que permitan al perito forense informático poder entregar un informe en donde presenten los hallazgos de manera lógica y con un sustento claro de lo que desea mostrar.

La informática forense se aplica tanto para las investigaciones de delitos tradicionales tales como: fraudes financieros, narcotráfico, terrorismo, etc.; como para aquellos que están estrechamente relacionas con las tecnologías de la información y las comunicaciones, entre los que se tienen la piratería de software, distribución pornográfica infantil, tráfico de bases de datos, etc.

Dentro de la informática forense encontramos varias definiciones como las siguientes:

Forensia en redes

El perito, debe comprender la manera en que los protocolos, configuraciones e infraestructuras de comunicaciones interactúan para poder obtener el comportamiento dado en un tiempo determinado, de esta manera es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción. En este contexto es primordial la capacidad de correlación de evento, muchas veces disyuntos y aleatorios, que en equipos particulares, es poco frecuente.

Forensia digital

Aplica los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de esclarecer una acto delictivo a través del análisis de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática.

1.2 Objetivos de la Informática Forense

La informática forense en estos tiempos está cobrando fundamental importancia en el esclarecimiento de un presunto delito, a través de la recuperación de los registros y mensajes de datos existentes dentro de un equipo informático, de tal manera que toda esa información digital, pueda ser usada como prueba ante un tribunal.
Los objetivos que persigue sin importar el tipo de delito o incidente y que pueden ser alcanzados a través de la evidencia digital son los siguientes:

1. La compensación de los daños causados por los criminales o intrusos.

2. La persecución y procesamiento judicial de los criminales.

3. Creación y aplicación de medidas para prevenir casos similares.

4. Entregar las pruebas para permitir demostrar la inocencia del imputado.

5. Recoger y examinar huellas dactilares y ADN.

6. Recuperar documentos de un dispositivo dañado.

7. Hacer una copia exacta de una evidencia digital.

8. Generar una huella digital con un algoritmo hash MD5 o SHA1 de un texto para asegurar que este no se ha modificado.

9. Firmar digitalmente un documento para poder afirmar que es auténtico y preservar la cadena de evidencias.

10. Obtener resultados objetivos e imparciales.

1.3 Usos de la Informática Forense

Tal como lo mencionan los autores Zuccardi y Gutiérrez en el documento Informática Forense (Zuccardi, 2006), *"Existen varios usos de la informática forense, muchos de estos usos provienen de la vida diaria, y muchas veces no están directamente relacionados con la informática forense,*

1. Prosecución Criminal: *Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.*

2. Litigación Civil: *Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.*

3. Investigación de Seguros*: La evidencia encontrada en computadoras, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.*

4. Temas corporativos: *Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.*

5. Mantenimiento de la ley: *La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.*

1.4 Ciencia Forense

Las ciencias forenses tradicionales han crecido durante los últimos años. Sin embargo, el desarrollo vertiginoso de la tecnología informática y la proliferación de dispositivos electrónicos, que van desde teléfonos celulares hasta los grandes dispositivos computacionales, van acompañados de una avanzada tendencia en materia de delitos informáticos.

En la última década se han desencadenado avances sustanciales que permiten solucionar problemas cuya causa son los delitos e incidentes informáticos. Estos avances han dado lugar a la ***Ciencia Forense Digital***. La ciencia forense nos proporciona los principios y técnicas que facilitan la investigación del delito criminal, en otras palabras: cualquier principio o técnica que puede ser aplicada para identificar, recuperar, reconstruir o analizar la evidencia durante una investigación criminal forma parte de la ciencia forense, y puede definirse según lo establecido por el organismo conocido como Digital Forensic Research Workshop (DFRWS) creado en el 2001 en Nueva York, como:

"El uso de métodos probados y derivados científicamente dirigidos a la preservación, recolección, validación, identificación, análisis, interpretación, documentación y presentación de la evidencia digital que proviene de una fuente de información digital, con el propósito de facilitar o auxiliar la reconstrucción de eventos encontrados y considerados criminales, o ayudando a anticiparse a la ejecución de actividades planeadas no autorizadas y consideradas perjudiciales". (DFRWS. A Road Map for Digital Forensics Research. Digital Forensics Research Workshop, 2001)

Se considera un método científico porque supone la adquisición de nuevos conocimientos, mediante el estudio de la evidencia observable y medible, aplicando un razonamiento lógico, elaborando modelos e hipótesis y corrigiendo o mejorando estas últimas según se obtiene más evidencia.

Un actor importante dentro de esta ciencia es el ***perito forense*** quien aporta su entrenamiento para ayudar a los investigadores a reconstruir el crimen y encontrar pistas. Aplicando un método científico analiza las evidencias disponibles, crea hipótesis sobre lo ocurrido para crear la evidencia y realiza

pruebas, controles para confirmar o contradecir esas hipótesis. Esto puede llevar a una gran cantidad de posibilidades sobre lo que pudo ocurrir, esto es debido a que un perito forense no puede conocer el pasado, no puede saber qué ocurrió ya que sólo dispone de una información limitada. Por esto, sólo puede presentar posibilidades basadas en la información limitada que posee.

Dentro de la ciencia forense existe un gran número de principios básicos que son necesarios independientemente de si se está examinando un ordenador o un cadáver. Estos principios son:

- **Evitar la contaminación:** La esterilidad de los medios es una condición fundamental para el inicio de cualquier procedimiento forense en informática, pues al igual que en la medicina forense, un instrumental contaminado puede ser causa de una interpretación o análisis erróneo de las causas de la muerte del paciente.

- **Actuar metódicamente:** El investigador debe ser el custodio de su propio proceso, por tanto cada uno de los pasos realizados, las herramientas utilizadas (sus versiones, licencias y limitaciones), los resultados obtenidos del análisis de los datos, deben estar claramente documentados, de tal manera, que cualquier persona externa pueda validar y revisar los mismos. Ante una confrontación sobre la idoneidad del proceso, el tener documentado y validado cada uno de sus procesos ofrece una importante tranquilidad al investigador, pues siendo rigurosos en la aplicación del método científico es posible que un tercero reproduzca sus resultados utilizando la misma evidencia.

- **Controlar la cadena de evidencia**, es decir, conocer quien, cuando y donde ha manipulado la evidencia: Este punto es complemento del anterior. La custodia de todos los elementos allegados al caso y en poder del investigador, debe responder a una diligencia y formalidad especial es para documentar cada uno de los eventos que se han realizado con la evidencia en su poder. Quién la entregó, cuándo, en qué estado, cómo se ha transportado, quién ha tenido acceso a ella, cómo se ha efectuado su custodia, entre otras, son las preguntas que deben estar claramente resueltas para poder dar cuenta de la adecuada administración de las pruebas a su cargo.

1.5 Situación actual de la Informática Forense

Actualmente la informática forense o Análisis forense digital, necesita de una estandarización a nivel nacional de los procedimientos y acciones a tomar.
Las infracciones en su mayoría no se detectan ya sea por falta de conocimiento del damnificado o en caso contrario, se detectan pero ya es demasiado tarde o simplemente no se quiere investigar.

La mayoría de investigaciones están relacionadas con:

- Pornografía infantil.
- Derechos de autor.
- Envío de información, mails perdidos.
- Acciones dañinas llevadas a cabo por empleados, ex empleados o personas externas.
- Fraudes.
- Asesinatos, entre otros.

Solo en aquellos casos en que vale la pena la inversión se realiza una investigación forense, porque la investigación puede no llevar a nada concluyente, las conclusiones no llevan a la captura del delincuente o sencillamente este ya no se encuentra al alcance.

1.6 El Proceso Forense a nivel mundial.

Desde el año 2000, se han desarrollado diversos modelos, principios y metodologías de Análisis Forense Digital, como así también han surgido varias instituciones que han alcanzado un reconocimiento internacional en el campo de la computación forense, algunas de estas instituciones han emitido una serie de mejores prácticas que contemplan el correcto manejo de la investigación y de la evidencia digital.

A continuación se detallan los modelos, principios y guías más relevantes existentes a nivel mundial en forensia informática:

1.6.1 Modelos forenses

Los modelos forenses pueden ser tomados como referencia para llevar a cabo un proceso forense digital.

El propósito de los móldelos de investigación digital es informar, formar y estandarizar las investigaciones digitales, algunos de los modelos forenses son: *(Ray)*

1.6.1.1 El modelo DFRWS (Digital Forensic Research Workshop).

El sistema DFRWS fue desarrollado entre 2001 y 2003 en el Digital Forensic Research Workshop. El sistema introduce "Clases de Acción en la Investigación Digital", las cuales sirven para clasificar las actividades de una investigación en grupos. Este modelo no dicta que acciones en particular deben ser perseguidas, en cambio proporciona una lista de técnicas, algunas de las cuales son requeridas. Lo específico del sistema debe ser claramente redefinido para cada investigación particular.

El sistema está representado por una tabla, que incluye columnas para la clase de actividad y un renglón para la técnica a seguir. Estas técnicas pueden realizarse en persecución de las metas de la clase de acción asociada.

1.6.1.2 El modelo de Reith, Carr y Gunsch

El modelo presentado por Reith, Carr y Gunsch (Mark Reith, 2002) es muy similar al sistema DFRWS. Los pasos en su modelo son:

1. La identificación
2. La preparación
3. La estrategia de acercamiento
4. La preservación
5. La colección
6. El examen
7. El análisis
8. La presentación
9. Devolviendo la evidencia

El modelo también agrega soporte para la preparación de herramientas y la formulación dinámica de acercamientos de investigación. Este modelo soporta iteraciones libres de clases de actividad individuales. Se pretende que el modelo pueda ser utilizado como base otros métodos más detallados para cada tipo específico de investigación.

1.6.1.3 El modelo de Séamus Ó Ciardhuain.

En el año 2004, el IJCE (International Journal of Digital Evidence) publica un modelo extendido para investigaciones de ciberdelitos, cuyo autor fue Séamus Ó Ciardhuáin (Ciardhuáin, 2004).

Está basado en modelos previos, pero expone una arquitectura de cascada aumentada. Las clases de actividad del modelo están doblemente ligadas, de manera que la búsqueda de trabajo en una clase de actividad, puede causar una iteración de algunos o todos los trabajos en las clases de actividad anteriores. La inclusión de estructuras conocidas como flujo de información permite una comprensión más profunda de la fuente de evidencias y otros datos. Este flujo debe estar definido sobre una base organizacional, pero puede aplicarse a diferentes investigaciones dentro de la misma organización.

1.6.1.4 El modelo Beebe y Clark.

El modelo de Beebe y Clark (Clark, 24) proporciona la estructura para las actividades mediante fases que consisten de múltiples sub fases, que van más allá que el agrupamiento por actividades. Las sub fases están basadas en objetivos, más que estrictamente en actividades.

Las sub fases basadas en objetivos caen en una fase particular y consiste en una jerarquía de actividades particulares que están subordinadas al objetivo particular.

Además, el modelo Beebe y Clark, incluye los principios de la investigación digital sobre todas las fases y sub fases, lo cual afecta la forma en que éstas son llevadas a cabo. Las últimas metas para cada sub fase, están

representadas como objetivos, más que como tareas específicas. Los objetivos son metas que espera alcanzar con actividades de naturaleza similar relacionadas con un caso específico. Las tareas están directamente ligadas a un caso específico, tipo de crimen, plataforma, etc.

1.6.2 GUIAS DE BUENAS PRÁCTICAS

A continuación se detallan a grandes rasgos las guías de buenas prácticas para la recolección más importantes a nivel mundial. Los mismos pueden ser tomados como referencia para llevar a cabo un proceso forense digital.

1.6.2.1 RFC 3227 "Guía para recolectar y archivar evidencia"

El "RFC 3227: Guía Para Recolectar y Archivar Evidencia" (Guide lines for Evidence Collection and Archiving).Es una guía de alto nivel que establece pautas para la recolección de evidencia por su grado de volatilidad, decidir que recolectar, cómo realizar la recolección y determinar cómo almacenar y documentar los datos. Además explica algunos conceptos relacionados a la parte legal.

Tal como lo citan Zuccardi y Gutierrez, su estructura es:

a) Principios durante la recolección de evidencia: orden de volatilidad de los datos, cosas para evitar, consideraciones de privacidad y legales.

b) El proceso de recolección: transparencia y pasos de recolección.

c) El proceso de archivo: la cadena de custodia y donde y como archivar. (Zuccardi, 2006)

De esta guía además se pueden extraer las siguientes recomendaciones:

- Considerar y determinar los tiempos para la generación de la línea de tiempo.
- A la hora de recopilar las evidencias, minimizar los cambios que alteren el escenario y eliminar los agentes externos que pueden hacerlo.
- Si hay dudas entre recoger y analizar las evidencias, dar prioridad a la recolección.

- Por cada tipo dispositivo o sistema operativo pueden existir diferentes métodos para la recolección de datos.
- El orden de recolección de datos debe quedar establecido en función de la volatilidad de los mismos.
- La copia de la información debería realizarse a nivel binario para no alterar ninguno de los datos.

1.6.2.2 ISO/IEC 27037 Guía para la Identificación, recolección, adquisición y preservación de evidencia digital

ISO / IEC 27037: 2012 proporciona directrices para las actividades específicas en el manejo de la evidencia digital, que son la identificación, recolección, consolidación y preservación de potencial evidencia digital que puede ser de valor probatorio.

Proporciona orientación a las personas con respecto a las situaciones comunes que se encuentran en todo el proceso de manipulación de evidencia digital y ayuda a las organizaciones en sus procedimientos disciplinarios y para facilitar el intercambio de potencial evidencia digital entre jurisdicciones.

De acuerdo con la ISO/IEC 27037:2012 la evidencia digital es gobernada por tres principios fundamentales: la relevancia, la confiabilidad y la suficiencia. Estos tres elementos definen la formalidad de cualquier investigación basada en evidencia digital, bien ésta sea utilizada para que sea admisible en corte o no.

La relevancia es una condición técnicamente jurídica, es necesario conocer los detalles del caso para hacer foco sobre aquellos elementos que son pertinentes a la situación que se investiga y poder excluir todo aquello que no sea importante para la investigación.

La confiabilidad es otra característica fundamental, se busca que el proceso permita repetir los pasos las veces que sea necesario, esto es que la evidencia que se extrae u obtiene es lo que deber ser y que, si un tercero sigue el mismo proceso, deberá obtener resultados similares verificables y comprobables.

Finalmente otra característica importante es ***la suficiencia***, lo que permite que con las evidencias recolectadas y analizadas se tengan elementos suficientes

para sustentar los hallazgos y verificar las afirmaciones efectuadas sobre la situación investigada.

Por otra parte la norma hace énfasis en los siguientes puntos:

- Minimizar el manejo del dispositivo con la evidencia digital original o con la evidencia digital potencial
- Dar cuenta de cualquier cambio y documentar las acciones que se tomen (mientras el experto se hace una opinión sobre su confiabilidad)
- Cumplir con las leyes locales sobre el manejo de la evidencia
- No tomar acciones más allá de sus competencias. *(ISO, 2012)*

1.6.2.3Guía de la IOCE

La IOCE, publicó “Guía para las mejores prácticas en el examen forense de tecnología digital” (Guide lines for the best practices in the forensic examination of digital technology) (IOCE, 2002). El documento provee una serie de estándares, principios de calidad y aproximaciones para la detección prevención, recuperación, exanimación y uso de la evidencia digital para fines forenses. Cubre los sistemas, procedimientos, personal, equipo y requerimientos de comodidad que se necesitan para todo el proceso forense de evidencia digital, desde examinar la escena del crimen hasta la presentación en la corte.

Cuenta con una estructura general de cuatro fases principales:

1) **Recolección de la evidencia sin alterarla o dañarla.**

El principio básico de cualquier investigación forense es tratar de mantener intacta la escena del delito, con el fin de preservar la evidencia ante cualquier variación del entorno.

La recolección inicial de la evidencia debe hacerse de manera tal que no afecte los datos que se encuentran en el sistema original, este debe ser sin lugar a dudas el principio básico de toda investigación

Es común pensar que para recolectar la evidencia solo basta con desconectar el cable de alimentación eléctrica de la computadora, sin tener en cuenta que esto solo asegura los datos del disco duro, mientras que los datos de la

memoria RAM se pierden por completo, al igual que los procesos en ejecución y las conexiones de red, esto puede representar la pérdida de evidencia vital para la investigación del caso. Por lo que decidir si se deja corriendo el sistema, si se desconecta el cable de alimentación eléctrica o se apaga de forma normal es una de las decisiones más difíciles que debe tomar la persona encargada de realizar el secuestro de la evidencia electrónica. Cada caso es diferente y cada investigador debe tener la flexibilidad necesaria para poder adaptarse a cada caso y tomar la decisión más adecuada. Sea cualquiera la decisión que se tome, está debe documentarse detalladamente en cada una de sus acciones, ya que estos documentos pueden ayudar luego a explicar el tipo de delito que se cometió en ese momento.

Algo importante de tomar en cuenta es la realización de una cadena de custodia adecuada, esto con el fin de proteger la evidencia cuando las personas tengan acceso a ella. Este proceso consiste en documentar donde se encuentra almacenada la evidencia, que persona se encuentra o estuvo a cargo de la evidencia, porque motivo y en qué periodo de tiempo tuvo acceso. Con esto se disminuye la posibilidad de que alguien modifique la evidencia o plante evidencia que desvié el rumbo de la investigación

2) Autenticación de la evidencia recolectada

Los diferentes dispositivos de almacenamiento se deterioran muy lentamente, pero los datos que contienen los mencionados dispositivos pueden variar rápidamente y como consecuencia cambiará también su significado.

Por esto es que se hace difícil demostrar que la evidencia recolectada es la original, por lo que la cadena de custodia es uno de los métodos más importantes a utilizar para asegurar que ningún cambio accidental o deliberado ha sido introducido en la evidencia.

3) Análisis de los datos sin modificarlos.

El proceso de análisis tiene como objetivo encontrar todos los datos que tengan un valor probativo en la investigación, y lo más importante que aporten información para poder reconstruir el incidente. El análisis puede realizarse sobre cualquier sistema operativo siempre y cuando se cumpla la denominada regla de oro en el manejo de evidencia: en cualquier acción que se realice no se debe dañar la evidencia.

Las piezas de evidencia digital contienen información relativa a las acciones del imputado, dichas piezas se encuentran dispersas en todo el sistema y pueden ser de distinta índole, pueden ser archivos de configuración del sistema, archivos borrados del sistema de archivos pero aún presentes en la superficie del disco duro, bitácoras de ingresos y salidas del disco duro, archivos ocultos, historiales de comandos ejecutados, procesos que se encuentren en ejecución dentro de la memoria del sistema, archivos personales de usuarios en ubicaciones propias para los archivos del sistema o en ubicaciones restringidas.

Existe un gran volumen de información que debe ser analizada, por tanto se debe organizar la búsqueda de manera adecuada, siguiendo un orden y análisis. Primero recolectar y estudiar los datos contenidos en memoria, luego recuperar los archivos borrados, continuar con el estudio de los archivos de configuración, las bitácoras del sistema y los archivos de usuario.

Para realizar el análisis de los datos es necesario recurrir a diferente software, que dependiendo la ubicación de los datos a analizar existen una gran variedad de herramientas por lo que es necesario saber identificar que herramienta ofrece la mayor cantidad de beneficios.

Como en cada uno de los pasos del proceso, en esta fase también es importante mantener la cadena de custodia reportando cada acción realizada.

4) Reporte final.

Una vez finalizadas las fases anteriores el perito debe elaborar un reporte final, en el mismo se debe mencionar el software utilizado con el número de versión que se utilizó para el análisis y la recolección de la evidencia; así como los métodos que se usaron para dichas tareas y por qué se decidió proceder de una u otra forma. La decisión del investigador debe fundamentarse en sus conocimientos, habilidad, circunstancias del caso y lo más importante su papel de neutralidad dentro del caso.

El reporte final debe estar fundamentado con base en las notas que se hicieron a lo largo de todo el proceso investigativo, debe ser detallado de forma extensa pero siempre haciendo hincapié en lo que es relevante para la investigación. El documento debe especificar la ubicación lógica que ocupa cierta evidencia

relevante dentro del documento, en el caso de datos borrados y recuperados, se debe especificar donde se encontraba exactamente, incluyendo información como el cilindro, cabeza y sector del dispositivo físico.

La estructura de esta guía permite:

a) Garantizar la calidad.

b) Determinar los requisitos para el examen del caso.

c) Brindar principios generales que se aplican a la recuperación de la evidencia digital (recomendaciones generales, documentación y responsabilidad).

d) Ofrecer prácticas aplicables al examen de la evidencia de digital.

e) Orientar en localización y recuperación de la evidencia de digital en la escena, a través de precauciones, búsqueda en la escena, recolección de la evidencia y empaquetado, etiquetando y documentación.

f) Permitir la priorización de la evidencia.

g) Garantizar el examen de la evidencia: protocolos de análisis y expedientes de caso.

h) Garantizar la evaluación e interpretación de la evidencia

i) Permitir la presentación de resultados (informe escrito).

j) Permitir la revisión del archivo del caso: Revisión técnica y revisión administrativa.

k) Garantizar la presentación oral de la evidencia.

l) Procedimientos de seguridad y quejas.

1.6.2.4 Guía para la "Investigación en la Escena del Crimen Electrónico".

El Departamento de Justicia de los Estados Unidos de América, publicó una guía para la "Investigación En La Escena Del Crimen Electrónico" (Electronic Crime Scene Investigation: A Guide for First Responders) (Justice, 2008). Esta

guía fue creada para que sea utilizada por las fuerzas policiales y las personas encargadas de proteger la escena del delito; se enfoca sobre todo a la identificación y recolección y preservación de evidencia en la escena del delito. Dicha guía refleja las situaciones más comunes encontradas en el proceso forense. Aborda los siguientes puntos:

a) Investigación de la escena del delito, identificar dispositivos electrónicos (tipos de dispositivos que pueden encontrar y cuál puede ser la posible evidencia).

b) Herramientas para investigar y equipo.

c) Asegurar y evaluar la escena.

d) Documentar la escena.

e) Recolección de evidencia.

f) Empaque, transporte y almacenamiento de la evidencia.

g) Examen forense y clasificación de delitos.

h) Anexos (glosario, listas de recursos legales, listas de recursos técnicos y listas de recursos de entrenamiento).

1.6.2.5 Guía para el "Examen Forense de Evidencia Digital"

Otra guía del Departamento de Justicia de los Estados Unidos, es "Examen Forense de Evidencia Digital" (ForensicExamination of Digital Evidence: A Guide for Law Enforcement) (Justice, U.S. Department of Justice Office of Justice Programs National Institute of Justice, 2004). Esta guía está pensada para ser usada por fiscalías y organismos encargados de hacer cumplir la ley. Esta guía aborda un proceso completo de investigación que va desde la escena del delito hasta la presentación ante la justicia.

Su estructura está comprende:

1- Desarrollo de políticas y procedimientos con el fin de darle un buen trato a la evidencia.
2- Determinación del curso de la evidencia a partir del alcance del caso.
3- Adquisición la evidencia.
4- Exanimación la evidencia.
5- Documentación y reportes.

6- Anexos (casos de estudio, glosario, formatos, listas de recursos técnicos y listas de recursos de entrenamiento).

1.6.2.6 Guía de buenas prácticas para Evidencia basada en Computadores (Guía Reino Unido)

La ACPO, Association of ChiefPoliceOfficers (Asociación de Jefes de Policía), del Reino Unido, mediante su departamento de crimen por computadora, publicó "Guía de Buenas Prácticas para Evidencia basada en Computadoras" (Association of Chief Police Officers, 2003). La policía del Reino Unido creó este documento para el personal policial que asiste a la escena del delito y que tiene un primer contacto con la evidencia, hace hincapié en la recolección de evidencia no así en el examen de dicha evidencia.

Las directrices de esta guía se refieren a:

- Personal que asisten a la escena del crimen
- Investigadores
- Personal de la recuperación Evidencia
- Testigos externos

Se basa en cuatro principios:

- Ninguna acción realizada por los peritos deben cambiar los datos contenidos en un dispositivo.
- En el caso de ser necesario el acceso a la información original, todos los pasos deben ser correctamente documentados.
- El proceso utilizado para la extracción de evidencia debe permitir a terceros poder realizar los mismos pasos y llegar siempre al mismo resultado.
- La persona encargada de la investigación debe garantizar la legalidad de las actividades.

1.6.2.7 Guía para el Manejo de Evidencia en IT (Guía Australia)

Estándares de Australia (Standards Australia) publico en agosto de 2003 “Guía Para El Manejo De Evidencia En IT” (Standards Australia handbook: HB-171: Guidelines for the Management of IT Evidence) (Ghosh, 2004). Es una guía creada con el fin de asistir a las organizaciones para combatir el crimen electrónico. Establece puntos de referencia para la preservación y recolección de la evidencia digital, presenta una metodología de ciclo de vida para la administración de la evidencia.

El ciclo de vida propuesto consta de seis fases:

1- **Diseño de la evidencia:** Hay cinco objetivos en el diseño de un sistema informático para maximizar la valides de la evidencia como prueba:
   a) Asegurar que los registros electrónicos identificados están disponibles y son utilizables
   b) Identificar el autor de los documentos electrónicos ;
   c) Establecer la hora y la fecha de creación o alteración de los datos.
   d) Determinar la autenticidad de los documentos electrónicos.
   e) Identificar la fiabilidad de los programas de la computadora.

2- **Producción de la evidencia.** El objetivo en esta etapa es ser capaz de establecer que:
   a) Un software en particular produce un registro electrónico ;
   b) El autor de los registros informáticos almacenados es una persona.
   c) El tiempo de la creación.
   d) Un software que está siendo utilizado está funcionando correctamente en el momento de la creación o modificación de un archivo.

3- **Recolección de la evidencia:** El objetivo de esta etapa del ciclo de vida es localizar toda la información pertinente y conservar los registros electrónicos originales para que la evidencia original no sea alterada.

4- **Análisis de la evidencia.** El objetivo de esta etapa del ciclo de vida es:
   a) Reunir el material probatorio;

b) Deducir la evidencia relacionada con la causa.

c) Determinar qué otras pruebas que se carece.

5- **Reporte y presentación.** El objetivo de esta etapa del ciclo de vida es presentar un reporte garantizando la validez de la evidencia y las pruebas realizadas.

6- **Determinación de la relevancia de la evidencia:** en esta etapa del ciclo de vida se realiza la evaluación de la evidencia por parte de un juez o un miembro del tribunal de justicia.

1.6.3 METODOLOGÍAS

1.6.3.1 METODOLOGÍA FORENSE DEL DEPARTAMENTO DE JUSTICIA DE LOS ESTADOS UNIDOS.

El Departamento de Justicia de los Estados Unidos, establecido el 22 de junio de 1870 e inaugurado el 1º de julio del mismo año, es un ministerio, que forma parte del Gobierno de los Estados Unidos, diseñado para hacer cumplir las leyes, defender los intereses del país de acuerdo con la ley y para asegurar una administración de justicia imparcial y justa para todos los estadounidenses.

El Laboratorio de Cibercrimen en la Sección de Propiedad Intelectual y Crimen Computacional (Computer Crime and Intellectually Property Section) desarrolló un diagrama de flujo en el cual se describe la Metodología de Análisis Forense Digital (METHODOLOGY, 2007), dicho trabajo se realizó después de consultar con numerosos analistas forenses de varias agencias federales. Los elementos claves del Proceso Forense se listan a continuación:

- El empleo de métodos científicos.
- Recolección y Preservación.
- Validación.

- Identificación.
- Análisis e Interpretación.
- Documentación y Presentación.

Plantea cuatro etapas del proceso forense, se explican partiendo de que los analistas ya han obtenido previamente la imagen de los datos, así como los recursos necesarios para el análisis, y hasta antes de que se elabore el reporte y el análisis del nivel del caso.

Etapa 1: Preparación/Extracción.

Los analistas comienzan preguntándose si hay suficiente información para proceder. Se aseguran de que la petición es clara y de que cuentan con los datos suficientes para poder responder a dicha petición. Si algo hace falta, establecen coordinación con quien realizó la petición, de otra manera dan inicio al proceso.

La primera etapa en cualquier proceso forense es la validación del hardware y software a emplear, para asegurarse de que éste funcione de forma adecuada.

Cuando la plataforma de los analistas está lista, realizan un duplicado de los datos forenses proporcionados en la petición y verifican su integridad. Este proceso asume que las autoridades ya han obtenido los datos a través de un proceso legal y realizado la imagen forense de dichos datos. También se asume que el analista ha recibido una copia de trabajo de los datos asegurados, en caso de que el analista cuente con la evidencia original, debe realizar una o varias copias de trabajo y guardar la cadena de custodia de la evidencia original.

El analista se asegura de que la copia en su posesión está intacta y sin alteraciones, lo cual normalmente se lleva a cabo verificando el hash o huella digital de la evidencia, si se encuentra algún problema, el analista consulta con el solicitante acerca de cómo proceder.

Después de que los analistas han verificado la integridad de los datos, se desarrolla un plan para la extracción de los datos, se organiza y detalla la petición forense en preguntas que ellos comprendan y puedan responder. Seleccionan las herramientas que permiten responder a

estas preguntas. Generalmente, los analistas cuentan con ideas preliminares acerca de que es lo que se debe buscar, basándose en la petición o requerimiento, lo cual agregan a una "Lista de Búsqueda Principal", que recopila los elementos solicitados. Los analistas manejan esta lista para ayudar a enfocarse en el examen forense. Para cada búsqueda los analistas extraen los datos relevantes y marcan esa búsqueda como "procesada" y anexan cualquier dato extraído a otra lista llamada "Lista de Datos Extraídos". Los analistas llevan el seguimiento de todas las búsquedas, agregando los resultados a esta segunda lista y continúan con la siguiente etapa de la metodología, la Identificación.

Etapa 2: Identificación.

Los analistas repiten el proceso de identificación para cada elemento de la "Lista de Datos Extraídos". Primero se determina qué tipo de elemento es. Si el elemento no es relevante para la investigación, simplemente se marca como "procesado" y se mueve. Tal como en una búsqueda física, si el investigador se encuentra con un elemento incriminatorio, pero que está fuera del alcance de la orden de registro, se recomienda que detenga toda actividad inmediatamente y notifique el descubrimiento a las personas apropiadas, incluyendo al solicitante y espere nuevas instrucciones. Si un elemento es relevante para la investigación, el analista lo debe documentar en una tercera lista, la "Lista de Datos Relevantes", la cual es una colección de datos que dan respuesta al requerimiento original.

Un elemento puede apuntar a una nueva fuente de datos. Por ejemplo, es posible encontrar que el sospechoso estaba empleando otra cuenta de correo electrónico y las autoridades pueden desear citar el contenido de esta nueva cuenta. Se puede encontrar también que el sospechoso almacenaba información en un medio removible (USB) - alguno no encontrado en la búsqueda inicial. Bajo estas circunstancias, las autoridades considerarán obtener una nueva orden de registro para buscar el dispositivo USB. Un análisis forense puede apuntar a muchos tipos diferentes de evidencia, tales como log de firewall, registros de acceso a edificios, videos de seguridad, lo cual se documenta en una cuarta lista, la "Lista de Nuevas Fuentes de Datos".

Tras haber procesado la Lista de Datos Extraídos, los investigadores regresan a las nuevas pistas encontradas. Para cualquier nueva búsqueda de datos, se considera volver a la etapa de Extracción para procesarlos. De la misma manera, para cualquier nueva fuente de datos que conduzca a nueva evidencia, se considera regresar a la etapa de obtención y realización de imágenes de los nuevos datos para la investigación forense.

En este punto del proceso, es aconsejable que el investigador informe al solicitante de sus conclusiones iniciales. Dependiendo de la etapa en la que se encuentre un caso, los datos obtenidos hasta ese momento pueden otorgar al solicitante la información suficiente para continuar con el caso y que los investigadores no tengan que seguir trabajando en la búsqueda de información. Si los datos obtenidos hasta esta etapa no son suficientes se procede a la siguiente etapa, el análisis.

Etapa 3: Análisis.

En la etapa de análisis, los investigadores relacionan todos los datos encontrados y bosquejan una imagen completa del caso al solicitante. Para cada elemento de la "Lista de Datos Relevantes", los investigadores responden a las preguntas ¿Quién?, ¿Qué?, ¿Cuándo?, ¿Dónde? Y ¿Cómo? Tratan de explicar que usuarios o aplicaciones crearon, editaron, recibieron o enviaron cada elemento y la forma en que existía originalmente; explican también lo que han encontrado, pero principalmente explican y justifican el porqué toda esa información analizada es importante y qué relación tiene con el caso. A menudo, es posible que los investigadores generen un análisis de mucho más valor, observando el momento en que ocurrieron las cosas, produciendo una línea de tiempo que haga más coherente las conclusiones obtenidas. Para cada elemento relevante, se trata de explicar cuando fue creado, accedido, modificado, recibido, enviado, visto, borrado y ejecutado. Se observa y se obtiene una secuencia de los eventos y se anota cuales eventos ocurrieron al mismo tiempo.

Los investigadores documentan todo su análisis y otra información relevante a la petición hecha, agregando todo lo anterior a una quinta lista, la "Lista de Resultados del Análisis", la cual es una lista de todos los datos

significativos que responden al ¿Quién, cuando, como, donde, qué? entre otras preguntas. Finalmente, después de que los investigadores han repetido este proceso varias veces, es posible que puedan responder satisfactoriamente las necesidades del solicitante del análisis forense y es hasta ese entonces, que proceden con la siguiente etapa, la etapa de Reporte de Resultados.

Etapa 4: Reporte de Resultados.

Esta es la etapa en la que los investigadores documentan y detallan todos sus hallazgos, de tal manera que el solicitante pueda entenderlos y emplearlos en su proceso judicial. El reporte final es la mejor manera que tienen los investigadores de comunicar los resultados del análisis forense a los interesados.

1.6.3.2 METODOLOGÍA FORENSE DEL INSTITUTO NACIONAL DE ESTÁNDARES DE TECNOLOGÍA (NIST).

El Instituto Nacional de Estándares de Tecnología (NIST) es una agencia federal no regulatoria dentro del Departamento de Comercio de los E.U. y que tiene como misión promover la innovación y competitividad industrial mediante la medición avanzada de la ciencia, estándares y tecnología, de forma que se mejore la seguridad económica y la calidad de vida.

Esta metodología (Karen Kent, 2006) se enfoca en el análisis forense de evidencia digital, cuya meta principal es obtener una mejor comprensión del caso a investigar, encontrando y analizando los hechos relacionados al mismo.

El análisis forense es necesario en diferentes situaciones, tales como la recopilación de evidencia para los procedimientos judiciales y medidas disciplinarias internas, el manejo de incidentes relacionados con código malicioso y problemas operativos. Independientemente de las necesidades, el proceso de análisis forense debe realizarse en cuatro etapas.

a) Recolección
b) Revisión
c) Análisis
d) Reporte.

Los detalles precisos de estas etapas, pueden variar de acuerdo al requerimiento del análisis forense, las políticas organizacionales, directivas, procedimientos.

El proceso forense transforma los medios en evidencia, donde la evidencia es necesaria para las autoridades o para uso interno de las organizaciones. La primera transformación ocurre cuando se examinan los datos recolectados y se convierten a un formato que sea compatible con las herramientas forenses. Segundo, los datos se transforman en información a través del análisis. Finalmente la transformación de la información en evidencia se da en forma análoga a la acción de transferir el conocimiento - usando la información producida por el análisis en una o más formas durante la etapa de reporte.

Etapa 1: Recolección de Datos.

El primer paso en el proceso forense es identificar las fuentes potenciales de datos y la adquisición de éstos.

a. Identificar las posibles fuentes de datos. El uso cada vez más generalizado de la tecnología digital tanto para fines profesionales como personales, da lugar a una abundante fuente de datos. Las fuentes de datos más comunes y evidentes son las computadoras de escritorio, servidores, dispositivos de almacenamiento en red, y laptops. Estos sistemas típicamente cuentan con unidades internas que aceptan medios digitales, como CD y DVD, también cuentan con varios tipos de puertos (USB, Firewire, PCMCIA) para conectar dispositivos de almacenamiento externo. Algunos ejemplos de dispositivos de almacenamiento externo que pueden ser fuentes de datos son las unidades extraíbles y tarjetas de memoria. Los sistemas de cómputo estándar también contienen datos volátiles que están disponibles temporalmente (antes de que el sistema de apague o reinicie). Además de estos dispositivos, muchos dispositivos digitales portátiles pueden contener datos (PDA's, celulares, cámaras digitales, videocámaras digitales, reproductores de audio). Los analistas deben ser capaces de localizar estos dispositivos durante la inspección en la escena del crimen y emplearlos como fuentes de datos.

Los analistas deben tener en mente las fuentes de datos localizadas en otros lugares, por ejemplo, actividades en la red y el uso de aplicaciones. La información también puede ser almacenada por otras organizaciones, por ejemplos los registros del proveedor del servicio de internet (ISP). Durante la recolección de datos, el analista debe tomar en cuenta al propietario de la fuente de datos. Por ejemplo, el obtener una copia de los registros del ISP requiere de una orden judicial.

Los analistas deben considerar además, las políticas de la organización y los aspectos legales, en relación a las propiedades externas a la organización, por ejemplo, la laptop de un empleado o de un contratista. La situación puede ser más complicada aún si se consideran controles fuera de la organización. A veces, simplemente no es posible obtener datos de una fuente primaria, por lo que se debe tomar en cuenta fuentes de datos alternas, que pueden contener algunos o la totalidad de los mismos datos y usar esas fuentes en lugar de la original.

Las organizaciones por su parte, pueden tomar medidas proactivas para recopilar datos que puedan emplearse en un proceso forense, por ejemplo, configurar como parte del funcionamiento normal, el que los sistemas operativos auditen y registren ciertos tipos de eventos, como intentos de autenticación y cambios a las políticas de seguridad. Los registros de auditoría proporcionan información valiosa, incluyendo la hora en que se suscitó el evento y el origen de éste. Otra acción útil es implementar el registro centralizado, lo que implica que ciertos sistemas y aplicaciones envíen copia de sus registros a un servidor central.

El registro centralizado evita que los usuarios manipulen la información y empleen técnicas anti-forenses para impedir su análisis. El realizar copias de seguridad con regularidad, permite a los analistas ver el estado del sistema en un momento predeterminado. Además, los controles de monitoreo de seguridad, como Sistemas Detector de Intrusos (IDS), Antivirus,

Utilidades de Detección y Eliminación de Programas Espías, pueden generar registros de cuando y como se llevó a cabo un ataque o intrusión.

Otra medida proactiva de recolección de datos es monitorear la actividad del usuario, por ejemplo que teclas presiona, cuales registros de un sistema en particular usa el teclado. Aunque esta medida proporciona un registro valioso de la actividad del usuario en el equipo de cómputo, también puede significar una violación a su intimidad, a menos que se le comunique por medio de las políticas de la organización que estas medidas pueden ser tomadas.

a- **Adquisición de los Datos.** Después de que se han identificado las fuentes de datos, el analista debe proceder ahora con la obtención de los datos de esas fuentes. La adquisición debe realizarse llevando a cabo el proceso de tres pasos: Desarrollar un plan de obtención de datos, Obtener los datos y Verificar su integridad. Desarrollar un plan de adquisición de datos.

   Debido a la gran diversidad de fuentes de datos que se pueden localizar en una escena de crimen, es necesario que el analista elabore un plan en el cual se prioricen las fuentes, estableciendo el orden en el que van a obtenerse los datos.

b- **Obtención de datos.** El proceso general para la obtención de datos, involucra el empleo de herramientas forenses para la recolección de datos volátiles, el duplicado de fuentes de datos no volátiles para obtener sus datos y el aseguramiento de las fuentes originales. El proceso de obtención de datos es posible realizarlo tanto de manera local, como en red.

c- **Verificar la integridad de los datos.** Una vez que se han obtenido los datos, se debe verificar su integridad. Es particularmente importante para un analista, probar que los datos no han sido alterados, lo cual es necesario por razones legales.

   Antes de que el analista inicie la recolección de los datos, él o el administrador, de acuerdo con las políticas de la organización y a las disposiciones legales, deben decidir sobre la necesidad de recolectar y preservar la evidencia, de manera que ésta se pueda emplear posteriormente en situaciones legales o en un procedimiento interno.

   En tales situaciones, se debe llevar de manera estricta un registro preciso, proceso conocido como cadena de custodia, el cual permitirá

evitar acusaciones respecto a un mal manejo o manipulación de la evidencia.

Etapa 2: Revisión.

Después de haber recolectado los datos, la siguiente fase consiste en examinar los datos, lo cual implica la evaluación y extracción de las partes de información relevantes de los datos recolectados. Esta fase también puede involucrar evitar o mitigar las características de Sistemas Operativos o aplicaciones que oculten datos y código (compresión de datos, cifrado y mecanismos de control de acceso).

El disco duro obtenido puede contener cientos o miles de archivos, la identificación de los archivos que contienen información de interés puede ser una tarea desalentadora. Esta lista de archivos debe depurarse ya que por ejemplo un firewall puede tener millones de registros, pero solo cinco de ellos están relacionados con el incidente.

Sin embargo, es posible utilizar diversas herramientas para reducir la cantidad de archivos de datos que deben ser analizados. Se pueden emplear búsqueda de documentos por un patrón en particular, un texto en el archivo, información relacionada con alguna persona o una dirección de correo electrónico. Otra técnica, es emplear herramientas que pueden determinar el tipo de contenido de los archivos (texto, música, gráficos, archivos comprimidos), lo cual sirve para identificar archivos que merezcan un estudio más detallado, así como para excluir aquellos que no sean relevantes al caso en investigación.

Etapa 3: Análisis.

Una vez que ha sido extraída la información más relevante, el analista debe estudiarla y analizarla para generar las conclusiones del caso. La fundación de análisis forense emplea un enfoque metódico para obtener resultados con los datos disponibles o determinar que aún no es posible concebir una conclusión adecuada.

El análisis debe incluir la identificación de personas, lugares, objetos, eventos y la forma en que estos se relacionan, de modo que permita formar una conclusión preliminar.

Si la evidencia es necesaria en un juzgado, el analista debe documentar detalladamente todos los hallazgos y cada una de las actividades realizadas.

Etapa 4: Elaboración de Informes.

La etapa final es la elaboración del informe de resultados del análisis forense, en la cual se prepara y se presenta la información resultante de la etapa de análisis. Existen algunos factores que influyen en la elaboración del informe, entre ellos:

a. Explicaciones alternas. Cuando la información relacionada con un evento no está completa, puede que no sea posible llegar a una explicación definitiva sobre lo ocurrido. Cuando un evento resulte con más de una explicación, cada una de ellas deben presentarse en el reporte. El analista debe emplear un enfoque metódico para probar o refutar cada explicación propuesta.

b. Considerar a la audiencia. Es importante conocer a quien se le presentará el informe. Un reporte para las autoridades judiciales, requiere un informe muy detallado de toda la información recopilada y es posible que se exija una copia de todas las evidencias obtenidas. Un administrador puede requerir ver todo el tráfico de la red y estadísticas con gran detalle. El personal directivo puede querer simplemente un panorama general de lo sucedido, tal como una representación visual de cómo se produjo el ataque y que medidas deberían tomarse para prevenir situaciones similares.

c. Información procesable. El reporte también incluye la identificación de información procesable que puede permitir al analista recolectar nuevas fuentes de datos.

Como parte del proceso de elaboración de reportes, el analista debe identificar problemas que deban ser solucionados, tales como deficiencias en las políticas o errores en los procedimientos. Muchos equipos de respuesta a

incidentes y análisis forense se reúnen a discutir los resultados obtenidos, en la que se incluye un examen a conciencia de las posibles mejoras a las directivas y procedimientos y por lo general, se aprueban algunos cambios menores.

Una vez que se han aplicado los cambios propuestos, se informa a todos los miembros del equipo y recordar con frecuencia de los procedimientos a seguir. Los equipos suelen tener mecanismos de control de cambios e identificación de versiones de cada proceso y procedimiento. Además de esto, se puede contar con posters montados en puertas y paredes con los pasos a seguir. (Kent, 2006.)

1.6.3.3 METODOLOGIA DE LA RED EUROPEA DE INSTITUTOS FORENSES. (ENFSI).

La Red Europea de Institutos de Ciencias Forenses (ENFSI, European Network of Forensic Science Institutes) (Institutes, 2009) generó una serie de estándares que cubren todo el proceso forense, desde la primera acción que el perito realiza en la escena del delito, pasando por la inspección de la escena, el análisis en un laboratorio, hasta la interpretación y presentación del informe de resultados para mostrar ante una corte, no son prescriptivos y reconocen que existe más de una forma para llevar a cabo una tarea. Describen lo que un profesional forense debe realizar, pero no como hacerlo. Genéricamente pueden ser aplicados a todas las disciplinas forenses.

Consta de nueve actividades y cada una de ellas se desglosa en uno o varios estándares o normas:

Actividades Iniciales en la Escena.

En esta etapa, se busca congelar la escena del delito para que se mantenga intacto para cuando arriben los peritos encargados de la investigación.

Estándar o norma que contempla:

a. Preservación inicial y acciones de control en la escena.

- Verificar que en realidad se haya cometido un delito.
- Restringir el acceso a la escena.
- Realizar un análisis de riesgos de la escena.
- Recolectar la evidencia.
- Mantener la escena asegurada.
- Contar con la autorización correspondiente para llevar a cabo la búsqueda de evidencia en la escena.

Desarrollar Estrategia de Investigación.

Se debe tener en claro cuáles son los requisitos de la investigación y de los investigadores, además de realizar una evaluación de la escena y determinar las medidas necesarias para cumplir con dichos requisitos.

a. Determinar los requisitos de la investigación.

- Comprobar las anotaciones proporcionadas por el investigador acerca del incidente y de la escena, además de otras fuentes y asegurarse de que estén debidamente documentadas.
- Determinar el tipo de análisis que se llevará a cabo, de acuerdo a la información proporcionada.
- Considerar la posibilidad de que existan otros escenarios vinculados de forma que se asegure la línea de investigación.
- Determinar la logística de la investigación y resolver los problemas conocidos, haciendo énfasis en la eficacia, eficiencia y economía.
- Considerar la seguridad de todo el personal y verificar que todas las precauciones se lleven a cabo.
- Identificar los recursos y equipo necesario para la investigación y hacer los arreglos necesarios para llevarlos a la escena.

b. Evaluar la escena y determinar los requisitos.

- Llevar un registro de todas las personas que estuvieron en la escena antes de que fuera restringida.
- Revisar los hallazgos iniciales en la escena, identificar y consultar otras fuentes de información.

• Identificar los recursos y equipo necesario para la investigación y hacer los arreglos necesarios para llevarlos a la escena.

• Registrar los datos relevantes, relacionados con la investigación, al momento del análisis.

Investigación en la escena.

Esta actividad está directamente relacionada con la revisión de la escena, así como con la ubicación, identificación y recuperación de la posible evidencia, la cual será analizada con mayor detenimiento.

a. Establecer y preservar el control de la escena.

• Establecer y comunicar las responsabilidades de la búsqueda en la escena.

• Confirmar si es necesario modificar los límites de la escena del crimen.

• Mantener el área debidamente acordonada.

• Restringir la entrada y salida de personal al área protegida.

• Mantener control de la escena para que la evidencia no sufra daño, contaminación o pérdida.

b. Preparativos para inspeccionar la escena.

• Documentar y registrar la integridad de la escena antes de que sufra cualquier alteración.

• Establecer comunicación con el personal pertinente, a fin de gestionar la investigación científica.

• Evaluar, determinar y acordar el tipo y secuencia de análisis que serán necesarios.

• Asesorar a otros miembros respecto a los requisitos para recolección de evidencia y que se registren todas sus observaciones al momento del análisis.

• Preparar el equipo necesario verificando que éste funcione correctamente.

c. Inspeccionar la escena.

• Asegurarse de que la inspección se lleve a cabo de conformidad con los requisitos legales y de la organización.

• Realizar la inspección en un orden lógico, de modo que se garantice la detección y recuperación óptima de todo tipo de evidencia.
• Seleccionar y usar métodos óptimos de recuperación de evidencia.
• Registrar toda la información relevante al momento de la inspección.

d. *Recolección de evidencia.*

• Priorizar y recolectar, de manera secuencial la evidencia con apoyo de otro personal especializado.
• Preservar la evidencia recolectada, sin daños, degradados o contaminados.
• Establecer y mantener la seguridad del material recolectado.
• Documentar todas las actividades realizadas.

e. Empacar los elementos y muestras.

• Empacar y manipular la evidencia de modo tal que se preserve su integridad y se evite la contaminación.
• Identificar claramente cada empaque.
• Sellar, etiquetar y registrar la evidencia de acuerdo a los lineamientos legales y de la organización.
• Mantener la continuidad e integridad de la evidencia.

Interpretar los hallazgos y ordenar nuevo análisis.

Esta actividad se refiere a la interpretación de los hallazgos iniciales encontrados en la escena de forma que sea posible determinar la secuencia de eventos acontecidos.

a. *Analizar la probable secuencia de eventos.*

• Basar el análisis sobre los hallazgos encontrados y la información proporcionada acerca de la escena.
• Consultar fuentes de información que puedan ayudar a la reconstrucción de los hechos.
• Considerar más de una explicación de lo que pudo haber ocurrido.
• Documentar toda la información.
• Decidir cuales elementos serán analizados a fondo.

- Registrar y revisar todos los elementos de evidencia obtenidos.
- Estimar los elementos que puedan proporcionar más información en un análisis más detallado.

- En caso de ser necesario solicitar asesoría de otros especialistas en otros campos.
- Solicitar de ser necesario los análisis adicionales que pudieran ayudar a obtener más información.

c. Transferir los elementos a los lugares designados.

- Seleccionar un método de transporte legal, seguro y sin riesgo de contaminación, destrucción o pérdida.
- Segregar en caso de que sea necesario los diferentes elementos cuidando mantener su integridad.
- Mantener la continuidad e integridad de la evidencia durante su transporte.
- Descontaminar los contenedores y los vehículos para transporte en caso de ser necesario haciéndolo de una manera segura o en su caso llegar hasta la destrucción.
- Documentar todas las actividades.

d. *Almacenar los elementos y muestras de evidencia.*

- Manipular la evidencia de tal manera que ésta sea preservada, manteniendo su continuidad, evitando la contaminación y que se ajuste a los requisitos de salud y seguridad.

- Conservar la evidencia en las mejores condiciones y que encaso de que se elimine algún elemento, esto se haga de manera segura.

- De ser necesario, descontaminar el área de almacenamiento, de acuerdo a los requerimientos de salud y seguridad.

Desarrollar estrategia de análisis en laboratorio.

Actividad que se refiere a la elaboración de una estrategia para análisis forense, que responda a las necesidades del caso en investigación, dicha estrategia debe tomar en cuenta los principios y prácticas científicas.

a. Establecer los requerimientos del caso en investigación.

• Confirmar que los elementos presentados son apropiados para la labor que se llevará a cabo.

• Determinar los requerimientos de almacenamiento para la evidencia y hacer los arreglos para que dichas instalaciones estén limpias y seguras.
• Registrar la información relevante de manera completa, precisa, y legible.
• Preparar el equipo y área en que se llevará a cabo el análisis.
• Identificar, documentar y corregir el equipo que no sea adecuado.

b. Determinar la estrategia de análisis.

• Confrontar los detalles del caso contra las necesidades de la investigación.
• Determinar una estrategia de análisis tomando en cuenta las necesidades del caso.
• Revisar y hacer ajustes a la estrategia en acuerdo con el personal apropiado.

Preparación para análisis en laboratorio.

Esta actividad busca garantizar que se lleven a cabo los preparativos adecuados antes de que se realice el análisis de los elementos de evidencia encontrados, esta preparación se realiza en todos los casos, independientemente del medio ambiente que se trate.

La preservación, integridad y continuidad de la evidencia son críticas y deben mantenerse en todo momento.

a. Determinar la integridad de los elementos y muestras.

• Transportar la evidencia de manera segura a las instalaciones donde serán almacenadas.
• Confrontar los elementos contra los registros para identificar cualquier diferencia y hacer las correcciones que se consideren necesarias.
• Registrar los detalles de almacenamiento, manipulación, traslado y embalaje de los elementos para garantizar su continuidad.
• Identificar y documentar cualquier problema de empaquetado y tomar las medidas apropiadas.

• Almacenar y transportar el material de evidencia de una manera tal que se evite la contaminación.

• Almacenar y mover el material de evidencia dentro del laboratorio de manera que se evite la contaminación, daño o pérdida.

b. Inspeccionar el material de evidencia que se presentaron para su análisis.

• Remover la evidencia de su paquete y manipularlo de forma segura para evitar que sufra cualquier tipo de daño o alteración.
• Confirmar la identidad del material de evidencia conforme a la documentación presentada.
• Identificar la posible evidencia y seleccionar el método de análisis más adecuado.
• Tomar las medidas adecuada en caso de identificar un problema o posibilidad de éste.
• Decidir la estrategia de muestreo a seguir para los elementos que se analizarán.
• Mantener la continuidad del material de evidencia en todo momento.
• Registrar la información que vaya resultando de manera, clara y precisa.

Analizar evidencia.

En esta actividad se trata de localizar, identificar y recuperar la evidencia de todo el material recolectado. Esta función suele ser llevada a cabo, ya sea en la misma escena del incidente, en un laboratorio u otro lugar adecuado.

a. Vigilar y mantener la integridad del material.

• Manipular el material de forma que se evite la contaminación, daño parcial o total del mismo.
• Etiquetar el material y mantener en todo momento su integridad y continuidad.
• Registrar la información de las actividades realizadas, de manera, clara y precisa, en todo momento.

b. Identificar y recuperar la evidencia potencial.

• Realizar los análisis en un orden en el que se garantice la óptima detección y recuperación de evidencia.

- Localizar y recuperar evidencia física potencial y huellas.
- Identificar nuevas áreas de especialización.

- Mantener durante todo el proceso, la integridad y continuidad del material recuperado.
- Seleccionar y utilizar métodos que optimicen la recuperación.
- Registrar en todo momento, toda la información que se genere, de forma clara y precisa.

c. Determinar los análisis que se realizarán en el caso.

- Seleccionar los análisis que se llevarán a cabo de acuerdo al contexto del caso.
- Planear y calendarizar los análisis, de manera que sean confiables y brinden resultados fiables.
- Solicitar la asesoría de expertos, en caso de que se requiera otro tipo de información especializada.
- Registrar en todo momento la información generada de la planeación, en forma clara y precisa.

d. Llevar a cabo el análisis.

- Llevar a cabo los análisis al material con las medidas de seguridad adecuadas.
- Adaptar los procedimientos y prácticas de trabajo, a las diferentes situaciones y condiciones y documentar dichas adaptaciones.
- Identificar resultados insuficientes y tomar las acciones correctivas que procedan.
- En caso de que se requiera información más especializada, solicitar asesoría de expertos.
- Asegurarse que los resultados sean registrados de forma clara y precisa durante todo el proceso de análisis.

e. Producción de notas y registros de laboratorio.

- Generar notas y registros de laboratorio en el momento del análisis, claros, precisos y sin ambigüedades.

• Ordenar las notas y registrar la información de forma que sirva como apoyo al control por parte de terceros.
• Únicamente designar registros y archivos que ayuden a la fácil recuperación.
• Ordenar y combinar todas las anotaciones generadas durante el proceso de análisis acerca del caso.

Interpretar hallazgos.

Esta actividad se refiere a resumir y evaluar los análisis forenses realizados, interpretar los resultados y sacar conclusiones antes de que el informe se prepare, dichas conclusiones, buscarán satisfacer los requerimientos del cliente o bien soportar una o más de las varias hipótesis que se han obtenido o simplemente desmentir una hipótesis dada.

a. Cotejar los resultados de los análisis.

• Reunir y combinar los resultados en un formato claro y sin ambigüedades.
• Completar una evaluación de los resultados obtenidos.
• Presentar un resumen de los resultados en un formato perfectamente estructurado.
• Asegurar que la evaluación, comentarios e información de apoyo sea precisa y se presente de manera clara.

b. Interpretar los resultados del análisis.

• Tener completos todos los datos de análisis.
• Basar la interpretación sobre los resultados obtenidos y documentados, así como en la información proporcionada acerca del caso.
• Consultar las fuentes de datos, en el momento adecuado de manera que contribuyan a interpretar más claramente los resultados.
• Confirmar los resultados y datos para precisar la validez y fiabilidad.
• Bosquejar las opiniones de los resultados, basados en criterios acordados y que dichas opiniones estén debidamente documentados.
• Registrar en todo momento, la información que se genere durante la interpretación de resultados.

• Considerar la posibilidad de dar explicaciones alternas y probar otras hipótesis, generando el dictamen pertinente.

Reporte de resultados.

Esta activad es la presentación de informes acerca de los resultados de un análisis forense.

a. Generar el reporte.

• Determinar el tipo, alcance y propósito de la información.
• Utilizar información actual en el reporte, precisa y sin ambigüedades.
• Informar todos los resultados expresando claramente las limitaciones de la evidencia utilizada.
• Presentar un informe lógico, imparcial, exacto y adecuado que responda a las necesidades del usuario final.
• Expresar dictámenes y conclusiones dentro del área de especialización del investigador, firmemente basadas en los resultados y la información disponible.
• Asegurar que el informe se ajusta a los requisitos legales y que se hacen las referencias apropiadas a las notas del caso y material relacionado.
• Considerar la posibilidad de más de una explicación a los hallazgos.

b. Participar en consultas previas al juicio.

• Proporcionar asesoría basada en principios científicos establecidos y que sean equilibrados y realistas dentro del contexto del caso.
• Explicar claramente los resultados y su interpretación dentro del contexto de la investigación.
• Considerar la posibilidad de más de una explicación y probar más de una hipótesis, generando los dictámenes correspondientes.
• Identificar, aclarar y resumir los puntos de acuerdo y desacuerdo.
• Buscar la retroalimentación para verificar que los participantes comprenden los resultados.
• Registrar toda información relevante.
• Crear relaciones de trabajo eficaces con los clientes.

c. Presentar la evidencia oralmente ante los tribunales.

- Entregar la evidencia en forma audible y comprensible.
- Dar pruebas de que es coherente con el informe escrito.
- Contestar las preguntas con imparcialidad, sinceridad y flexibilidad de manera inequívoca y admisible.
- Pedir se aclaren las preguntas confusas antes de responder.
- Explicar de manera específica las preguntas, de modo que faciliten el entendimiento de los presentes.
- Tomar en cuenta la información adicional, así como analizar las hipótesis alternas que sean presentadas, considerando las limitaciones de no contar con un análisis más detallado.
- Distinguir claramente entre hechos y dictámenes y asegurar que las opiniones emitidas están dentro del área de especialización.

1.7 Delitos Informáticos

1.7.1 Definición

Otro concepto importante, es el de **Delito Informático**, pues éste ha evolucionado en los últimos tiempos. En principio un delito informático se entendía como cualquier evento anómalo que pudiese afectar a la seguridad de la información, como podría ser una pérdida de disponibilidad, su integridad o confidencialidad, etc. Pero la aparición de nuevos tipos de delitos ha hecho que este concepto haya ampliado su definición. Actualmente un delito informático puede considerarse como una violación o intento de violación de la política de seguridad, de la política de uso adecuado o de las buenas prácticas de utilización de los sistemas informáticos. A continuación se detallan diferentes definiciones de delitos informáticos:

Según el "Convenio de Ciberdelincuencia del Consejo de Europa" (CIBERDELINCUENCIA, 2001), define 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".

La Organización de Cooperación y Desarrollo Económico (OCDE) (seguridadinformaticaufps) define los delitos informáticos como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos." "Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma".

Según Julio Tellez Valdes (TÉLLES VALDEZ, 1996) conceptualiza al "delito Informático" como "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)".

1.7.2 Entornos donde se podría realizar investigaciones

La investigación forense puede realizarse en diferentes escenarios, por ejemplo:

Intrusión a sistemas informáticos

- Web defacement
- Uso no autorizado de equipo informático corporativos
- Abuso de E-mail

Contenidos ilícitos

- Pornografía infantil: CDs, P2P, Internet
- Amenazas

Cualquier crimen físico en el que se implique infraestructura, dispositivos que trata contenido digital, no sólo PCs

- Fraudes
- Estafas
- Propiedad intelectual – Piratería de software
- Etc.

1.7.3 Características de los delitos informáticos

Los delitos informáticos por lo general tienen determinadas características que los identifican, algunas de ellas son las siguientes:

- Sólo una determinada cantidad de personas pueden llegar a cometerlos.
- El sujeto tiene cierto status socioeconómico y la comisión del delito no puede explicarse por pobreza, carencia de recursos, baja educación, poca inteligencia, ni por inestabilidad emocional.
- Son acciones ocupacionales, ya que generalmente se realizan cuando el sujeto atacado se encuentra trabajando.
- Son acciones de oportunidad, ya que se aprovecha una ocasión creada por el atacante.
- Provocan pérdidas económicas.
- Ofrecen posibilidades de tiempo y espacio.
- Son muchos los casos y pocas las denuncias.
- Presentan grandes dificultades para su comprobación, por su carácter técnico.
- Tienden a proliferar, por lo que se requiere su urgente regulación legal.
- Son delitos difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas.
- Son actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.
- Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de los mismos.

Una vez cometido el incidente solo queda:

- Deducir que ha pasado.

- Qué ha motivado que esto haya pasado.
- Qué ha permitido llegar a ello.
- Qué acciones han sido consecuencia de ello.
- Qué podemos hacer para evitar que vuelva a suceder.

1.7.4 Tipos de delitos informáticos

Según la Organización de las Naciones Unidas (ONU) define los siguientes Delitos en las redes electrónicas (ONU, 2000):

- Espionaje industrial

Los piratas pueden realizar tareas de espionaje avanzado para las empresas o para su propio provecho copiando secretos comerciales que abarcan desde información sobre técnicas o productos hasta información sobre estrategias de comercialización.

- Sabotaje de sistemas

Los ataques como el «bombardeo electrónico» consisten en el envío de mensajes repetidos a una dirección o a un sitio electrónico, impidiendo así que los usuarios legítimos tengan acceso a ellos. El flujo de correspondencia puede hacer rebosar el cupo de la cuenta personal del que la recibe y paralizar sistemas enteros. Aunque ésta sea una práctica extremadamente disruptiva, no es necesariamente ilegal.

- Sabotaje y vandalismo de datos

Los intrusos pueden acceder a sitios electrónicos o bases de datos y borrarlos o cambiarlos, corrompiendo los datos mismos y causando perjuicios aún mayores si se usan datos incorrectos posteriormente para otros fines.

- «Pesca» u «olfateo» de claves secretas

Los delincuentes suelen engañar a los usuarios nuevos e incautos de la Internet para que revelen sus claves personales haciéndose pasar por

agentes de la ley o empleados del proveedor del servicio. Los «sabuesos» utilizan programas para identificar claves de usuarios, que más tarde se pueden usar para esconder su verdadera identidad y cometer otras fechorías, desde el uso no autorizado de sistemas de computadoras hasta delitos financieros, vandalismo o actos de terrorismo.

- Estratagemas

Los estafadores utilizan diversas técnicas para ocultar computadoras que se «parecen» electrónicamente a otras para lograr acceso a algún sistema generalmente restringido y cometer delitos. El famoso pirata Kevin Mitnick se valió de estratagemas en 1996 para introducirse en la computadora de la casa de Tsutomo Shimamura, experto en seguridad, y distribuir en la Internet valiosos útiles secretos de seguridad.

- Pornografía Infantil

La distribución de pornografía infantil por todo el mundo a través de la Internet está en aumento. Durante los pasados cinco años, el número de condenas por transmisión o posesión de pornografía infantil ha aumentado de 100 a 400 al año en un país norteamericano. El problema se agrava al aparecer nuevas tecnologías, como la criptografía, que sirve para esconder pornografía y demás material «ofensivo» que se transmita o archive.

- Juegos de Azar

El juego electrónico de azar se ha incrementado a medida que el comercio brinda facilidades de crédito y transferencia de fondos en la Red. Los problemas ocurren en países donde ese juego es un delito o las autoridades nacionales exigen licencias. Además, no se puede garantizar un juego limpio, dadas las inconveniencias técnicas y jurisdiccionales que entraña su supervisión.

- Fraude

Ya se han hecho ofertas fraudulentas al consumidor tales como la cotización de acciones, bonos y valores o la venta de equipos de computadora en regiones donde existe el comercio electrónico.

- Blanqueo de dinero

Se espera que el comercio electrónico sea el nuevo lugar de transferencia electrónica de mercancías o dinero para lavar las ganancias que deja el delito, sobre todo si se pueden ocultar transacciones.

Según el "Convenio de Ciberdelincuencia del Consejo de Europa" (Ciberdelincuencia, 2001) firmado en Budapest el 1 de Noviembre de 2001, propone una clasificación de los delitos informáticos en cuatro grupos:
Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos.
- Interferencia en el funcionamiento de un sistema informático.
- Abuso de dispositivos que faciliten la comisión de delitos.
- Algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes no autorizadas y la utilización de spyware y de keylogger.

Delitos informáticos

- Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
- Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.
- El borrado fraudulento de datos o la corrupción de ficheros algunos ejemplos de delitos de este tipo.

Delitos relacionados con el contenido

- Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos

contenidos en un sistema informático o medio de almacenamiento de datos.

Delitos relacionados con infracciones de la propiedad intelectual y derechos afines

- Piratería informática.

De acuerdo a la **"Guía de Manejo de Incidentes de Seguridad Informática"** del NIST existen cinco tipos de incidentes, dentro de los cuales se pueden clasificar a los incidentes que ocurran en un sistema informático o de telecomunicaciones. Estos cinco tipos son:

- **Denegación de Servicios (DoS):** Son un tipo de delito cuya finalidad es obstaculizar, dañar o impedir el acceso a redes, sistemas o aplicaciones mediante el agotamiento de sus recursos.
- **Código malicioso:** Cualquier tipo de código ya sea, virus, gusano, “caballo de Troya”, que pueda ejecutarse en un sistema e infectarlo.
- **Acceso no autorizado:** Se produce cuando un usuario o aplicación accede, por medio de hardware o software, sin los permisos adecuados a un sistema, a una red, a una aplicación o los datos.
- **Uso inapropiado:** Se dan cuando los usuarios se “saltan” la política de uso apropiado de los sistemas (por ejemplo descargar contenidos ilegales desde la red de una empresa).
- **Delitos múltiples**: Se produce cuando el delito implica varios de los tipos anteriores.

Capítulo II

El perito

2.1 Función del Perito

2.2 Especificidad y competencia del Perito Informático.

2.3 Características específicas del perito informático

2.4 Experiencia en un área informática.

2.5 Capacitación para el Perito Informático

2.6 La actuación de los peritos informáticos en el ámbito judicial

2.7 Problemáticas a las que se enfrenta

2.8 Las pericias informáticas y su alcance.

2.9 Principales recaudos en la recolección evidencia

2.10 Situación actual en la provincia de Córdoba

2.1 Función del Perito

La función del perito informático consiste en el análisis de elementos informáticos, en busca de aquellos datos que puedan constituir una prueba o indicio útil para el litigio jurídico al que ha sido asignado. Las tareas a desarrollar por el perito informático no son distintas de la de otros peritos judiciales. Por lo tanto deberá recopilar la información que es puesta a su disposición, analizar la misma en busca de los datos que el juez le ha requerido y emitir un informe o dictamen en donde vuelque las conclusiones de la investigación realizada.

Existen tres categorías de peritos: Perito Oficial, Perito de Parte y Perito de Oficio;

Los peritos de oficio, están dentro de una lista de peritos de cualquier disciplina, a través de un sorteo son designados a una causa por un juez, generalmente un juez del fuero penal, luego que el perito acepta cargos se le asignan los elementos y son ellos los que realizan la pericia.

El perito oficial; es el perito que forma parte de la estructura policial. Para los peritos oficiales el procedimiento es similar al de los peritos de oficio; excepto que la asignación no es por sorteo sino por designación.

El perito de parte, es el perito que puede poner la parte sospechada o damnificada para supervisar la pericia realizada ya sea del perito oficial o de oficio.

Dentro del ámbito de la policía judicial, el perito oficial de la policía es el que tiene el elemento y gobierna la pericia desde el inicio hasta el fin; los peritos de parte van observando todo el proceso de lo que va ocurriendo independientemente que actúen en disidencia o coincidencia con los resultados. Algo parecido es lo que sucede con el perito de oficio; que es quien gobierna la pericia ya sea en el marco del juzgado o en el laboratorio; esta persona puede decir donde se va a realizar la pericia y designar a los responsables de los elementos; pero quien gobierna la pericia es el perito de oficio.

2.2 Especificidad y competencia del Perito Informático.

Este es un tema de relevancia que debe ser considerado por los jueces durante la selección de un Perito Informático. Por otra parte, la ciencia informática tiene muchos campos de especialización, por lo que el perito deberá considerar minuciosamente si los puntos de pericia a resolver están dentro de su área de competencia.

Relacionado con la especificidad, hay que tener en cuenta los conocimientos y áreas que podrá abarcar un perito. Todo profesional, tiene una formación general o de base, a la que luego suma otros conocimientos específicos y la experiencia propia en el ejercicio de la profesión.

2.3 Características específicas del perito informático

Un perito informático debe ser un profesional capacitado en las diferentes áreas de la informática, no un experto en una sola área de la informática. Pero debido a la gran variedad de especializaciones dentro de la informática, y aun más teniendo en cuenta los cambios vertiginosos de la tecnología, es muy difícil contar con profesionales informáticos preparados, e idóneos en varias disciplinas, por lo que muchas veces se requiere la capacidad de trabajar en equipos interdisciplinarios, para lograr un peritaje eficaz.

2.4 Experiencia en un área informática.

Debido al abanico de opciones con la que cuenta un profesional informático al momento de comenzar a desarrollar su carrera, es común que el mismo logre ser semi senior o senior en la práctica de determinadas herramientas, en función del área dónde se desempeñe.

Debido a los constantes cambios tecnológicos, y la constante aparición de nuevas herramientas, es necesario el que perito informático este constantemente capacitado y atento a las nuevas tendencias.

Si un profesional, a lo largo de su carrera decide capacitarse o tener experiencia en diversas áreas de la informática, adquirirá una visión general que le permitirá ejercer puestos de liderazgos, por su seniority lo más probable es que no muestre habilidades en el manejo de herramientas informáticas, pero sí le permitirá demostrar sus aptitudes para la conducción e interacción con el personal de cualquier área informática.

En el caso de los peritos informáticos, la experiencia en liderazgo es la que le permite interactuar con profesionales de diferentes ámbitos, poder pautar cuáles serán los pasos a seguir para el desarrollo eficaz de una pericia y utilizar algunas herramientas informáticas para el trabajo pericial. Un perito informático con experiencia práctica, trabajará con eficiencia los casos en los que se utilicen las herramientas informáticas de su especialidad, pero se verá limitado al querer actuar en otros.

2.5 Capacitación para el Perito Informático

Existen ciertas capacidades que debe adquirir un perito informático para realizar el peritaje en diferentes dispositivos. Para ello se requiere una capacitación específica en el uso de técnicas y herramientas informáticas utilizadas para pericias informáticas.

Actualmente en nuestro país no existen cursos relevantes ni carreras de perito informático, sin embargo, es posible encontrar algunas diplomaturas o posgrados en criminología o criminalística que ofrecen dentro del programa algún modulo dedicado a las pericias informáticas, por otra parte es posible encontrar en el exterior organizaciones o centros de capacitación que ofrecen programas de entrenamiento o cursos de especialización en este campo.

2.6 La actuación de los peritos informáticos en el ámbito judicial

Ante la aparición de nuevas modalidades delictivas con el uso de tecnología, el perito informático adquiere un rol fundamental para poder aportar pruebas

relevantes a la investigación judicial. Debido a la fragilidad de los elementos probatorios se hace necesario que los mismos sean resguardados en condiciones apropiadas, debiéndose mantener un registro detallado del traslado e intervención pericial sobre la evidencia desde el momento del secuestro hasta la finalización del procedimiento judicial. La evidencia digital pueda ser extraviada, dañada o sustituida si no se observa con detenimiento cada una de las formalidades mínimas establecidas a nivel forense durante las actuaciones judiciales. Por otra parte, es necesario que el operador judicial tenga conocimiento del alcance de la actividad pericial, para evitar que el mismo tienda a efectuar requerimientos ajenos a la disciplina.

Actualmente el Código Procesal Penal no presenta ninguna mención que haga referencia al tratamiento de la evidencia digital ni a su procedimiento de preservación, manipulación y análisis, aunque no implica el mismo proceder que para la recolección de una prueba física, muchas veces debe ser tomado como referencia al momento de tratar la evidencia digital, o en caso contrario el perito informático forense se ve obligado a regir su accionar con las guías de buenas prácticas impartidas por organismos internacionales para de algún modo encuadrar la actividad en un marco de legalidad.

2.7 Problemáticas a las que se enfrenta

Dentro de las actividades propias del peritaje informático, el perito se encuentra con diferentes dificultades en su labor que aumentan la labor y el estudio de dichos profesionales. Según lo señalan los autores (Ariel Podestá, 2013) en el documento de la metodología PURI, aalgunas problemáticas son las siguientes:

Diferentes de tecnologías: La recuperación podría requerirse en distintos tipos de dispositivos. Con el correr del tiempo ingresan al mercado nuevos productos, lo que nos lleva a tratar con diferentes equipos (servidores, notebooks, tabletas, celulares, etc.) para los cuales no siempre se encuentra disponible la herramienta apropiada de obtención de la información.

Diversidad de métodos de almacenamiento: Existen técnicas de almacenamiento y tratamiento de la información que son ampliamente conocidas. Con lo cual, obtener la información de un dispositivo que utilizó tales métodos no sería una tarea demasiado compleja. Pero no siempre es así, eventualmente puede existir un fabricante que utilice su propia técnica de administrar la información en sus dispositivos y que, a su vez, no la de a conocer. Éste, es un problema complejo para los informáticos forenses dado que si no es posible sobrellevar esta dificultad entonces muy probablemente no sea posible hallar evidencias.

Localización de la información: Cuando se tiene un dispositivo personal transportable, como ser un celular, es fácil acceder a él para luego intentar obtener evidencias. Pero si se trata de, por ejemplo, un servidor ya la tarea puede tornarse más compleja. Tal servidor, muy probablemente no sea de la propiedad de la persona en cuestión y hasta quizás ni siquiera se encuentre en la misma zona geográfica. Esto dificulta mucho la tarea de recuperación de la información dado que involucra el traslado de los peritos al lugar donde se encuentran los equipos y no siempre es posible.

Heterogeneidad de leyes que aplican en el planeta: Siempre que se tiene un caso a resolver se requiere del aval legal para realizar pericias sobre los dispositivos relacionados al hecho en cuestión. Este aval debe ser provisto por una entidad que tenga jurisdicción en la zona geográfica donde se encuentran tales dispositivos.

Entonces, es claro que el problema ocurre cuando los equipos se encuentran en una zona geográfica en la cual tal entidad no tiene jurisdicción. Por ende es posible que no se sea posible realizar pericias sobre los equipos.

Tecnologías que naturalmente eliminan evidencias: El dejar evidencias de información eliminada no es interés de los fabricantes de dispositivos y menos cuando eso va en contra de la performance de los mismos. Ciertamente, por ejemplo, los medios de almacenamiento de tipo SSD que hoy en día pueden observarse cada vez más en computadoras personales, son dispositivos que necesitan mantener limpios los espacios libres para maximizar su eficiencia, lo que va en claro desmedro de la posibilidad de recuperar información.

Mecanismos internos de protección de la información: Es atractivo para los usuarios que el dispositivo que adquieran no revele información sin su consentimiento. Los fabricantes, aprovechando esta tendencia, pueden ofrecer equipos que garanticen tal propiedad. Este hecho puede ser un importante impedimento para el forense de acuerdo a que tan robusta e inviolable sea la tecnología con la cual se fabricó el dispositivo a analizar.

Falta de herramientas: Se conoce que los fabricantes proveen herramientas forenses que aplican a sus propios productos. Pero la distribución de tales herramientas se ve directamente afectada por los intereses de los mismos. Solo y exclusivamente si es rentable producirlas y distribuirlas, entonces lo harán. De otra manera, las mismas no se encontrarán disponibles en el mercado, agregando otra dificultad al desempeño de los peritos informáticos.

Criptografía: A medida que los sistemas ganan más y más interconexión las medidas de seguridad crecen por necesidad. Una de ellas es el encriptado. De esta manera, cuando un forense informático realiza un estudio es muy probable que se encuentre con información encriptada. Si el método de encriptado es conocido y se tiene lo necesario para desencriptar tal información, entonces no debería haber mayores problemas para tratar con tal información. Pero no siempre es así. Existen mecanismos de encriptado propios de algunos productores de dispositivos que no son dados a conocer y que pueden, obviamente, dificultar mucho la tarea de recuperación de la información.

Herramientas que cubren solo una parte del proceso: En el proceso de obtención de evidencias sería deseable que mediante una sola herramienta de software se pudieran realizar todas las tareas que son demandadas. Pero lo cierto es que raramente esto ocurre así. Con lo cual es necesario que eventualmente que el resultado de una herramienta pueda ser tomado por otra como punto de partida para continuar el proceso, lo que no siempre es posible.

Desconocimiento de la efectividad y cota de error de las herramientas: Cuando las herramientas utilizadas no son específicamente las provistas por los fabricantes de los dispositivos analizados, y aun cuando sean las provistas, es probable que no tengan una efectividad absoluta. Por ejemplo, un software podría ser capaz de obtener solo ciertas secciones de la información. Así entonces se llevarían a cabo inspecciones, con información resultante

incompleta. Es importante conocer la efectividad y cota de error de la herramienta utilizada, con el fin de considerar la posibilidad de utilizar otras que brinden la misma funcionalidad.

Falta de guías y mecanismos de validación: Al presente aún no existe un modelo universal a seguir en el proceso de recolección de evidencias informáticas y su validación. Entonces en un contexto tan complejo como el comentado se hace evidente que el éxito de la extracción de evidencias termina dependiendo de la destreza, experiencia e inventiva del forense.

2.8 Las pericias informáticas y su alcance.

El alcance de las pericias informáticas va mucho más allá de los delitos informáticos exclusivamente, es decir, no siempre que la informática forma parte de un asunto judicial es con motivo de un delito. La informática puede ser protagonista tanto cuando es utilizada como medio para cometer un delito (por ejemplo una estafa); como cuando es el objeto propio del delito (por ejemplo la compra de software ilegal); cuando tiene lugar en el conflicto de forma colateral, (por ejemplo los incumplimientos de contratos de programación y desarrollo). La Pericia Informática, se presenta como una ciencia auxiliar para el mundo legal, brindando apoyo técnico al juez, que permita iluminar sobre los oscuros puntos, que por su especialidad no alcanza a interpretar.

2.9 Principales recaudos en la recolección de evidencia.

En lo que respecta al tratamiento de la evidencia física en los procedimientos policiales, y por más que parezca redundante, es necesario resaltar la necesidad de brindar un mínimo conocimiento generalizado al personal policial que no posea idoneidad técnica, ya que serán los encargados de realizar el secuestro de la evidencia física, contenedora de la posible evidencia digital.

La búsqueda y el hallazgo de la prueba en todas las investigaciones, lo que por supuesto demanda cierta idoneidad, y seguramente esfuerzo, paciencia y dedicación por parte de los investigadores, no resulta suficiente para el éxito si hubo un mal manejo durante el allanamiento. Aquello que se halló mediante un

procedimiento policial, en un ámbito computarizado, "aquel día, en aquel lugar, y en poder de aquella persona", debe ser exactamente lo que llegue al ámbito del perito, para su análisis y dictamen.

Por otra parte, suele suceder que el perito no cuente con los conocimientos de todos los sistemas y todo tipo de hardware o software, etc. necesarios para peritar en caso.

Todo esto supone la necesidad de que los organismos estatales como la Policía, encargada de llevar a cabo esta clase de actividad, tengan una preparación, capacitación y experiencia más que suficiente para la eficiente realización de tales actividades.

2.10 Situación actual en la provincia de Córdoba

Con respecto al procedimiento oficial en la provincia de Córdoba, la policía judicial participa de la recolección de la evidencia; hay varios medios para la recolección de la evidencia, uno es a través de un de allanamiento, que es el medio más común, donde un órgano judicial, mediante una orden judicial autoriza al personal policial a ingresar al domicilio del sospechoso y secuestrar la evidencia.

Otro medio de recolección es la entrega espontanea, donde la evidencia es facilitada por una persona civil, quien trae un elemento para que sea peritado; en ese momento un policía se encarga de labrar un acta para que sea introducido en la causa.

Además el personal de la policía judicial trabaja como recolector de evidencia, es decir, en un allanamiento pueden identificar otros materiales susceptibles de poseer evidencia y solicitar el secuestro de los mismos.

Con respecto a la evidencia podemos decir que existen dos tipos de evidencia; lógica y física.

Evidencia Lógica abarca cualquier tipo información en formato digital que pueda establecer una relación entre un delito y su presunto autor. Por ejemplo relevar una cuenta de correo electrónico; una cuenta de Facebook.

Toda evidencia lógica, está contenida dentro de un elemento físico, por lo que una evidencia lógica que se encuentra contenida dentro de un elemento físico

se vuelve evidencia física y perdurable en el tiempo, por lo que toda evidencia lógica que es intangible, por su elemento contenedor se vuelve tangible.
Si bien no es el más idóneo en cuanto al tiempo de durabilidad, el elemento contenedor que habitualmente se usa es un cd o dvd, ya que permite la portabilidad y el traslado de la evidencia.

Actualmente, otras secciones dentro de la policía como ser planos, fotos, huellas; también realizan recolecciones de evidencia, es decir, en la escena recolectan los elementos que ellos consideran relevantes para la causa, pero que también es evidencia para la policía judicial, por ejemplo secuestran un Smartphone cuando llegan de un allanamiento entregan la evidencia física que recolectaron del trabajo de campo, la desdoblan y entregan el elemento para que sea analizado, a esto se lo llama cooperación técnica.
En todas las operaciones donde participa la policía judicial tienen preestablecidos mecanismos de cadena de custodia, que en realidad es una cadena de custodia interna del equipo; se considera que no es la mejor pero al menos es la que llevada a cabo bajo ciertas condiciones dan garantías de que se preserva la evidencia.
En el caso de que el allanamiento sea realizado por la policía de otra provincia, el material secuestrado va a la provincia desde donde se solicitó el allanamiento, entonces la policía judicial aplica la cadena de custodia, y los métodos de preservación para que se lo lleve.
En los casos donde la policía no participa de la recolección, por ejemplo en la entrega espontanea, donde no hay cadena de custodia, dicha cadena comienza en el momento que ingresa al área de forense, donde en el laboratorio se aplica la misma la cadena de custodia utilizada en la recolección de campo; el tema que al aislamiento se le suma otro tema que es el depósito; que serían los contenedores hasta que llega la cadena de custodia; de todos modos a la evidencia se le aplico el mecanismo de custodia de campo; el área de forensia informática son los guardadores; pasa la puerta del área; se hace otro procedimiento para determinar que se reciben en el depósito; y recién se saca la evidencia cuando se va a analizar se entra en proceso y se sigue el circuito.
En el caso de la entrega espontanea; como no se hizo el análisis de campo se comienza a trabajar una vez que se comienza a analizar la evidencia.

En el caso de la cooperación de otros equipos técnicos donde no aplica la misma cadena de custodia; el análisis comienza a partir que lo recibe el área de informática forense; donde desde que ingresa el material físico hasta que se da el despacho sigue todo el tratamiento.
En los casos de narcotráfico existe un procedimiento vigente, que se divide en cinco segmentos: dinero, estupefacientes, tecnológicos, armas, balística. Se definió un mecanismo que se aplica desde el secuestro hasta que se lo envía al depósito.
Una vez que se secuestra la evidencia se lo lleva al depósito de narcotráfico; y cuando se va a analizar el fiscal o juez da la orden para que sea retirado del depósito y lo envíen al área que lo va a analizar; respetando siempre la cadena de custodia establecida. Una vez que el área encargada de realizar el análisis termino su actividad, despacha nuevamente la evidencia, y esta vuelve al depósito; para este tipo de delitos existe reglamentada una cadena de custodia.

Realizar la cadena de custodia segmentada, no tiene sentido, la cadena de custodia tiene sé que ser integral, debería ser la misma tanto para un vehículo como para una muestra química.

El problema actual es que las diferentes áreas quieren implementar procedimientos parecidos; ante la inexistencia de un procedimiento troncal; para lograr esto es necesario definir políticas de trabajo, que no solamente estén escritas sino que además se respeten; pero para ello es necesario realizar una inversión; es decir se deben conseguir los materiales necesarios, envoltorios, mecanismos para identificar, etc.

La modificación, la alteración de la evidencia es un problema, por lo que hace tiempo se viene trabajando sobre este tema; en base a la experiencia los procedimientos de cadena de custodia han ido mejorando; pero la falencia actual es la falta de integración.

Con respecto a la recolección de la evidencia, en la medida de lo posible se realiza un secuestro selectivo; es decir el procedimiento es cuando alguien te permite el acceso, un allanamiento es un ejemplo de esto; una vez que se toma contacto con la evidencia por ejemplo una maquina se trabaja con prácticamente las mismas herramientas que en el laboratorio, excepto aquellas que no se pueden transportar.

En el caso del software, se trata de utilizar software portable, para poder realizar un análisis en vivo es decir en el momento; lo que permite poder realizar un análisis selectivo de la evidencia, ya que en un allanamiento se pueden encontrar varios dispositivos de diferentes tipos. En el caso que en un allanamiento se arrase con todos los dispositivos que se encuentren en el lugar se sabe que se cuenta con un conjunto de elementos físicos pero en realidad no se sabe si contienen evidencia sustancial para la causa.

Por tal motivo la policía judicial intenta hacer un análisis selectivo y en base a ese análisis se secuestra o no la evidencia.

En el caso de un pedófilo, en muchos casos la solución sea traer la pc o el elemento contenedor, porque el objetivo es hacer cesar la acción, puede que el elemento contenedor no contenga evidencia sustancial, pero lo que se busca es evitar que se siga distribuyendo material.

En los casos de estafa o cuestiones económicas, son escasas las veces donde se secuestra el material físico, en ese caso se trae el conjunto de archivos o elementos lógicos que configuran esos tipos de directivas. Se trae el conjunto de archivos bajo ciertas normas de procedimientos para garantizar que no se modificó el material, informando donde estaba, en que máquina, etc, se realiza todo un procedimiento de trabajo para dejar sentado donde surgió.

En los procedimientos se llevan bloqueadores, editores, aplican técnicas de rescarven, para realizar un análisis selectivo, este tipo de procedimiento es lento, pero tiene como ventaja que permite poder informar al fiscal si de manera preliminar si hay o no elementos de lo que se está buscando.

Si en cambio se busca obtener un resultado con más profundidad, porque existe la sospecha de que hay más elementos de los que ya se encontraron lo conveniente es secuestrar ese material, pero la policía supeditada a quien los manda, en este caso el juez o fiscal a cargo, entonces se debe pedir autorización para secuestrar dicho material, ya que la orden de allanamiento original no autoriza el secuestro del elemento.

Capítulo III

Evidencia Digital

3.1 Importancia de la Evidencia Digital: Algunos casos relevantes.

3.1.1 Jurisprudencia: Nulidad de pericia informática por fallas en la Cadena de Custodia

3.1.2 Jurisprudencia: Estafas e Internet

3.1.3 Jurisprudencia: Pornografía infantil

3.2 **Evidencia digital**

3.3 Características

3.4 Clasificación de la evidencia

3.5 Como obtener la evidencia

3.6 Cadena de custodia

3.6.1 La cadena de custodia implica

3.6.2 Características de la Cadena de Custodia

3.1 Importancia de la Evidencia Digital: Algunos casos relevantes.

A continuación se detallan algunos casos relevantes en la justicia Argentina, en los que la valides de la evidencia informática jugó un papel fundamental.

3.1.1 Jurisprudencia: Nulidad de pericia informática por fallas en la Cadena de Custodia

(Pericial, 2005)Las prácticas "periciales" llevadas adelante por personal no calificado de la División de Apoyo Tecnológico de la Policía Federal Argentina no tuvieron en cuenta procedimientos elementales de la ciencia forense sobre la cadena de custodia y **contaminaron la evidencia** en el caso Jaime en el que se investiga un enriquecimiento ilícito.

Por ello, a pesar del recurso de apelación promovido por el Fiscal de Cámara, la Sala I de la Cámara Federal ratificó la resolución que decretó la nulidad de las pruebas logradas con las pericias informáticas sobre mails en la causa Jaime.

A la postre de una labor rudimentaria y carente de conocimientos en este área de especialidad efectuada por el personal policial, se suma la ausencia de control de un perito de parte -calificado para tales labores- que hubiera evitado el proceder incorrecto y sin metodología, técnicas y herramientas forenses de los supuestos "idóneos" en informática forense.

Literalmente extraído de la resolución de la Cámara Federal:

"... las prácticas llevadas adelante por la Policía Federal Argentina sobre el material secuestrado contaminaron la evidencia, convirtiendo lo que el juez instructor había considerado una "operación pericial extremadamente simple" y "repetible" en una medida irreproducible."

"…los peritos de la UBA no se refieren a la ausencia de fajado de los puertos de alimentación eléctrica… a los que alude el Sr. Fiscal de Cámara como si sólo eso hubieran dicho, sino a las circunstancias de lugar, tiempo y modo en que las computadoras secuestradas fueron manipuladas antes de que aquellos peritos las tuvieron a su disposición luego para estudio. Y entre esas circunstancias se encuentra, entre muchas otras que hablan de los rudimentarios métodos empleados por la Policía Federal, una de vital importancia: a diferencia de los peritos de la UBA, que emplearon sistemas bloqueadores de escritura de hardware (marca Tableau, tecnología SCSI, en

todos los casos salvo en dos, que se empleó un Live CD de Linux denominado Knoppix) para "…evitar que al acceder a los discos rígidos se inserte información espuria contaminando la evidencia..." (conf. fs. 12.319 y12.320) los peritos policiales no utilizaron ningún sistema de ese tipo".

"Cuando la justicia penal no está a la altura de su propia retórica y las normas que reglamentan su actuación son circunvaladas o ignoradas sin mayores consecuencias, el derecho simplemente se vuelve deshonesto. Y un derecho deshonesto es un mal derecho"…. (Guariglia, 2005)

3.1.2 Jurisprudencia: Estafas e Internet

(Bloj, 2011)La Cámara del Crimen confirmó el procesamiento de una persona por estafa. El denunciado vendió por Internet un objeto y la víctima la abonó, pero nuca fue entregado.

La sala IV de la Cámara del Crimen, integrada por Alberto Seijas y Julio Lucini (Carlos González no suscribió la resolución por no haber presenciado la audiencia), confirmó el procesamiento de una persona por el delito de estafa que fue realizada utilizando páginas de venta online.

Se trata de la causa "R., J. E. s/estafa" en la que una persona publicó por Internet la venta de un objeto, que fue comprado y abonado por la víctima por ese mismo medio, pero nunca fue entregado.

Según consigan en el fallo los camaristas "las constancias de la causa llevan a sostener que el imputado indujo a error al damnificado para lograr que le enviara el [objeto] junto a mil cuatrocientos pesos ($1.400) por medio de la compañía de transporte….., logrando mediante engaño el desapoderamiento de los bienes mencionados".

Para los magistrados "cobran especial relevancia los correos electrónicos intercambiados por las partes" a partir de los cuales se desprende que "ante la propuesta de concretar el negocio enviando parte del dinero mediante... E incluso concertar un encuentro personalmente, el imputado refirió que ello le parecía un gasto innecesario y una situación arriesgada, por lo que propuso que la operación se materialice a través de la empresa de transporte".

Estos correos “echan por tierra el descargo del encausado” ya que “si bien éste manifestó que había incumplido con su parte del trato alegando que el damnificado no le había remitido el dinero pactado”.

Es que, el denunciado, “luego de retirar el objeto de la oficina de diligenciamiento, se comunicó vía correo electrónico con el denunciante, oportunidad en la que no sólo omitió mencionar tal circunstancia, sino que incluso se comprometió a enviar el objeto adquirido a la brevedad”.

“En este tipo de operaciones es frecuente que las personas utilicen identidades diferentes”, explica la sala, pero en la causa “luego de que el imputado retirara la encomienda con una identidad simulada y con un número de documento y domicilio que no le correspondían, intentó vender el mismo objeto en otro sitio de Internet” registrándose con otro usuario diferente.

Por todo ello, los camaristas confirmaron el procesamiento de la persona por el delito de estafa - artículos 45 y 172 del CPN y 306 del CPPN

3.1.3 Jurisprudencia: Pornografía infantil

(SEIJAS & CARLOS ALBERTO GONZÁLEZ, 2011)La Cámara del Crimen confirmó el procesamiento de una persona que distribuía imágenes de pornografía infantil mediante internet encubriendo tal distribución bajo la aparente comercialización de ropa.

La sala IV de la Cámara del Crimen, integrada por Alberto Seijas, Carlos González y Julio Lucini, confirmó el procesamiento de un imputado por distribuir imágenes de pornografía infantil por internet.

En la causa “S., S. A. s/ publicaciones, reproducciones y distribución de pornografía infantil” en primera instancia se procesó al imputado. La defensa apeló el procesamiento por lo que el expediente recayó en la Cámara.

La Cámara sostuvo que las pruebas colectadas hasta el momento acreditan provisoriamente que el imputado “diseñaba y administraba diversos sitios de Internet dedicados a la distribución de pornografía infantil, utilizando como pantalla un portal, donde bajo la apariencia de comercializar prendas de vestir, los interesados debían registrarse y abonar una suma mensual, tras lo cual el imputado les remitía vía e-mail el nombre de usuario y contraseña para acceder a los contenidos".

El acusado explicó que “las impresiones de pantalla obrantes no guardaban relación con su página web” argumentando que “uno no puede introducirse en la programación de una página ajena”, y “sin quererlo uno puede ser redireccionado… a páginas pornográficas”.

Sin embargo, los expertos consultados explicaron que “si se está direccionando desde un origen hacia una página como las cuestionadas (que puede haber cambiado de normal a pornográfica), quien debe cortar ese vínculo es el webmaster del origen, pues tiene todos los elementos para hacerlo, y no depende en absoluto, de lo que el otro webmaster haga”.

Asimismo, luego del secuestro de la computadora del imputado se le descubrieron diversos programas especializado como el Global Scape, Cute FTP, Macromedia Dreamweaver MX u otros que permiten la confección, diseño y administración de páginas web e imágenes como el Adobe Illustrator 9.0, Adobe Photoshop CS2, Macromedia Flash MX, que fueron considerados por los jueces como de “considerable complejidad y no resulta habitual para el usuario común el manejo de herramientas específicas como las señaladas, debiendo, por tal motivo ser ponderado como un elemento de cargo que refuerza la hipótesis investigada”.

Además de los programas que permiten suponer que el imputado era el administrador de este y otros sitios web, fueron detectados así más de 600.000 archivos gráficos y de

videoimágenes entre los que se encontraban menores de edad realizando actividades sexuales explícitas o exhibiendo sus genitales, "lo que justifica la provisoria tipificación de la conducta reprochada con los alcances del auto de mérito cuestionado".

A todo ello se agregó el fax procedente del Agregado Jurídico de la Embajada de los Estados Unidos de América mediante el cual se daba cuenta de la investigación emprendida en ese país por distribución de pornografía infantil a través de Internet por medio de diferentes sitios entre los cuales se hallaba el investigado.

Los camaristas confirmaron el procesamiento del imputado por los delitos previstos en el artículo 128 primera parte del Código Penal, según Ley 25.087. Esto es, distribución de imágenes de pornografía infantil.

En la actualidad los peritos forenses extraen pruebas digitales de un mayor número de dispositivos, con mayor capacidad de almacenamiento, los dispositivos que se pueden investigar en relación a un delito incluyen computadoras, laptops, memorias flash, dispositivos de almacenamiento externo, cámaras digitales, las consolas de videojuegos y los teléfonos celulares. Indudablemente muchos más dispositivos de los que se tenía tan solo hace un par de años.

Los datos contenidos en estos dispositivos digitales pueden ayudar a hacer cumplir la ley en una investigación criminal o enjuiciamiento de delitos en una variedad de maneras.

Le evidencia es el aspecto más importante en cualquier disputa legal o extrajudicial y dentro de un delito donde esté involucrado directa o indirectamente un equipo informático.

3.2 Evidencia digital

Todo dato generado por un dispositivo informático ya sea una computadora personal, una notebook, un celular, etc. como así también los movimientos que el usuario realiza en el equipo, pueden considerarse como evidencia digital ya que quedan registrados incluso luego de que el disco duro ha sido formateado, pudiendo ser recuperado, procesado y analizado de forma correcta para que sea presentado como prueba dentro de un proceso legal. Analizar esta evidencia permite saber con la mayor exactitud qué fue lo que ocurrió. Podemos entender evidencia como:

- El último acceso a un fichero o aplicación (unidad de tiempo)
- Un Log en un fichero
- Una cookie en un disco duro
- El uptime de un sistema
- Un fichero en disco
- Un proceso en ejecución
- Archivos temporales
- Restos de instalación
- Un disco duro, pen-drive, etc.

En esta tesis se han considerado las siguientes definiciones de Evidencia Digital dada por distintos autores en el contexto del análisis forense en equipos computacionales.

- "Cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático". (HB: 171 2003 Guidelinesforthe Management of IT Evidence).

- “Cualquier dato almacenado o transmitido utilizando una computadora que confirme o niegue una teoría sobre la manera en que ocurrió una ofensa”. (Chisum 1999).

- “Cualquier dato que puede establecer que un crimen ha sido cometido o que suministre un enlace entre el crimen y la víctima o entre el crimen y su perpetrador”. (Casey 2000).

- “Cualquier información de valor probatorio que sea almacenada o transmitida de manera digital”. (SWGDE (Grupo de trabajo científico de evidencia digital) - 1999).

- “Información almacenada o transmitida de manera binaria que pueda ser confiable en una corte”. (IOCE (International Organization on Computer Evdence) 1999).

Estas definiciones no se limitan a aquella evidencia encontrada en aquellos escenarios donde existen computadoras, sino que además permite incluir todos los dispositivos electrónicos capaces de almacenar datos, etc.

La evidencia digital, es un insumo crítico, y necesario para poder llevar a cabo proceso de investigación del presunto delitos informáticos, por lo que debe ser tratada por parte de los especialistas, y conservando todas las medidas de precaución necesarias para no contaminarla y que sea objeto de desestimación ante un proceso litigioso.

3.3 Características

Como toda evidencia, la evidencia digital se trata de un material crítico que representa un constante desafío para aquellos que la identifican y analizan en la búsqueda de la verdad:

1. Es volátil
2. Es anónima
3. Es duplicable
4. Es alterable y modificable
5. Es eliminable

Esta evidencia debe cumplir con algunos preceptos para poder ser presentada como prueba en un juicio, ya que sin algunos de estos puntos carecerá de valor probatorio. Dichos aspectos son los siguientes:

Autentica

Debe garantizarse para que sea irrefutable como prueba legal, por lo que será auténtica si cumple con dos elementos:

- El primero, demostrar que la evidencia ha sido extraída y registrada en el lugar de los hechos.
- El segundo, la evidencia digital debe mostrar que los medios originales no han sido alterados.

A diferencia de la evidencia tradicional, en los dispositivos digitales se presenta gran volatilidad y alta capacidad de manipulación. Por lo que resulta indispensable verificar la autenticidad de dichas pruebas digitales. Para asegurar que las pruebas no han ido adulteras se requiere que una arquitectura exhiba mecanismos que certifiquen la integridad de los archivos y el control de cambios de los mismos a través de mecanismos de encriptación, de esta manera disminuye la incertidumbre sobre la manipulación no autorizada de la evidencia aportada, y el proceso se concentra en los hechos y no en errores técnicos de control de la evidencia digital bajo análisis.

Completa

Debe poder reproducir los acontecimientos que ocurrieron previos a los hechos desde el punto de vista técnico, sin juicios o perspectivas particulares. Esta es una característica que igual a las anteriores es crítica en el éxito de las investigaciones, frecuentemente la falta de pruebas o la falta de elementos probatorios ocasionan la terminación de un proceso que pudo haberse resuelto. Para que una prueba esté considerada dentro del criterio de la suficiencia debe estar completa por lo que resulta necesario contar con mecanismos que proporcionen integridad, sincronización y centralización de los datos, para lograr una visión general de la situación, para ello es necesario llevar a cabo un análisis de la correlación de eventos, ya sea manual o sistematizada. Para obtener relaciones entre los datos y eventos generalmente se recurre al análisis y la gestión de logs. Si se analiza esta posibilidad, es posible obtener relaciones entre los datos y eventos presentados, canalizando las inquietudes y afirmaciones de las partes sobre comportamientos y acciones de los involucrados, sustentando esas relaciones con hechos y con registros que previamente han sido asegurados y sincronizados.

Confiable

Nada debe dejarse librado al azar ni dentro del marco legal vigente ni el trato tecnológico desde el punto de vista metodológico, ya que otorgara una autenticidad y veracidad de la prueba recabada, que con posterioridad se analizará y presentará.

Jeimy Cano dice que “los registros de eventos de seguridad son confiables si provienen de fuentes que son creíbles y verificables”. Para probar esto, se debe contar con una arquitectura de computación en correcto funcionamiento, la cual demuestre que los logs que genera tiene una forma confiable de ser identificados, recolectados, almacenados y verificados. El mismo autor menciona que una prueba digital es confiable si el “sistema que lo produjo no ha sido violado y estaba en correcto funcionamiento al momento de recibir, almacenar o generar la prueba”. La arquitectura de computación del sistema logrará tener un funcionamiento correcto siempre que tenga algún mecanismo de sincronización de registro de las acciones de los usuarios del sistema y que posea un registro centralizado e íntegro de los mismos registros

Creíble / admisible

Debe ser lo suficientemente interpretada por cualquier persona, sin dejar dudas sobre la calidad técnico legal utilizado. Esta característica se refiere a que la evidencia digital debe cumplir con los códigos de procedimientos y disposiciones legales del ordenamiento del país. Es decir, debe respetar y cumplir las normas legales vigentes en el sistema jurídico. Así como también a los procedimientos internacionalmente aceptados para la recolección, aseguramiento, análisis y reporte de la evidencia digital.

3.4 Clasificación de la evidencia

EN el escrito sobre evidencia digital, publicado en la revista de Derecho, comunicaciones y nuevas tecnologías, los autores (Cano Martines Jeimy José, 2005) clasifican la evidencia digital en 3 categorías:

Registros generados por computador: Estos registros son aquellos, que como dice su nombre, son generados como efecto de la programación de un computador. Los registros generados por computador son inalterables por una persona. Estos registros son llamados registros de eventos de seguridad (logs) y sirven como prueba tras demostrar el correcto y adecuado funcionamiento del sistema o computador que generó el registro.

Registros no generados sino simplemente almacenados por o en computadores: Estos registros son aquellos generados por una persona, y que son almacenados en el computador, por ejemplo, un documento realizado con un procesador de palabras. En estos registros es importante lograr demostrar la identidad del generador, y probar hechos o afirmaciones contenidas en la evidencia misma. Para lo anterior se debe demostrar sucesos que muestren que las afirmaciones humanas contenidas en la evidencia son reales.

Registros híbridos que incluyen tanto registros generados por computador como almacenados en los mismos: Los registros híbridos son aquellos que combinan afirmaciones humanas y logs. Para que estos registros sirvan como prueba deben cumplir los dos requisitos anteriores.

Harley Kozushko (Kozushko, 2003), menciona que la evidencia digital se puede clasificar, comparar, e individualizar, es decir es el proceso por el cual se buscan características generales de archivos y datos, características que diferencian evidencia similar y que deben ser utilizadas a criterio del investigador, por ejemplo:

- **Contenido:** Un e-mail, por ejemplo, puede ser clasificado por su contenido como SPAM, y puede ser individualizado a partir del contenido de sus encabezados, información que por lo general no es visible para el usuario. Por ejemplo, por su dirección de origen.
- **Función:** El investigador puede examinar cómo funciona un programa para clasificarlo y algunas veces individualizarlo. Por ejemplo, un programa que inesperadamente transfiere información valiosa desde un computador confiable a una locación remota podría ser clasificado como un caballo de Troya y puede ser individualizado por la localización remota a la que transfiere la información.
- **Características:** los nombres de archivo, extensiones e inclusive los encabezados internos que identifican los diferentes formatos de archivo que existen pueden ser de utilidad en la clasificación de la evidencia digital.

3.5 Como obtener la evidencia

Como regla general se debe obtener la evidencia de la forma menos destructiva posible, y siempre en orden de más volátil a menos volátil, gráficamente seria de la siguiente manera:

Contenido de la memoria
Conexiones de red establecidas
Procesos corriendo en el sistema
Puertos abiertos
Usuarios conectados al sistema
Contenidos de archivos de paginación y swap
Contenidos de sistemas de archivos
Configuración de hardware y periféricos

Según la volatilidad se puede clasificar de la siguiente manera de acuerdo a la Volatilidad de la evidencia

Alta

Tipo de almacenamiento	Importancia Forense
CPU (Registros, Cache), Memoria de video	Por lo general la información en estos dispositivos es de mínima utilidad, pero debe ser capturada como parte de la imagen de la memoria del sistema

Media

Tipo de almacenamiento	Importancia Forense
RAM	Incluye información sobre los

	procesos en ejecución.
Tablas del Kernel (Estado de la red y procesos en ejecución)	Permite analizar la actividad de red y los procesos que pueden ser evidencia de actividades no autorizadas
Muy Baja	

Tipo de almacenamiento	Importancia Forense
Medios fijos (discos duros)	Incluye área de swap, colas, directorios temporales, directorios de registro, logs y otros directorios.
Medio removible (pendrive, CR-Rom)	Usualmente son dispositivos para almacenamiento de contenidos históricos del sistema.

Es importante que el perito tenga conocimiento de la causa para que el mismo pueda hacer foco en aquella información que realmente es importante para la causa, además esto ayudara que ante una gran cantidad de material, ya sean conexiones, procesos ejecutados, etc. el perito sepa identificar el orden en el que es conveniente realizar análisis.

3.6 Cadena de Custodia

Según lo menciona Federico Campos (Campos, 2008) "…La cadena de custodia en el proceso del análisis forense consiste en controlar y limitar el acceso a la evidencia que debe ser recabada de los diferentes medios informáticos, cuidando la celosamente, mediante la utilización de buenas prácticas. Dicho control es utilizado para asegurar que la información no ha

sido dañada, alterada, contaminada o destruida durante todo el desarrollo de la práctica forense, permitiendo demostrar que los diferentes elementos de prueba, obtenidos en las diferentes etapas que comprenden al procedimiento, son los mismos que fueron recolectados en el lugar de los hechos…"

El ingeniero Gustavo D. Presman define en un artículo periodístico a la cadena de custodia como:
"… un registro minucioso de las personas que han tomado contacto con la evidencia, indicando claramente los intervalos de posesión. La idea es simple pero muy efectiva: Conocer en todo momento quien estuvo en contacto con la evidencia a fin de poder evaluar las actividades que se efectuaron con relación a la misma y conocer quién es el responsable por las mismas." (Presman, 2009, pág. 2)

3.6.1 La cadena de custodia implica:

- La utilización de procedimientos o metodologías respaldadas legalmente como así también la utilización de materiales idóneos para la extracción adecuada del material probatorio.
- Utilizar herramientas específicas para la extracción de evidencia en cada tipo de dispositivo.
- Proteger la evidencia de posibles daños naturales como artificiales, ya sean intencionales o no.
- Identificar adecuadamente la evidencia para evitar confusiones, o extravíos.
- A diferencia de las pruebas tradicionales, en la forensia informática, las pruebas no pueden ser trasladadas sin los recaudos adecuados, la evidencia debe ser protegida de posibles daños o alteraciones durante el traslado, ya sea por el movimiento o cambios en los factores climáticos.
- Durante todo el proceso, se debe dejar constancia de quien manipulo la prueba, de manera tal que se pueda mantener registro de quien la recolectó, dónde y que circunstancias.

- La recolección debe estar a cargo de personas autorizadas y con al menos el mínimo conocimiento técnico para manipularla sin causar alteración o destrucción.

- Todos los implicados en la recolección de la evidencia deberán velar por la seguridad, integridad y preservación de los elementos secuestrados.

3.5.2 Características de la Cadena de Custodia

Entre las Características básicas de la cadena de custodia, se encuentran las siguientes:

• Garantiza la autenticidad de las pruebas recolectadas y examinadas.

• Tiene el aval de los funcionarios y personas bajo cuya responsabilidad se encuentran los elementos probatorios en las diferentes etapas de la investigación.

• Tiene su inicio con la autoridad que recolecta los elementos de prueba, tomando como punto de partida la orden de allanamiento impartida por autoridad competente, y finaliza con el resultado de laboratorio del elemento material objeto de análisis o estudio.

• La cadena de custodia se aplica a todos y cada uno de los elementos físicos probatorios. Como así también de manera idéntica sobre las actas y oficios que acompañan este material.

• El personal involucrado en el allanamiento o secuestro de la posible evidencia, debe conocer los procedimientos generales y específicos establecidos para tal fin.

• Todos los elementos secuestrados deben tener la descripción completa de los mismos.

• Todo elemento probatorio debe estar debidamente embalado y rotulado, para evitar confusiones.

• El perito deberá dejar sentado el estado en el que recibió los elementos a ser analizados.

• El dictamen pericial deberá dejar constancia escrita de la descripción detallada de la evidencia, de las técnicas y procedimientos de análisis utilizados.

• Los elementos de prueba como los documentos que los acompañan, se deben mantener siempre en lugar seguro.

Capítulo IV

Aspectos Legales

4.1 Argentina: Aspecto legal

4.2 Convenio de Budapest

4.5 Referencias

4.1 Argentina: Aspecto legal

En los últimos años se puede observar en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del deficiente uso que se hace de los recursos informáticos, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

En Argentina se sancionó el 4 de junio del 2008 la Ley 26.388 que modifica el Código Penal a fin de incorporar al mismo diversos delitos informáticos, tales como la distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones.

En el nuevo ordenamiento se establece que el término **documento** comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos **firma** y **suscripción** comprenden la firma digital, la creación de una firma digital o firmar digitalmente y los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente (Artículo siete Código Penal).

En el nuevo ordenamiento pasan a ser considerados delitos los siguientes hechos vinculados a la informática:

Artículo 128: “Será reprimido con prisión de seis meses a cuatro años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores. Será reprimido con prisión de cuatro meses a dos años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un mes a tres años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce años".

Artículo 153: "Será reprimido con prisión de quince días a seis meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.
En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.
La pena será de prisión de un mes a un año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.
Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena".

Artículo 153 bis: "Será reprimido con prisión de quince días a seis meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.
La pena será de un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros".

Artículo 155: "Será reprimido con multa de pesos un mil quinientos a pesos cien mil, el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público".

Artículo 157: Será reprimido con prisión de un mes a dos años e inhabilitación especial de un a cuatro años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

Artículo 157 bis: Será reprimido con la pena de prisión de un mes a dos años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
2. Ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un a cuatro años"

Artículo 173 inciso 16: "(Incurre en el delito de defraudación)...El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos".

Artículo 183 del Código Penal: "(Incurre en el delito de daño)...En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños".

Artículo 184 del Código Penal: "(Eleva la pena a tres meses a cuatro años de prisión, si mediare cualquiera de las circunstancias siguientes):

Inciso 5: Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte

colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;
Inciso 6: Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público".

Artículo 197: "Será reprimido con prisión de seis meses a dos años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida".

Artículo 255: "Será reprimido con prisión de un mes a cuatro años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo "Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos"

4.2 Convenio de Budapest

La Convención sobre ciberdelito firmada en Budapest en el año 2001, se presenta hoy como el único instrumento internacional que intenta aliviar la imperiosa necesidad de cooperación internacional que reclama la lucha contra este fenómeno.

Basándonos en el estudio comparativo realizado por expertos sobre el nivel de compatibilidad entre la convención mencionada y teniendo en cuenta el texto de la ley 26.388 (delito informático), podemos analizar el grado de receptividad en las normas vigentes en nuestro país y las adecuaciones que fueron necesarias para poder adherir a dicho convenio.

Cabe destacar que la mayor parte de las reformas requeridas, ya han sido sancionadas por nuestro país, sin embargo resulta necesario efectuar nuevas

reformas legales a fin de hostilizar adecuadamente este tipo de delitos por su esencia transfronteriza y los obstáculos consustanciales a su persecución, por lo que el Convenio de Budapest se introduce como una herramienta eficaz para tal fin, por lo que va más allá de la reforma en materia penal mencionada, creando institutos y mecanismos de cooperación internacional indispensables a los efectos de combatir dichas conductas.

En cuanto a la estructura del Convenio, éste consta de 48 artículos y un preámbulo inicial. En concreto encontramos hasta cuatro capítulos, divididos en secciones y títulos. **El primer capítulo** tan sólo comprende un precepto, referido a la terminología usada en el texto.

El capítulo segundo «Medidas que deberán adoptarse a nivel nacional», incluye elementos tanto de Derecho material, como procesal. La llamada a la tipificación de determinadas conductas, supone un enorme paso hacia la armonización del Derecho sustantivo de los Estados parte, que resulta fundamental en la lucha contra el ciberdelito, permitiendo aunar los criterios punitivos en torno a dichas conductas. Incluye conductas que los Estados se comprometen a incorporar en sus cuerpos de regulación procesal.

La primera sección, artículos primero al trece, que la convención llama **Derecho Penal Material**, incluye conductas que los Estados se comprometen a sancionar penalmente. Este tramo de la Convención no presenta grandes contradicciones con nuestro ordenamiento jurídico, ya que la mayoría de las conductas tipificadas en el convenio se encuentran contempladas en nuestra legislación a partir de la sanción de la Ley Nº 26388.

Respecto a las figuras delictivas en particular, mencionadas en los artículos 2 (Acceso ilícito)*(1)*, 3 (Interceptación ilícita) *(2)*, 4 (atentados contra l integridad de los daos) *(3)* y 5 (Atentados contra la integridad del sistema) *(4)*, podemos decir que se encuentran contemplados en la Ley Nº 26388, mediante la modificación de la redacción de los artículos 153 bis y 183 del Código Penal Argentino.

Con relación a las conductas previstas en el articulo 7 (*Falsedad informática)* *(5)*, estas figuras se encuentran comprendidas, entre las previstas en la nueva redacción de los artículos 183, 173 inciso 16, 255, 77, del código penal.

Frente a las conductas previstas en el articulo 8 *(Estafa informática)* *(6)*, solo el párrafo b) queda comprendido en el concepto de “fraude informático” que la Ley 26388 incorporo en el inciso 16 del artículo 77 del Código Penal.

Por su parte, el párrafo a) se ve alcanzada por el párrafo incorporado en el artículo 183 por de la ley de delitos informáticos.

Respecto al artículo 9 *(Infracciones relativas a la pornografía infantil)* *(7)*
No sólo llama a la punición de la venta, difusión, oferta, puesta a disposición, etc., de pornografía, sino que además establece el castigo de la posesión de datos relativos a ella. Reconoce igualmente el derecho de los Estados a reservarse la aplicación de las partes conflictivas.

En la **segunda sección**, que la convención llama **Derecho Procesal**, incluye disposiciones que los Estados se comprometen a incorporar en su regulación procesal.

En su primer título, Disposiciones comunes, establece Artículo 14*(Ámbito de aplicación de las medidas de derecho procesal)* *(8)* el ámbito de aplicación de los procedimientos que regula, alcanzando a los tipos penales resultantes de la primera sección de la convención, como así también al conjunto de tipos penales vigentes en un Estado contratante, siempre que los medios comisivos sean informáticos o que la evidencia con que se cuente, o se pretenda reunir, sea digital.

La única excepción que admite esta regla general es la posibilidad que los Estados parte ejerzan su derecho de reserva y limiten la aplicación de las medidas establecidas en los artículos 20 (Recogida en tiempo real de datos de tráfico) *(9)* y 21 (Interceptación de datos relativos al contenido) *(10)* solo a ciertas figuras típicas.

En este sentido se puede sostener que, a través del artículo 14 párrafo 2c, de la convención, los procedimientos que establece podrán extenderse a todo tipo de delito, aun cuando no haya sido cometido a través de medios informáticos. Por lo que a fin de evitar que el ámbito de aplicación del convenio se extienda mas allá de los limites propios de los delitos bajo análisis, a nivel nacional se

restringe la aplicación de los dispositivos procedimentales establecidos por la convención a las tipificaciones de los incisos a) y b), excluyendo su alcance a los procesos que solo se vinculan a esta temática por la presencia de evidencia digital, sin que los medios comisivos o los bienes afectados sean informáticos.

Por su parte en el articulo 15 (condiciones y garantías) *(11)*, establece la obligación de los estados contratantes de garantizar una protección adecuada de los derechos del hombre y las libertades, con una particular referencia a los derechos derivados de las obligaciones que haya asumido en aplicación del convenio para la protección de los derechos humanos y libertades fundamentales. Este artículo introduce entre las garantías requeridas la supervisión judicial de los procedimientos, en concordancia con las garantías establecidas por los artículos 18 y 19 de la Constitución Nacional.

Cabe recordar que según la legislación argentina la facultad de autorizar procedimientos que impliquen el acceso a datos de contenido ya sea en una comunicación electrónica o de información digitalizada corresponde a la investidura judicial. En cuanto aquellos procedimientos que involucren la obtención de datos de tráfico o la conservación de información sin acceso a su contenido o la identificación de equipos o personas intervinientes, podrán ser autorizados por el Ministerio Publico Fiscal, órgano constitucionalmente conformado para promover la actuación de la justicia en defensa de la legalidad de los intereses generales de la sociedad.

Al llegar al artículo 16 (Conservación inmediata de datos informáticos almacenados)(12) se debe resaltar la existencia de dos visiones divergentes en la interpretación jurídica y doctrinaria del texto del artículo 18 de la Constitución Nacional, donde algunos sostienen que cualquier manipulación de información, incluso su simple almacenamiento, requerirá de una orden judicial previa; mientras que otros consideran que las facultades establecidas podrán ser ejercidas con inmediata puesta en conocimiento de la autoridad judicial de turno para su control mediante un acto fundado y motivado.

Prestando especial atención a lo estipulado en el artículo 17 (Conservación y divulgación inmediata de datos de tráfico) (13) se encuentra en concordancia con los plazos estipulados por nuestra legislación a fin de que permita la efectiva realización de las medidas previstas.

Con relación a los procedimientos establecidos en los artículos 20 (Recogida en tiempo real de datos de tráfico) y 21 (Interpretación de datos relativos al contenido), resulta razonable el requerimiento de una orden judicial previa a su ejecución, debido a su potencial causa de perjuicio.

El artículo 22(Competencia)(14), fija los principios de competencia obligando a los Estados parte a ejecutarla cuando las infracciones sean realizadas en cuatro contextos 1- En su territorio; 2- a bordo de una nave que ondee pabellón de ese Estado; 3- a bordo de una aeronave matriculada en ese Estado; 4- por uno de sus súbditos; si la infracción es punible penalmente en el lugar cometido o si la infracción no pertenece a la competencia territorial de ningún Estado. EN nuestra legislación interna la competencia penal se encuentra definida en razón de territorio, extendiendo este concepto a los buques de bandera nacional o aeronaves matriculadas en el país, aun cuando la infracción sea cometida en el extranjero, si sus efectos se producen en el país.

Sin embargo el supuesto de las infracciones cometidas en otros territorios cuyos efectos se produzcan fuera del país, será competente al Estado argentino cuando “fueren ejecutados por agentes o empleados de autoridades argentinas en el desempeño de su cargo”, posición que difiere del apartado b) del primer párrafo del artículo 22 de la Convención. El segundo párrafo de dicho artículo prevé la posibilidad de establecer una reserva en este sentido, lo que tornaría compatible dicho artículo con la normativa vigente.

Por otra parte establece la obligación del Estado parte de atribuirse competencia sobre las infracciones cuyo presunto autor se encuentre en su territorio y no sea posible extraditarlo en razón de su nacionalidad.

En cuanto al **tercer capítulo**, se introduce directamente en la cooperación internacional. Abarca cuestiones como la extradición, la asistencia entre Estados, la información, el intercambio de datos y el estableciendo a través del articulo 35 una red 24/7 la implementación de un único punto centralizado de contacto para todas las comunicaciones referidas a la convención resulta compatible con nuestra legislación y deseable en tanto propenderá a la eficacia de la aplicación de la propia convención.

En cuanto a la posibilidad de extradición, el artículo 24(Extradición)(15) se presenta como una obligación de los estados firmantes de incorporar las infracciones previstas en la Convención entre aquellas con potencialidad de provocar un proceso de extradición, tanto en los tratados sobre la materia vigentes como en los que suscriba el Estado parte en el futuro. Además termina estipulando la obligación de atribuirse competencia sobre el delito al estado parte que deniegue una extradición en razón de la nacionalidad del presunto infractor.

Por su parte el artículo 25 (principios generales relativos a la colaboración)(16) se presenta compatible con nuestro derecho interno.

El artículo 27 (procedimiento relativo a las demandas de colaboración en ausencia de acuerdo internacional aplicable)(17), se presenta como adaptable a nuestro ordenamiento, siempre que su reglamentación prevea la participación del Poder Judicial y/o el Ministerio Publico Fiscal en el organismo designado como autoridad encargada de tramitar las demandas de colaboración.

EL articulo 28 (confidencialidad y restricciones de uso)(18) se presenta como la clausula convencional que permitiría, establecer los procedimientos destinados al momento de la ratificación, de manera que resulten compatibles con lo establecido en la ley 25.326 de Protección de Datos Personales.

El articulo 30 (Comunicación inmediata de los datos informáticos conservados) (19)en su texto abre la posibilidad de que el Estado requerido descubriera que un prestador de servicios de otro Estado ha participado en la transmisión, dado que esta posibilidad podría implicar que el Estado requerido deba efectuar un análisis del contenido de los datos conservados, actividad que supera ampliamente los términos de una simple conversación y que ineludiblemente en nuestro sistema requeriría de la intervención judicial para su habilitación.

En el articulo 31 (Asistencia concerniente al acceso a datos informáticos almacenados)(20) se advierte que ante el supuesto de existir “motivos para sospechar que los datos solicitados son particularmente vulnerables por existir riesgo de pérdida o modificación” el Estado requerido esté obligado a responder a una demanda de “registro o acceso de otro modo, decomiso u obtención por otro medio o comunicación de datos almacenados”, aun cuando

la misma se realice en contradicción con lo dispuesto por los instrumentos internacionales, convenios y la legislación argentina.

El articulo 32 (acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso)(21), se refiere a datos informáticos de acceso público o cuyo acceso se encuentra consentido legalmente por quien posea derecho, esta conducta se encuentra admitida en la Ley 25326 de Protección de Datos Personales.

En cuanto a lo establecido por el articulo 35 (Red 24/7)(22), la implementación de un único punto centralizado de contacto para todas las comunicaciones referidas a la convención resulta compatible con nuestra legislación y deseable en tanto propenderá a la eficacia de la aplicación de la propia convención. Se espera de dicho punto de contacto, la necesaria unidad o coordinación con la autoridad responsable de la colaboración internacional y el trámite de las extradiciones, así como la obligatoriedad de contar con personal idóneo a fin de garantizar el funcionamiento de la red.

El último capítulo contiene las disposiciones finales propias de un Tratado internacional: adhesión, entrada en vigor, aplicación territorial, efectos, régimen de reservas, denuncias, notificaciones, etc.

4.3 Referencias

(1)Art 2 Convención de Budapest sobre Ciberdelito (CB) "Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, el acceso doloso3 y sin autorización a todo o parte de un sistema informático. Los Estados podrán exigir que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático."

(2) Artículo 3. Interceptación ilícita "Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la interceptación, dolosa y sin autorización,

cometida a través de medios técnicos, de datos informáticos --en transmisiones no públicas-- en el destino, origen o en el interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos informáticos. Los Estados podrán exigir que la infracción sea cometida con alguna intención delictiva o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.

(3) Artículo 4. Atentados contra la integridad de los datos

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la conducta de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos.

2. Los Estados podrán reservarse el derecho a exigir que el comportamiento descrito en el párrafo primero ocasione daños que puedan calificarse de graves.

(4) Artículo 5. Atentados contra la integridad del sistema

Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

(5)Artículo 7. Falsedad informática

Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos, con independencia de que sean directamente legibles e inteligibles. Los Estados podrán reservarse el derecho a exigir la concurrencia de un ánimo fraudulento o de cualquier otro ánimo similar para que nazca responsabilidad penal.

(6)Artículo 8. Estafa informática

Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de:

c. la introducción, alteración, borrado o supresión de datos informáticos,

d. cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero.

(7)Artículo 9. Infracciones relativas a la pornografía infantil

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:

a. la producción de pornografía infantil con la intención de difundirla a través de un sistema informático;

b. el ofrecimiento o la puesta a disposición de pornografía infantil a través de un sistema informático;

c. la difusión o la transmisión de pornografía infantil a través de un sistema informático;

d. el hecho de procurarse o de procurar a otro pornografía infantil a través de un sistema informático;

e. la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 arriba descrito, la «pornografía infantil» comprende cualquier material pornográfico que represente de manera visual:

a. un menor adoptando un comportamiento sexualmente explícito;

b. una persona que aparece como un menor adoptando un comportamiento sexualmente explícito6;

c. unas imágenes realistas que representen un menor adoptando un comportamiento sexualmente explícito7.

3. A los efectos del párrafo 2 arriba descrito, el término «menor» designa cualquier persona menor de 18 años. Los Estados podrán exigir un límite de edad inferior, que debe ser como mínimo de 16 años.

4. Los Estados podrán reservarse el derecho de no aplicar, en todo o en parte, los párrafos 1 (d) y 1 (e) y 2 (b) y 2 (c).

(8)Artículo 14. Ámbito de aplicación de las medidas de derecho procesal

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para instaurar los poderes y procedimientos previstos en

la presente sección a los efectos de investigación o de procedimientos penales específicos.

2. Salvo disposición en contrario, prevista en el artículo 21, los Estados podrán aplicar los poderes y procedimientos mencionados en el párrafo 1:

a. a las infracciones penales establecidas en los artículos 2 a 11 del presente Convenio;

b. a cualquier otra infracción penal cometida a través de un sistema informático;

c. a la recogida de pruebas electrónicas de cualquier infracción penal.

3.

a. Los Estados podrán reservarse el derecho de aplicar la medida mencionada en el artículo 20 a las infracciones especificadas en sus reservas, siempre que el número de dichas infracciones no supere el de aquellas a las que se aplica la medida mencionada en el artículo 21. Los Estados tratarán de limitar tal reserva de modo que se permita la aplicación lo más amplia posible de la medida mencionada en el artículo 20.

b. Cuando un Estado, en razón de las restricciones impuestas por su legislación vigente en el momento de la adopción del presente Convenio, no esté en condiciones de aplicar las medidas descritas en los artículos 20 y 21 a las comunicaciones transmitidas en un sistema informático de un prestador de servicios que

i. es utilizado en beneficio de un grupo de usuarios cerrado, y

ii. no emplea las redes públicas de telecomunicación y no está conectado a otro sistema informático, público o privado, ese Estado podrá reservarse el derecho de no aplicar dichas medidas a tales comunicaciones. Los Estados tratarán de limitar tal reserva de modo que se permita la aplicación lo más amplia posible de las medidas mencionadas en los artículos 20 y 21.

(9)Artículo 20. Recogida en tiempo real de datos de tráfico

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para:

a. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio;

b. obligar a un prestador de servicios, en el ámbito de sus capacidades técnicas existentes, a

i. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio, o

ii. prestar a las autoridades competentes su colaboración y su asistencia para recopilar o grabar, en tiempo real, los datos de tráfico asociados a comunicaciones específicas transmitidas en su territorio a través de un sistema informático.

2. Cuando un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas enunciadas en el párrafo 1 (a), podrá, en su lugar, adoptar otras medidas legislativas o de otro tipo que estime necesarias para asegurar la recogida o la grabación en tiempo real de los datos de tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio.

3. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a un prestador de servicios a mantener en secreto la adopción de las medidas previstas en el presente artículo, así como cualquier información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

(10)Artículo 21. Interceptación de datos relativos al contenido

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes respecto a infracciones consideradas graves conforme a su derecho interno para:

a. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio; y

b. obligar a un prestador de servicios, en el ámbito de sus capacidades técnicas existentes, a

i. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio, o

ii. prestar a las autoridades competentes su colaboración y su asistencia para recopilar o grabar, en tiempo real, los datos relativos al contenido de concretas comunicaciones en su territorio, transmitidas a través de un sistema informático.

2. Cuando un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas enunciadas en el párrafo 1 (a), podrá, en su lugar, adoptar otras medidas legislativas o de otro tipo que estime necesarias para asegurar la recogida o la grabación en tiempo real de los datos relativos al contenido de concretas comunicaciones transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio.

3. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a un prestador de servicios a mantener en secreto la adopción de las medidas previstas en el presente artículo, así como cualquier información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

(11)Artículo 15. Condiciones y garantías.

1. Los Estados velarán para que la instauración, puesta en funcionamiento y aplicación de los poderes y procedimientos previstos en la presente sección se sometan a las condiciones y garantías dispuestas en su derecho interno, que debe asegurar una protección adecuada de los derechos del hombre y de las libertades y, en particular, de los derechos derivados de las obligaciones que haya asumido en aplicación del Convenio para la protección de los derechos humanos y libertades fundamentales del Consejo de Europa (1950) y del Pacto internacional de derechos civiles y políticos de Naciones Unidas (1966) o de otros instrumentos internacionales relativos a los derechos del hombre, y que debe integrar el principio de proporcionalidad.

2. Cuando ello sea posible, en atención a la naturaleza del poder o del procedimiento de que se trate, dichas condiciones y garantías incluirán, entre otras, la supervisión judicial u otras formas de supervisión independiente, la

motivación justificante de la aplicación, la limitación del ámbito de aplicación y la duración del poder o del procedimiento en cuestión.

3. Los Estados examinarán la repercusión de los poderes y procedimientos de esta Sección sobre los derechos, responsabilidades e intereses legítimos de terceros, como exigencia dimanante del interés público y, en particular, de una correcta administración de justicia.

(12)Artículo 16. Conservación inmediata de datos informáticos almacenados

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación inmediata de datos electrónicos especificados, incluidos los datos de tráfico, almacenados a través de un sistema informático, especialmente cuando hayan razones para pensar que son particularmente susceptibles de pérdida o de modificación.

2. Los Estados adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a una persona a conservar y proteger la integridad de los datos --que se encuentran en su poder o bajo su control y respecto de los cuales exista un mandato previo de conservación en aplicación del párrafo precedente-- durante el tiempo necesario, hasta un máximo de 90 días, para permitir a las autoridades competentes obtener su comunicación. Los Estados podrán prever que dicho mandato sea renovado posteriormente.

3. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar al responsable de los datos o a otra persona encargada de conservarlos a mantener en secreto la puesta en ejecución de dichos procedimientos durante el tiempo previsto por su derecho interno.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

(13)Artículo 17. Conservación y divulgación inmediata de los datos de tráfico

1. A fin de asegurar la conservación de los datos de tráfico, en aplicación del artículo 16, los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para:

a. procurar la conservación inmediata de los datos de tráfico, cuando uno o más prestadores de servicio hayan participado en la transmisión de dicha comunicación; y

b. asegurar la comunicación inmediata a la autoridad competente del Estado, o a una persona designada por dicha autoridad, de datos de tráfico suficientes para permitir la identificación de los prestadores de servicio y de la vía por la que la comunicación se ha transmitido.

2. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

(14)Artículo 22. Competencia

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para atribuirse la competencia respecto a cualquier infracción penal establecida en los artículos 2 a 11 del presente Convenio, cuando la infracción se haya cometido:

a. en su territorio;

b. a bordo de una nave que ondee pabellón de ese Estado;

c. a bordo de una aeronave inmatriculada en ese Estado;

d. por uno de sus súbditos, si la infracción es punible penalmente en el lugar donde se ha cometido o si la infracción no pertenece a la competencia territorial de ningún Estado.

2. Los Estados podrán reservarse el derecho de no aplicar, o de aplicar sólo en ciertos casos o condiciones específicas, las reglas de competencia definidas en los párrafos 1b a 1d del presente artículo o en cualquiera de las partes de esos párrafos.

3. Los Estados firmantes adoptarán las medidas que se estimen necesarias para atribuirse la competencia respecto de cualquier infracción mencionada en el artículo 24, párrafo 1 del presente Convenio, cuando el presunto autor de la misma se halle en su territorio y no pueda ser extraditado a otro Estado por razón de la nacionalidad, después de una demanda de extradición.

4. El presente Convenio no excluye ninguna competencia penal ejercida por un Estado conforme a su derecho interno.

5. Cuando varios Estados reivindiquen una competencia respecto a una infracción descrita en el presente Convenio, los Estados implicados se reunirán, cuando ello sea oportuno, a fin de decidir cuál de ellos está en mejores condiciones para ejercer la persecución.

(15)Artículo 24. Extradición

1. a. El presente artículo se aplicará a la extradición por alguna de las infracciones definidas en los artículos 2 a 11 del presente Convenio, siempre que éstas resulten punibles por la legislación de los dos Estados implicados y tengan prevista una pena privativa de libertad de una duración mínima de un año.

b. Aquellos Estados que tengan prevista una pena mínima distinta, derivada de un tratado de extradición aplicable a dos o más Estados, comprendido en la Convención Europea de Extradición (STE nº 24), o de un acuerdo basado en la legislación uniforme o recíproca, aplicarán la pena mínima prevista en esos tratados o acuerdos.

2. Las infracciones penales previstas en el apartado 1 del presente artículo podrán dar lugar a extradición si entre los dos Estados existe un tratado de extradición.

Los Estados se comprometerán a incluirlas como tales infracciones susceptibles de dar lugar a extradición en todos los tratados de extradición que puedan suscribir.

3. Si un Estado condiciona la extradición a la existencia de un tratado y recibe una demanda de extradición de otro Estado con el que no ha suscrito tratado alguno de extradición, podrá considerar el presente Convenio fundamento jurídico suficiente para conceder la extradición por alguna de las infracciones penales previstas en el párrafo 1 del presente artículo.

4. Los Estados que no condicionen la extradición a la existencia de un tratado podrán levar a cabo la extradición siempre que prevean como infracciones las previstas en el párrafo 1 del presente artículo.

5. La extradición quedará sometida a las condiciones establecidas en el derecho interno del Estado requerido o en los tratados de extradición vigentes, quedando asimismo sometidos a estos instrumentos jurídicos los motivos por los que el país requerido puede denegar la extradición.

6. Si es denegada la extradición por una infracción comprendida en el párrafo 1 del presente artículo, alegando la nacionalidad de la persona reclamada o la competencia para juzgar la infracción del Estado requerido, éste deberá someter el asunto –la demanda del Estado requirente—a sus autoridades competentes a fin de que éstas establezcan la competencia para perseguir el hecho e informen de la conclusión alcanzada al Estado requirente. Las autoridades en cuestión deberán adoptar la decisión y sustanciar el procedimiento del mismo modo que para el resto de infracciones de naturaleza semejante previstas en la legislación de ese Estado.

(16)Artículo 25. Principios generales relativos a la colaboración

1. Los Estados firmantes acordarán llevar a cabo una colaboración mutua lo más amplia posible al objeto de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o al de recoger pruebas electrónicas de una infracción penal.

2. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que estimen necesarias para dar cumplimiento a las obligaciones establecidas en los artículos 27 a 35.

3. Los Estados firmantes podrán, en caso de emergencia, formular una demanda de colaboración, a través de un medio de comunicación rápido, como el fax o el correo electrónico, procurando que esos medios ofrezcan las condiciones suficientes de seguridad y de autenticidad (encriptándose si fuera necesario) y con confirmación posterior de la misma si el Estado requerido lo exigiera. Si el Estado requerido lo acepta podrá responder por cualquiera de los medios rápidos de comunicación indicados.

4. Salvo disposición en contrario expresamente prevista en el presente capítulo, la colaboración estará sometida a las condiciones fijadas en el derecho interno del Estado requerido o en los tratados de colaboración aplicables y comprenderá los motivos por los que el Estado requerido puede negarse a colaborar. El Estado requerido no podrá ejercer su derecho a rehusar la colaboración en relación a las infracciones previstas en los artículos 2 a 11, alegando que la

demanda se solicita respecto a una infracción que, según su criterio, tiene la consideración de fiscal.

5. Conforme a lo dispuesto en el presente capítulo, el Estado requerido estará autorizado a supeditar la colaboración a la exigencia de doble incriminación. Esa condición se entenderá cumplida si el comportamiento constitutivo de la infracción --en relación a la que se solicita la colaboración— se encuentra previsto en su derecho interno como infracción penal, resultando indiferente que éste no la encuadre en la misma categoría o que no la designe con la misma terminología.

(17)Artículo 27.- Procedimiento relativo a las demandas de colaboración en ausencia de acuerdo internacional aplicable

1. En ausencia de tratado o acuerdo en vigor de asistencia basado en la legislación uniforme o recíproca, serán aplicables los apartados 2 al 9 del presente artículo. Éstos no se aplicarán cuando exista un tratado, acuerdo o legislación sobre el particular, sin perjuicio de que las partes implicadas puedan decidir someterse, en todo o parte, a lo dispuesto en este artículo.

2. a. Los Estados designarán una o varias autoridades centrales encargadas de tramitar las demandas de colaboración, de ejecutarlas o de transferirlas a las autoridades competentes para que éstas las ejecuten.

b. Las autoridades centrales se comunicarán directamente las unas con las otras.

c. Los Estados, en el momento de la firma o del depósito de sus instrumentos de ratificación, aceptación, de aprobación o de adhesión, comunicarán al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en aplicación del presente párrafo.

d. El Secretario General del Consejo de Europa creará y actualizará un registro de autoridades designadas por las partes. Los Estados deberán garantizar la exactitud de los datos obrantes en el registro.

3. Las demandas de asistencia basadas en el presente artículo serán ejecutadas conforme al procedimiento especificado por el Estado requirente, siempre que resulte compatible con la legislación del Estado requerido.

4. Al margen de los motivos previstos en el artículo 15 párrafo 4 para denegar la asistencia, ésta podrá ser rechazada por el Estado requerido:

a. si la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o;

b. si el Estado requerido estima que, de acceder a la colaboración, se pondría en peligro su soberanía, seguridad, orden público u otro interés esencial.

5. El Estado requerido podrá aplazar la ejecución de la demanda cuando ésta pueda perjudicar investigaciones o procedimientos en curso llevados a cabo por las autoridades nacionales.

6. Antes de denegar o retrasar la asistencia, el Estado requerido deberá examinar, tras consultar al Estado requirente, si es posible hacer frente a la demanda de forma parcial o si es posible establecer las reservas que estime necesarias.

7. El Estado requerido informará inmediatamente al Estado requirente del curso que pretende dar a la demanda de asistencia. De denegar o retrasar la tramitación de la demanda, el Estado requerido hará constar los motivos.

Asimismo, dicho Estado deberá informar al Estado requirente sobre los motivos que hacen imposible, de ser así, la ejecución de la demanda o que retrasan sustancialmente su ejecución.

8. El Estado requirente podrá solicitar que el Estado requerido mantenga en secreto la propia existencia y objeto de la demanda interpuesta al amparo de este capítulo, salvo en aquellos aspectos necesarios para la ejecución de la misma. Si el Estado requirente no pudiera hacer frente a la petición de confidencialidad, éste deberá informar inmediatamente al otro Estado, quien decidirá si la demanda, pese a ello, debe ser ejecutada.

9. a. En caso de urgencia, las autoridades judiciales del Estado requirente podrán dirigir directamente a las autoridades homólogas del Estado requerido las demandas de asistencia y las comunicaciones. En tales casos, se remitirá simultáneamente una copia a las autoridades del Estado requerido con el visado de la autoridad central del Estado requirente.

b. Todas las demandas o comunicaciones formuladas al amparo del presente parágrafo podrán ser tramitadas a través de la Organización Internacional de la Policía Criminal (INTERPOL).

c. Cuando una demanda haya sido formulada al amparo de la letra (a) del presente artículo, y la autoridad que le dio curso no sea la competente para ello, deberá transferir la demanda a la autoridad nacional competente y ésta informará directamente al Estado requerido.

d. Las demandas o comunicaciones realizadas al amparo del presente párrafo que no supongan la adopción de medidas coercitivas podrán ser tramitadas directamente por las autoridades del Estado requirente y las del Estado requerido.

e. Los Estados podrán informar al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que, por motivos de eficacia, las demandas formuladas al amparo del presente párrafo deberán dirigirse directamente a su autoridad central.

(18)Artículo 28. Confidencialidad y restricciones de uso

1. En ausencia de tratado o acuerdo en vigor de asistencia basados en la legislación uniforme o recíproca, será aplicable lo dispuesto en el presente artículo. Éste no se aplicará cuando exista un tratado, acuerdo o legislación sobre el particular, sin perjuicio de que las partes implicadas puedan decidir someterse, en todo o parte, a lo dispuesto en este artículo.

2. El Estado requerido podrá supeditar la comunicación de la información o del material requerido en la demanda al cumplimiento de las siguientes condiciones:

a. que se mantenga la confidencialidad sobre las mismas, siempre que la demanda corra el riesgo fracasar en ausencia de dicha condición; o

b. que éstas no sean utilizadas en investigaciones o procedimientos diversos a los establecidos en la demanda.

3. Si el Estado requirente no pudiera satisfacer alguna de las circunstancias establecidas en el apartado 2 del presente artículo, podrá exigir de la otra parte la concreción de las condiciones de uso de la información o del material.

(19)Artículo 30. Comunicación inmediata de los datos informáticos conservados

1. Si, en ejecución de una demanda de conservación de datos de tráfico relativos a una concreta comunicación al amparo del artículo 29, el Estado requerido descubriera que un prestador de servicios de otro Estado ha participado en la transmisión de la comunicación, comunicará inmediatamente al Estado requirente los datos informáticos de tráfico, con el fin de que éste identifique al prestador de servicios y la vía por la que la comunicación ha sido realizada.

2. La comunicación de datos informáticos de tráfico prevista en el párrafo 1 únicamente podrá ser denegada:

a. si la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o;

b. si el Estado requerido estima que de acceder a la demanda se pondría en peligro su soberanía, su seguridad, orden público o otro interés esencial.

(20)Artículo 31. Asistencia concerniente al acceso a datos informáticos almacenados

1. Cualquier Estado podrá solicitar a otro el registro o acceso de otro modo, el decomiso u obtención por otro medio, o la comunicación de datos almacenados en un sistema informático que se encuentre en su territorio, incluidos los datos conservados conforme a lo dispuesto en el artículo 29.

2. El Estado requerido dará satisfacción a la demanda aplicando los instrumentos internacionales, convenios y la legislación mencionada en el artículo 23 siempre que no entre en contradicción con lo dispuesto en el presente capítulo.

3. La demanda deberá ser satisfecha lo más rápidamente posible en los siguientes casos:

a. cuando existan motivos para sospechar que los datos solicitados son particularmente vulnerables por existir riesgo de pérdida o modificación; o

b. cuando los instrumentos, convenios o legislación referida en el párrafo prevean una cooperación rápida.

(21) Artículo 32. Acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso

Cualquier Estado podrá sin autorización de otro:

a. acceder a los datos informáticos almacenados de libre acceso al público (fuentes abiertas), independientemente de la localización geográfica de esos datos; o

b. acceder a, o recibir a través de un sistema informático situado en su territorio, los datos informáticos almacenados situados en otro Estado, si se obtiene el consentimiento legal y voluntario de la persona autorizada para divulgarlos a través de ese sistema informático.

(22) Artículo 35. Red 24/7

1. Los Estados designarán un punto de contacto localizable las 24 horas del día, y los siete días de la semana, con el fin de asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos o en la recogida de pruebas electrónicas de una infracción penal. Esta asistencia comprenderá, si lo permite el derecho y la práctica interna, facilitar la aplicación directa de las siguientes medidas:

a. aportación de consejos técnicos;

b. conservación de datos según lo dispuesto en los artículos 29 y 30; y

c. recogida de pruebas, aportación de información de carácter jurídico y localización de sospechosos.

2. a. Un mismo punto de contacto podrá ser coincidente para dos Estados, siguiendo para ello un procedimiento acelerado.

b. Si el punto de contacto designado por un Estado no depende de su autoridad o autoridades responsables de la colaboración internacional o de la extradición, deberá velarse para que ambas autoridades actúen coordinadamente mediante la adopción de un procedimiento acelerado.

3. Los Estados dispondrán de personal formado y dotado a fin de facilitar el funcionamiento de la red.

Capítulo V

Metodología de Trabajo para la Investigación Forense

5.1 Metodología para el análisis de datos

5.1.1. Asegurar la escena del delito.

5.1.2. Identificar y obtener la evidencia.

5.1.3. Preservar la evidencia.

5.1.4. Analizar la evidencia.

5.1.5. Emitir un dictamen.

5.1 Metodología para el análisis de datos

Actualmente en nuestro país, la principal problemática en la informática forense se detecta durante la actividad de la obtención de evidencias. Esta actividad se desarrolla bajo un entorno complejo donde el informático forense debe enfrentar una serie de inconvenientes poniendo atención a numerosas dificultades como la pluralidad de tecnologías, procedimientos de ocultamiento de información, tiempos estrechos, falta de guías de ejecución, normativas vigente, intereses de fabricantes, entre otras, todo esto determina que el éxito o no de la tarea dependa de su competencia profesional guiada por su criterio y no por un proceso formal. Se requiere por lo tanto, un proceso formal que permita guiar y certificar la actividad del informático forense en la obtención de evidencias, para que las mismas sean válidas en un proceso legal.

Una metodología formal le permite al perito abordar e investigar un delito informático de manera racional y rápida, sin perder la minuciosidad del trabajo. Lo más importante es que a través de ella se establece un protocolo mediante el cual la evidencia digital (física y lógica) es reunida y manejada, contribuyendo a minimizar los casos en los que la evidencia es contaminada o alterada a través del seguimiento de la cadena de custodia. Sin tal metodología, será más difícil realizar una investigación exitosa que garantice la admisibilidad de la evidencia.

Como toda metodología o procedimiento de investigación implementado para realizar el análisis forense debe cumplir las características de una metodología científica, cada uno de los pasos deben ser bien diseñados de manera tal que puedan ser repetidos en todas las investigaciones. Tales pasos deben ayudar a evitar que se generen resultados inconsistentes o imparciales, mediante la aportación de un marco de trabajo dentro del cual las actividades de investigación puedan llevarse a cabo. Sin una metodología de trabajo formal un perito forense no puede efectuar correctamente su labor. La evidencia que se reúne sin una metodología seguramente no será admitida como válida para la justicia.

En este capítulo se describe una metodología de análisis forense sobre computadoras personales indistintamente si el sistema operativo con el que

trabajan es Linux o Windows. Dicha metodología se ha construido siguiendo normas, recomendaciones y guías de buenas prácticas conocidas mundialmente para la recolección de evidencia digital. La misma se propone como modelo a seguir por la practicidad, simplicidad y eficiencia que ofrece en cinco etapas claramente definidas:

1. Asegurar la escena del delito.

2. Identificar y obtener la evidencia.

3. Proteger la evidencia.

4. Analizar la evidencia.

5. Documentación y presentación de los resultados.

Fig.1 Metodología para el análisis forense de evidencia digital

Respetando esta secuencia, sin alterar el orden de precedencia, que debe ser rigurosamente respetado, el proceso de investigación logra trazabilidad, consistencia y precisión en la obtención de la evidencia digital.

Las tres primeras etapas propuestas normalmente se deberían hacer en la escena del crimen sobre todo por obtener toda evidencia “in-situ” que pueda ayudar al caso, debido a que una vez levantada la escena del crimen no será posible obtenerlas.

La fase de análisis se debería realizar en el laboratorio forense, donde tendremos las condiciones y el equipo idóneo para dicho proceso.

La presentación del dictamen se hará ante un tribunal de justicia.

Antes de iniciar un allanamiento es indispensable preparar todo para poder realizar la investigación correspondiente, algunas de las actividades que consideramos necesarias realizar son las siguientes:

- Establecer lo que se necesita para realizar la investigación tanto a nivel operacional como técnico.

- Se requiere de todas las autorizaciones legales para poder llevar a cabo el allanamiento y el levantamiento de la información.

- Todo el personal involucrado debe conocer la estrategia con la que se debe identificar, recolectar, embalar, analizar y transportar toda la evidencia.

- Determinar los perfiles que participaran en la causa, oficiales, investigadores, peritos, líder del caso.

Como se menciono anteriormente, es necesario que simultáneamente a estas etapas se realice en todas y cada una de ellas la documentación detallada y conservación de la cadena de custodia de la evidencia.

La cadena de custodia debe comenzar desde el momento que se llega a la escena del delito, donde se recomienda tomar fotografías o grabar videos de la evidencia, además de dejar registrado cada uno de los pasos realizados en cada una de las etapas propuestas, sobretodo dejando registro del día, hora, condiciones especiales, las personas que participaron y tuvieron cualquier tipo de contacto o control de la evidencia, hasta que se finalice la redacción del dictamen judicial, por otra parte se debe tener en cuenta la fragilidad de los medios de almacenamiento de datos y la volatilidad de la información. En este sentido, para mantener la cadena de custodia del material secuestrado, tal como lo describe el protocolo de actuación para pericias informáticas del poder judicial de la provincia de Neuquén (Neuquén, 2013) se hace necesario:

a) Se deben separar las personas que trabajen sobre los equipos informáticos lo antes posible y no permitirles volver a utilizarlos. Si es una empresa, se debe identificar al personal informático interno (administradores de sistemas, programadores, etc.) o a los usuarios de aplicaciones específicas que deban someterse a peritaje. Dejar registrado el nombre del dueño o usuarios del equipamiento informático ya que luego pueden ser de utilidad para la pericia.

Siempre que sea posible obtener contraseñas de aplicaciones, dejarlas registradas en el acta de allanamiento.

b) Se deben procurar fotografiar todos los equipos informáticos antes de moverlos o desconectarlos. Fotografiar una toma completa del lugar donde se encuentren los equipos informáticos, y fotos de las pantallas de las computadoras, si están encendidas. Excepcionalmente, si se debiera inspeccionar los equipos informáticos o material tecnológico en el lugar del hecho, puede ser conveniente realizar una filmación o bien una descripción del trabajo que se lleva a cabo ante los testigos.

c) Evitar tocar el material informático sin uso de guantes descartables. Dependiendo el objeto de la investigación, el teclado, monitores, mouse, CDs, DVDs, etc., pueden ser utilizados para análisis de huellas dactilares, ADN, etc. Si se conoce que no se realizarán este tipo de pericias puede procederse sin guantes.

d) Si los equipos están apagados deben quedar apagados, si están prendidos deben quedar prendidos y consultar con un especialista la modalidad de apagado (En caso de no contar con asesoramiento, proceder a apagarlos desenchufando el cable de corriente desde el extremo que conecta al gabinete informático). Si los equipos están apagados, desconectarlos desde su respectiva toma eléctrica y no del enchufe de la pared. Si son notebooks o netbooks es necesario quitarles la o las baterías y proceder a secuestrar los cables y la fuente de alimentación.

e) Identificar si existen equipos que estén conectados a una línea telefónica, y en su caso el número telefónico para registrarlo en el acta de allanamiento.

f) Impedir que nadie realice búsquedas sobre directorios o intente ver la información almacenada en los dispositivos ya que es posible que se altere y destruya evidencia digital (esto incluye intentar hacer una “copia” sin tener software forense específico y sin que quede documentado en el expediente judicial el procedimiento realizado).

g) Identificar correctamente todo el material tecnológico a secuestrar:

g.1) Siempre debe preferirse secuestrar únicamente los dispositivos informáticos que almacenen grandes volúmenes de información digital (computadoras, notebooks y discos rígidos externos). Respecto a DVD, CDs, pendrives, etc., atento a que pueden encontrarse cantidades importantes, debe evitarse el secuestro de este material si no se tiene una fuerte presunción de hallar la evidencia en estos medios de almacenamiento.

g.2) Rotular el hardware que se va a secuestrar con los siguientes datos:

Para computadoras, notebooks, netbooks, celulares, cámaras digitales, etc.: N° del Expediente Judicial, Fecha y Hora, Número de Serie, Fabricante, Modelo.

Para DVDs, CDs, Pendrives, etc: almacenarlos en conjunto en un sobre antiestático, indicando N° del Expediente Judicial, Tipo (DVDs, CDs, Pendrives, etc.) y Cantidad.

g.3) Cuando haya periféricos muy específicos conectados a los equipos informáticos y se deban secuestrar, se deben identificar con etiquetas con números los cables para indicar dónde se deben conectar. Fotografiar los equipos con sus respectivos cables de conexión etiquetados.

h) Usar bolsas especiales antiestática para almacenar discos rígidos y otros dispositivos de almacenamiento informáticos que sean electromagnéticos (si no se cuenta, pueden utilizarse bolsas de papel madera). Evitar el uso de bolsas plásticas, ya que pueden causar una descarga de electricidad estática que puede destruir los datos.

i) Precintar cada equipo informático en todas sus entradas eléctricas y todas las partes que puedan ser abiertas o removidas. Es responsabilidad del personal policial que participa en el procedimiento el transporte sin daños ni alteraciones de todo el material informático hasta que sea peritado.

j) Resguardar el material informático en un lugar limpio para evitar la ruptura o falla de componentes. No deberán exponerse los elementos secuestrados a

altas temperaturas o campos electromagnéticos. Los elementos informáticos son frágiles y deben manipularse con cautela.

k) Mantener la cadena de custodia del material informático transportado. Es responsabilidad del personal policial la alteración de la evidencia antes de que sea objeto de una pericia informática en sede judicial. No se podrá asegurar la integridad de la evidencia digital (por lo tanto se pierde la posibilidad de utilizar el medio de prueba) si el material informático tiene rotos los precintos al momento de ser entregado, siempre que no esté descripta en el expediente judicial la intervención realizada utilizando una metodología y herramientas forenses por profesionales calificados.

5.1.1. Asegurar la escena del delito

Como en cualquier investigación criminal, el primer paso dentro del proceso de investigación informática forense, es asegurar la escena del delito informático, para evitar la contaminación del lugar y poder documentar la condición original de la escena. Todo el personal que interviene debe estar capacitado y hacer el máximo esfuerzo para poder mantener asegurada y protegida dicha escena. El aseguramiento inicial de la escena precisa mantener en el estado original el espacio físico donde sucedió el hecho, con el propósito de evitar cualquier variación, adulteración, corrupción, destrucción, pérdida o robo de los elementos, huellas o indicios vinculados con el hecho.

En una investigación forense tradicional la escena del crimen es caracterizada conforme su aislamiento por lo que, según lo menciona Cristóbal Abdias (Abdias, 2014) se clasificada en dos tipos:

Escena Abierta: No tiene límites precisos, por lo que un ejemplo claro de una escena abierta seria la vía pública.

Escena Cerrada: Los límites son precisos, claramente identificables como paredes y el suelo. Un ejemplo claro de este tipo de escenas seria dentro de una oficina, una casa.

Un componente electrónico puede hallarse en cualquiera de estas escenas, pero en contraposición a la clasificación forense tradicional, algunos autores

sostienen que la escena de un delito informático puede clasificarse de la siguiente manera:

Escena virtual cerrada: Cuando la evidencia se halla en una escena tradicional abierta.

Escena virtual abierta: Cuando la evidencia se halla en una escena física tradicional cerrada.

Cuando se presume o se tiene seguridad de la ocurrencia de un hecho sospechoso, se debe bloquear el uso y acceso a todos los dispositivos, electrónicos, magnéticos u ópticos que puedan estar comprometidos. En la escena de un delito tradicional se procede a aislar dicha escena; en cambio para una escena virtual se deben aislar los elementos electrónicos considerando que los mismos pueden estar conectados en red, o conectados de manera remota.

Generalmente se recomienda que en la escena del delito, una vez identificados los dispositivos electrónicos, se proceda a retirar la alimentación eléctrica de forma inmediata, sin apagarla previamente en el caso de computadoras personales, en cambio si se trata de una notebook se apagará quitando la batería o el botón de energía.

Además se debe evitar contaminar la evidencia utilizando, encendiendo o apagando los dispositivos a secuestrar, de igual manera se debe evitar conectar una memoria (USB), ya que se estaría modificando la escena del delito introduciendo elementos ajenos al hecho en investigación.

Esta etapa la debe realizar el personal policial que posea al menos un mínimo conocimiento técnico, o en caso contrario debería realizar acompañado de un experto en informática forense. Se recomienda que la persona que tenga contacto con las pruebas sea un perito o un experto en informática, y sea éste quien se encargue de congelar la evidencia contenida dentro del dispositivo electrónico.

Para concluir esta etapa, podemos recomendar los siguientes pasos a seguir descriptos en el trabajo realizado por David González (González, 2003):

1. Identificar la escena del delito. Para ello se debe establecer un perímetro. Esto puede incluir una única sala, incluir varias salas e incluso varios edificios en los cuales el sospechoso hubiese estado trabajando con una compleja red de ordenadores.

2. Realizar una lista con los sistemas involucrados en el delito.

3. Restringir el acceso a la escena del delito, acceso tanto de personas como acceso de otros equipos informáticos.

4. Preservar toda huella digital, uso de guantes de látex.

5. Fotografiar, grabar y esquematizar la escena del delito. Si la información de una fotografía o grabación no es identificable, copiar manualmente la información observable.

6. Mantener el estado de los dispositivos.

6.1 Comprobar si el dispositivo está apagado, por ejemplo mirando los leds del dispositivo. Muchas veces el aparato puede estar en modo sleep, con protector de pantalla, etc.

6.2 Si el dispositivo está apagado y es un ordenador portátil, quitar la batería.

6.3 Si el dispositivo está encendido

6.3.1 Si el dispositivo tiene pantalla, fotografiar y grabar la misma.

6.3.2 Identificar las evidencias volátiles.

7. Desconectar las conexiones de red.

8. Comprobar y desconectar si existieran las conexiones inalámbricas que puedan permitir la activación de conexiones remotas.

9. Si hay impresoras imprimiendo, dejar que terminen de imprimir.

10. Anotar hora y fecha del sistema antes de apagarlo, documentándolo con fotografías o grabándolo en vídeo si es posible.

11. Los dispositivos encendidos apagarlos quitando la alimentación de la parte posterior del mismo, no del enchufe. Esto evita que se escriban datos en el

disco duro del aparato o en el sistema de almacenamiento del dispositivo, si éste tiene alguna protección frente a interrupciones de alimentación. NOTA: Apagando de esta forma se pierden algunas evidencias, pero se asegura la integridad de las evidencias no pérdidas.

12. Etiquetar cables y componentes

13. Fotografiar y grabar de nuevo los dispositivos con las etiquetas colocadas en los mismos.

5.1.2 Identificación y obtención de la evidencia

Antes de realizar cualquier allanamiento es necesario realizar una investigación excautiva del caso con el objeto de identificar con precisión la ubicación y características técnicas generales de los posibles elementos a secuestrar, conocer los datos, dónde podrían estar localizados y cómo podrían estar almacenados. Tal como lo menciona Santiago Acurio del Pino (Pino, 2009): " Debido a que la adquisición de datos puede involucrar un amplio abanico de dispositivos contenedores de información, que pueden abarcar desde un disquette o un disco rígido de una computadora hasta un conjunto de discos de un servidor, un juego de cintas, varias computadoras de una organización o un conjunto de dispositivos móviles (entre otros), es que antes de comenzar con el proceso de adquisición de datos es necesario realizar un reconocimiento y una correcta documentación de los diferentes tipos de evidencia que se debe adquirir, del sistema informático que se pretende analizar y también, se debe tener en cuenta cuál es el camino del delito, ya que no es lo mismo analizar un caso de homicidio que uno de fraude, por las características inherentes a cada uno de ellos.

Debido a la desventaja tecnológica con la que cuentan los operadores judiciales con respecto a los posibles delincuentes, la pericia informática conlleva tiempos elevados de trabajo y no es posible realizarla sobre grandes cantidades de elementos, por tal motivo debe evitarse el secuestro masivo de elementos informáticos, en especial CDs, DVDs, los que deberán ser enviados

a peritaje únicamente si se tienen presunciones con un alto grado de probabilidad de poseer la evidencia buscada.

Por otra parte, es necesario que el perito encargado de realizar la extracción de datos, tenga conocimientos mínimos, o lineamientos sobre el tipo de información es relevante para el caso, de esta manera el perito puede hacer foco en la información valiosa evitando pérdidas de tiempo.

Otro punto a tener en cuenta dentro de la identificación de evidencias digitales es la diferenciación entre evidencias volátiles y no volátiles.

Es esencial obtener las evidencias volátiles lo más pronto posible, para evitar la pérdida de información valiosa.

Además se debe tener en cuenta la clasificación de las evidencias en función del tipo de sistema o dispositivo donde se encuentren las mismas:

a) Computadoras personales o notebook

Podemos obtener evidencias en:

1. Monitores, teclados
2. Dongles (Mochilas).
3. Cámaras digitales o cámaras web.
4. Cintas de backups
5. Tarjetas
6. Discos duros, disquetes, CDs, DVDs.
7. Impresoras
8. Escáneres

b) Redes

Podemos obtener evidencias en:

1. Tarjetas de red de ordenadores.
2. Routers.
3. Hubs.
4. Switch.

5. Modems.

c) Redes inalámbricas

Podemos obtener evidencias en:

1. Tarjetas inalámbricas.
2. Puntos de accesos.

d) Dispositivos móviles:

Podemos obtener evidencias en:

1. Teléfonos móviles
2. Organizadores de mano (PDA, PocketPC, etc).

e) Sistemas embebidos

Podemos obtener evidencias en:

1. Memory Stick
2. Memory Cards (Smart Cards y Compact Flash)

Además se debe considerar el tipo de presunto delito que está siendo investigado por ejemplo, según el Instituto Nacional de Justicia de los Estados Unidos (Justice, U.S. Department of Justice Office of Justice Programs National Institute of Justice, 2004)

"En un caso de fraude se podría considerar el análisis de diferentes componentes perimetrales que no sean computadoras, como por ejemplo, tarjetas de crédito, informes, impresoras, scanners, etc…, sin embargo, en casos como la pornografía infantil, se debe establecer énfasis en otros objetos, como por ejemplo, en las cámaras digitales

Entonces luego de asegurar la escena del delito, la siguiente etapa del proceso de análisis forense da lugar a la identificación y captura de evidencias, el perito tiene la difícil tarea de descubrir qué datos pueden ser considerados como evidencias del delito en el proceso judicial, en qué lugar están ubicados y

donde están almacenados. Además el equipo forense deberá decidir que metodología utilizar, y que herramientas son las adecuadas para llevar a cabo la extracción.

5.1.3 Proteger la evidencia digital

Esta fase es la más importante y critica ya que cualquier error puede provocar la pérdida de evidencias, por lo que es imprescindible definir los métodos adecuados para el manejo, almacenamiento y etiquetado de las mismas. Una vez que se cuenta con todas las evidencias es necesario mantenerlas integras ya que podrán ser utilizadas como pruebas en un posible proceso judicial.

Por otra parte se requiere almacenar la evidencia en un ambiente adecuado para ello, por lo que se debe disponer de laboratorios especiales para investigar y analizar los componentes tecnológicos definidos.

De igual manera, es necesario tomar medidas para que el acceso a la evidencia sea muy restrictivo quedando claramente documentado, posibilitando detectar y pedir responsabilidades ante manipulaciones incorrectas, intentos de accesos no autorizados o que algún otro dispositivo electromagnético se use dentro de un determinado radio.

Recomendaciones para preservar las evidencias digitales:

1- Recoger primeramente las evidencias volátiles, y almacenarlas en lo posible dentro de otro dispositivo de almacenamiento, ajeno al dispositivo donde la evidencia obtenida, de esta manera se asegura la integridad de la evidencia original.

2- Desconectar las conexiones de red.

3- Comprobar la existencia de conexiones inalámbricas, en el caso de descubrir dichas conexiones, desconectarlas para evitar posibles conexiones remotas.

4- Si en la pantalla del dispositivo a secuestrar se identifica información que se considera relevante, se sugiere sacar una fotografía de la misma a la vez que se elabora un acta con dicha información.

5- Apagar los dispositivos encendidos, quitando la alimentación de la parte posterior del mismo, no del enchufe. Como así también se recomienda no apagar el dispositivo a través del sistema operativo.

6- Si se secuestran notebooks se le debe quitar la batería.

7- Identificar la evidencia digital de las copias.

8- Se aconseja que el análisis de la evidencia se realice sobre la capia, y no sobre la evidencia original.

9- Las copias se deben realizar de manera tal que el procedimiento asegure que la evidencia original no fue alterada.

10- Aplicar sobre la copia de la evidencia algún mecanismo de comprobación de integridad.

11- Si por algún motivo se debe trabajar sobre la evidencia original, extremar los recaudos para garantizar que la evidencia no sufrió alteraciones.

12- Si hay impresoras imprimiendo, dejar que terminen de imprimir.

13- Incluir en el acta de allanamiento las contraseñas identificadas, como así también cualquier otra información que se considere pueda ser relevante como hora y fecha del sistema antes de apagarlo, esto es importante ya que si la configuración de las propiedades de fecha y hora no son las correctas, los ficheros puede que no sean correspondientes con la fecha real.

14- Siempre que sea posible trabajar con zonas de tiempo GMT. El delito puede involucrar varias zonas de tiempo y usando GMT puede ser un punto de referencia que haga el análisis de las evidencias más sencillo.

15- Documentar quien fue el responsable de manipular la evidencia en cada una de las etapas, desde el momento de su secuestro, hasta el informe final.

16- Etiquetar con la descripción necesaria cada uno de los cables y componentes.

17- Fotografiar y grabar en lo posible cada uno de los pasos realizados durante el allanamiento y secuestro.

18- Rotular y detallar cada uno de los elementos secuestrados, evitando omitir información relevante.

19- Empaquetar los dispositivos que contiene las evidencias, con la información necesaria para poder identificarla.

20- Utilizar bolsas antiestáticas para los dispositivos que así lo requieran, como por ejemplo un disco duro.

21- Preservar las evidencias de factores externos tal como electricidad estática, calor, humedad.

22- Toda evidencia debe ser transportada a un lugar seguro y cerrado.

23- Se requiere la colaboración y compromiso de todo el equipo involucrado durante todas las etapas del proceso forense.

24- Documentar todos y cada uno de los pasos realizados durante todo el proceso forense.

5.1.3.1 Algunos Problemas

Que el personal involucrado no cuente con los conocimientos técnicos necesarios puede incurrir en la pérdida de datos probatorios fundamentales o la imposibilidad de analizar cierta información digital, perjudicando de esta manera la causa.

Otro aspecto crítico, donde se encuentran muchas veces grandes falencias, se refiere a la correcta rotulación y detalle de los elementos secuestrados. En la mayoría de los allanamientos no se rotulan todos los elementos secuestrados o las especificaciones técnicas son generales y poco detalladas.

5.1.4 Analizar de la evidencia

Luego de que ya se han realizado los procesos de identificación y preservación de las evidencias digitales, el siguiente paso es el Análisis Forense de dichas evidencias cuyo objetivo fundamental es la de restaurar con todos los datos disponibles, la cronología de los pasos realizados para cometer el delito hasta su descubrimiento. En esta instancia el campo de acción del perito se desarrolla principalmente dentro del laboratorio, y sus actividades permiten el asesoramiento científico para el juez.

En primer lugar, antes de comenzar el trabajo de esta etapa, cualquier elemento enviado para su análisis forense debería ser evaluado para verificar el estado del paquete y ante cualquier falla se debería informar y documentar las mismas.

El punto sensible en esta fase es ubicar la información relevante vinculada con una determinada causa, esta información debe ser analizada para posteriormente reconstruir la línea de tiempo. Este trabajo requiere la participación de un equipo interdisciplinario donde participe tanto el perito forense, quien aportara los conocimientos técnicos, como el operador judicial que aportara los conocimientos legales para poder determinar palabras claves de la investigación, ya que el análisis requiere un conocimiento profundo de lo que se está buscando y como obtenerlo.

Generalmente el concepto de evidencia digital está conformado por la información almacenada en los archivos y en los metadatos de esos archivos.

Dentro del conjunto de actividades a realizar para proceder con la extracción de información el perito debe:

- Utilizar más de una herramienta de extracción de información, con el objetivo de dar mayores garantías al proceso.
- Extraer información acerca del correo electrónico.
- Logs del sistema, ingresados al mismo.
- Identificación de volatilidad de la información más volátil a la menos volátil.
- Extracción de los datos y filtrado de los mismos.

- Identificar y recuperar datos que han sido: Eliminados, escondidos, cifrados, corruptos.
- Determinar líneas de tiempo o secuencia en que los eventos se presentaron.
- Evaluación del perfil del atacante.
- Construir un marco del caso en donde, de manera lógica y secuencial, se relaten los hechos identificados basados en los hallazgos.

El perito debe poder identificar:

- El tipo de datos a analizar.
- El tipo de evidencia física (ordenadores, dispositivos móviles, etc.).
- El tipo de delito (fraude, pornografía infantil, drogas, etc.)
- El tipo de dato, lógicamente accesibles, eliminados, ocultos, logs…
- El tipo de sistema operativo, y que datos analizar en cada uno.

5.1.5 Documentación y presentación de los resultados

El último paso del proceso de análisis forense, corresponde a la elaboración del dictamen que contiene toda la documentación y resultados de la investigación. En esta etapa es sumamente importante haber mantenido la cadena de custodia desde el primer contacto con la evidencia, ya que cualquier omisión o equivocación puede provocar la anulación de las pruebas. En esta presentación se detallan los resultados de los análisis realizados, los hechos, y los procedimientos utilizados y las conclusiones finales.

Es recomendable, generar un formulario en cada etapa para documentar todas las acciones realizadas y de esta manera asegurar la cadena de custodia, tal como lo menciona Miguel López Delgado (Delgado, 2007)

- Documento de custodia de la evidencia.
- Formulario de identificación los equipos y componentes.

- Formulario de incidencias tipificadas.
- Formulario de publicación del incidente.
- Formulario de recogida de evidencias.
- Formulario de discos duros.

Para que el documento final pericial sobre el análisis de datos sea objetivo, conciso y contenga los elementos necesarios para repetir el proceso en caso de ser necesario, es importante tener en cuenta algunas consideraciones como por ejemplo:

1- Utilizar certificaciones digitales para garantizar la autenticación e integridad del material informático.

2- Describir detalladamente de todos los pasos realizados durante la investigación.

3- Detallar el nombre y versión de las herramientas forenses utilizadas.

4- Dejar registro de todos los inconvenientes encontrados durante el análisis de la evidencia.

5- Detallar el estado inicial del material recibido por el perito.

6- No se deben tener en cuenta juicios de valor por parte de quien redacta el informe.

7- Debe ser claro, conciso, breve y simple para enlazar todos los hechos identificados.

8- Los argumentos, deben estar basados en las pruebas encontradas.

9- La caratula debe ser representativa del caso, y no se debe omitir indicar información relevante.

10- Los reportes sean entregados en medios no modificables.

El informe debe poseer como mínimo la siguiente estructura básica:

Introducción: Quién solicitó el informe, qué se buscó, quién escribió el informe, cuándo y qué fue encontrado.

- **Resumen de evidencias:** Qué evidencias fueron examinadas, cuándo, de dónde y cuándo se obtuvieron las pruebas.
- **Resumen de proceso:** Qué herramientas fueron utilizadas, qué datos fueron recuperados.
- **Examen de las evidencias**: Archivos de logs, tráficos de red o archivos.
- **Análisis**: Descripción del o los análisis realizados.
- **Conclusiones:** Resumen que se enlace lógicamente y se refiera a todas las evidencias recolectadas.
- **Glosario de términos:** Explicación de los términos técnicos utilizados.
- **Apéndices**: Relación de la evidencia encontrada de manera numerada y ordenada.
- **Cierre:** Esta última fase lo que busca es que en el lugar donde se revisó la información siga todos los protocolos definidos en cada una de las fases del análisis, de igual manera y siempre que sea posible se busca devolver las evidencias a sus respectivos dueños.

Capítulo VI

HERRAMIENTAS Y EQUIPOS PARA EL ANÁLISIS FORENSE

6.1 Herramientas

6.2 Análisis sobre las herramientas y equipos para la aplicación de la Informática Forense.

6.2.1 Herramientas para la Recolección de Evidencias:

6.2.1.1 Cuidados en la Recolección de Evidencia

6.2.2 Herramientas para el Monitoreo y/o Control de Computadores

6.2.3 Herramientas de Marcado de documentos

6.2.4 Herramientas de Hardware

6.3 Comparación de Herramientas

6.4 Dificultades del Investigador Forense

6.1 Herramientas

Las herramientas utilizadas en la informática forense, son la base principal para realizar la extracción y análisis de las evidencias digitales en los medios informáticos. Sin embargo, es necesario validar la confiabilidad de los resultados arrojados por dicha herramienta, como así también se debe tener presente la formación y conocimiento del perito que las utiliza. Estos dos elementos generan una constante reflexión y cuestionamiento por parte de los profesionales de la informática forense en el mundo.

6.2 Análisis sobre las herramientas y equipos para la aplicación de la Informática Forense.

Hasta el momento las herramientas y la guía o pasos que se deben tomar en el acontecimiento de un delito informático no se encuentran adecuadamente definidos, nuestra labor para esta tesis es proponer herramientas (software libre) y equipos óptimos que ayuden a realizar actividades válidas y certeras con la finalidad de obtener evidencias contundentes y ser presentadas en la corte.

Las herramientas presentadas se basaran en la clasificación descripta en el documento de investigación realizada por los autores Lopez, Amaya y León (Óscar López):

- Herramientas para recolección de evidencias.
- Herramientas para el Monitoreo y/o Control de Computadores.
- Herramientas de Marcado de documentos.
- Herramientas de Hardware.

6.2.1 Herramientas para la Recolección de Evidencias:

Existen una gran cantidad de herramientas para recuperar evidencia. El uso de herramientas sofisticadas se hace necesario debido a:

- La gran cantidad de datos que pueden estar almacenados en un computador.
- La variedad de formatos de archivos, los cuales pueden variar enormemente; aún dentro del contexto de un mismo sistema operativo.
- La necesidad de recopilar la información de una manera exacta, y que permita verificar que la copia es exacta.
- Limitaciones de tiempo para analizar toda la información.
- Facilidad para borrar archivos de computadores.
- Mecanismos de inscripción, o de contraseñas.

6.2.2 Herramientas para el Monitoreo y/o Control de Computadoras

Algunas veces se necesita información sobre el uso de los computadores, por lo tanto existen herramientas que monitorean el uso de las mismas, para poder recolectar información. Existen algunos programas simples como key loggers o recolectores de pulsaciones del teclado, que guardan información sobre las teclas que son presionadas, hasta otros que guardan imágenes de la pantalla que ve el usuario del computador, o hasta casos donde la máquina es controlada remotamente.

- Las herramientas no deben permitir que un dispositivo protegido sea modificado.
- La herramienta no evitará la obtención de cualquier información de o acerca de cualquier dispositivo.
- La herramienta no evitará ninguna operación sobre un dispositivo que no está protegido.

"KeyLogger" es un ejemplo de herramientas que caen en esta categoría. Es una herramienta que puede ser útil cuando se quiere comprobar actividad

sospechosa; guarda los eventos generados por el teclado, por ejemplo, cuando el usuario teclea la tecla de 'retroceder', esto es guardado en un archivo o enviado por e-mail. Los datos generados son complementados con información relacionada con el programa que tiene el foco de atención, con anotaciones sobre las horas, y con los mensajes que generan algunas aplicaciones.
Existen dos versiones: la registrada y la de demostración. La principal diferencia es que en la versión registrada se permite correr el programa en modo escondido. Esto significa que el usuario de la máquina no notará que sus acciones están siendo registradas

6.2.3 Herramientas de Marcado de documentos

Un aspecto interesante es el de marcado de documentos; en los casos de robo de información, es posible, mediante el uso de herramientas, marcar software para poder detectarlo fácilmente.

La seguridad está centrada en la prevención de ataques. Algunos sitios que manejan información confidencial o sensitiva, tienen mecanismos para validar el ingreso, pero, debido a que no existe nada como un sitio 100% seguro, se debe estar preparado para cualquier tipo de incidentes.

6.2.4 Herramientas de Hardware

Debido a que el proceso de recolección de evidencia debe ser preciso y no debe modificar la información se han diseñado varias herramientas para ello.

Las herramientas que se presentan serán evaluadas según los siguientes factores:

- Software libre o comercias.
- Características.
- Confiabilidad ante la recuperación de evidencias.
- Plataforma de trabajo.

Para la puesta en marcha en el manejo de evidencias digitales el forense o los forenses informáticos asignados a esta área, pueden apoyarse en determinadas herramientas que además de automatizar tareas, también le ayudaran a secuenciar sus pasos y a documentar cada uno de ellos.

6.3 Comparación de Herramientas

Se presenta mediante un cuadro comparativo y evaluado, las herramientas que poseen más cualidades que otras y son más recomendables.

Herramienta	Costo	Características	Plataforma
BACKTRACK 	Libre	• Es una de las más conocidas y apreciadas distribuciones GNU/Linux • Ocupa el puesto 32 en el famoso ranking de Insecure.org. • Se presenta como un LiveCD (no requiere de instalación) • Posee 300 herramientas de todo tipo (sniffers, exploits, auditoría wireless, análisis forense, etc) perfectamente organizadas.	GNU/Linux

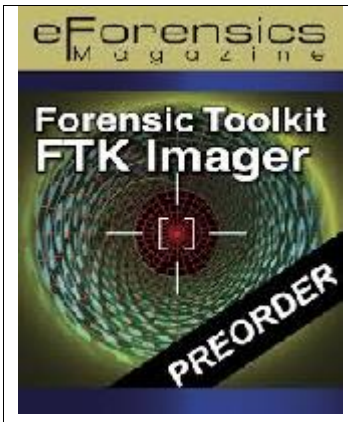
		• Los programas que trae este software ya vienen todos configurados y listos para ser usados	

Herramienta	Costo	Características	Plataforma
AUTOPSY	Libre	• Análisis de la línea de tiempo: muestra los eventos del sistema en una interfaz gráfica para ayudar a identificar la actividad. • Búsqueda por Palabra: módulos de extracción de texto e índice de búsquedas que permiten encontrar archivos mencionando términos específicos o patrones de expresiones regulares. • Artefactos Web: Extrae la actividad Web de los navegadores más habituales para ayudar a	Unix/Linux, Windows

		identificar la actividad del usuario. • Análisis del Registro: Usos RegRipper para identificar los documentos usados recientemente y dispositivos USB. • Análisis de correo electrónico: Analiza los mensajes de formato MBOX, como Thunderbird. • EXIF: Extractos de geo ubicación y la información de los archivos JPEG de la cámara. • Clasificación de tipo de Archivo: agrupa los ficheros por su tipo para encontrar todas las imágenes o documentos. • Soporte para reproducción: Ver vídeos e imágenes en la aplicación y no requiere un visor externo. • Análisis del sistema de archivos robusto: Soporte para sistemas de archivos comunes, incluyendo NTFS, FAT12, FAT16, FAT32, HFS +, ISO9660 (CD- ROM), Ext2, Ext3 y UFS de el Sleuth Kit.	

		• Filtrado de Hash Set: Filtrado de archivos buenos conocidos usando NSRL y la bandera de los archivos malos conocidos usando hashsets personalizados en HashKeeper , md5sum y formatos EnCase .	

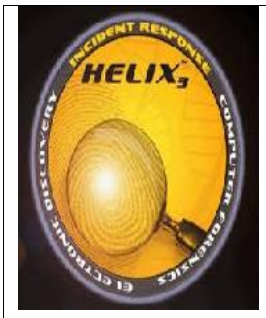
Herramienta	Costo	Características	Plataforma
FTK IMAGER	LIBRE	• Crea imágenes de discos duros, disquete, discos Zip, CD-ROMs, DVD-ROMs, carpetas o ficheros individuales. • Vista previa de los ficheros y carpetas en discos duros, disquete, discos Zip, CD-ROMs y DVD-ROMs. • Monta la imagen para visualizar el contenido de la imagen exactamente como el usuario con la unidad original. • Exportar ficheros y carpetas de imágenes	WINDOWS

		de disco. • Ver y recuperar ficheros que se han borrado desde la papelera de reciclaje, pero que aún no se han sobrescrito en la unidad. • Crear *hashes* de ficheros mediante dos funciones: MD5 y SHA-1. • Generar informes de hashes para fichero y para imágenes de disco para comprobar la integridad de los contenidos. El *hash* es la prueba de que los ficheros no se han alterado ni modificado en ningún caso.	

Herramienta	Costo	Características	Plataforma
ENCASE 	COMERCIAL	• Aumentar la confianza en los resultados mediante el uso de la probada, confianza, solución forense líder en la industria • Descubrir las posibles pruebas utilizando las funciones de búsqueda de avance • Mejorar la eficiencia mediante la automatización de tareas comunes de investigación • Formato de archivo de pruebas Preservar la integridad de la evidencia a la corte vetados • Resultados confiables – Los investigadores pueden tener confianza en sus resultados cuando se utiliza la probada, confianza, solución forense líder en la industria. • Potentes capacidades de búsqueda – Descubre las pruebas crítica utilizando funciones de búsqueda	WINDOWS

		avanzada para identificar los datos que serían irrecuperables con otras aplicaciones forenses equipo. • Mejora de la eficiencia mediante la automatización de tareas de investigación con EnScript ®; la extensión de script incorporado en EnCase ® Forensic. • EnCase Forensic datos conservas en un formato de archivo de pruebas (E01, L01, LX01, Ex01) con un récord sin igual de la aceptación de tenis. • Aprobado y examinados en los tribunales de todo el mundo.	

Herramienta	Costo	Características	Plataforma
HELIX	Libre	HELIX está basada en KNOPPIX. • Live CD. • Posee una variedad de herramientas para realizar un análisis forense tanto a equipos como imágenes de discos. • Para MS Windows posee un conjunto de herramientas de 90 Mb, permitiendo trabajar con sistemas vivos, y recupera información Volátil. • En el entorno Linux, dispone de un Sistema Operativo completo, con un núcleo modificado para conseguir una excelente detección de hardware. • No realiza el montaje de particiones swap, ninguna otra operación sobre el disco duro del equipo sobre el que se arranque.	Windows, Solaris, Linux

		• Es muy bueno para el análisis de equipos muertos, sin que se modifiquen las evidencias pues montará los discos que encuentre en el sistema en modo sólo lectura. • Contiene más y nuevas versiones de SleuthKit y Autopsy. • Su documentación no es amplia. • Permite elegir entre usar los kernels (2.4.26 o 2.6.5). • Tiene una excelente detección de hardware. • HELIX está pensado específicamente para no realizar ningún tipo de alteración sobre los sistemas en los que se usa. • Tiene una configuración autorun para Windows con herramientas para este SO.	

6.4 Dificultades del Investigador Forense

Durante la investigación realizada, pudimos detectar diferentes obstáculos con los que el perito forense se puede encontrar, por ejemplo:

1. Carencia de software especializado, o muchas veces el software con el que cuenta se encuentra obsoleto.

2. Puede encontrarse con datos dañados.

3. Si existen grandes volúmenes de datos, será difícil encontrar toda la información valiosa, por lo que es fundamental que el perito conozca los detalles de la causa para poder identificar dicha información.

4. Al tratarse de herramientas tecnologías, las mismas quedan obsoletas en poco tiempo por lo que es difícil ser 'experto' en una herramienta.

5. Cualquier error cometido puede anular la prueba.

6. Dificultad al conseguir el software y hardware para guardar, preservar y presentar los datos como evidencia.

Es por esto que, antes de lanzarse a ser un investigador forense, se necesita bastante estudio y experiencia, entre otras cosas, y si no se cumple con los requisitos, es aconsejable trabajar con un equipo interdisciplinario.

CAPÍTULO VIII

Ataques Informáticos

7.1 Vulnerabilidades del Sector Informático

7.2 Tipos de Atacantes

7.2.1 Hackers

7.2.2 Cracker

7.3 Tipos de siniestros

7.3.1 Difusión de pornografía

7.3.2 Manipulación de los datos

7.3.3 Manipulación de programas

7.3.4 Manipulación informática

7.4 Metodología de ataque

7.4.1 Identificación

7.4.3 Exploración

7.4.3 Enumeración

7.4.4 Obteniendo acceso

7.5 Prevenir ataques

7.1 Vulnerabilidades del Sector Informático

A pesar de los grandes avances tecnológicos, los sistemas informáticos siguen presentando grandes vulnerabilidades, es decir que poseen determinados aspectos débiles a través de los cuales pueden ser atacados y recibir algún tipo de daño en cualquiera de sus componentes Afectando el funcionamiento normal o previsto de dicho sistema informático.

En este sentido la **seguridad de un sistema informático** representa el estado de protección que posee el mismo, para evitar la aparición de las distintas amenazas posibles que puedan alterar su normal funcionamiento.

7.2 Tipos de Atacantes

A nivel mundial se han dado diferentes denominaciones a las personas o grupo de personas que aprovechan las vulnerabilidades y atacan los sistemas informáticos, algunas de ellas son:

7.2.1 Hackers

Son personas apasionadas a la informática que invierten esfuerzos más allá de los habituales y convencionales en la tarea que realizan. A pesar de que la palabra hacker esta estigmatizada socialmente asociado a algo malo, en realidad un hacker es una persona con un gran sentido de curiosidad, y utilizan esa virtud para detectar vulnerabilidades en los sistemas y evitar que personas maliciosas provoquen daño.

7.2.2 Cracker

Es aquella persona que haciendo gala de grandes conocimientos sobre computación y con un obcecado propósito de luchar en contra de lo que le está prohibido, empieza a investigar la forma de bloquear protecciones hasta lograr su objetivo. Los crackers modernos usan programas propios o muchos de los que se distribuyen gratuitamente en cientos de páginas web en Internet, tales como rutinas desbloqueadoras de claves de acceso o generadores de números

para que en forma aleatoria y ejecutados automáticamente pueden lograr vulnerar claves de accesos de los sistemas. Obviamente que antes que llegar a ser un cracker se debe ser un buen hacker. Asimismo se debe mencionar que no todos los hackers se convierten en crackers.
Se distinguen varios tipos de cracker:

PIRATA.:
Su actividad consiste en la copia ilegal de programas, rompiendo sus sistemas de protección y licencias. Luego distribuye los productos por Internet, a través de CD"s, entre otros.

LAMER:
Se trata de personas con poco conocimiento de informática que consiguen e intercambian herramientas no creadas por ellos para atacar ordenadores. Ejecutan aplicaciones sin saber mucho de ellas causando grandes daños.

PHREAKERS:
Son los crackers de las líneas telefónicas. Se dedican a atacar y "romper" los sistemas telefónicos ya sea para dañarlos o realizar llamadas de forma gratuita.

TRASHER: Su traducción al español es la de 'basurero'. Se trata de personas que buscan en la basura y en papeleras de los cajeros automáticos para conseguir claves de tarjetas, números de cuentas bancarias o información secreta para cometer estafas y actividades fraudulentas a través de Internet.

INSIDERS: Son los crackers 'corporativos', empleados de las empresas que las atacan desde dentro, movidos usualmente por la venganza. (Ingrid, 2008)

7.3 Metodología de ataque

Los ataques cometidos a un sistema pueden tener diferentes objetivos por ejemplo: fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados

internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red.

Conocer las metodologías de ataque utilizadas permite saber con qué soluciones contamos para prevenir, detectar y reparar un siniestro de este tipo.

7.4.1 Identificación

- Networks Scanners.- Realizan un escaneo de la red que les permite obtener información sin realizar un ataque, entre otras cosas descubren: dominios, servidores, sistemas operativos, los servidores activos, servidores de correo, entre otras rango de direcciones IP.

7.4.2 Exploración

PortsScanners.- Al igual que el punto anterior se realiza un escaneo, pero en este caso no de la red sino de los puertos de las maquinas, de esta manera detectan puertos abiertos, a fin de identificar posibles exposiciones o vulnerabilidades a explotar.

7.4.3 Enumeración

Obtención de usuarios válidos o recursos compartidos mal protegidos

7.4.4 Obteniendo acceso

PasswordsCrakers.- detectan configuraciones de usuarios y sus contraseñas de acceso validas.

7.5 Prevenir Ataques

"Todos podemos ser objeto de un delito informático sin importar si somos famosos o no. Y los peores no son los hurtos de fotos, sino el robo de identidad o el 'phising', como se llama cuando alguien se hace pasar por una autoridad bancaria para quedarse con tus datos", *señala Cristian Borghello, licenciado en Sistemas y director del portal Segu-info.*

Para evitar los diferentes tipos de ataques se pueden seguir algunas recomendaciones, como por ejemplo:

1- Mantener las máquinas seguras con un antivirus.
2- Instalar un firewall seguro y asegurase de que el mismo este funcionando correctamente.
3- Habilitar actualización automática de Windows. o descargar actualizaciones de Microsoft con regularidad para mantener su sistema operativo protegidos contra las vulnerabilidades conocidas.
4- Mantener personal especializado y capacitado en cuestiones de seguridad.
5- Aunque una máquina no contenga información valiosa, hay que tener en cuenta que puede resultar útil para un atacante, a la hora de ser empleada en un DoS coordinado o para ocultar su verdadera dirección.
6- No permitir el tráfico "broadcast" desde fuera de nuestra red. De esta forma evitamos ser empleados como "multiplicadores" durante un ataque Smurf.
7- Filtrar el tráfico IP Spoof.
8- No permitir la descarga de programas sospechosos.
9- Auditorias de seguridad y sistemas de detección.
10- Mantenerse informado constantemente sobre cada unas de las vulnerabilidades encontradas y parches lanzados.
11- Concientizar a los usuarios.

Conclusión

A través de la investigación realizada en este trabajo de tesis se ha puesto manifiesto lo siguiente:

- Hace ya varios años nuestro país trabaja para poder encuadrar dentro de la legislación nacional todos los delitos cometidos a través de medios informáticos.

- Si bien notamos que nuestro país ha tenido grandes avances con respecto a este tema, consideramos que es necesario además, educar y concientizar a la población sobre estos delitos para que los mismos sean denunciados, y de esta manera lograr que los abogados y la justicia en general se vean obligados a profundizar sobre esta problemática, que evoluciona constantemente y a pasos agigantados.

- La informática forense permite dar una estructura a la investigación, a través de un proceso de evaluación de la evidencia, para garantizar la valides de las pruebas ante la justicia.

En lo que respecta al objetivo planteado “Investigar y analizar las normas y guías de buenas prácticas más importantes utilizadas a nivel mundial para el tratamiento de la evidencia digital; concluimos lo siguiente:

- No existe un proceso que sea aceptado universalmente para llevar a cabo un análisis forense, lo cual puede tener origen en la falta de comunicación y de intercambio de ideas y conocimientos en la materia, por parte de las organizaciones internacionales dedicadas a la investigación forense digital.
- Los documentos estudiados parten del mismo inicio, un incidente de seguridad o delito y culminan con la explicación de los hechos que generaron ese incidente o delito, la diferencia radica principalmente en el

número de etapas y actividades mediante las cuales se lleva a cabo este proceso.

- Para llevar a cabo una investigación forense, lo más importante no es la metodología que se utilice, sino documentar cada paso dentro del proceso para mantener intacta la cadena de custodia. Por otra parte, y no menos importante es que cada actividad realizada sea probada, documentada, sustentada y alineada con las leyes vigentes.
- Existe un gran número de guías de buenas prácticas, normas, sin embargo el enfoque varía de acuerdo a la institución que lo aplica.

Además pudimos identificar las siguientes falencias a nivel nacional:

- Falta de profesionales con conocimiento informático y legal.
- Inexistencia de una metodología de trabajo regulada a nivel nacional.
- Perdida de pruebas por no haber realizado los procedimientos de la forma correcta.

Con respecto al objetivo planteado de “Elaborar una guía de buenas prácticas para la extracción de evidencia digital”, el mismo queda satisfecho ya que:

- En base al análisis de las guías de buenas prácticas utilizadas a nivel mundial, y tomando como referencia las mejores características de cada una de ellas se ha propuesto una metodología para el análisis forense en computadoras personales.
- La metodología permite la recolección, manejo y análisis de evidencia digital almacenada en computadoras personales.
- Al finalizar la investigación pudimos determinar que los pasos aplicados en la metodología son completamente independientes del sistema operativo con el cual se trabaje.
- Creemos que la metodología propuesta satisface las siguientes condiciones:

    Universal: fue generada en base a las consideraciones de las mejores prácticas internacionales.

Autocontenida; contiene todos los elementos necesarios para que una persona con un perfil informático pueda realizarla si sigue los pasos propuestos.

Formal; los resultados pueden ser reproducibles en caso de que se requiera su validación y admisibilidad ante la justicia.

Confiable; ya que pretende garantizar la cadena de custodia de la evidencia que se adquiere y custodia.

Procesos documentados; en todos y cada uno de los pasos para garantizar la cadena de custodia.

Además pudimos concluir lo siguiente:

- Si la evidencia es recolectada de manera adecuada habrá mayores posibilidades de establecer una ruta hacia los atacantes y contar con mayores elementos probatorios en caso de un posible juicio.
- Con la aplicación de una guía de procedimientos para la recolección de evidencias se obtendrá una consistencia de la evidencia y por lo tanto la valides de misma.
- Se debe mantener la evidencia intacta por lo cual se debe realizar en lo posible, una copia o backup de la misma.
- Unificar la metodología de trabajo, implica que todo el país trabaje de manera uniforme, permitiendo además compartir experiencias para lograr la mejora continua del proceso forense digital.
- Requerir de profesionales especializados motivaría a las instituciones educativas a ampliar sus ofertas educativas incluyendo el estudio de la ciencia forense informática.

El objetivo planteado “Seleccionar una herramienta open source que mejor se adapte a nuestra guía de buenas prácticas, garantizando la integridad de las evidencias”, se concluye que:

- Al finalizar de la investigación pudimos determinar que los pasos aplicados en la metodología son completamente independientes de las herramientas de software que se decida utilizar.

- De acuerdo a donde está contenida la evidencia que se quiere extraer, existen diferentes herramientas disponibles en el mercado, todas con buenos beneficios y similares características, por lo que en la mayoría de los casos queda a criterio del perito la selección de dicha herramienta, debido a esto no encontramos una única herramienta que se adapte a la metodología propuesta y por lo tanto la utilización de una u otra no contamina la prueba.

En lo que respecta al objetivo “Analizar e investigar herramientas de forensia informática open sourse, para la extracción y análisis de evidencia digital sobre computadoras personales”, concluimos lo siguiente:

- En el mercado actual existe una gran variedad de herramientas para el análisis forense de datos, pero queda en manos del perito forense saber que herramienta es la adecuada para cada caso específico
- Los costos de las licencias de las herramientas para el análisis forense pagas, son muy altos, lo que genera que muchas veces se opte por trabajar con herramientas open sourse.
- Falta de una herramienta de uso unificado a nivel nacional, hoy cada juzgado utiliza de manera independiente, la herramienta que pudo adquirir.
- El costo de las licencias muchas veces genera que la herramienta utilizada no sea la más actualizada en el mercado.

En lo que respecta al objetivo “Simular un caso práctico donde se realiza un dump de memoria de un dispositivo personal”, concluimos lo siguiente:

- Debido a la sensibilidad de la información, no pudimos acceder a realizar pruebas en un laboratorio sobre un caso real, por lo que tuvimos que realizar pruebas en base a supuestos.

- En un análisis forense es de vital importancia conseguir una copia exacta de la memoria RAM, debido a la volatilidad que implica el poder llegar a perder los datos si la alimentación fallase, la memoria RAM sólo almacenará datos cuando el sistema esté encendido. Es por esto que en nuestro trabajo práctico enfocamos como prioridad las primeras

acciones que deben realizar un perito informático para recolectar evidencias y analizarlo posteriormente sin alterar ningún dato.

- Después de realizar un dump de memoria, consideramos que una de las ventajas que tiene esta herramienta al ser en un entorno gráfico, es que cuando conseguimos hacer la copia, podemos examinar el valor de la misma y así ver por ejemplo algún password que haya quedado almacenada en la memoria RAM al loguearnos en algún portal, los procesos que estaban abiertos y las conexiones activas.

Del objetivo “Interpretar los resultados de la extracción de evidencia digital”, concluimos lo siguiente:

- Se han expuesto las diferencias a la hora de llevar a cabo un análisis forense en dos de los sistemas operativos más extendidos, Windows y UNIX/Linux, se pre visualizaron pruebas, archivos de evidencia de las exportaciones, se crearon imágenes forenses, dump de memoria ram, recuperar archivos de extensión BMP, GIF, JPEG, EMF, PDF, HTML y documentos de Microsoft Office, se crearon informes, se utilizo palabras clave de búsqueda de expresiones regulares, se recolecto contraseñas, se realizo copias físicas o clonado forense bit a bit, por medio de hash se autentifico la evidencia, se logro conocer y operar una de las herramientas más utilizadas por los investigadores y expertos forenses informáticos de todo el mundo,

Citas Bibliográficas

Abdias, C. (27 de 06 de 2014). *La escena del crimen y criminalística.* Recuperado el 2015, de http://es.slideshare.net/abdiasjove/la-escena-del-crimen-y-criminalstica

Ariel Podestá, B. C. (2013). *http://redi.ufasta.edu.ar/.* Recuperado el 2015, de REDI - Universidad FASTA: http://redi.ufasta.edu.ar/xmlui/handle/123456789/427

Association of Chief Police Officers, A. (10 de 2003). Recuperado el 2015, de Good Practice Guide for Computer-Based Electronic Evidence: http://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence[1].pdf

Bloj, Y. (14 de 09 de 2011). *www.diariojudicial.com/.* Recuperado el 2015, de http://www.diariojudicial.com/documentos/2011_Setiembre/Nx_143_-_R_J_E_-.pdf

Campos, F. (17 de 03 de 2008). *La relevancia de la custodia de la evidencia en la investigación judicial.* Obtenido de http://enj.org/web/biblioteca-docman/search_result.html

Cano Martines Jeimy José, M. G. (04 de 2005). *Revista de Derecho, Comuniaciones y nuevas tecnologias.* Recuperado el 2015, de www.derechoytics.uniandes.edu.co: https://derechoytics.uniandes.edu.co/components/com_revista/archivos/derechoytics/ytics90.pdf

Ciardhuáin, S. Ó. (2004). An Extended Model of Cybercrime Investigations. *An Extended Model of Cybercrime Investigations - https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf*, (pág. 22).

CIBERDELINCUENCIA, C. S. (6 de 2001). *CONVENIO SOBRE LA CIBERDELINCUENCIA.* Recuperado el 2015, de http://www.agpd.es/portalwebAGPD:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf

Ciberdelincuencia, C. S. (23 de 11 de 2001). *http://www.coe.int/.* Recuperado el 2015, de http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF

Clark, B. a. (24). A Hierarchical, Objectives-Based Framework for the Digital Investigations Process. *Digital Investigations Process Framework - http://www.dfrws.org/2004/day1/Beebe_Obj_Framework_for_DI.pdf*, (pág. 17). Baltimore, Maryland.

Delgado, M. L. (06 de 2007). *"Análisis Forense Digital".* Recuperado el 10 de 08 de 2015, de http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

(2001). *DFRWS. A Road Map for Digital Forensics Research. Digital Forensics Research Workshop.* New York. : Utica.

Ghosh, A. (3 de 2004). *Guidelines for the Management of IT Evidence.* Recuperado el 2015, de http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf

Gómez, L. Á. (s.f.). *Ministerio de Seguridad - República Argentina*. Recuperado el 10 de 08 de 2015, de http://www.minseg.gob.ar/node/1050

González, D. (7 de 11 de 2003). *http://cp4df.sourceforge.net/.* Recuperado el 2015, de CÓDIGO DE PRÁCTICAS PARA DIGITAL FORENSICS: http://cp4df.sourceforge.net/flashmob03/doc/03-Metodologia-rev3.pdf

Guariglia, F. (2005). *"Concepto, fin y alcance de las prohibiciones de valoración probatoria en el procedimiento penal. Una propuesta de fundamentación".* Buenos Aires: Editores del Puerto.

Ingrid, P. p. (08 de 09 de 2008). *Hackers y Crackers*. Recuperado el 2015, de http://hackersycrackers-yi.blogspot.com.ar/2008_09_01_archive.html

Institutes, E. N. (20 de 04 de 2009). *http://www.enfsi.eu/.* Recuperado el 2015, de Guidelines for best practice in the forensic examination of digital technology:

http://es.scribd.com/doc/171509237/ENFSI-Forensic-It-Best-Practice-Guide-v6-0#scribd

IOCE, T. F. (4 de 2002). *The FBI Federal Bureau of Investigation*. Recuperado el 03 de 2015, de IOCE, Guidelines for the best practices in the forensic examination of digital technology.: https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/

ISO. (15 de 10 de 2012). *www.iso.org*. Recuperado el 10 de 2015, de http://www.iso.org/iso/catalogue_detail?csnumber=44381

Justice, U. D. (04 de 2004). *U.S. Department of Justice Office of Justice Programs National Institute of Justice.* Recuperado el 2015, de Forensic Examination of Digital Evidence: A Guide for Law Enforcement: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Justice, U. D. (04 de 2008). *www.ncjrs.gov.* Recuperado el 2015, de Electronic Crime Scene Investigation:A Guide for First Responders, Second Edition: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

Karen Kent, S. C. (8 de 2006). *Guide to Integrating Forensic Techniques into Incident Response.* Recuperado el 2015, de http://www.ncjrs.gov: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

Kent, K. (2006.). *"Guide to integranting forensic techniques into incident response", NIST Special Publication 800-86.*

Kozushko, H. (23 de 11 de 2003). *Digital Evidence.* Recuperado el 2015, de ttp://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/DigitalEvidencePaper.pdf

Mark Reith, C. C. (2002). An Examination of Digital Forensic Models International Journal of Digital Evidence Fall 2002, Volume 1, Issue 3 . *International Journal of Digital Evidence - http://digital4nzics.com/Student%20Library/An%20Examination%20of%20Digital%20Forensic%20Models.pdf* (pág. 12). Wright-Patterson AFB, OH 45433-7765.

METHODOLOGY, D. F. (22 de 8 de 2007). *The United States Departament of Justice.* Recuperado el 2015, de The United States Departament of Justice:

http://www.justice.gov/sites/default/files/criminalccips/legacy/2015/03/26/forensics_chart.pdf

Neuquén, P. J. (05 de 07 de 2013). *Pericias Informaticas.* Recuperado el 2015, de Protocolo de Actuación para Pericias Informáticas: http://periciasinformaticas.sytes.net/index.php?option=com_docman&task=cat_view&gid=39&Itemid=59

ONU. (10 al 17 de 04 de 2000). *Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente.* Recuperado el 2015, de http://www.un.org/es/conf/xcongreso/prensa/2088hs.shtml

Óscar López, H. A. (s.f.). *Universidad de Los Andes Bogotá, Colombia .* Obtenido de INFORMÁTICA FORENSE : GENERALIDADES,ASPECTOS TÉCNICOS Y HERRAMIENTAS : http://luctus.es/wp-content/uploads/2010/06/CIBSI02_ba2.pdf

Pericial, I. (2005). *Informática Pericial.* Recuperado el 2015, de http://periciasinformaticas.sytes.net/index.php?option=com_content&view=article&id=188:jurisprudencia-nulidad-de-pericia-informatica-por-fallas-en-la-cadena-de-custodia&catid=45:articulos-para-abogados-y-personal-judicial&Itemid=63

Pino, S. A. (07 de 07 de 2009). *Organization of American States.* Obtenido de Manual de Manejo de Evidencias Digitales y Entornos Informáticos v 2.0: http://www.oas.org/juridico/english/cyb_pan_manual.pdf

Ray, D. A. *Models of Models: Digital Forensics and Domain-Specifc Languages.*

seguridadinformaticaufps. (s.f.). *https://seguridadinformaticaufps.wikispaces.com*. Obtenido de Seguridad Informatica: https://seguridadinformaticaufps.wikispaces.com/Definicion,+Leyes,+Sanciones+y+Tipificacion+de+los+DELITOS+INFORMATICOS

SEIJAS, A., & CARLOS ALBERTO GONZÁLEZ, J. M. (18 de 05 de 2011). *http://www.diariojudicial.com.* Recuperado el 2015, de http://www.diariojudicial.com/documentos/2011_Mayo/Fallo_-_pornografxa_infantil.pdf

TÉLLES VALDEZ, J. (1996). *Derecho Informático. 2° Edición.* México: Mc Graw Hill.

Zuccardi, J. D.-G. (11 de 2006). *google doc.* Recuperado el 08 de 2015, de https://docs.google.com/document/d/1_uCOcecybF3sQMC_ApE373xob9xyXLx2CWZfrzxBwoY/edit?pli=1

Bibliografía

IOCE, Guidelines for the best practices in the forensic examination of digital technology. Tomado de: http://www.ioce.org/2002/ioce_bp_exam_digit_tech.html

(Guariglia, Fabricio "Concepto, fin y alcance de las prohibiciones de valoración probatoria en el procedimiento penal. Una propuesta de fundamentación", Editores del Puerto, Buenos Aires, 2005, pág. 124)

Cano Martines Jeimy José, Mosquera González José Alejandro, Certain Jaramillo Andrés Felipe. Evidencia Digital: contexto, situación e implicaciones nacionales. Abril de 2005.

Campos, Federico: La Relevancia De La Custodia De La Evidencia En La Investigación Judicial, 31 de Agosto 2010, http://enj.org/portal/biblioteca/penal/la_prueba_proceso_penal/2.pdf

Acurio del Pino, Santiago: Manual de Manejo de Evidencias Digitales y Entornos Informáticos v 2.0, 7 de Julio 2009, http://www.oas.org/juridico/english/cyb_pan_manual.pdf

Justice, U. D.: Forensic Examination of Digital Evidence: A Guide for Law Enforcement, Abril 2004, http://nij.gov/nij/pubs-sum/199408.html

Kleiman, Dave: The Official CHFI Exam 312-49 Study Guide for Computer Hacker Forensics Investigators, 2007.

Campos, Federico: La Relevancia De La Custodia De La Evidencia En La Investigación Judicial, 31 de Agosto 2010, http://enj.org/portal/biblioteca/penal/la_prueba_proceso_penal/2.pdf

TheNational Center forForensicsScience: Digital Evidence in theCourtroom: A GuideforPreparing DigitalEvidenceforCourtroomPresentation, 12 de Diciembre 2003,

http://www.classstudio.com/scaltagi/papers/grad_papers/forensics/Palmer/digital_evidence_in_courtroom.pdf

Artículos

- www.federicoarnaboldi.com.ar
- www.delitosinformaticos.com.
- http://sebastiangomez.sytes.net
- www.cysi.com.ar
- www.rdynt.com.ar
- http://periciasinformaticas.sytes.net/index.php?option=com_content&view=article&id=164:estafas-e-internet&catid=45:articulos-para-abogados-y-personal-judicial&Itemid=63

- http://periciasinformaticas.sytes.net/index.php?option=com_content&view=article&id=166:jurisprudencia-pornografia-infantil&catid=45:articulos-para-abogados-y-personal-judicial&Itemid=63
- http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/DigitalEvidencePaper.pdf
- https://www.ncjrs.gov/pdffiles1/nij/219941.pdf
- https://www.ncjrs.gov/pdffiles1/nij/178280.pdf
- http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf
- http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf
- https://www.segu-info.com.ar/delitos/tiposdelito.htm
- http://www.iso.org/iso/catalogue_detail?csnumber=44381
- www.cepal.org
- http://sans.org /top20

Anexo A

Aplicación de herramientas al Análisis Forense

1. Herramienta FTK

1.1 FTK IMAGER VOLCADO DE MEMORIA RAM

1.1.1 Analizaremos los datos en una memoria RAM antes de apagar o reiniciar el PC.

1.1.2 Montar un dump de memoria RAM, como una unidad física, para obtener archivos recuperados.

1.2 FTK IMAGER CREAR IMAGEN FORENSE DE UNA UNIDAD FISICA.

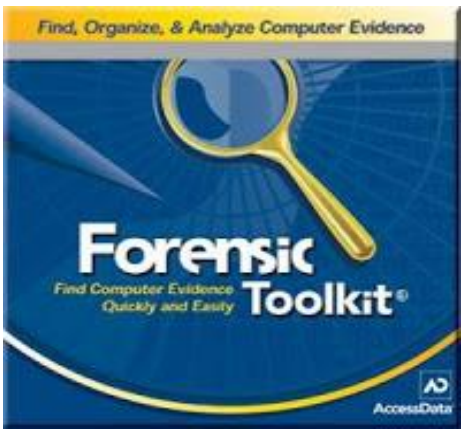
1.2.1 Crear una copia de imagen del disco USB y poder recuperar archivos eliminados

1.3 BACK TRACK 5

1.3.1 Recuperar Imágenes Borradas de un USB

1. Herramienta FTK

FTK Imager es una herramienta de análisis forense disponible en la Web de AccessData, es un paquete gratuito, que pueden descargar los usuarios de FTK AccessData. El atributo más importante de FTK Imager es que permite varios formatos para la creación de imágenes. Forensic Toolkit (FTK) es una herramienta reconocida alrededor del mundo como el estándar en software forense de computadoras. Esta plataforma digital de investigaciones, validada por la corte internacional como última tecnología de análisis forense de computadoras, descifrado de contraseña y de información, todo ello en una interfaz intuitiva y personalizable. FTK 3 ha sido construido con la velocidad, análisis y escalabilidad que la clase empresarial requiere. Conocido por su interfaz intuitiva, el análisis de correo electrónico, vistas personalizables de datos y la estabilidad, FTK establece el marco para una expansión sin problemas, por lo que el equipo forense puede crecer con su organización. El kit de herramientas forenses es ahora el equipo más avanzado en software de análisis forense, proporcionando una funcionalidad que normalmente sólo las organizaciones con decenas de miles de dólares podrían pagar. Sin embargo, estamos comprometidos en hacer que nuestra tecnología esté a disposición de todos los investigadores y analistas, ya sea en cumplimiento de la ley, la educación, una agencia gubernamental, una empresa o la realización de investigaciones digitales como proveedor de servicios de informática forense.



Forensic Toolkit (FTK) es una herramienta reconocida alrededor del mundo como el estándar en software forense de computadoras. Esta plataforma digital de investigaciones, validada por la corte internacional como última tecnología de análisis forense de computadoras, descifrado de contraseña y de información, todo ello en una interfaz intuitiva y personalizable. FTK 3 ha sido construido con la velocidad, análisis y escalabilidad que la clase empresarial requiere. Conocido por su interfaz intuitiva, el análisis de correo electrónico, vistas personalizables de datos y la estabilidad, FTK establece el marco para una expansión sin problemas, por lo que el equipo forense puede crecer con su organización. El kit de herramientas forenses es ahora el equipo más avanzado en software de análisis forense, proporcionando una funcionalidad que normalmente sólo las organizaciones con decenas de miles de dólares podrían pagar. Sin embargo, estamos comprometidos en hacer que nuestra tecnología esté a disposición de todos los investigadores y analistas, ya sea en cumplimiento de la ley, la educación, una agencia gubernamental, una empresa o la realización de investigaciones digitales como proveedor de servicios de informática forense.

Con Ftk imager podemos:

- Crear imágenes forenses de Discos duros, Cds, Dvds, USBs, carpetas, archivos.
- Pre visualizar archivos y carpetas de los mismos.
- Pre visualizar el contenido de las imágenes forenses almacenadas.
- Montar una imagen forense y visualizar en solo lectura permitiendo ver los contenidos.
- Exportar archivos o carpetas de las imágenes forenses.
- Recuperar archivos o carpetas de las imágenes forenses.
- Recuperar archivos borrados.
- Crear hashes de archivo utilizando Md5 o Sha -1
- Generar reportes de hashes para archivos regulares e imágenes.

Ftk imager fue desarrollado por Accesdata Forensics Toolkit que es una plataforma donde podemos realizar investigaciones forenses digitales de una manera rápida, estable y fácil de usar.

Link para descargar el software open source:

http://www.accesdata.com

Ingresamos a producto> download > seleccionamos el software Ftk Imager.

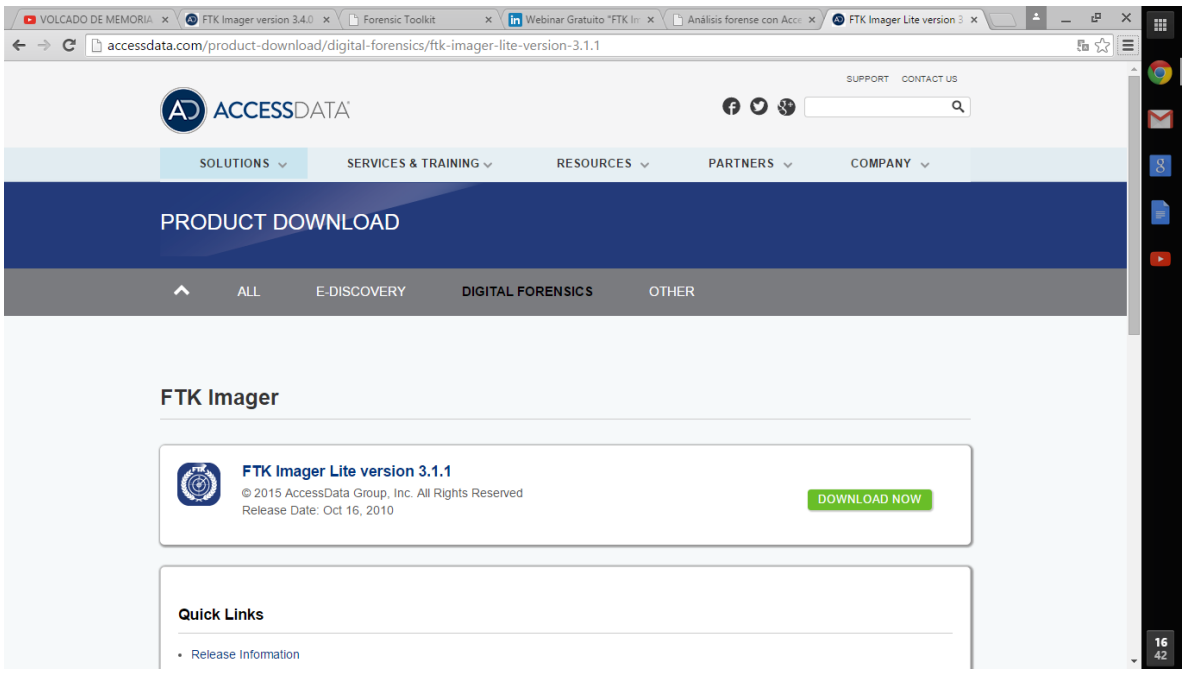


Figura 1.1 Pagina web de Accesdata.

Completamos el siguiente formulario donde nos pide el email.

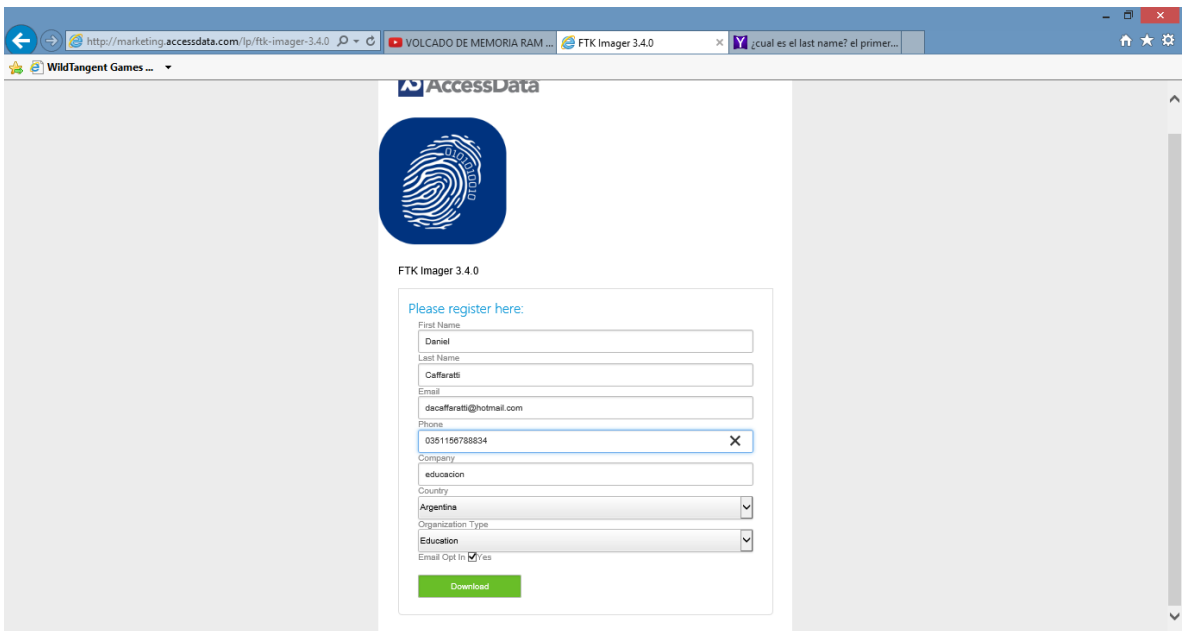


Figura 1.2 formulario.

Descargamos el link que nos llega por correo electrónico.

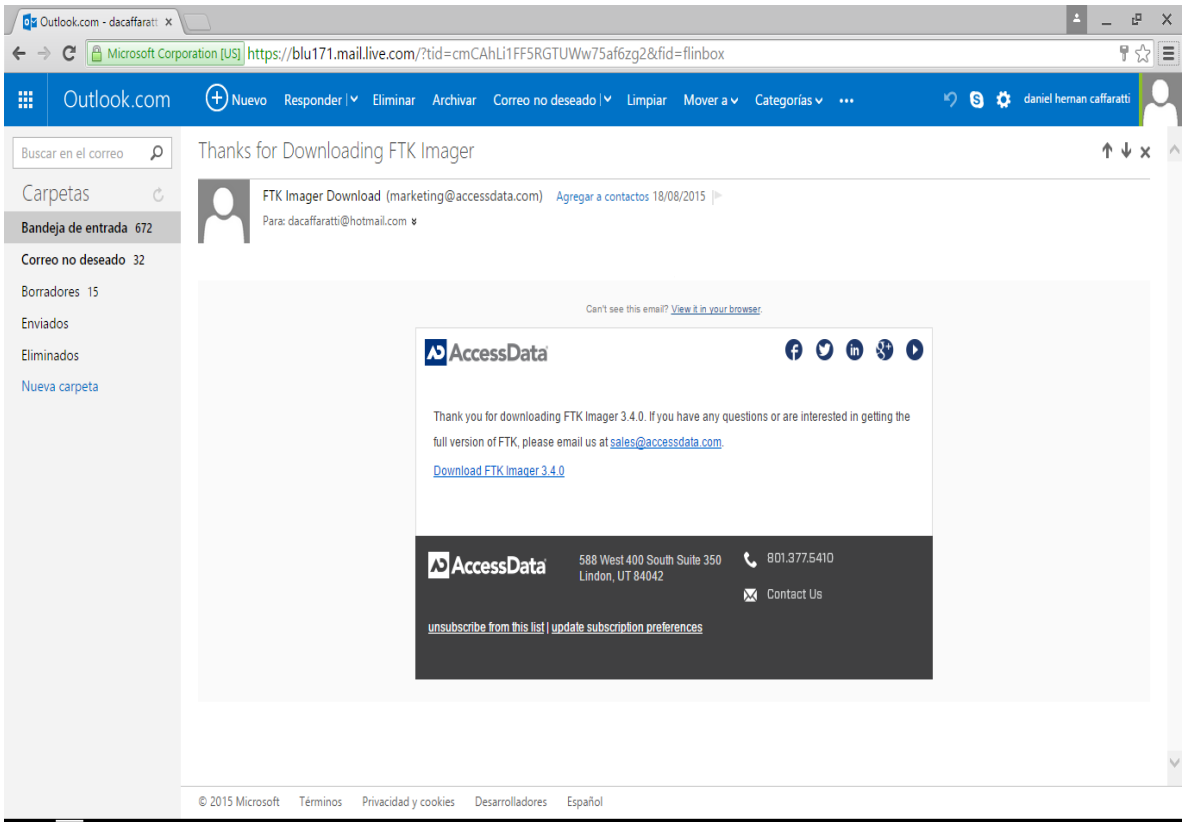


Figura 1.3 link de descarga.

Instalamos el software ftk imager > next (siguiente)

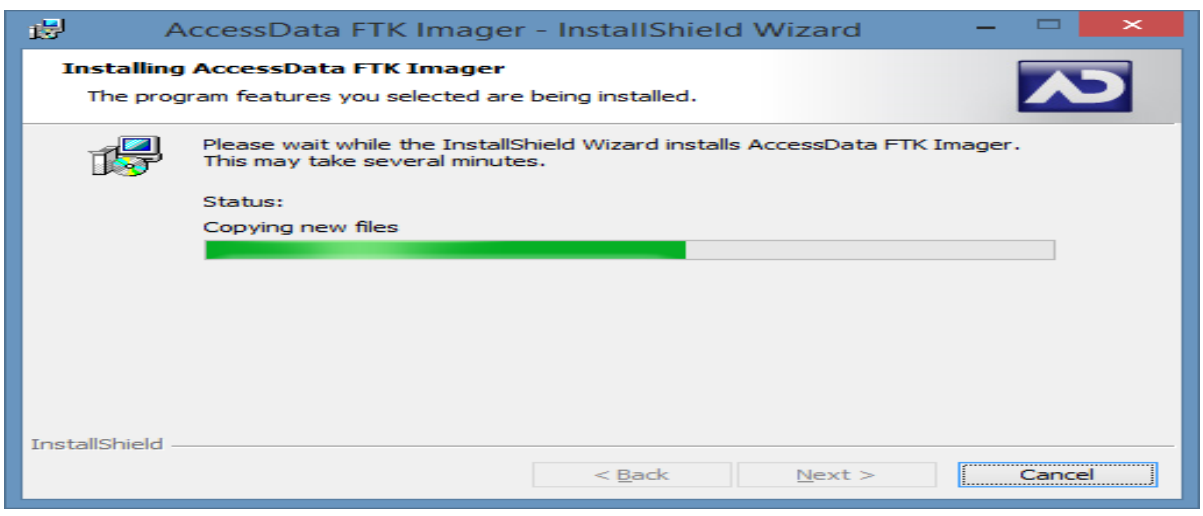


Figura 1.4 Instalación

1.1 FTK IMAGER VOLCADO DE MEMORIA RAM:

1.1.1 Analizaremos los datos en una memoria RAM antes de apagar o reiniciar el PC.

Abrimos el programa Ftk imager, seleccionamos en el menú File>Capture Memory. (captura de memoria) > enter.

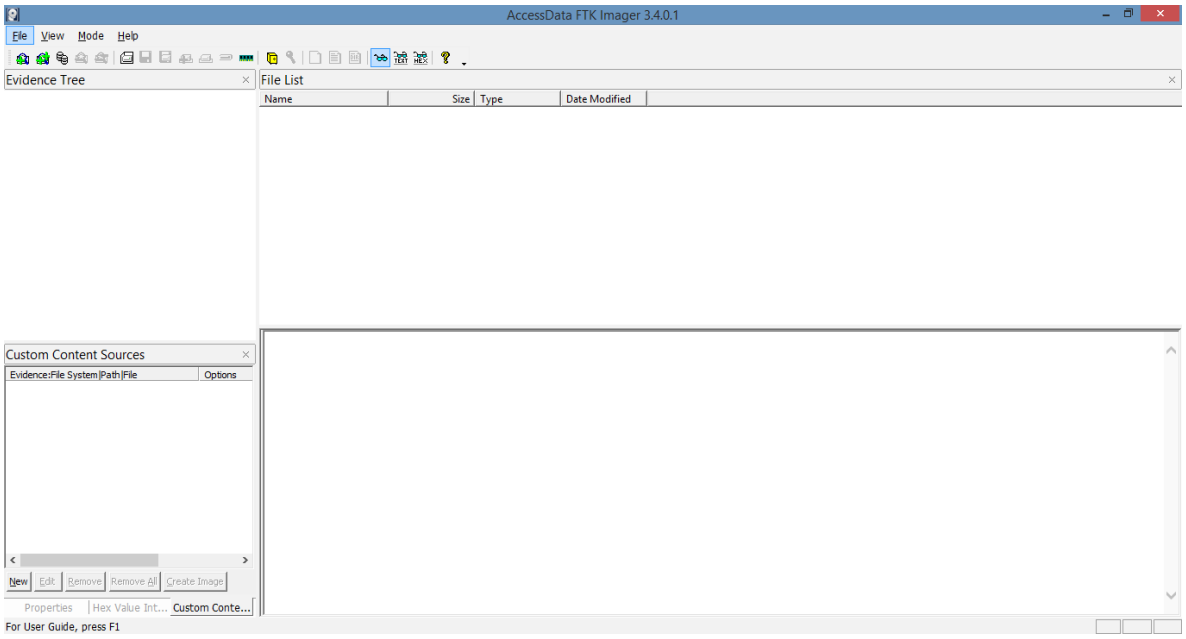


Figura 1.5 software Ftk imager.

Nos abre la siguiente pantalla.

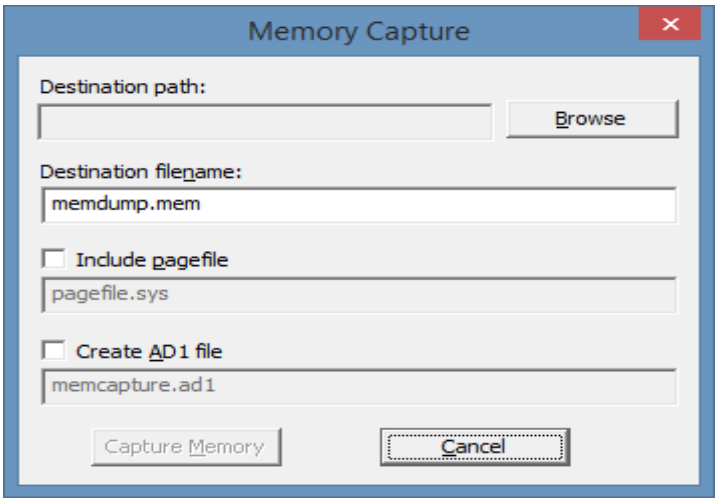


Figura 1.6 Capture Memory.

Seleccionamos la ruta donde se guardara la captura de la memoria. En este caso la unidad es " C: \ Users\ danielhernan\Desktop. Hacemos clic en capturar memoria.

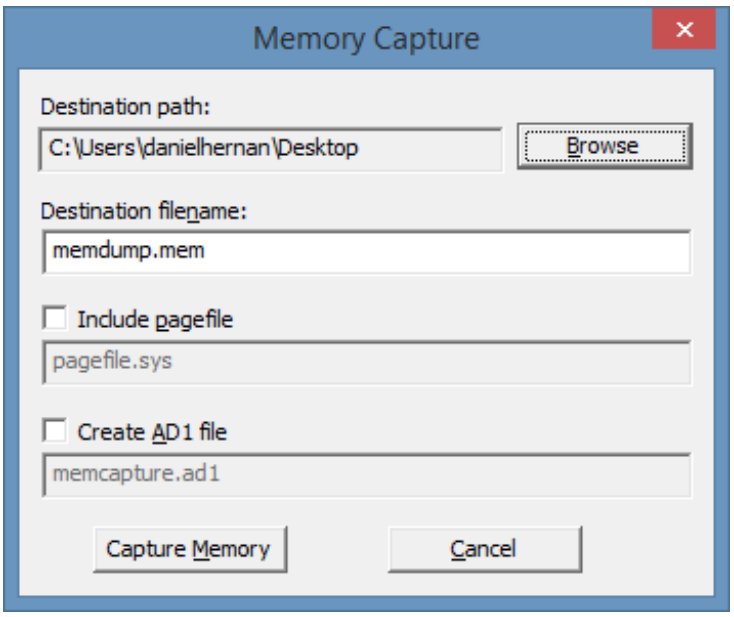


Figura 1.7 Path Capture Memory

Proceso de volcado de memoria.

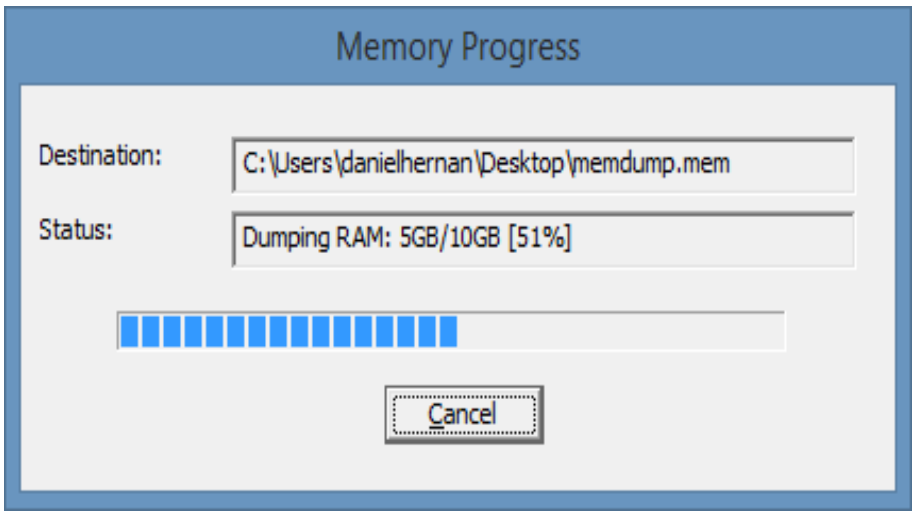


Figura 1.8 Progress Memory

Se genera el archivo de volcado de memoria memdump.men

Figura 1.9 Escritorio de Pc.

Abrimos el Ftk imager menu> file >Add evidence Item (elemento de evidencia)> enter.

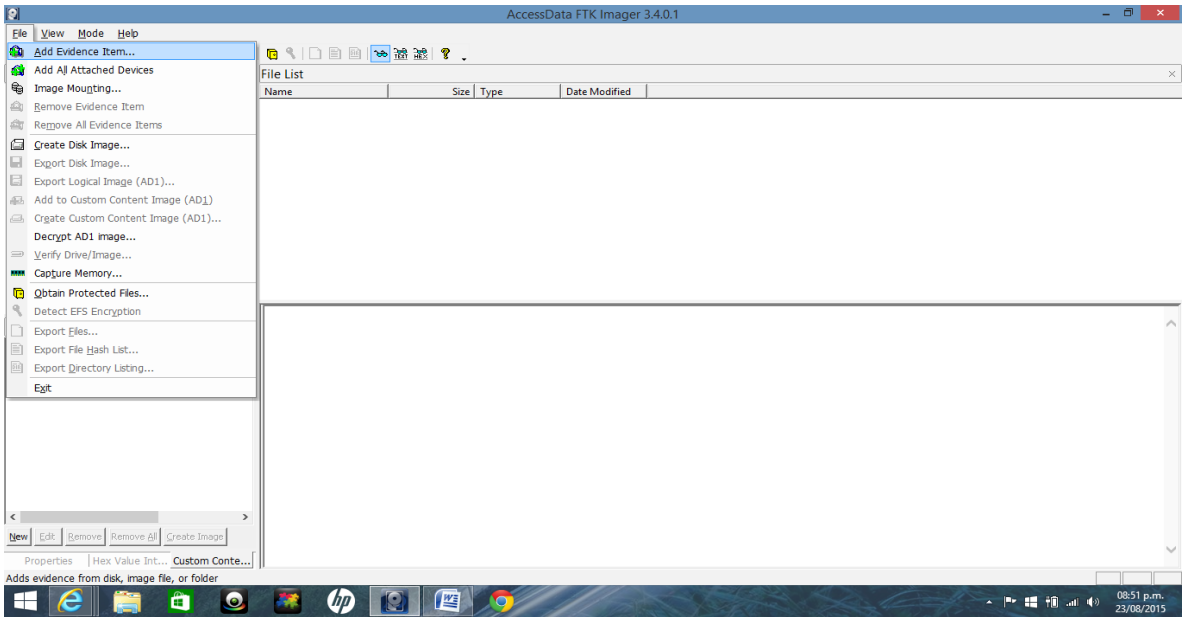


Figura 2.0 Software Ftk Imager.

Seleccionamos > Image file (archivo de imagen)

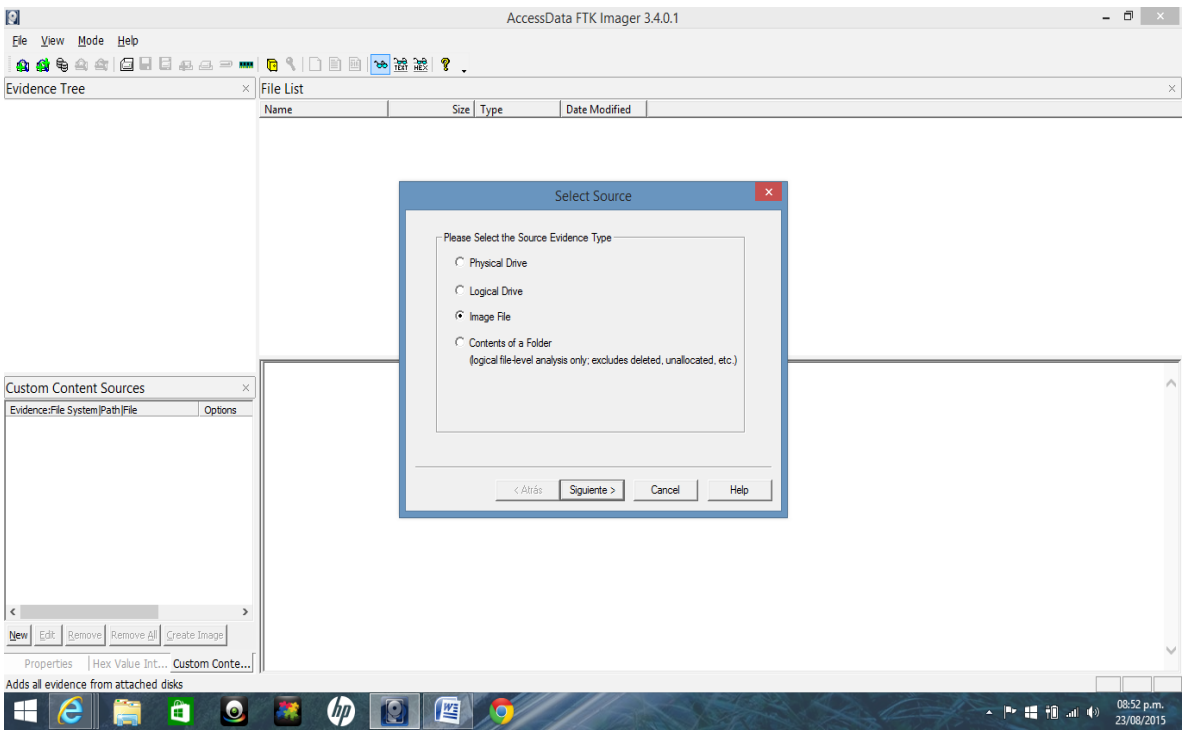


Figura 2.1 Select Source.

Seleccionamos el archivo antes generado, memdump.mem > abrir.

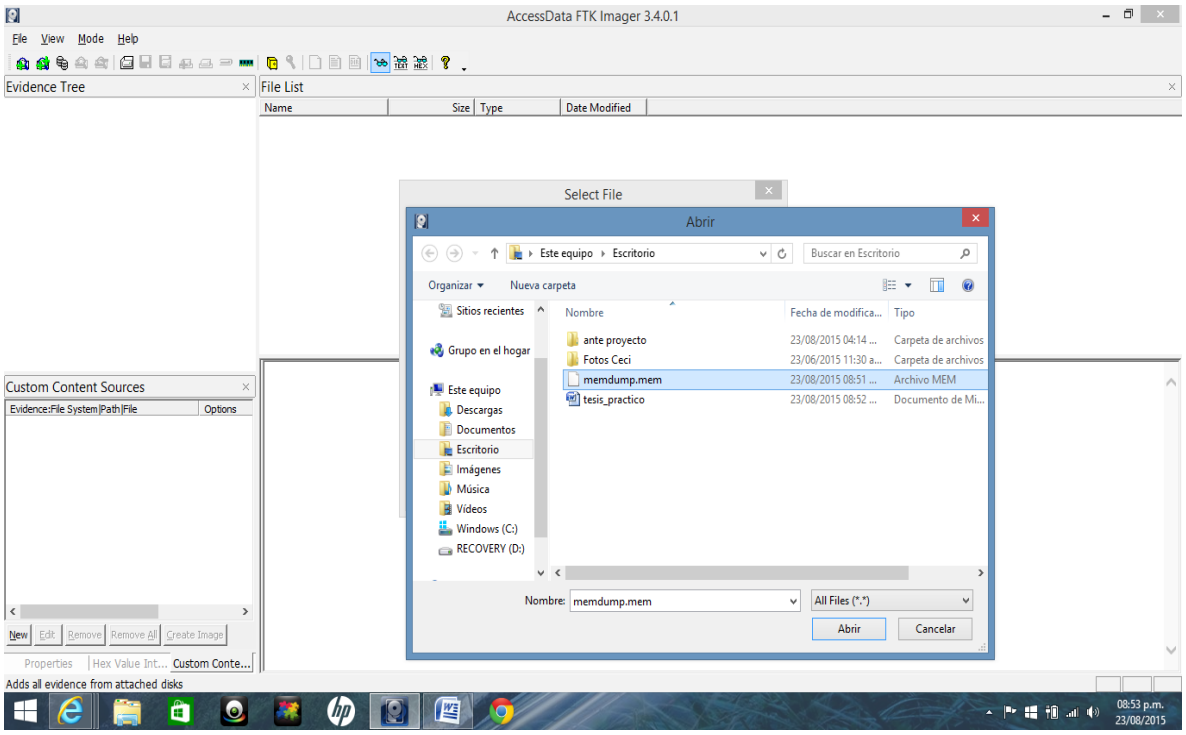


Figura 2.2 Select File.

En la siguiente pantalla nos va a figurar el path: C:\Users\danielhernan\Desktop\memdump.men> seleccionamos Finish...

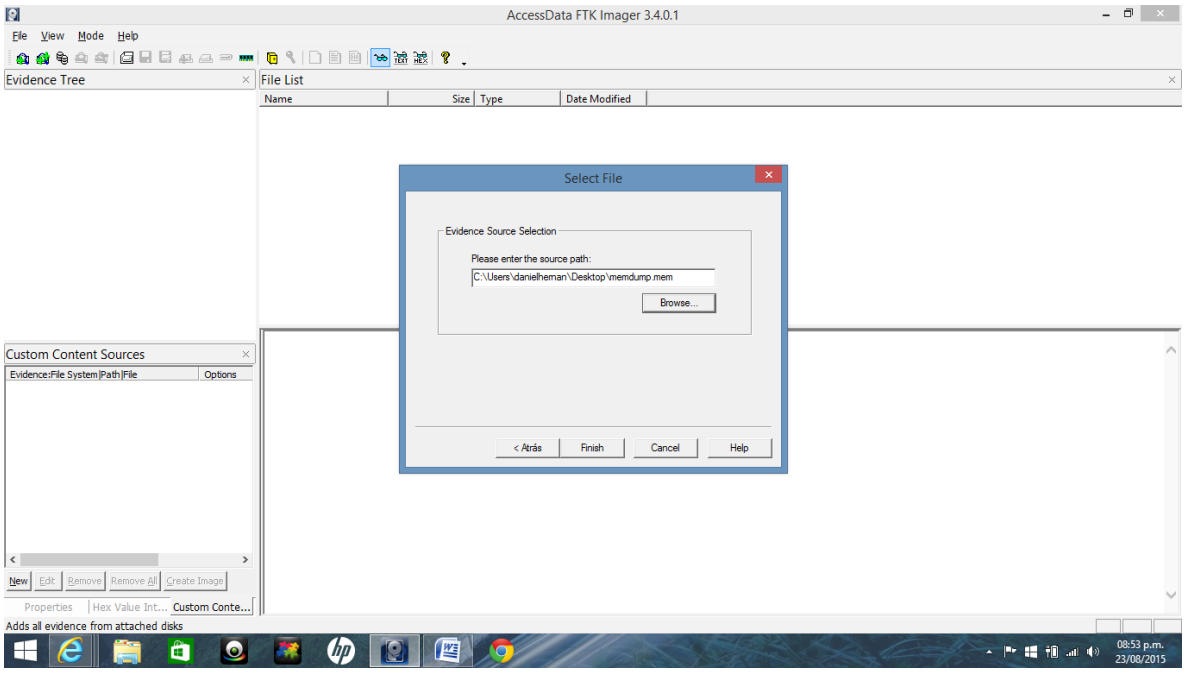


Figura 2.3 Path Select File.

Nos va a traer el volcado de memoria RAM, del lado izquierdo se encuentra el árbol de evidencia, nos posicionamos en el archivo, en el encabezado nos muestra todos ceros, esto se debe a la falta de existencia de un sistema de archivos en la memoria RAM

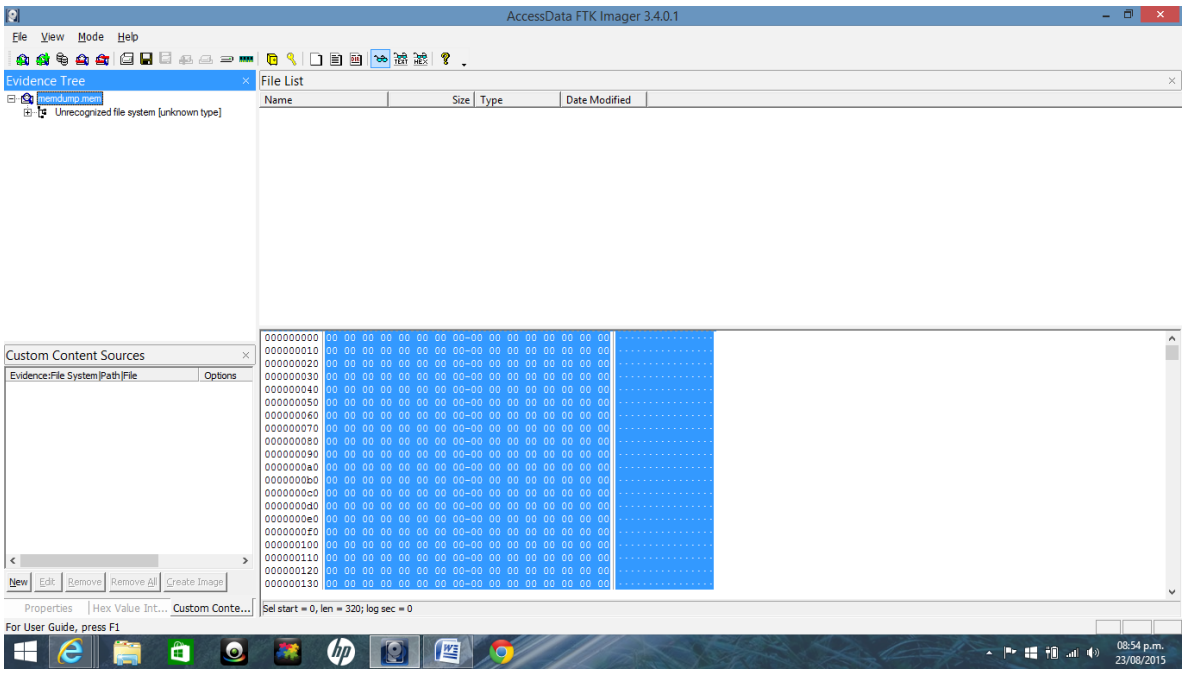


Figura 2.4 Encabezado.

Si bajamos con el cursor vamos a ver información contenida en la memoria. Ejemplo si queremos buscar información de un correo electrónico, seleccionamos click con el cursor derecho del mouse o con las teclas Control + F, nos abre una pantalla de búsqueda, le damos > find..... (Buscar)

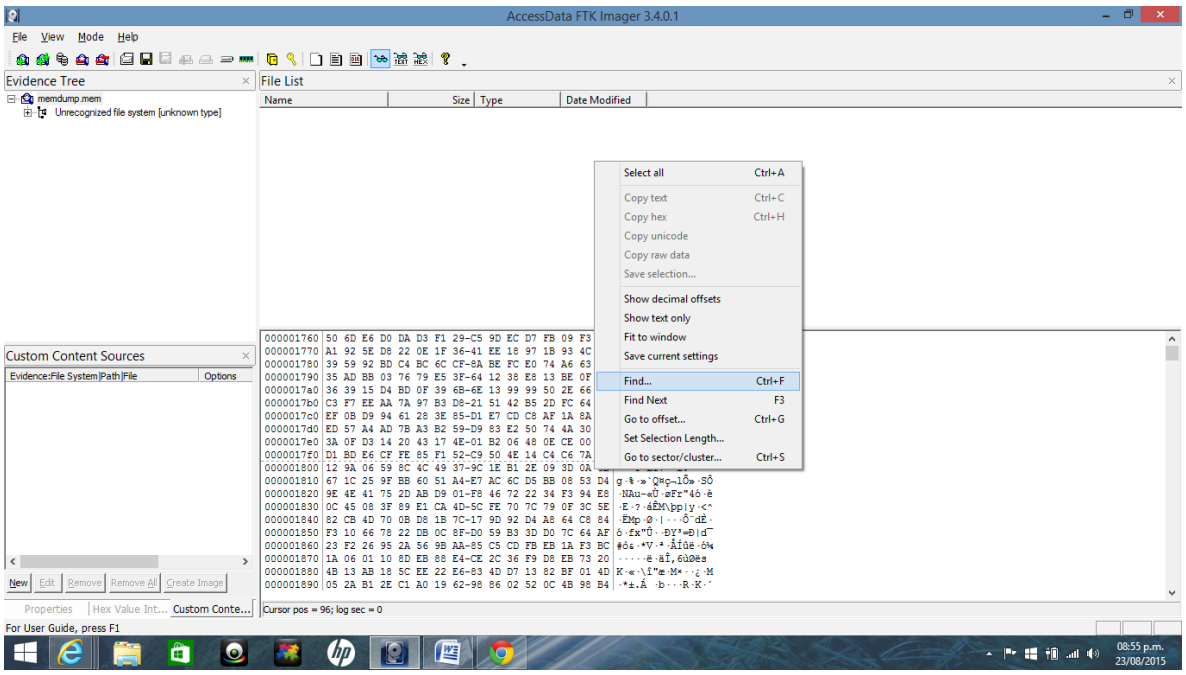


Figura 2.5 Búsqueda

Colocamos el correo que deseamos buscar o el servidor de correo. Por ejemplo: @hotmail.com @yahoo.com.ar etc. Seleccionamos> find

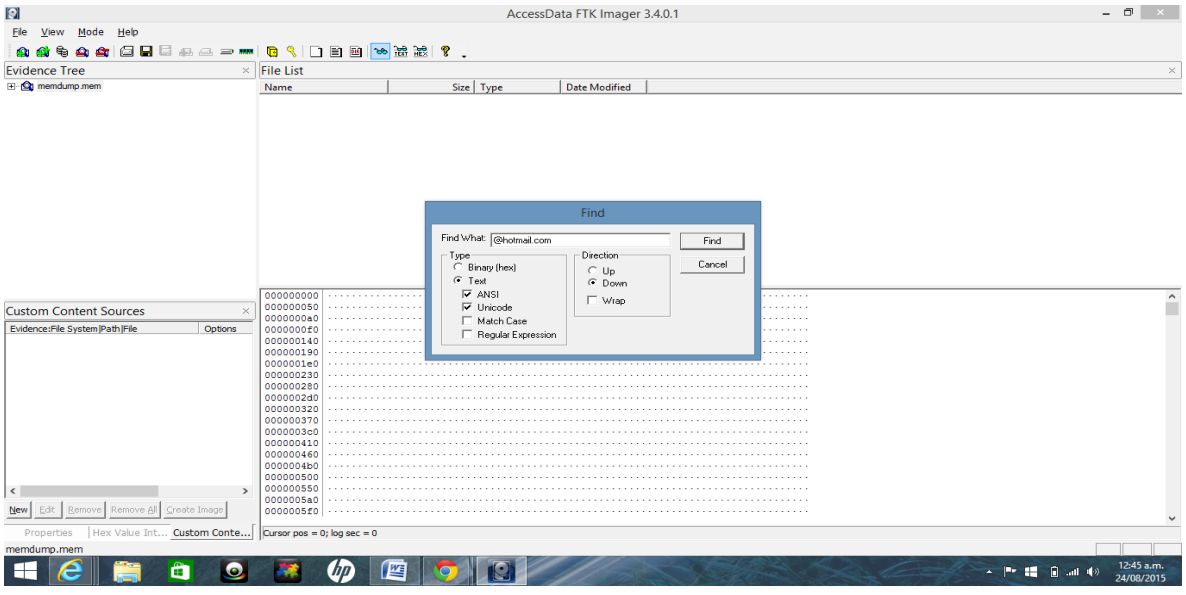


Figura 2.6 Búsqueda del servidor de correo.

En la siguiente pantalla nos muestra el resultado del cual obtenemos el correo electrónico del usuario.

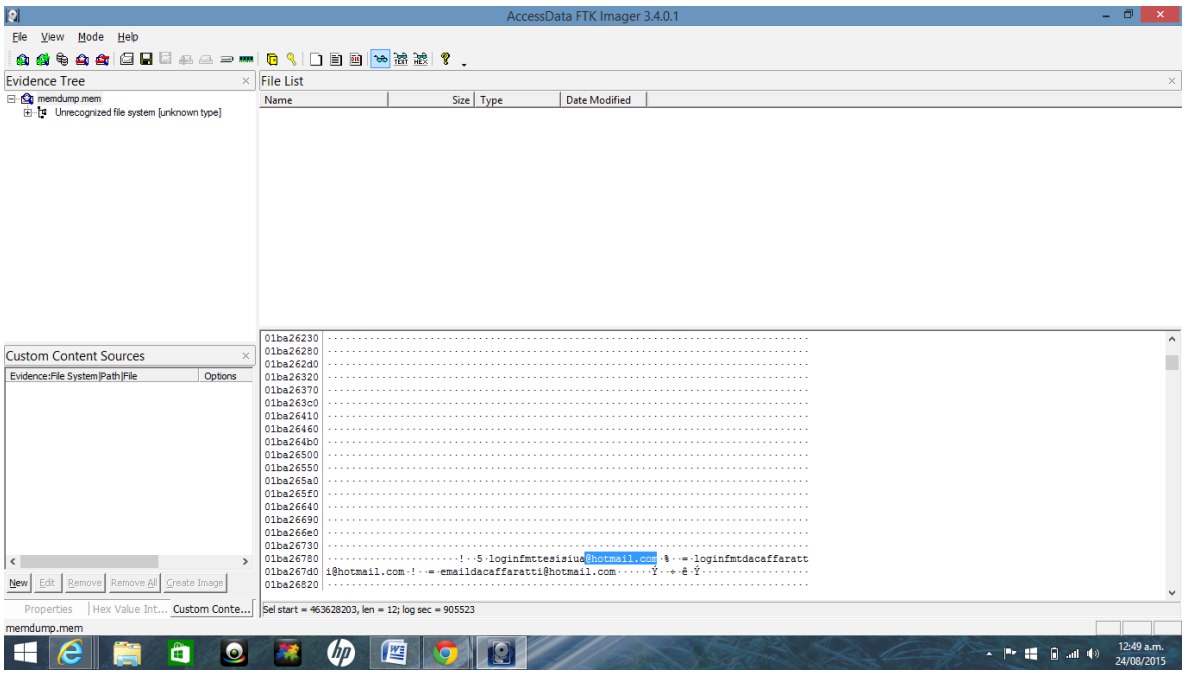


Figura 2.7 resultado de la búsqueda del servidor de correo

Para Obtener el password, seleccionamos > control + f > "&passwd=" > find

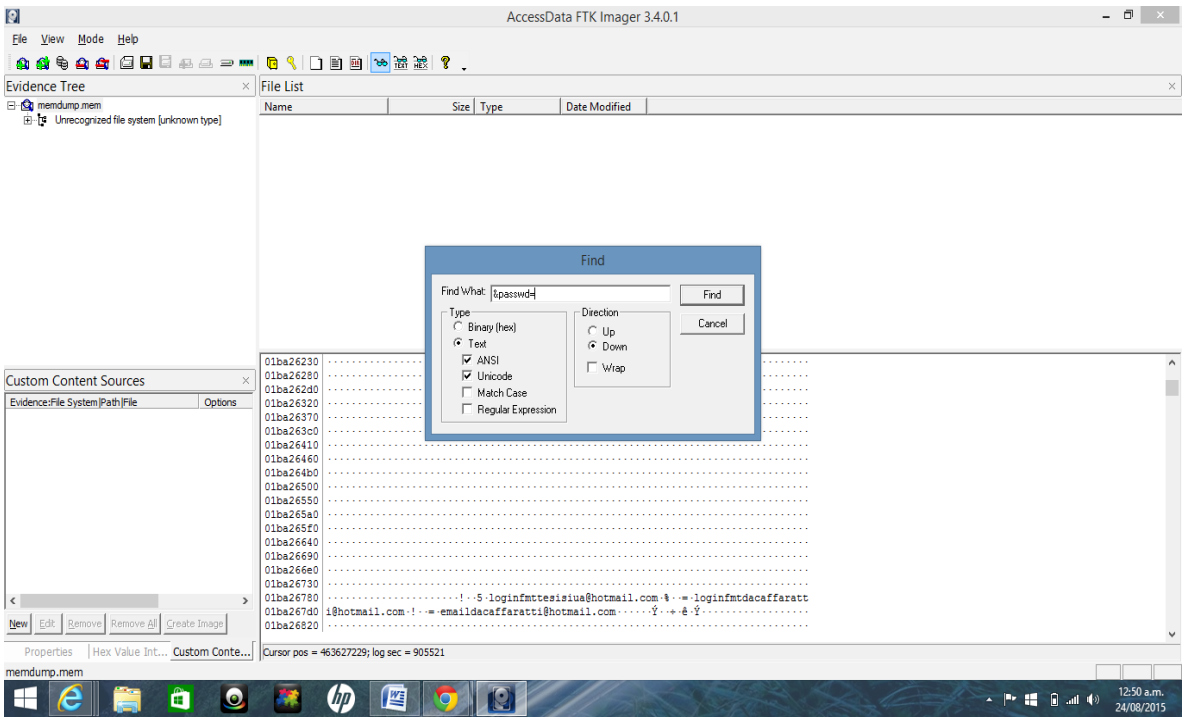


Figura 2.8 Búsqueda del password

En la siguiente pantalla nos muestra el resultado del password. Con las teclas F3 vamos a buscar todas las concordancias.

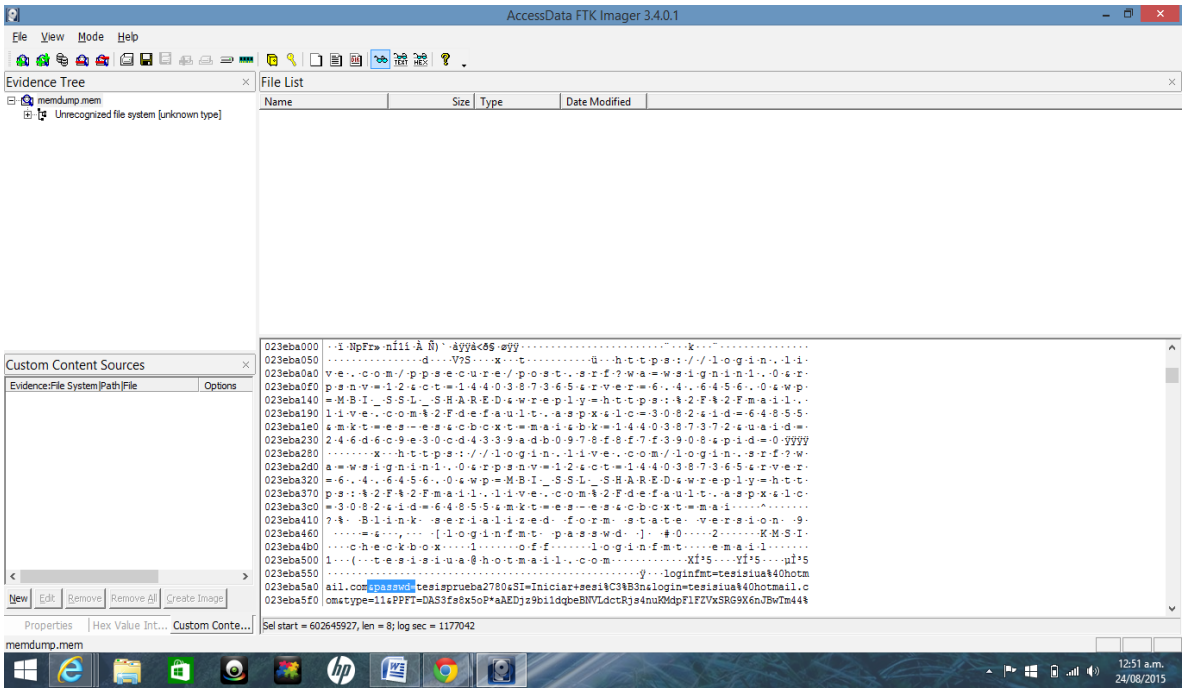


Figura 2.8 Resultado Búsqueda del password.

Validamos la imagen con md5 y Hash sha-1.

Nos posicionamos sobre la imagen memdump.men del árbol de evidencia > botón derecho del mouse> verify drive image.....> enter.

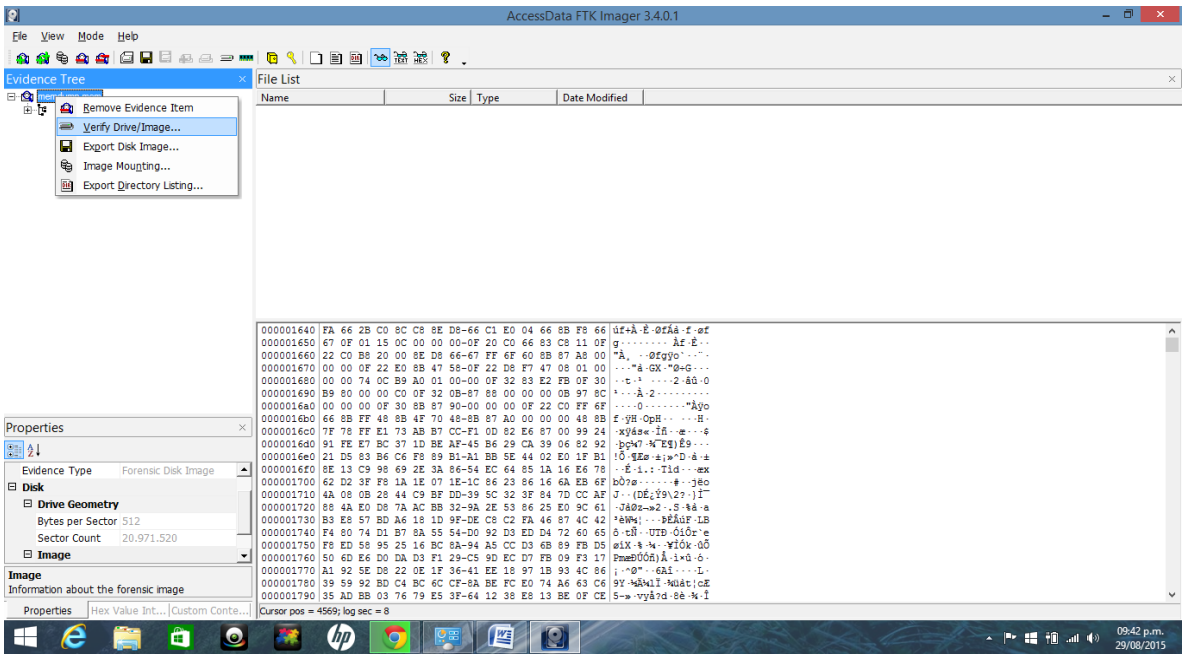


Figura 2.9 validar dump de memoria.

En la siguiente ventana nos muestra el proceso de verificación de la imagen.

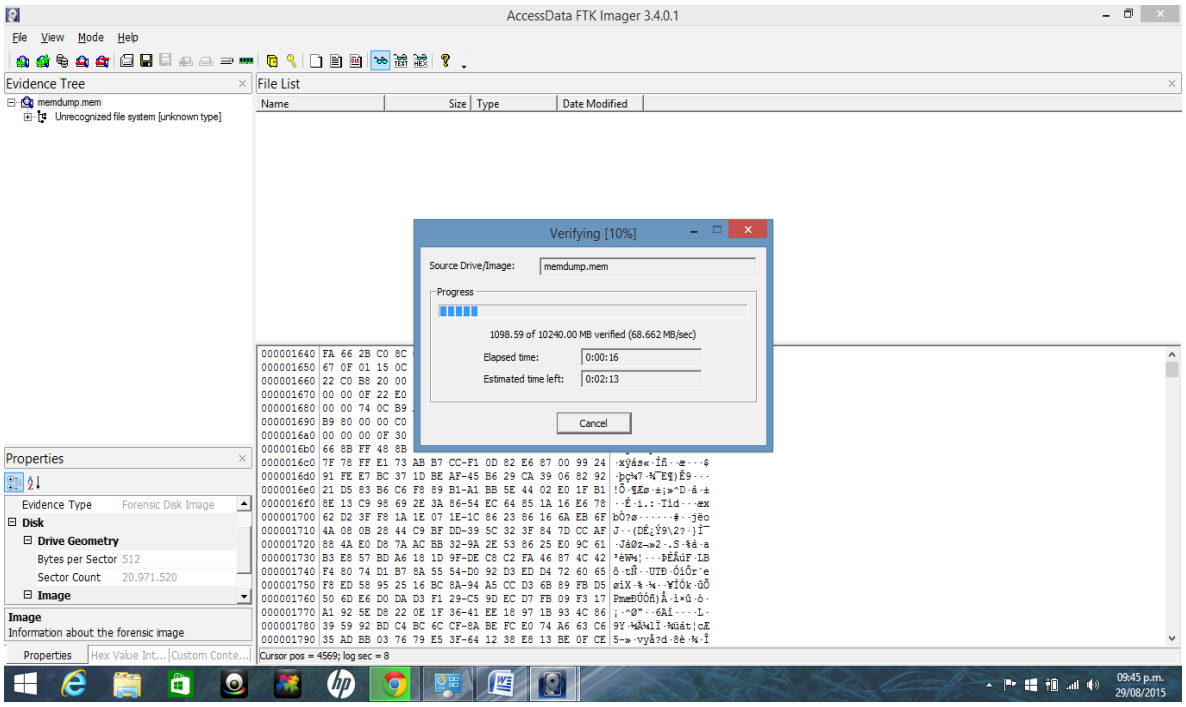


Figura 3.0 Proceso de Validación.

Obtenemos el resultado del Hash Md5 y Hash sha-1

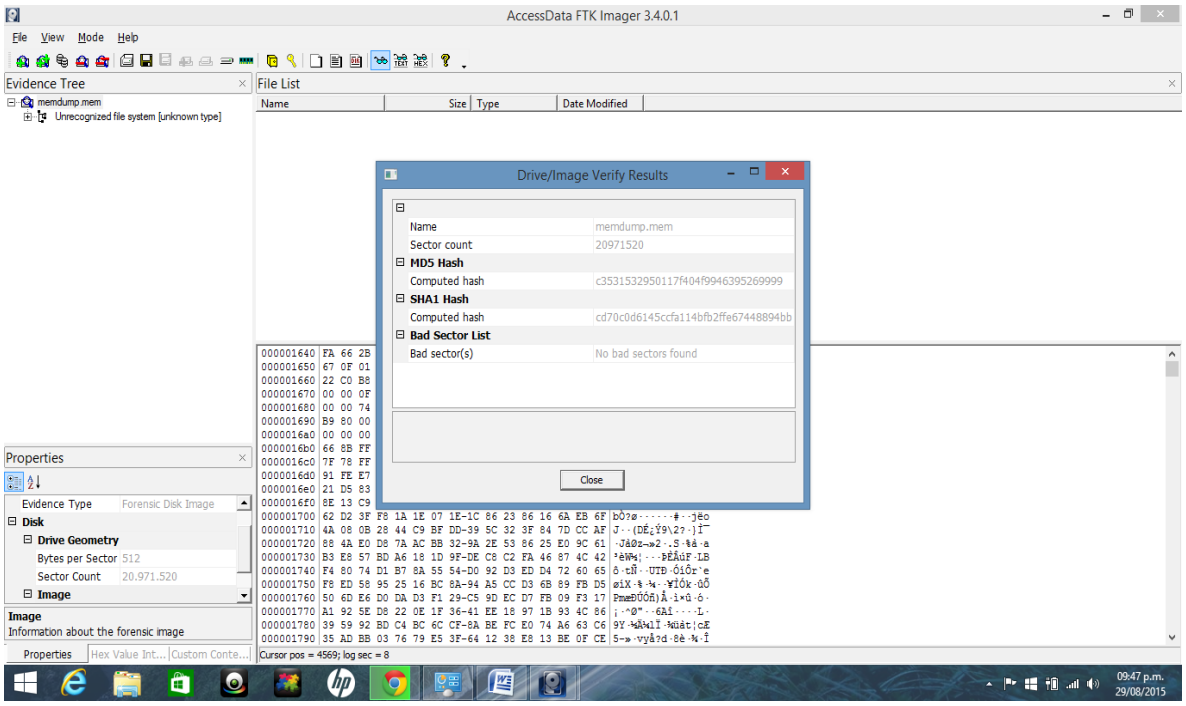


Figura 3.1 Md5 Hash y Sha1 Hash.

1.1.2 Montamos un dump de memoria RAM como una unidad física para recuperar archivos.

Ingresamos al software ftk imager, vamos a file >Image mounting.... (Montar Imagen) > Enter.

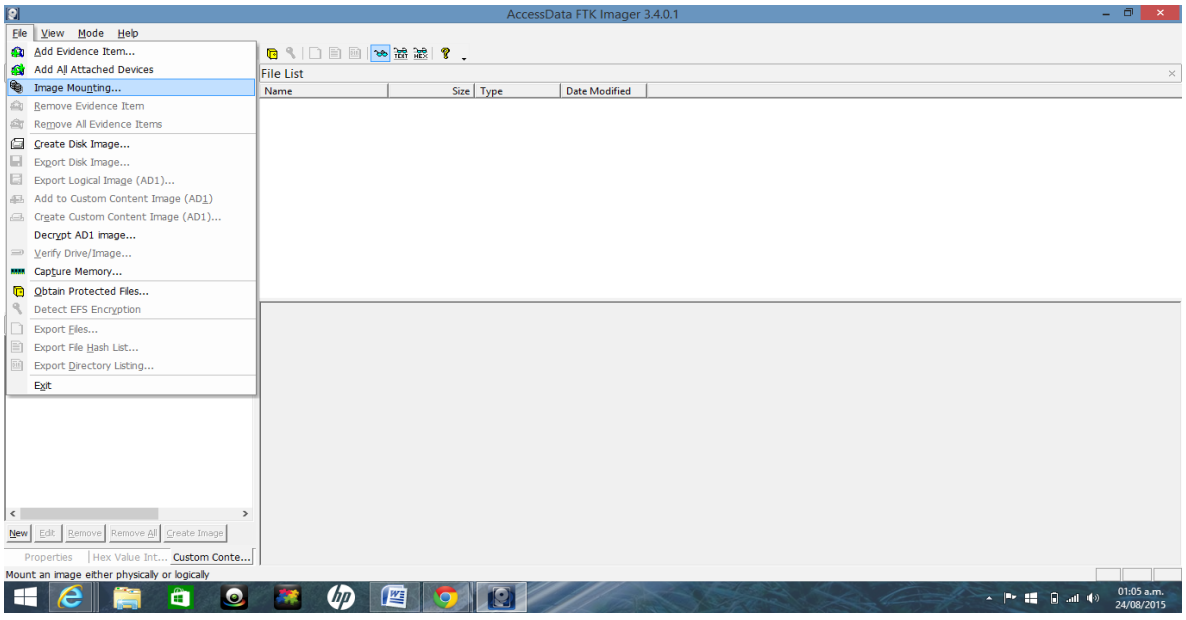


Figura 3.2 Ftk Imager Montar imagen.

1. Seleccionamos el archivo de Imagen > image file:

2. seleccionamos el tipo de mount type: physical only (unidad física)

3. mount (montar)

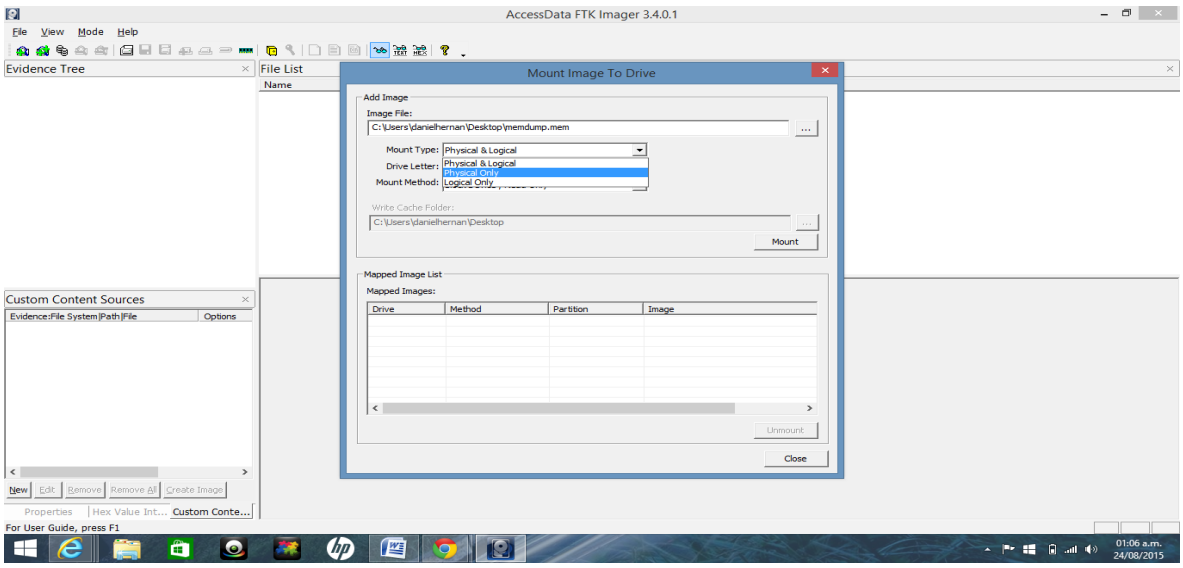


Figura 3.3 mount imagen.

Montamos la Imagen como unida física.

En nuestro ejemplo figura: PhysicalDrive1.

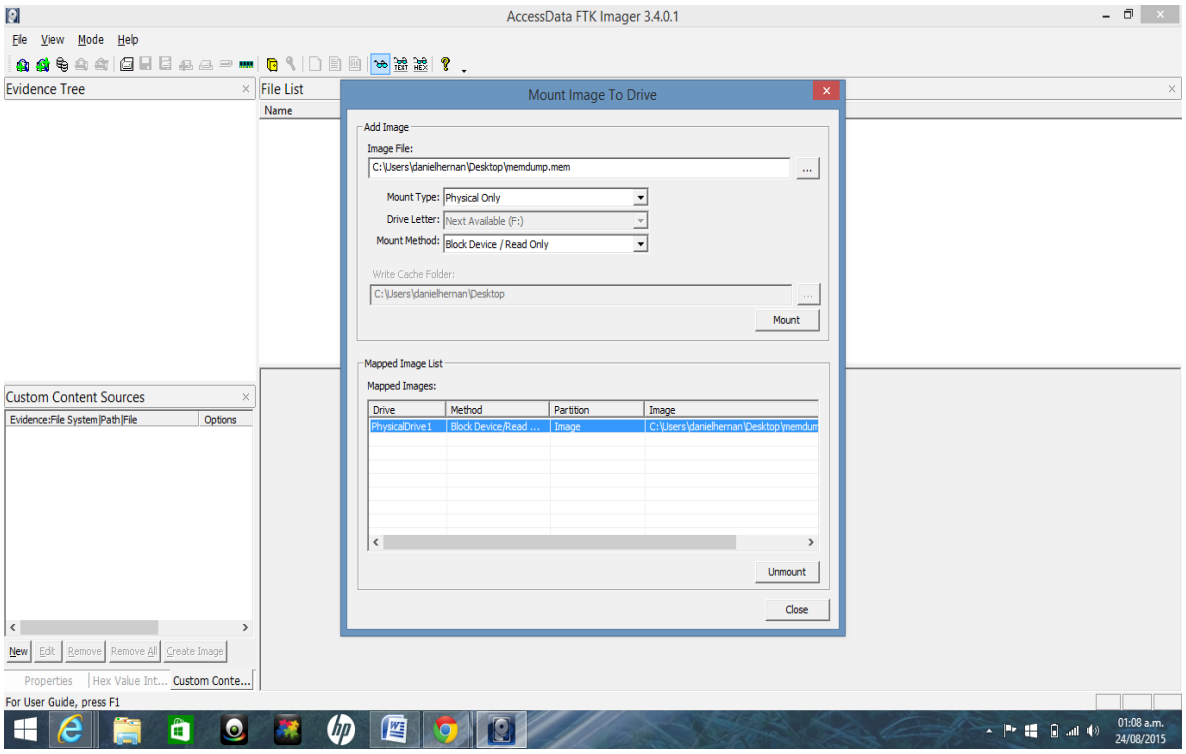


Figura 3.4 montar la unidad física.

Una vez montada la unidad, debemos utilizar un software Photorec, el cual nos muestra todas las unidades físicas, seleccionamos la unidad Physicaldrive1 creada con ftk imager > Enter.

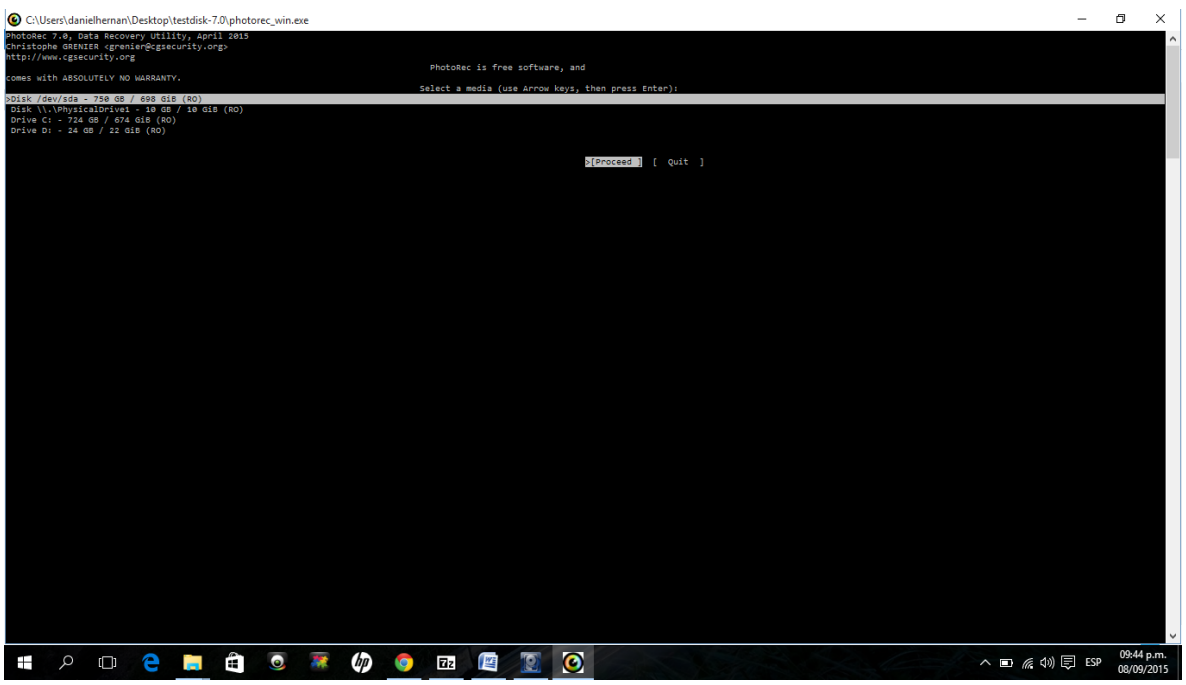


Figura 3.5 software photorec

En la siguiente ventana nos muestra los sectores de la memoria ram y vale aclarar que la memoria ram no posee una archivo especifico, seleccionamos > p unknown > enter.

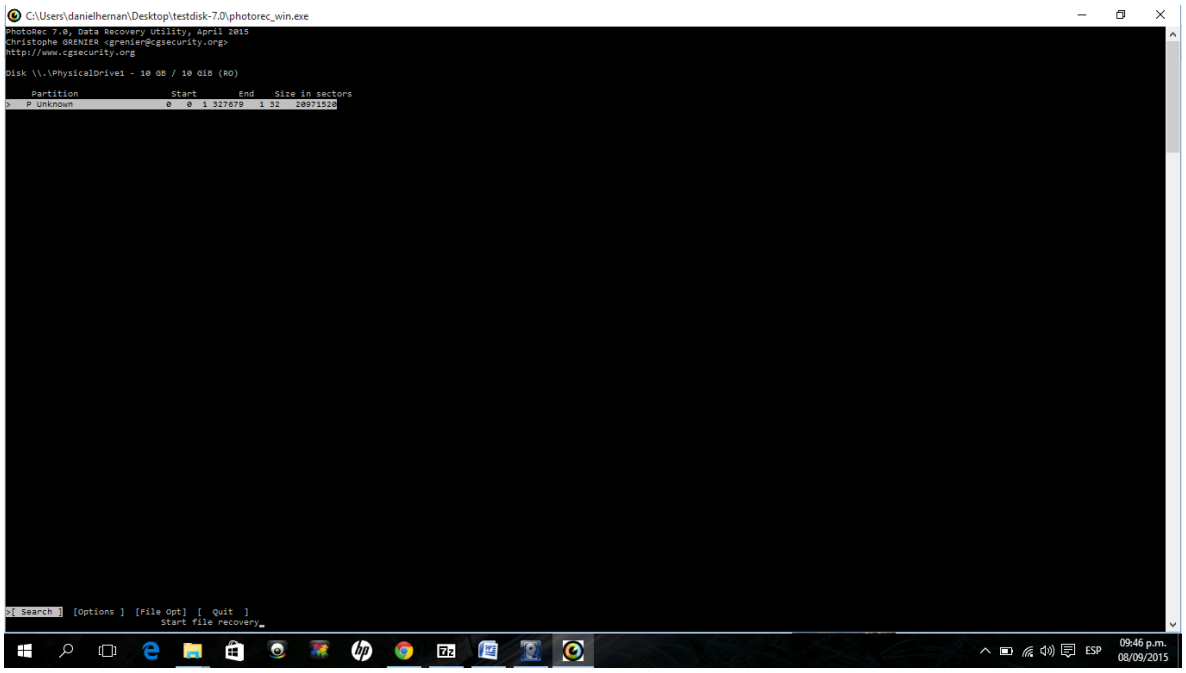


Figura 3.6 sectores de la memoria ram

En la siguiente ventana nos muestra el contenido de la memoria ram.

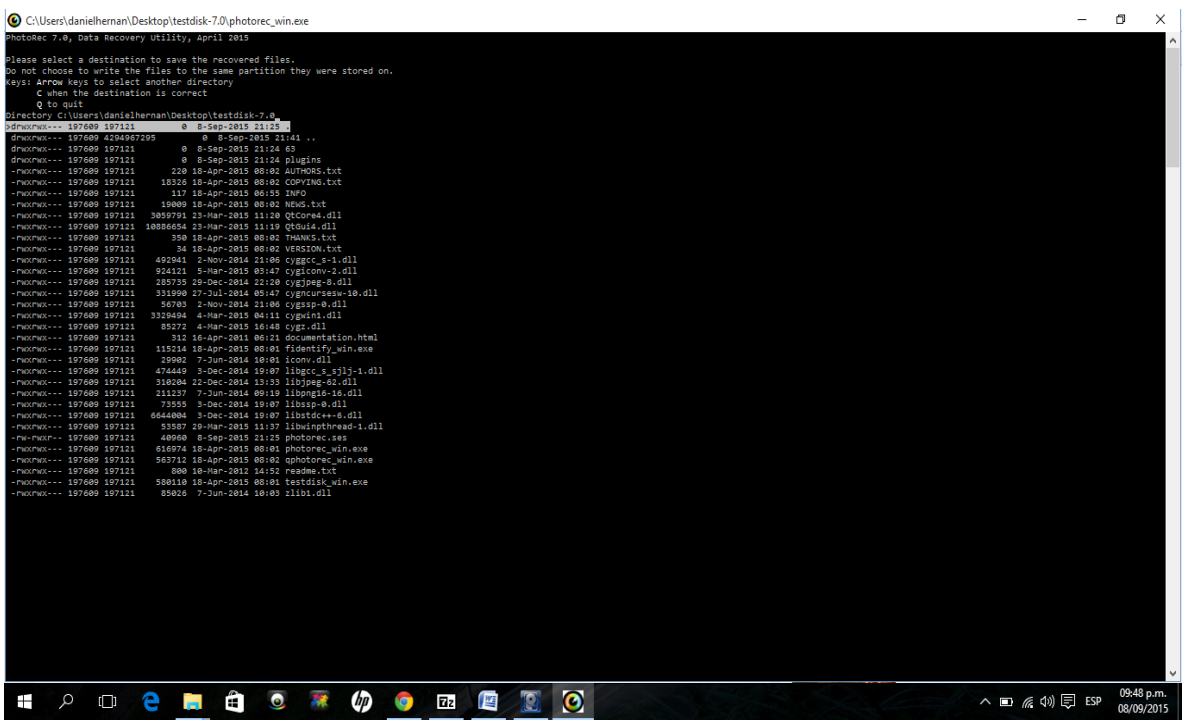


Figura 3.7 memoria ram

En el software photorec vamos a crear una carpeta memoria_ram donde se guardaran todos los archivos recuperados.

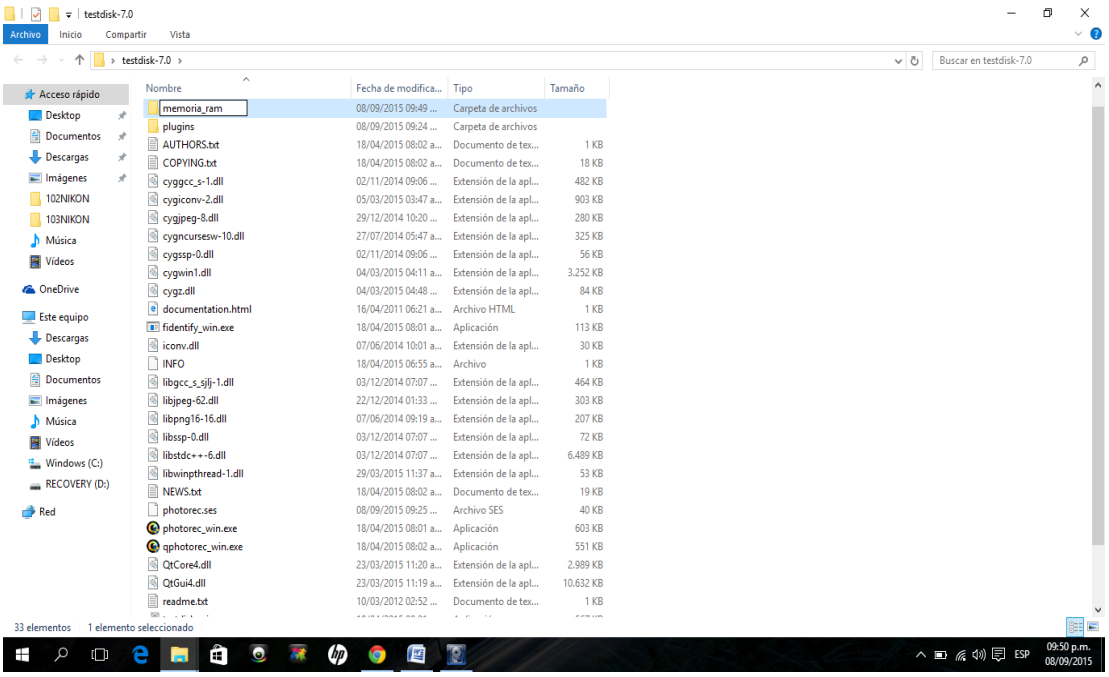


Figura 3.8 carpeta memoria_ram

Abrimos photorec, seleccionamos la carpeta memoria_ram > opción c > enter.

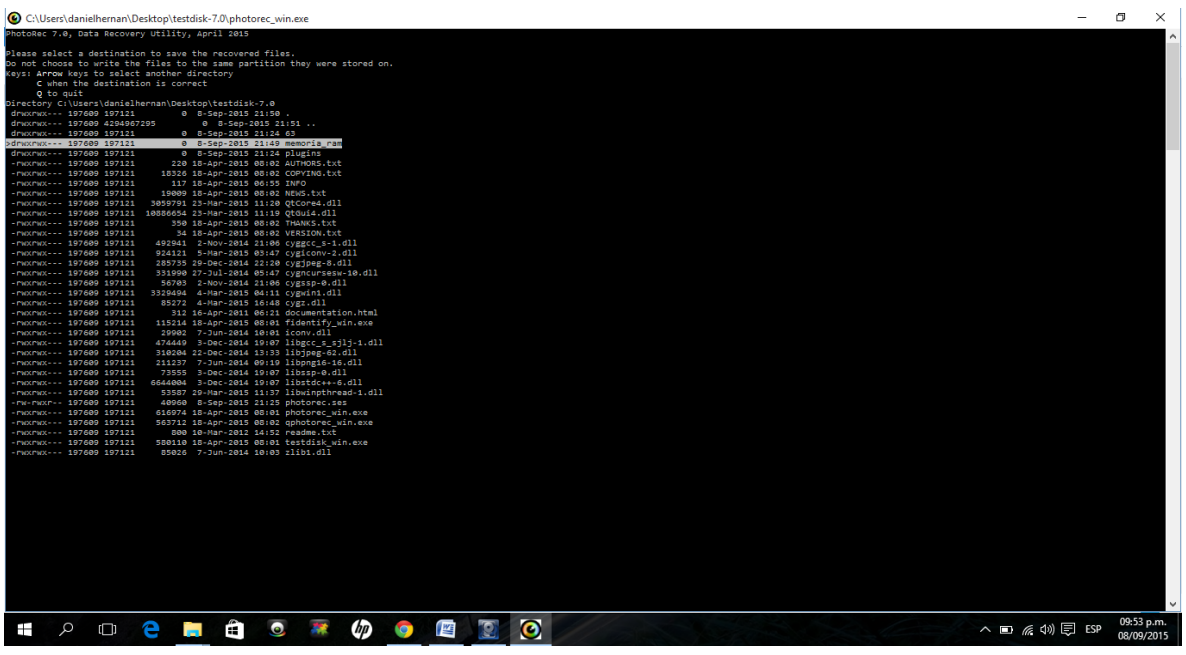


Figura 3.9 selección carpeta memoria_ram

Nos muestra el Proceso de extracción del contenido de la memoria ram, este proceso va a variar dependiendo la capacidad de la memoria ram.

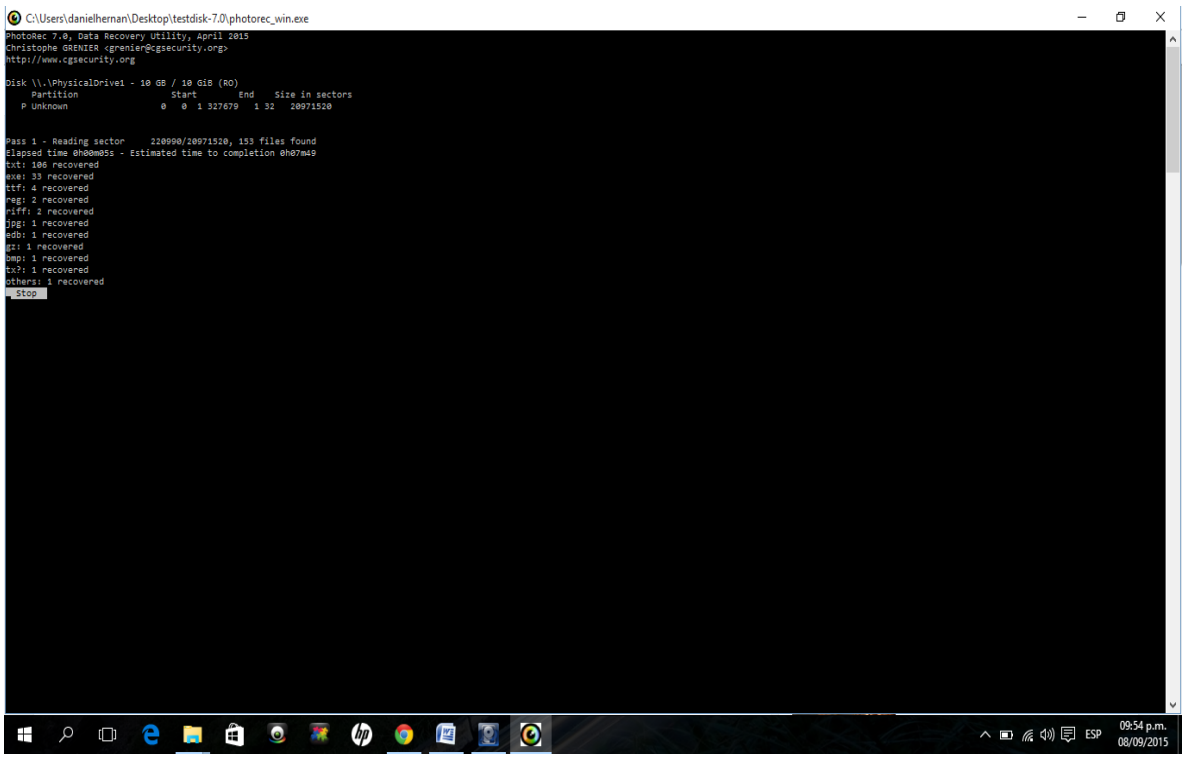
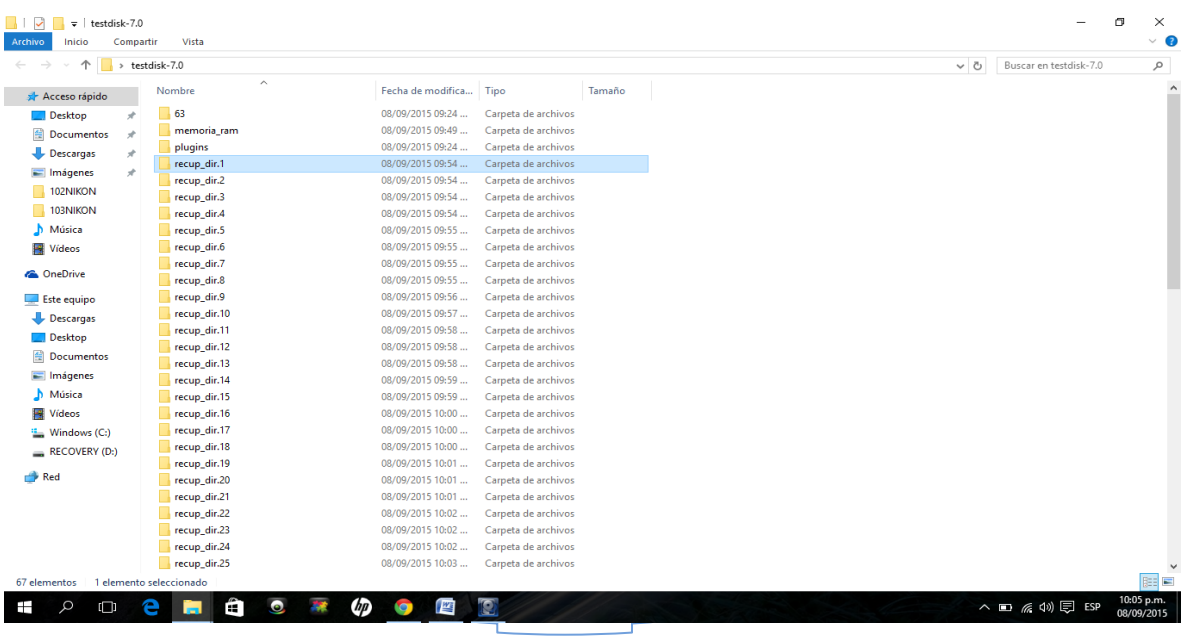


Figura 4.0 proceso de extracción.

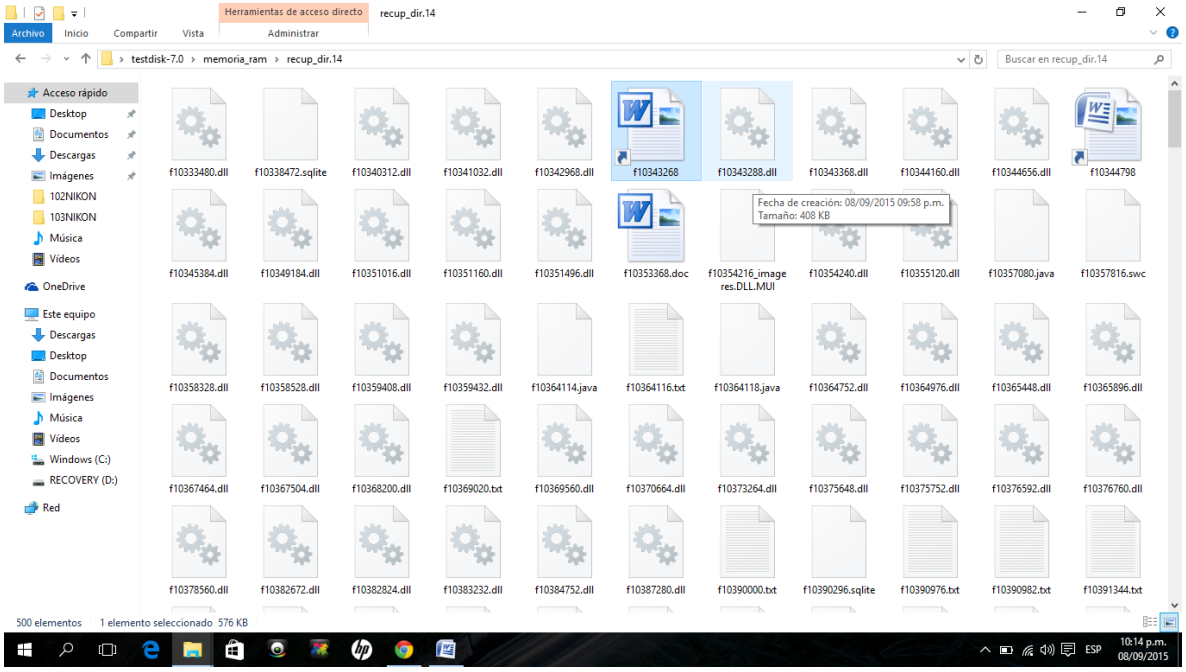
Resultado de la extracción de directorios de la memoria, nos aparece las carpetas recup_dir1. recup_dir2 y así continuado hasta terminar la



extracción.recup_dir2 y así continuado hasta terminar el proceso de extracción.

Figura 4.1 directorios recuperados

Ingresamos al directorio y podemos visualizar el contenido, dentro del mismo se puede llegar a encontrar, librerías, imágenes, paginas de navegación, documentos etc.



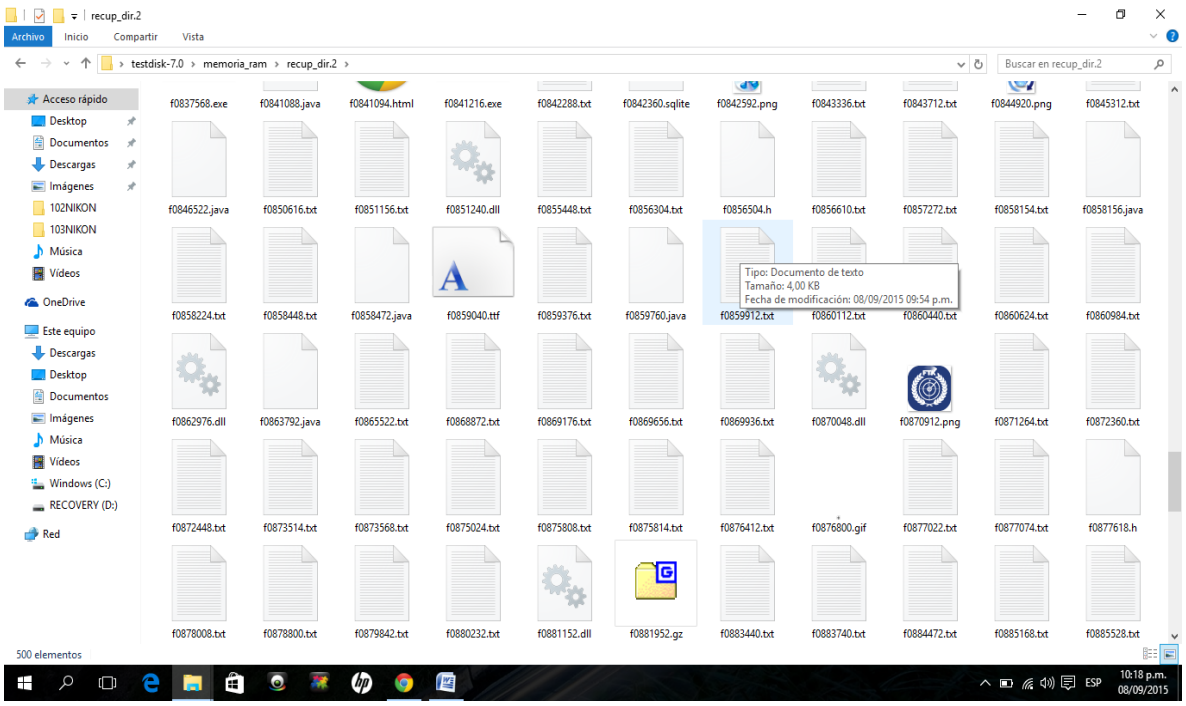


Figura 4.2 contenidos de los directorios recuperados.

1.2 FTK IMAGER CREAR IMAGEN FORENSE DE UNA UNIDAD FISICA.

1.2.1 Crear una copia de imagen del disco USB y poder recuperar archivos eliminados.

Hacer clic en la opción “File -> Create Disk Image” o Archivo -> Crear Imagen de Disco.

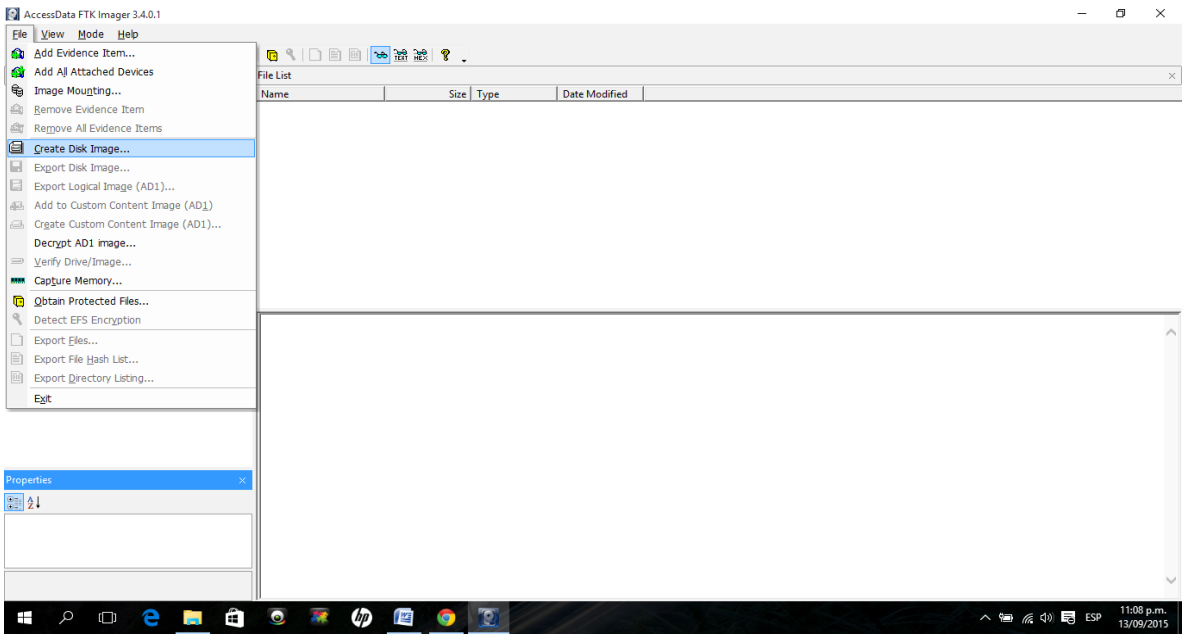


Figura 4.3 Crear imagen de disco.

Se presentará una nueva ventana donde se requiere definir la Fuente. Para propósito de la presente práctica se creará una imagen forense de toda una unidad USB o Memory Stick, por lo tanto se selecciona la opción “Physical Drive” o Unidad Física. Luego hacer click en el botón “Siguiente”.

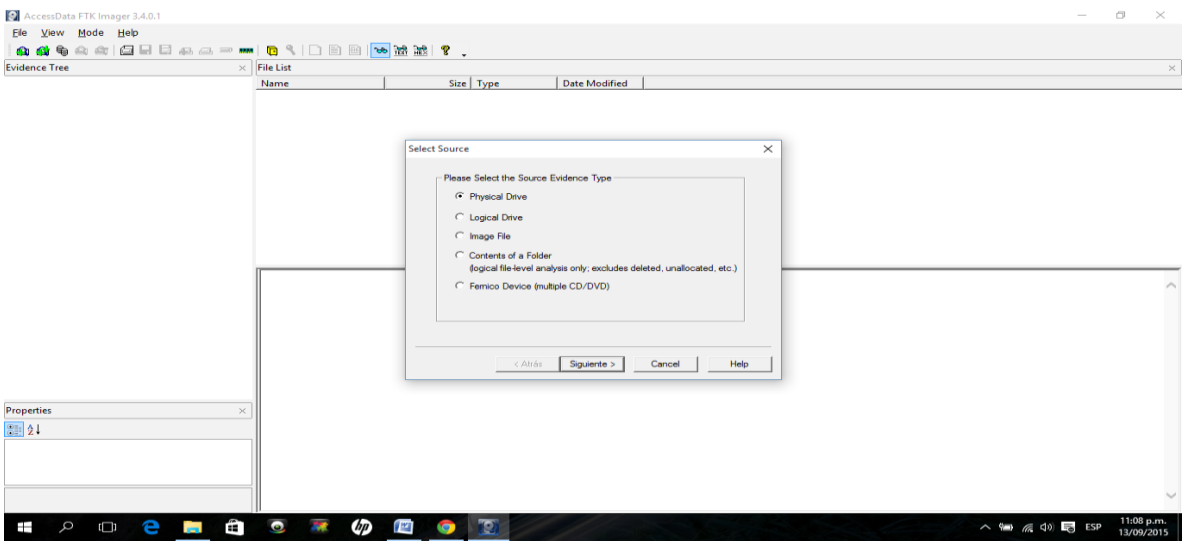


Figura 4.4 seleccionar la fuente.

En una nueva ventana se muestra un menú desplegable, en el cual se selecciona la Unidad Fuente correspondiente, para luego hacer clic en el botón “Finish” o Finalizar.

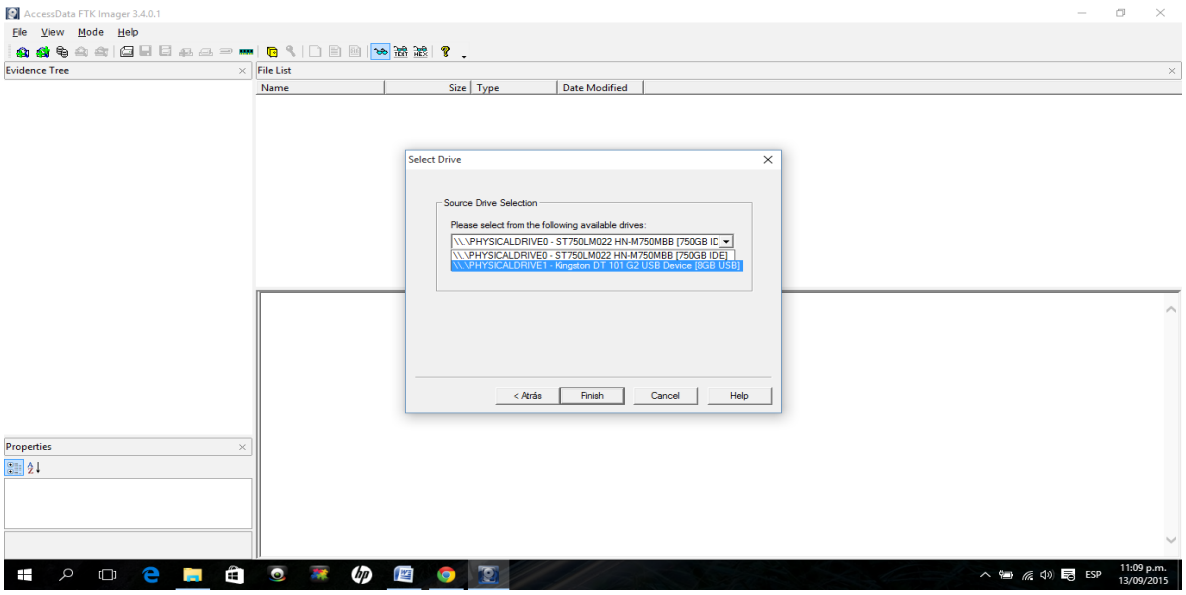


Figura 4.5 Seleccionar la unidad.

La siguiente ventana permite definir un Destino para la Imagen. Para esto es necesario hacer clic en el botón “Add...”

En esta ventana se define el tipo de la imagen de destino a crear. Para el caso de la presente práctica será una imagen “Raw” o en bruto, es decir tal y como sería creada utilizando una herramienta como dd o dcfldd.

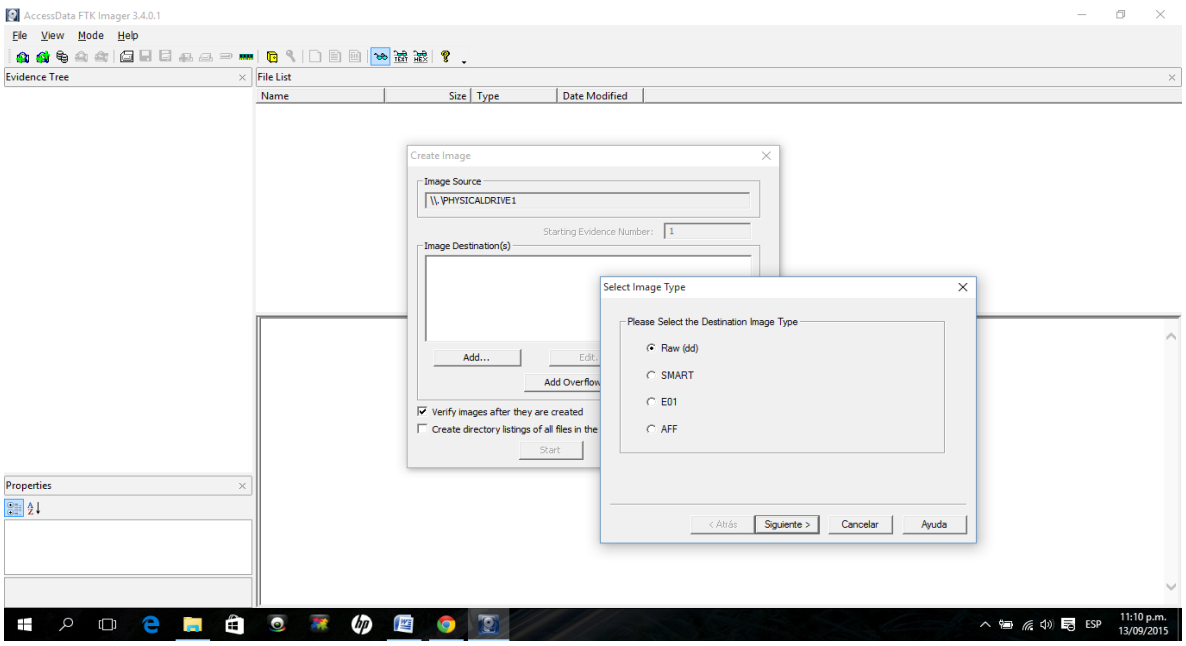


Figura 4.6 seleccionar tipo de imagen.

La siguiente ventana le dará la oportunidad de introducir información sobre el caso de la imagen. Esto es útil para fines de organización. Desde hacer el seguimiento de todo y tener notas detalladas, es muy útil introducir esta información. Haga clic en Siguiente.

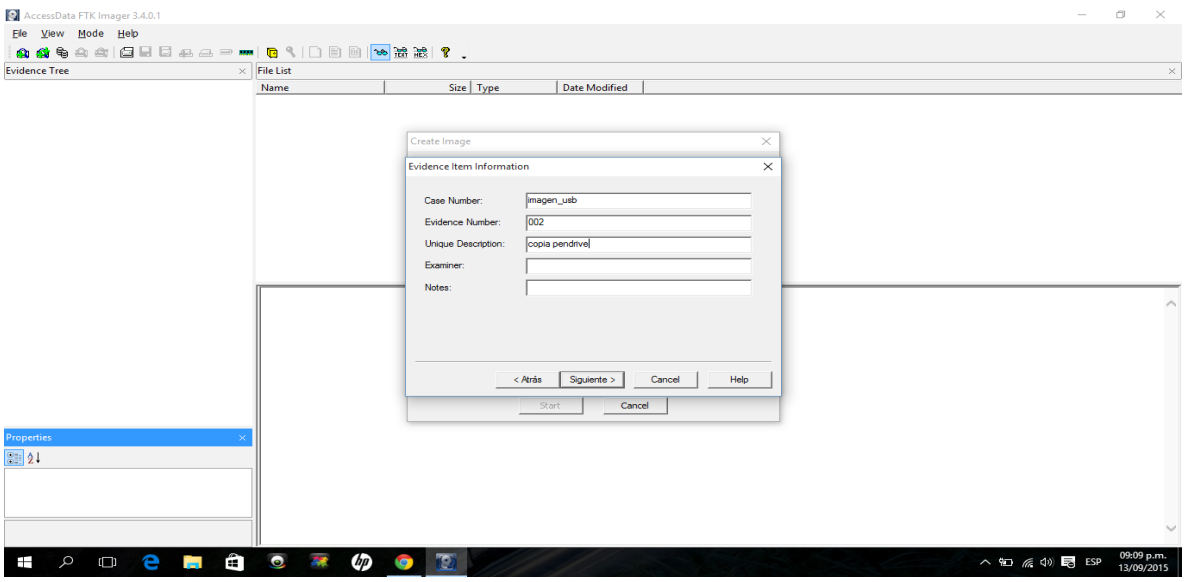


Figura 4.7 descripción de la evidencia.

Se requiere definir la carpeta donde se almacenará la imagen forense. La cual es seleccionada haciendo clic en el botón “Browse” o Navegar. A continuación se requiere nombrar la imagen forense (copia_usb). Y opcionalmente definir si la imagen resultante será dividida en varias partes o sino no será fragmentada, esto puede ser útil si la imagen es muy grande o se transportará en CD o DVD. Si se introduce un valor en este campo más grande que el tamaño de los datos para ser fotografiado , sólo un archivo se creará y será el tamaño de los datos Para el caso de la presente práctica no será divida, por lo tanto se define el valor “0” en el campo “Image Fragment Size (MB)” o Tamaño del Fragmento de la Imagen.

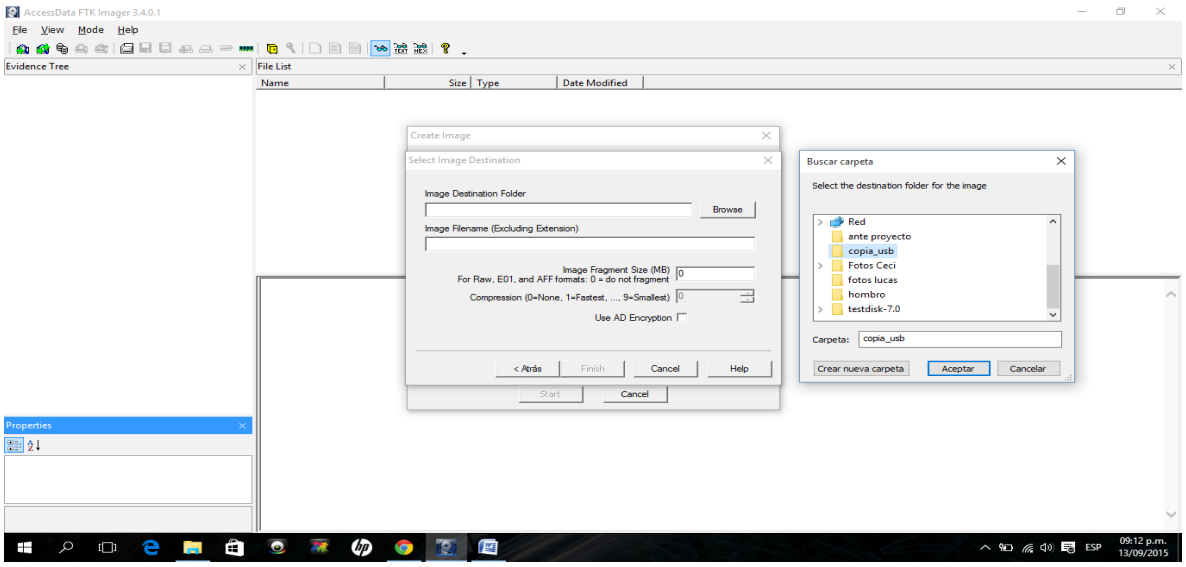


Figura 4.8 seleccionar la carpeta.

El proceso de creación de la imagen forense desde la unidad USB o Memory Stick iniciará al hacer clic en el botón “Start” o Iniciar. Esto puede llevar algún tiempo, dependiendo del tamaño.

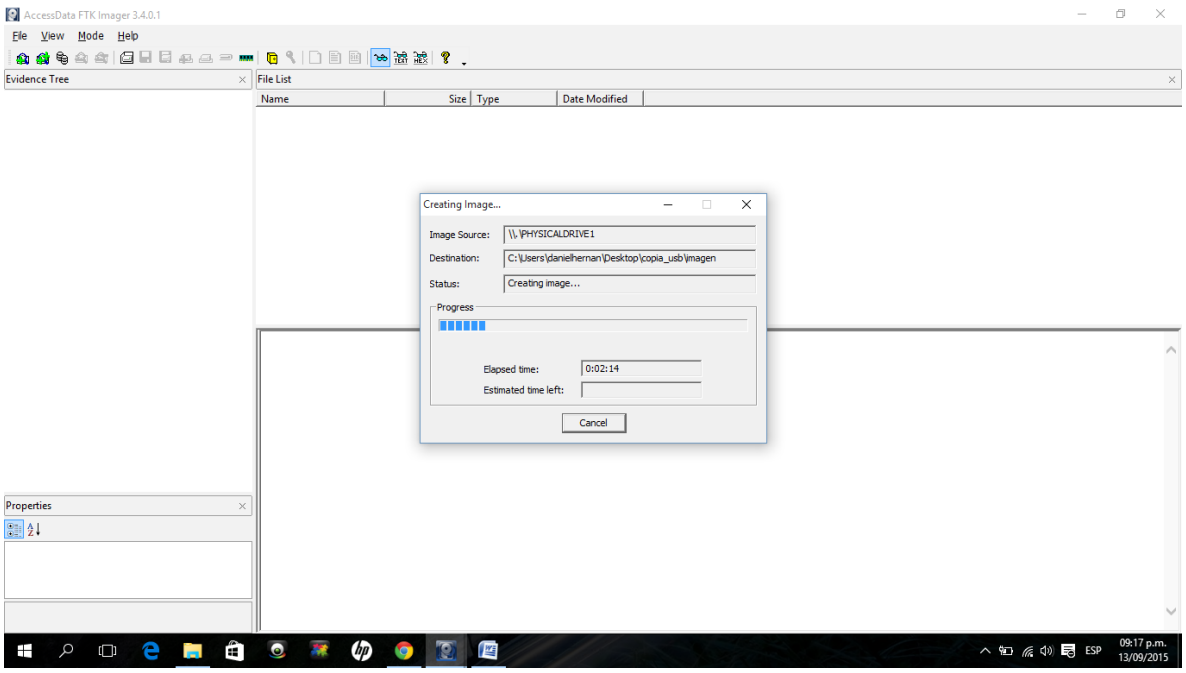


Figura 4.9 proceso de creación de imagen.

Al finalizar todo este procedimiento se presentan algunos resultados finales. Los resultados muestran el número de sectores copiados. La generación de un

Hash MD5 y un Hash SHA-1. Anotar la coincidencia entre el campo “Computed Hash” o Hash Calculado, es decir el hash obtenido desde la unidad USB o Memory Stick, y el campo “Report Hash” o Hash Reportado, el cual se genera desde la imagen forense creada de nombre “copia_usb”. Anotar también que no se han detectado sectores Malos.

Tenga en cuenta que tanto un MD5 y Hash SHA1 se han creado y verificado. El hash es la huella digital de la imagen de disco - si el disco imagen se altera, los valores hash va a cambiar. Hacer un seguimiento de estos hashes le permitirá verificar continuamente el hash del archivo de imagen durante el proceso de investigación. Cualquier otro investigador debe ser capaz de replicar este hash; esto mantiene la integridad de los ojos de la corte.

En el mismo directorio o unidad donde se ha creado la imagen forense, se encontrará un archivo de texto con el mismo nombre de la imagen forense creada (imagen.001.txt), en el cual reside toda la información detallada del proceso realizado.

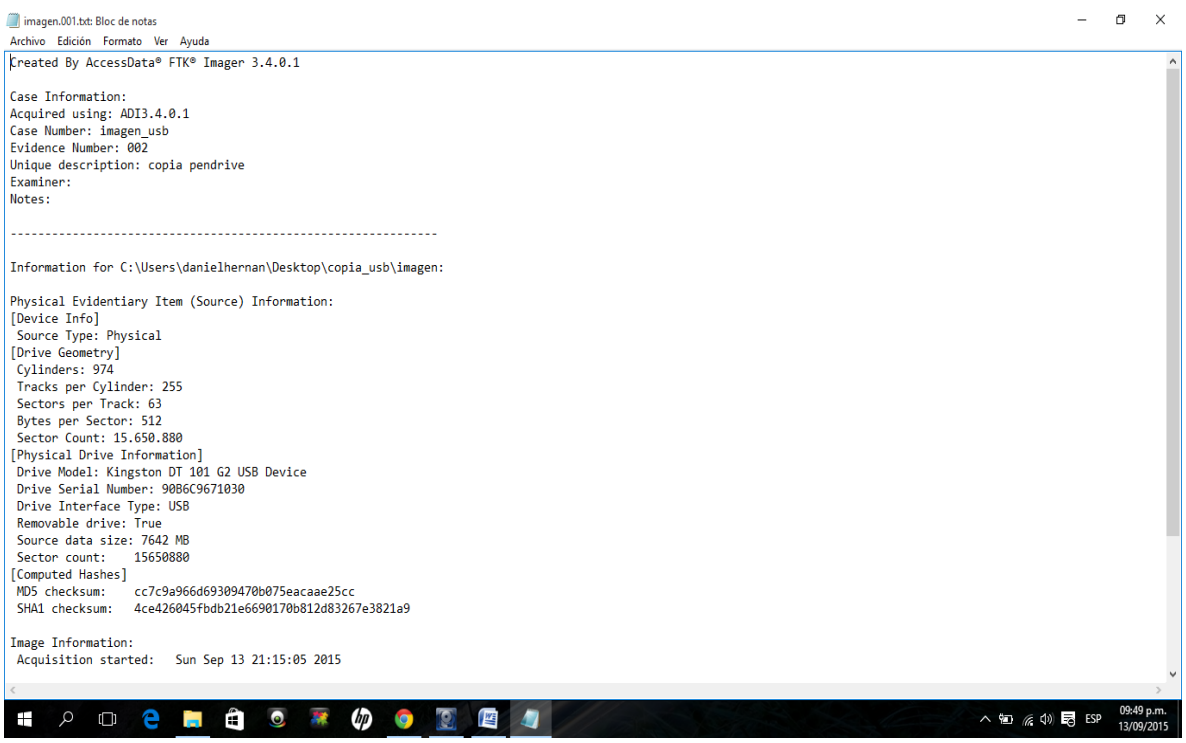


Figura 5.0 bloc de notas con información detallada.

En la siguiente ventana Hacer clic en la opción “File -> Add Evidence Item...” o agregar archivo de evidencia

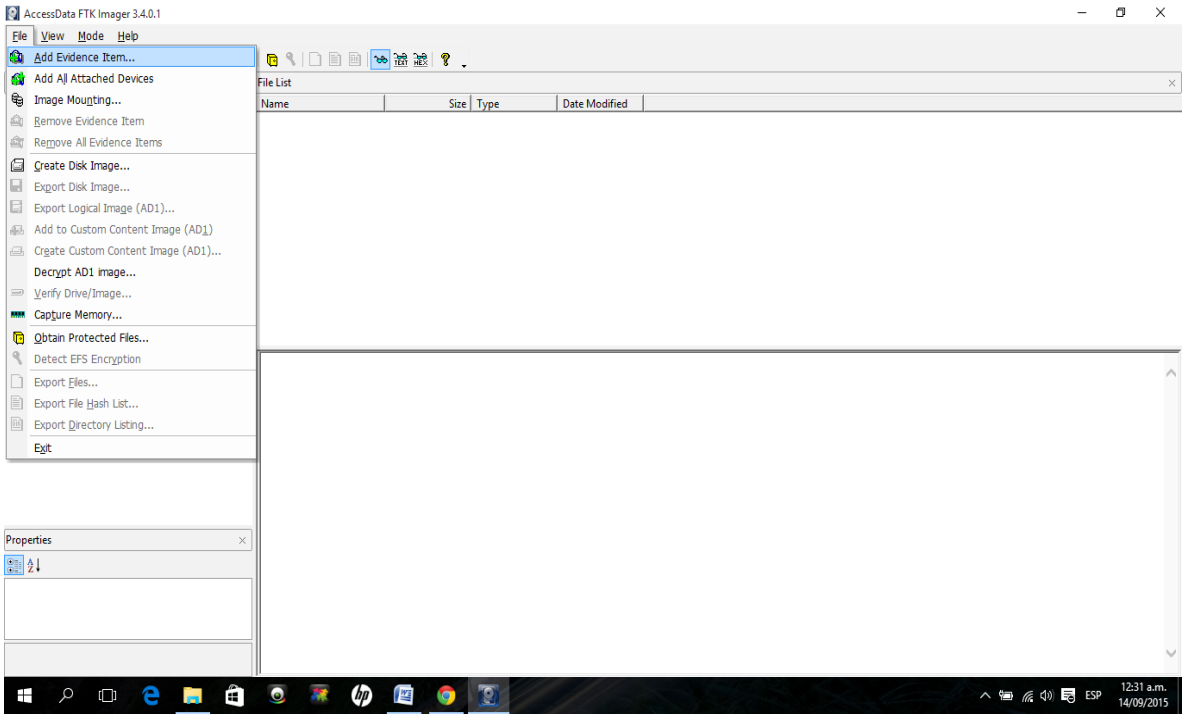


Figura 5.1 archivo de evidencia.

Seleccionamos image file> o archivo de imagen > siguiente

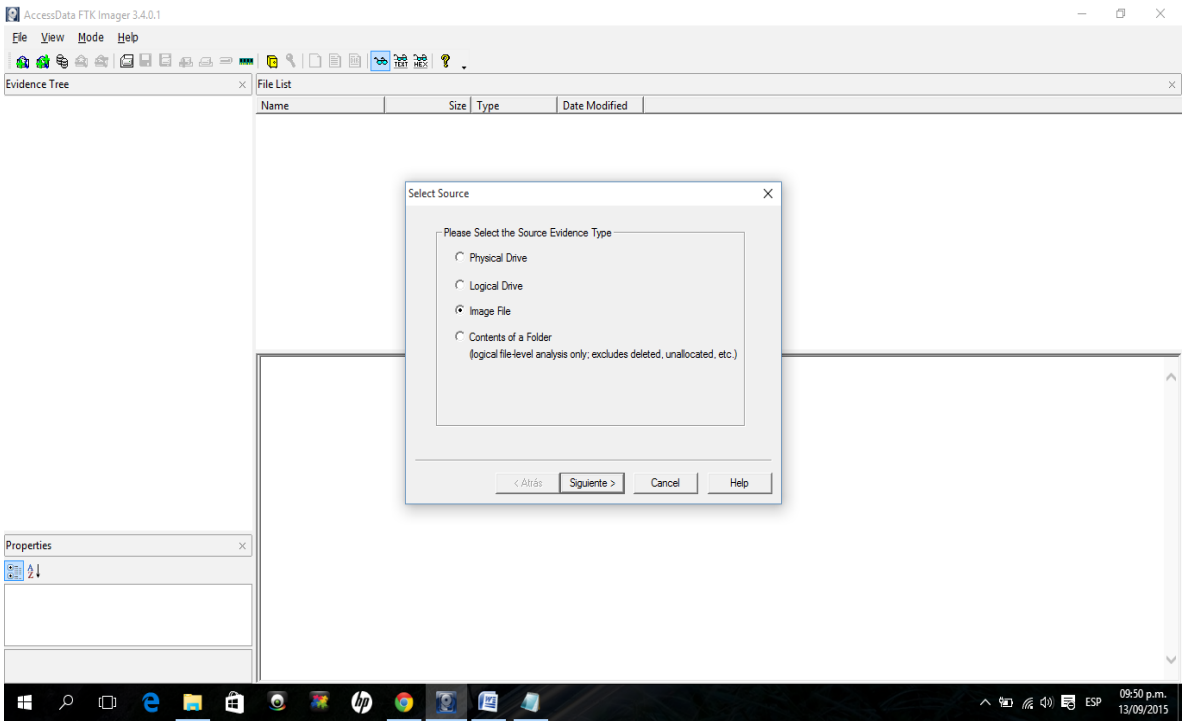


Figura 5.2 selección de archivo de imagen.

Seleccionamos el archivo de imagen en nuestro caso copia_usb > siguiente

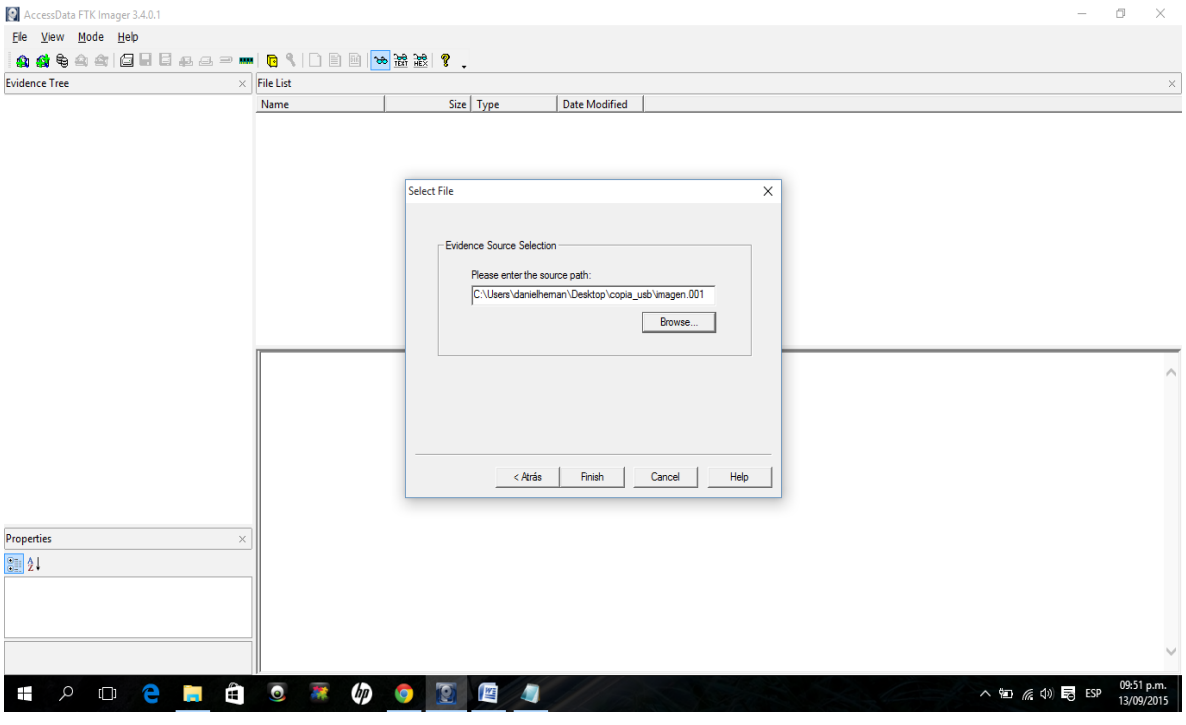


Figura 5.3 path de la evidencia.

Si nos posicionamos del lado izquierdo en Evidence Tree o Árbol de Evidencia, nos muestra todos los archivos que se encuentran en la unidad física (usb), los archivos que figuran con una x (roja) son archivos que fueron borrados o eliminado del mismo.

Vamos a recuperar un archivo borrado por ejemplo una imagen, nos paramos en la carpeta clic derecho > Export files o exportar carpeta.

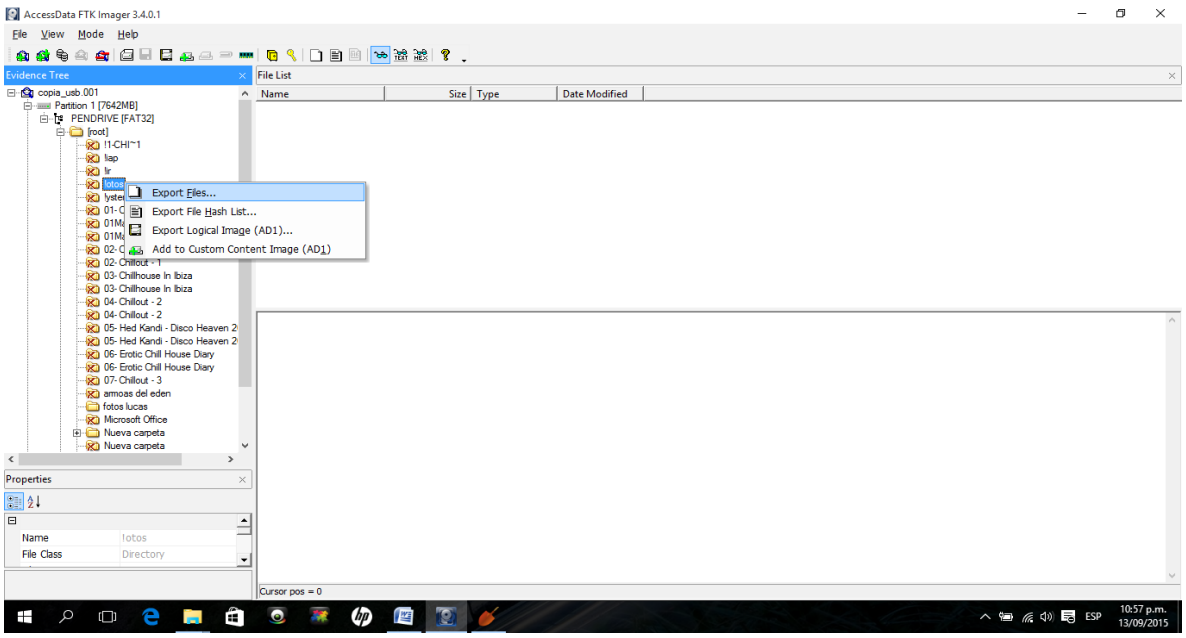


Figura 5.4 árbol de evidencia.

Utilizaremos el software DiskDigger para recuperar archivos eliminados, ingresamos al programa, nos posicionamos en Avanzado > buscar > y seleccionamos la imagen, en nuestro ejemplo copia_usb.001 > siguiente.

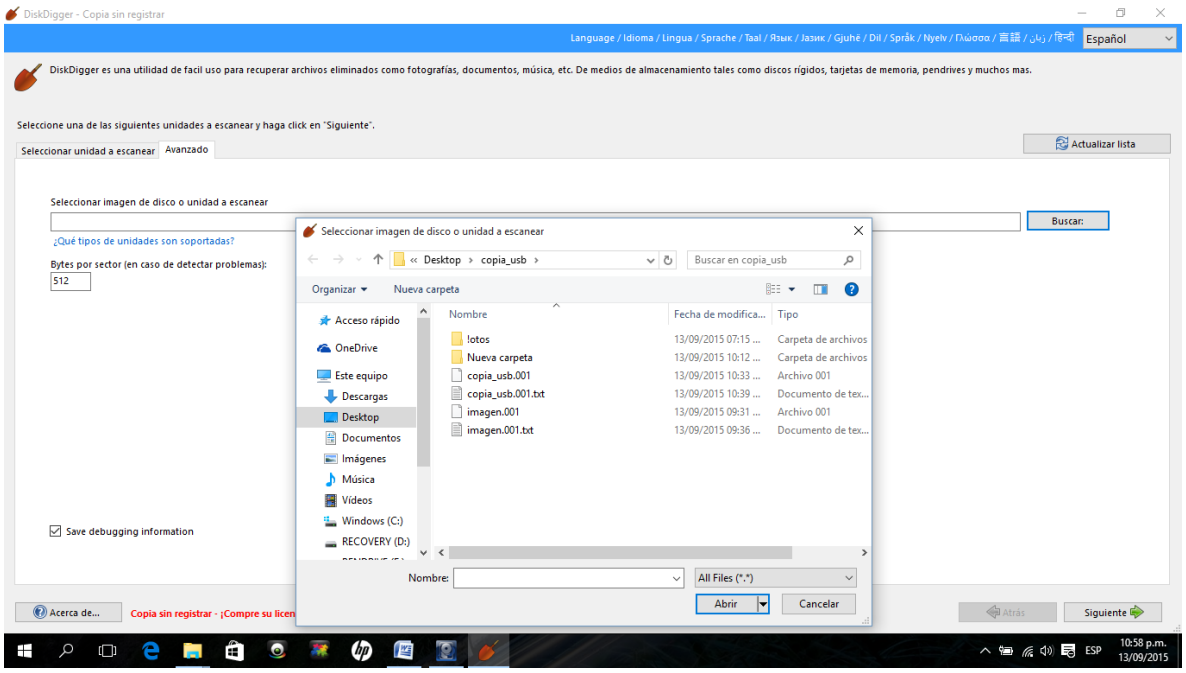


Figura 5.5 software diskdigger.

Marcamos con un tilde > Excavado Intenso

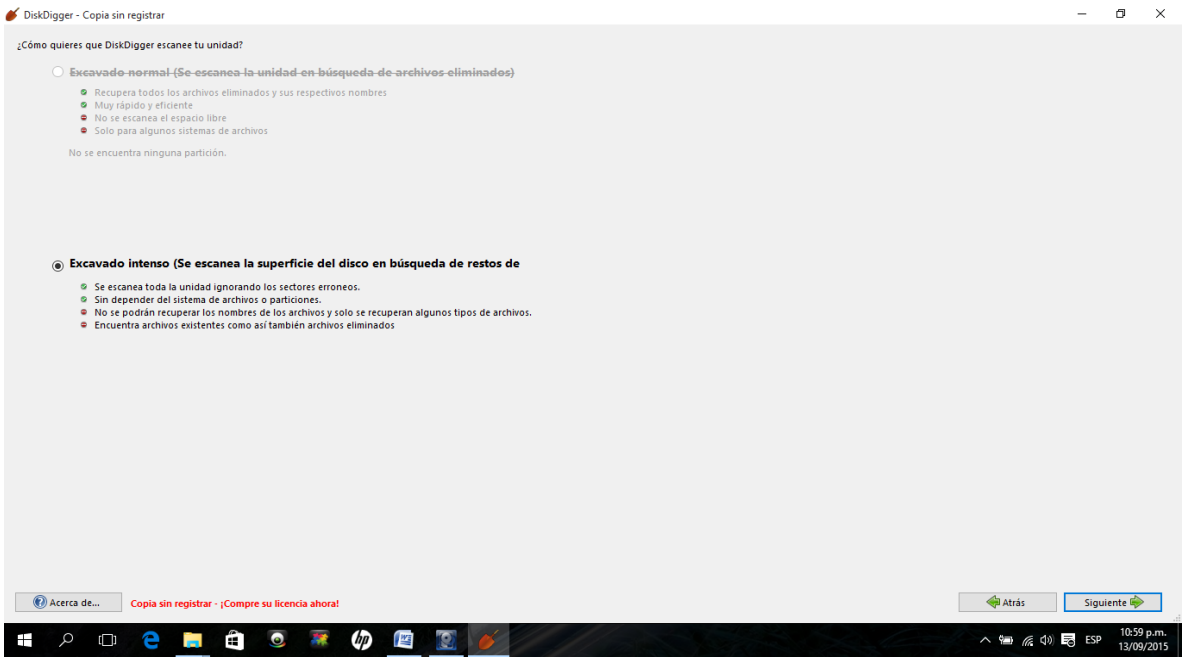


Figura 5.6 escaneo de unidad.

Nos muestra todo los formatos de archivos que podemos encontrar, en nuestro ejemplo seleccionamos .jpg (imagen) lo marcamos con un tilde > siguiente

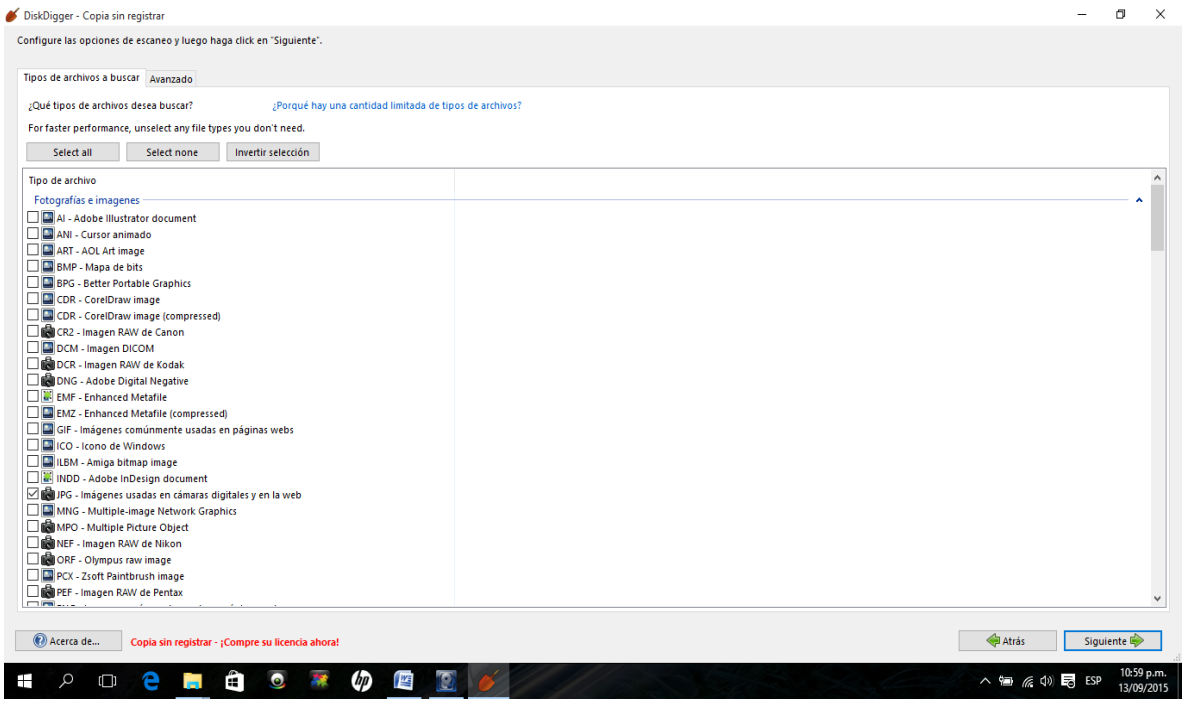


Figura 5.7 selección tipo de archivo.

Nos muestra una lista de todas las imágenes que se encuentran en el usb, si nos posicionamos en una imagen nos trae la información correspondiente.

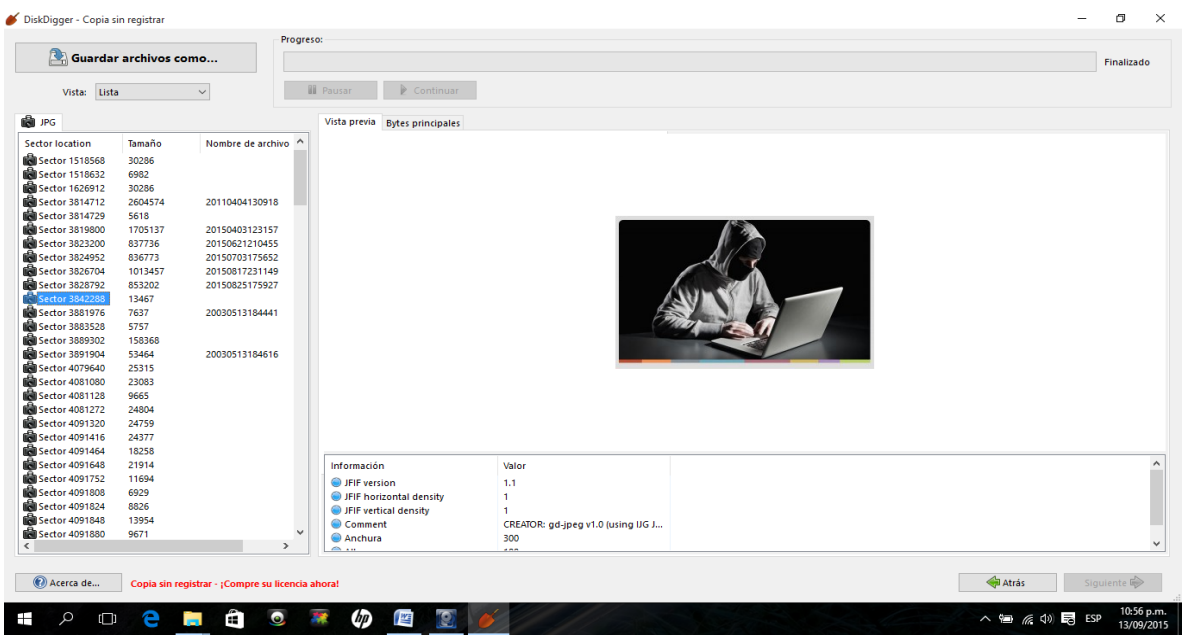


Figura 5.8 imágenes recuperadas del usb.

1.3 BACK TRACK 5

1.3.1 Recuperar Imágenes Borradas de un USB

Abrimos back track 5 y en la root: colocamos fdisk – l para listar las particiones, ver imagen:

Figura 5.9 sotfware back track 5

Nos muestra todas las particiones, copiamos la partición del usb: /dev/sdb, ver imagen:

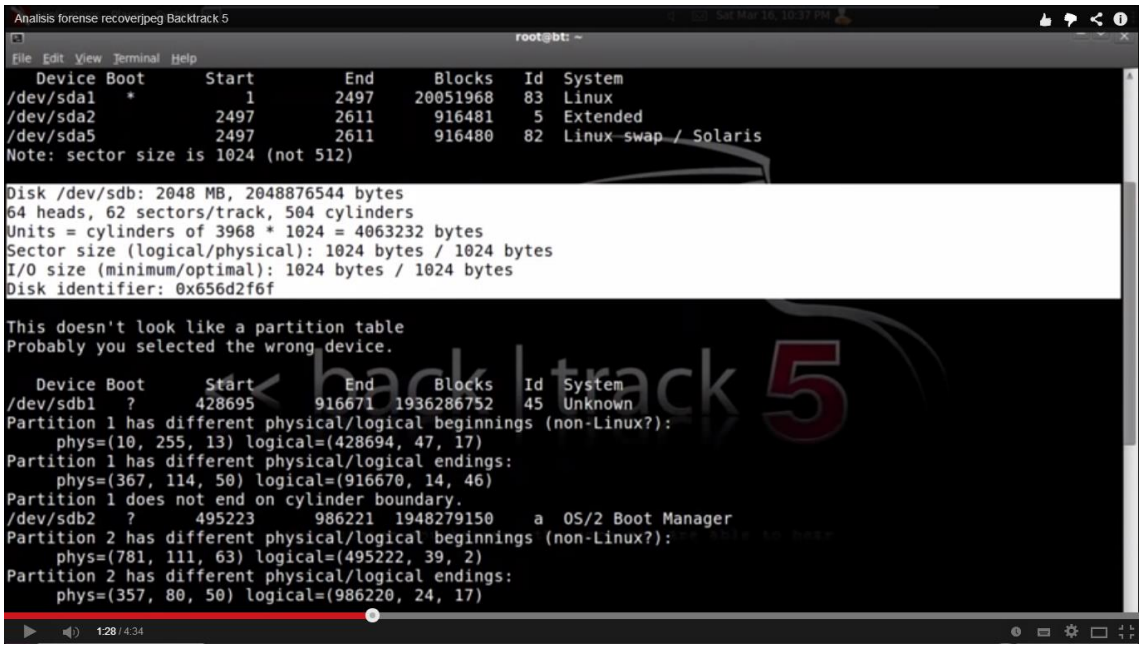


Figura 6.0 partición usb.

Colocamos recoverjpeg más el camino del usb /dev/sdb y back track comenzara el proceso de recuperación, ver imagen:

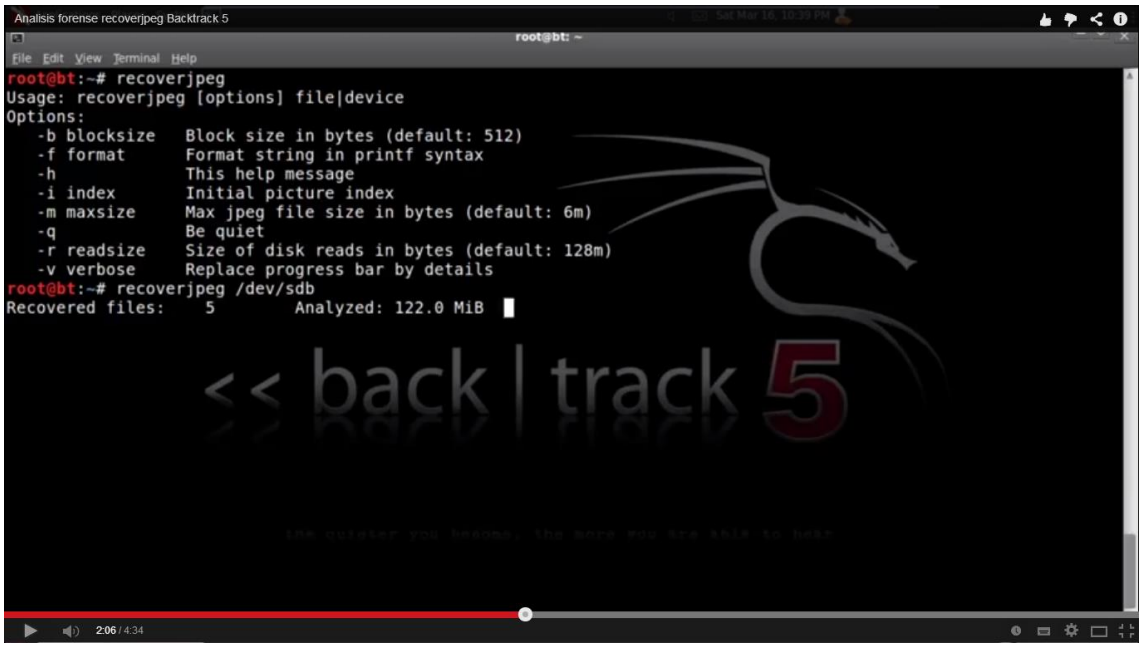


Figura 6.1 proceso de recuperación.

Back track recupero 5 imágenes jpeg que fueron borradas del usb, ver imagen:

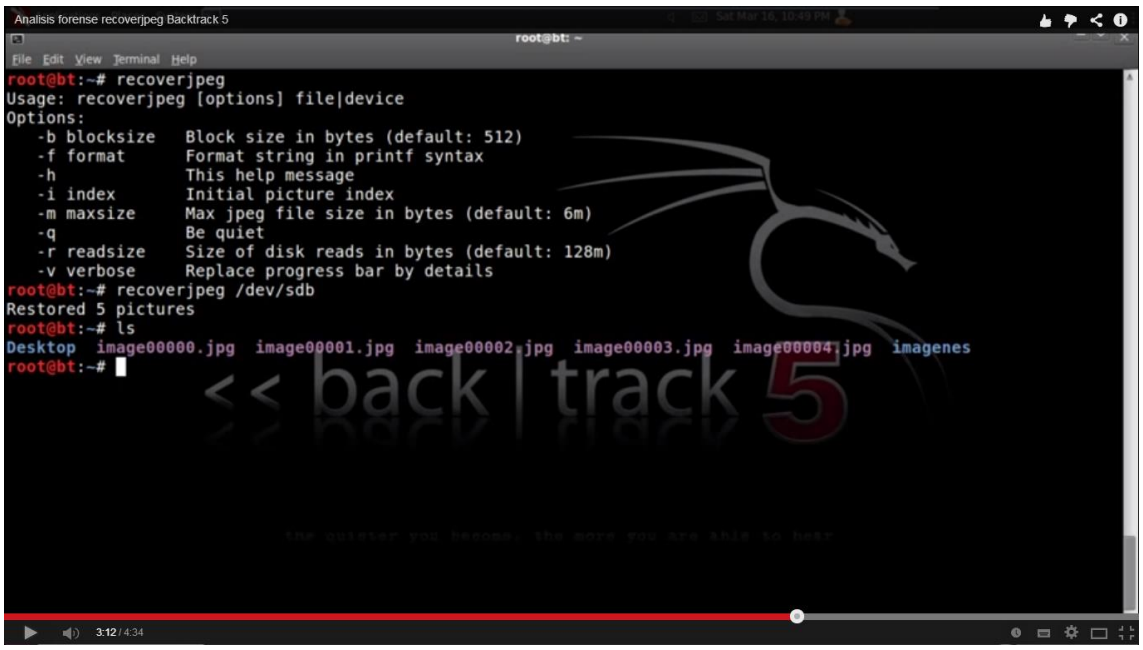


Figura 6.2 termina el proceso 5 imágenes recuperadas.

Como podemos observar estas son las cincos imágenes recuperadas del usb, ver imagen:

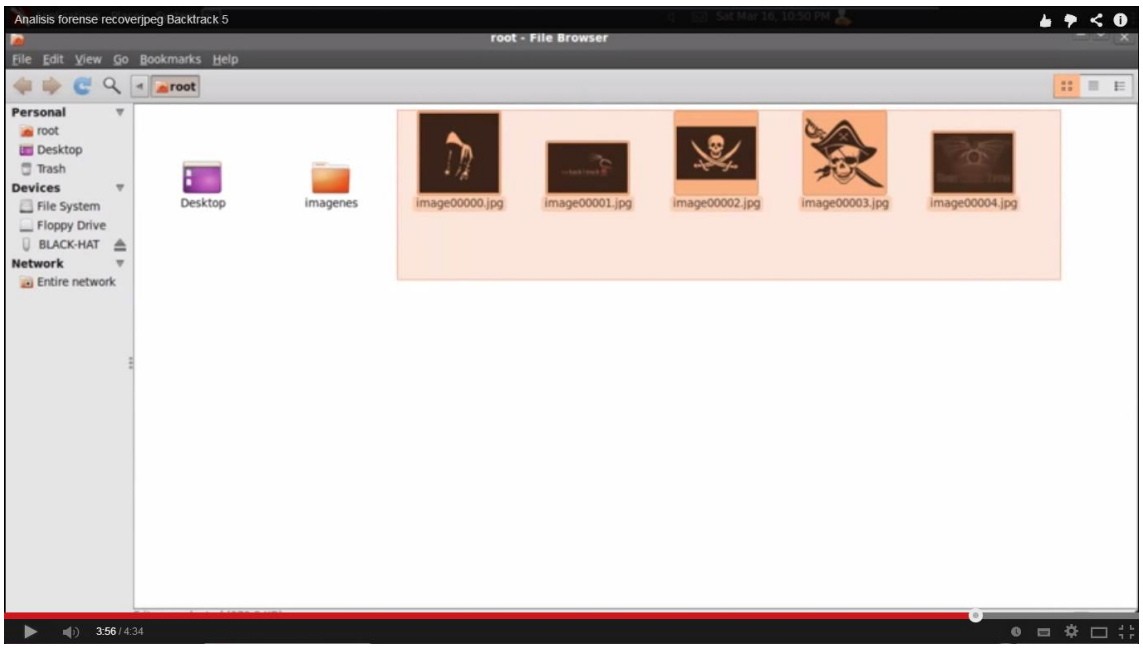


Figura 6.3 imágenes jpg. recuperadas.

Anexo B

Rastreo de Correo Electrónico

1.1 Utilización del sitio http://whatismyipaddress.com/trace-email para rastrear correos electrónicos de un sospechoso.

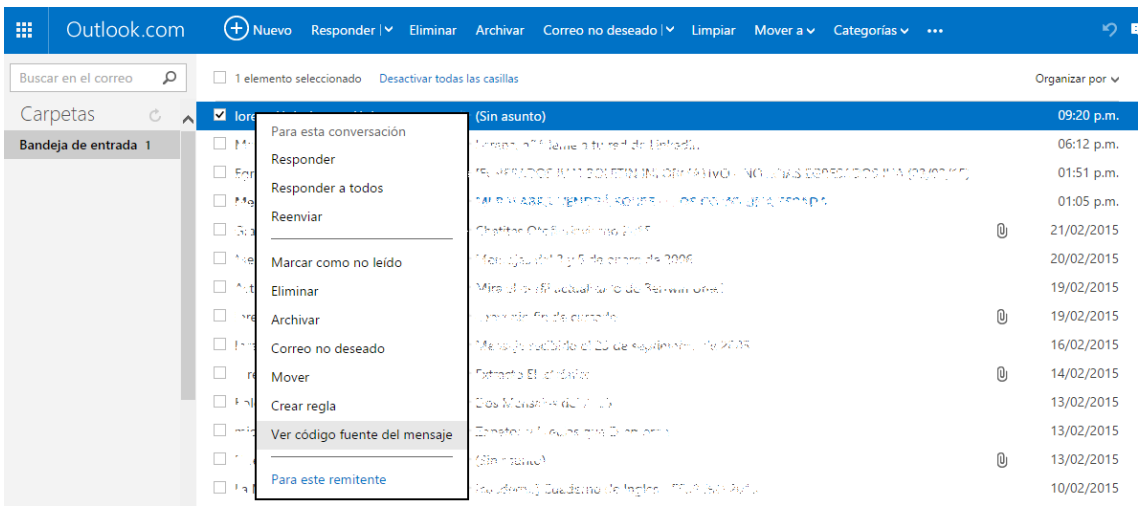
1.2 Descubrir datos del proveedor del servicio de internet (ISP)

1.1 Utilización del sitio http://whatismyipaddress.com/trace-email para rastrear correos electrónicos de un sospechoso.

Como parte del analisis forense digital, puede ocurrir que el perito requiera realizar el rastreo de e-mail recibidos por parte del sospecho.

En el mercado existen algunas herramientas para realizar esta analisis, pero la más utilizada es http://whatismyipaddress.com/trace-email que permite obtener a través de la cabecera del mail la dirección IP desde donde se envió el correo analizado.

1- Luego de acceder a la cuenta de correo; se selecciona el mail realizando un clic derecho y seleccionando la opción “Ver código fuente del mensaje”



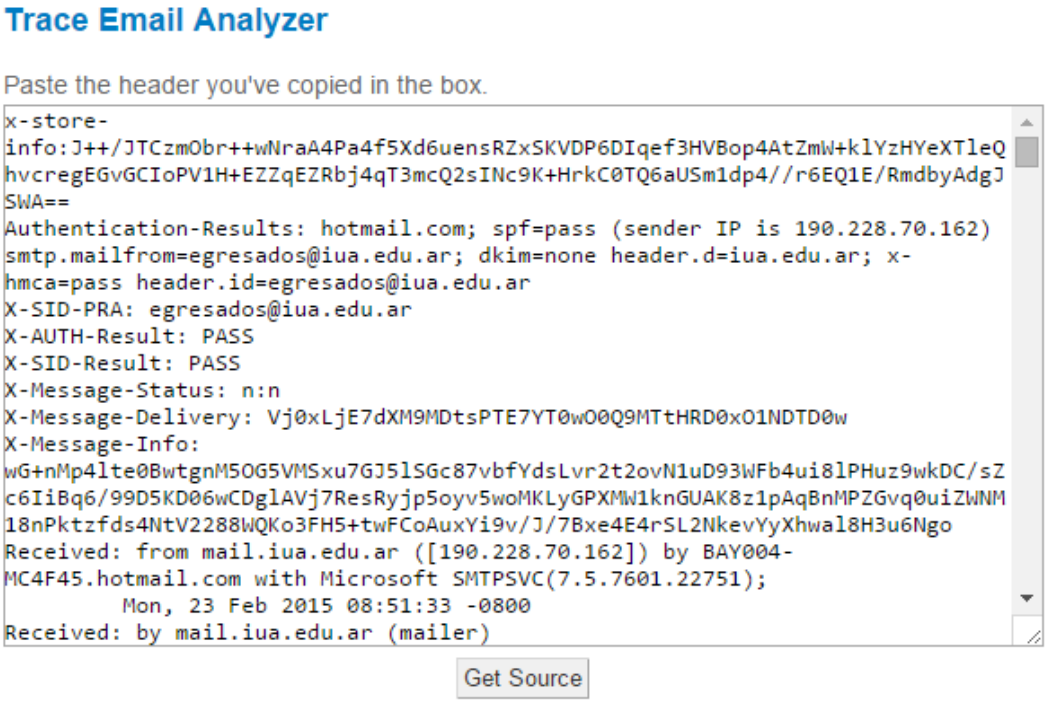
2- Seleccionar la cabecera del mensaje

```
x-store-info:J++/JTCzmObr++wNraA4Pa4f5Xd6uensRZxSKVDP6DIqef3HVBop4AtZmW+klYzHYeXTleQhvcregEGvGCIoPV1H+EZZqEZRbj4qT3mcQ2sINc9K+HrkC0TQ6aUSm1dp4//r6EQ1E/RmdbyAdgJSWA==
Authentication-Results: hotmail.com; spf=pass (sender IP is 190.228.70.162) smtp.mailfrom=egresados@iua.edu.ar; dkim=none header.d=iua.edu.ar; x-hmca=pass header.id=egresado
X-SID-PRA: egresados@iua.edu.ar
X-AUTH-Result: PASS
X-SID-Result: PASS
X-Message-Status: n:n
X-Message-Delivery: Vj0xLjE7dXM9MDtsPTE7YT0wO0Q9MTtHRD0xO1NDTD0w
X-Message-Info: wG+nMp4lte0BwtgnM5OG5VMSxu7GJ5lSGc87vbfYdsLvr2t2ovN1uD93WFb4ui8lPHuz9wkDC/sZc6IiBq6/99D5KD06wCDglAVj7ResRyjp5oyv5woMKLyGPXMW1knGUAK8z1pAqBnMPZGvq0uiZWNM18nPk
Received: from mail.iua.edu.ar ([190.228.70.162]) by BAY004-MC4F45.hotmail.com with Microsoft SMTPSVC(7.5.7601.22751);
         Mon, 23 Feb 2015 08:51:33 -0800
Received: by mail.iua.edu.ar (mailer)
        id 9AF581456532; Mon, 23 Feb 2015 13:51:07 -0300 (ART)
Delivered-To: egresados-iua-list@iua.edu.ar
Received: from localhost (localhost [127.0.0.1])
        by mail.iua.edu.ar (mailer) with ESMTP id 502991456537
        for <egresados-iua-list@iua.edu.ar>; Mon, 23 Feb 2015 13:51:07 -0300 (ART)
X-Virus-Scanned: amavisd-new at iua.edu.ar
Received: from mail.iua.edu.ar ([127.0.0.1])
        by localhost (mail.iua.edu.ar [127.0.0.1]) (amavisd-new, port 10024)
        with ESMTP id Sw2MDrWpJXk8 for <egresados-iua-list@iua.edu.ar>;
        Mon, 23 Feb 2015 13:51:07 -0300 (ART)
Received: by mail.iua.edu.ar (mailer, from userid 65534)
        id 002A61456535; Mon, 23 Feb 2015 13:51:06 -0300 (ART)
Delivered-To: egresados-iua@iua.edu.ar
Received: from localhost (localhost [127.0.0.1])
        by mail.iua.edu.ar (mailer) with ESMTP id 716E11456533
        for <egresados-iua@iua.edu.ar>; Mon, 23 Feb 2015 13:51:06 -0300 (ART)
X-Virus-Scanned: amavisd-new at iua.edu.ar
Received: from mail.iua.edu.ar ([127.0.0.1])
        by localhost (mail.iua.edu.ar [127.0.0.1]) (amavisd-new, port 10024)
        with ESMTP id uhp5R8FMh16s for <egresados-iua@iua.edu.ar>;
        Mon, 23 Feb 2015 13:51:06 -0300 (ART)
Received: from mail-qg0-f43.google.com (mail-qg0-f43.google.com [209.85.192.43])
        by mail.iua.edu.ar (mailer) with SMTP id 888ED1456532
```


3- Ingresar al sitio http://whatismyipaddress.com/trace-email

4- Copiar la cabecera del mensaje en el text box

5- Seleccionar la opción Get Source



6- Luego de realizar el análisis, se mostrara información valiosa, entre ellas la dirección IP; la localización de la misma, entre otras.

Analysis:

x-store-info:J++/JTCzmObr++wNraA4Pa4f5Xd6uensRZxSKVDP6DIqef3HVBop4AtZmW+klYzHYeXTleQhvcregEGvGCloPV1H+EZZqEZRbj4qT3mcQ2sINc9K+HrkC0TQ6aUSm1dp4//r6EQ1E/RmdbyAdgJSWA==
Authentication-Results: hotmail.com; spf=pass (sender IP is 190.228.70.162) smtp.mailfrom=egresados@iua.edu.ar; dkim=none header.d=iua.edu.ar; x-hmca=pass header.id=egresados@iua.edu.ar
X-SID-PRA: egresados@iua.edu.ar
X-AUTH-Result: PASS
X-SID-Result: PASS
X-Message-Status: n:n
X-Message-Delivery: Vj0xLjE7dXM9MDtsPTE7YT0wO0Q9MTtHRD0xO1NDTD0w
X-Message-Info: wG+nMp4lte0BwtgnM5OG5VMSxu7GJ5ISGc87vbfYdsLvr2t2ovN1uD93WFb4ui8lPHuz9wkDC/sZc6liBq6/99D5KD06wCDglAVj7ResRyjp5oyv5woMKLyGPXMW1knGUAK8z1pAqBnMPZGvq0uiZWNM18nPktzfd
Received: from mail.iua.edu.ar ([190.228.70.162]) by BAY004-MC4F45.hotmail.com with Microsoft SMTPSVC(7.5.7601.22751); Mon, 23 Feb 2015 08:51:33 -0800
Received: by mail.iua.edu.ar (mailer) id 9AF581456532; Mon, 23 Feb 2015 13:51:07 -0300 (ART)
Delivered-To: egresados-iua-list@iua.edu.ar
Received: from localhost (localhost [127.0.0.1]) by mail.iua.edu.ar (mailer) with ESMTP id 502991456537 for <egresados-iua-list@iua.edu.ar>; Mon, 23 Feb 2015 13:51:07 -0300 (ART)
X-Virus-Scanned: amavisd-new at iua.edu.ar
Received: from mail.iua.edu.ar ([127.0.0.1]) by localhost (mail.iua.edu.ar [127.0.0.1]) (amavisd-new, port 10024) with ESMTP id Sw2MDrWpJXk8 for <egresados-iua-list@iua.edu.ar>; Mon, 23 Feb 2015 13:51:07 -0300 (ART)
Received: by mail.iua.edu.ar (mailer, from userid 65534) id 002A61456535; Mon, 23 Feb 2015 13:51:06 -0300 (ART)
Delivered-To: egresados-iua@iua.edu.ar
Received: from localhost (localhost [127.0.0.1]) by mail.iua.edu.ar (mailer) with ESMTP id 716E11456533 for <egresados-iua@iua.edu.ar>; Mon, 23 Feb 2015 13:51:06 -0300 (ART)
X-Virus-Scanned: amavisd-new at iua.edu.ar
Received: from mail.iua.edu.ar ([127.0.0.1]) by localhost (mail.iua.edu.ar [127.0.0.1]) (amavisd-new, port 10024) with ESMTP id uhp5R8FMh16s for <egresados-iua@iua.edu.ar>; Mon, 23 Feb 2015 13:51:06 -0300 (ART)
Received: from mail-qg0-f43.google.com (mail-qg0-f43.google.com [209.85.192.43]) by mail.iua.edu.ar (mailer) with SMTP id 88BED1456532 for <egresados-iua@iua.edu.ar>; Mon, 23 Feb 2015 13:51:03 -0300 (ART)
Received: by mail-qg0-f43.google.com with SMTP id i50so25335659qgf.2 for <egresados-iua@iua.edu.ar>; Mon, 23 Feb 2015 08:51:02 -0800 (PST)

Source:

The source host name is "proxy.iua.edu.ar" and the source IP address is 190.228.70.180.

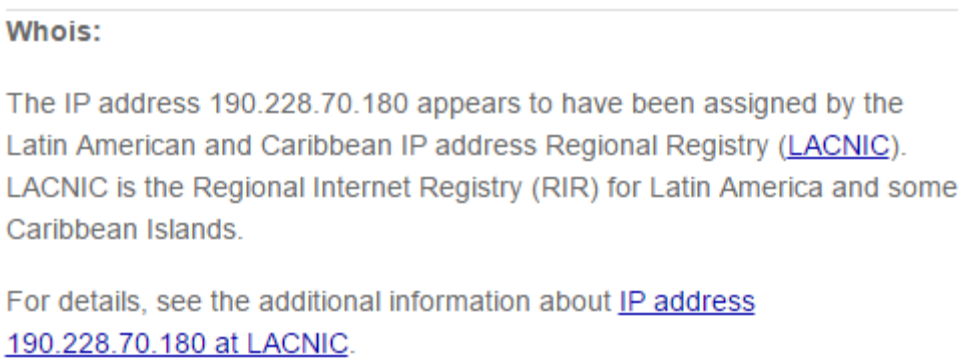
Geo-Location Information

Country	Argentina
State/Region	05
City	Cordoba
Latitude	-31.4135
Longitude	-64.1811
Area Code	

Geo-Location Map

1.2 Análisis del proveedor del servicio de internet.

Dentro del mismo sitio podemos encontrar el enlace a los Registros de Direcciones de Internet para Latinoamérica y el Caribe (LACNIC)



Seleccionando el link, se abrirá otra ventana con la información necesaria sobre el proveedor de internet, como así también los datos del responsable de la contratación del servicio; entre otras.

% 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.

% 2015-02-23 22:05:04 (BRT -03:00)

inetnum: 190.228.70.160/27

status: reallocated

owner: ASOCIACION DE INVESTIGACIONES TECNOLOGICAS

ownerid: AR-AITE1-LACNIC

responsible: ING. GUILLERMO FAUS

address: AV FUERZA AEREA ARGENTINA, 1, -

address: 5010 - CORDOBA -

country: AR

phone: +54 351 155463684 []

owner-c: IUA

tech-c: ADA

abuse-c: ADA

created: 20090317

changed: 20090317

inetnum-up: 190.228/14

nic-hdl: ADA

person: Administrador Abuse

e-mail: abuse@TA.TELECOM.COM.AR

address: Alicia Moreau de Justo, 50, -

address: 1107 - Ciudad Autónoma de Buenos Aires -

country: AR

phone: +54 11 49684000 []

created: 20030211

changed: 20110316

nic-hdl: IUA

person: Instituto Universitario Aeronáutico

e-mail: ebanchio@IUA.EDU.AR

address: Av. Fuerza Aérea, 6500,

address: 5022 - Córdoba - AR

country: AR

phone: +54 0351 4435000 [34115]

created: 20090316

changed: 20090721

% whois.lacnic.net accepts only direct match queries.

% Types of queries are: POCs, ownerid, CIDR blocks, IP

% and AS numbers.