INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA
Y ELÉCTRICA
UNIDAD CULHUACÁN

SEMINARIO DE TITULACIÓN
"SEGURIDAD DE LA INFORMACIÓN"

TESINA

"DETECCIÓN DE ImSeEx EN EQUIPOS DE CÓMPUTO DENTRO DE UNA RED DE DATOS LOCAL, UTILIZANDO FTK 3®"

QUE PRESENTAN PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN

BETZABÉ DE LA TORRE SUÁREZ
OMAR RODRIGO GALLARDO ABARCA

INGENIERO EN COMUNICACIONES Y ELECTRÓNICA

JESÚS EDUARDO PÉREZ ROMERO

Asesor:

DR. GABRIEL SÁNCHEZ PÉREZ

VIGENCIA: DES/ESIME-CUL-2008/23/2/10

México, D.F., Octubre 2010

IPN
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

TESINA

POR LA OPCIÓN DE TITULACIÓN SEMINARIO EN SEGURIDAD DE LA INFORMACIÓN

QUE PARA OBTENER EL TÍTULO DE INGENIERO EN COMPUTACIÓN

DEBERÁN DESARROLLAR: DE LA TORRE SUÁREZ BETZABÉ
GALLARDO ABARCA OMAR RODRIGO

Y QUE PARA OBTENER EL TÍTULO DE INGENIERO EN COMUNICACIONES Y ELECTRÓNICA

DEBERÁ DESARROLLAR: PÉREZ ROMERO JESÚS EDUARDO

"DETECCIÓN DE ImSeEx EN EQUIPOS DE CÓMPUTO DENTRO DE UNA RED DE DATOS LOCAL, UTILIZANDO FTK 3®"

INTRODUCCIÓN

LA PRESENTE TESINA TRATA SOBRE LA IDENTIFICACIÓN DE IMÁGENES SEXUALMENTE EXPLICITAS POR MEDIO DEL MODULO EXPLICIT IMAGE DETECTION DEL SOFTWARE FTK 3® DE ACCESS DATA, DENTRO DE EQUIPOS DE COMPUTO PERTENECIENTES A UNA RED LAN, ESTAS IMÁGENES SE PUEDEN ENCONTRAR EN CUALQUIER CARPETA, AUNQUE TENGAN UNA EXTENSIÓN DIFERENTE, HAYAN SIDO ELIMINADAS, O ESTÉN COMPRIMIDAS, PUEDEN LOCALIZARSE DENTRO DE UNA UNIDAD EXTRAÍBLE, COMO UN CD O UNA USB, ASÍ COMO EN UN EQUIPO REMOTO, PARA LO CUAL SE UTILIZA UN AGENTE EXISTENTE, EL CUAL ANALIZA LA MEMORIA Y LOS PROCESOS ACTIVOS; DADO EL CRITERIO DEL ANALISTA DE QUE LOS VALORES MAYORES A 60 EN LOS TRES PERFILES DE EID, SE CONSIDERABAN ImSeEx, SE OBTUVO DESPUÉS DE REALIZADAS LAS DIFERENTES PRUEBAS UN RESULTADO DE 91 % DE PRECISIÓN EN LA DETECCIÓN DE DICHAS IMÁGENES.

CAPITULADO

I. ESTADO DEL ARTE
II. MARCO TEÓRICO
III. PRUEBAS

México D.F., Octubre de 2010

VIGENCIA: DES/ESIME-CUL-2008/23/2/10

ESP. LIDIA PRUDENTE TIXTECO
Instructor del Seminario

DR. GABRIEL SÁNCHEZ PÉREZ
Asesor

M. EN C. LUIS CARLOS CASTRO MADRID
Jefe de la carrera de I.C.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

AGRADECIMIENTOS

Agradezco en primera instancia a mi madre que me brindó el apoyo y me impulsó para llegar a ser una profesionista, a mi abuelita por darme el consuelo en mis tropiezos para superar mis fracasos.

A mi esposo por desvelarse conmigo ayudándome en todo y siendo el soporte para lograr mis retos.

A mi abuelito que estoy segura que desde el cielo me cuida y que desde allá se enorgullece de mí, a mis tíos y primos por sus consejos y su ánimo en tiempos difíciles.

A Eduardo y Omar por haber hecho posible que este proyecto sea una realidad y a mis amigos que siempre creyeron y confiaron en mí.

Con Cariño.

Betzy.

Primeramente al único Dios verdadero, al Creador del cielo y la tierra, por darme la bendición de alcanzar una meta más en mi vida. ¡Gracias mi Señor!

A mi esposa Karin, por impulsarme en todo momento a superarme y seguir adelante con su amor y cariño, sacrificando en ocasiones el tiempo. De ti he aprendido a ser más perseverante. ¡Gracias amor!

A mi mamá Guadalupe, que aunque no está ya conmigo, siempre me brindó su amor, ayuda y apoyo para que fuera mejor. Enseñándome que el encomendar a Dios mi camino es lo principal.

A mi hermana Blanca, porque sin su sacrificio, amor y cariño no tendría la profesión que ahora culmino. El dar sin esperar nada a cambio es algo que aprendí de ti. ¡Gracias hermana!

A mis hermanas Martha y Cristina por su apoyo, dedicación, amor y tiempo invertido en mi. ¡Gracias por lo que sembraron en mí!

A mí cuñado Maurilio, porque sin su consejo y orientación, no hubiera decidido ser politécnico. A mi cuñado Juan por sus consejos, tiempo y amor durante mi niñez y juventud que tan importantes fueron en mi vida. ¡Gracias!

A mis compañeros, Betzabé y Omar por apoyarme durante el seminario que vivimos juntos. ¡Lo logramos!

Con amor.

Eduardo

Toda mi gratitud y respeto a mis Padres por su comprensión, sacrificios constantes y por su apoyo en mi tarea de terminar mis estudios profesionales.

Gracias mamá por ser tan locamente creativa e inteligente, y por haber insuflado un poco de todas esas virtudes en mi mezcla genética.

Gracias papá por enseñarme que a base de trabajo duro y perseverancia se logran los objetivos de ti aprendí a ver que la vida es algo por lo que vale la pena luchar.

Con gratitud y amor.

Omar

OBJETIVOS

GENERAL

Detectar imágenes sexualmente explícitas (ImSeEx) para su uso en un análisis forense en un equipo de cómputo perteneciente a una red de datos local, así como, en medios extraíbles, mediante FTK 3®.

PARTICULARES.

- Analizar diferentes tipos de piel mediante el módulo Explicit Image Detection (EID).
- Detectar la ubicación y la cantidad de imágenes dentro de los directorios en un equipo de cómputo perteneciente a una red de datos local para poder identificar si son o no explícitas y clasificarlas.
- Determinar si existen imágenes sexualmente explícitas en medios extraíbles.

ALCANCES

Este proyecto permitirá: detectar, identificar y clasificar imágenes sexualmente explícitas dentro de un equipo de cómputo perteneciente a una red de datos local y en medios extraíbles, aunque estén como archivos ocultos, comprimidos o que hayan sido eliminados.

JUSTIFICACIÓN

Ante el actual crecimiento del uso y posesión de imágenes sexualmente explícitas en nuestra sociedad, se necesita contar con una herramienta eficaz para la detección de este tipo de imágenes. Actualmente existen algunas herramientas para su detección, dentro de las cuales se encuentra el software FTK 3®.

La detección de estas imágenes permitirá localizar los equipos de cómputo que contengan imágenes sexualmente explícitas dentro de una red de datos local, para que el personal indicado tome las acciones que considere necesarias.

RESUMEN

Este trabajo de investigación fué desarrollado con la finalidad de brindar el apoyo técnico del manejo del módulo de detección de imágenes explicitas conocido como ***EID (Explicit Image Detection)***, para detectar ***ImSeEx (Imágenes Sexualmente Explícitas)*** en un equipo de cómputo perteneciente a una red de datos local ***LAN (Local Area Network)***, así como en medios extraíbles, con el software ***FTK 3® (Forensic Tool Kit 3®)***.

Este permitió detectar, identificar y clasificar una gran gama de imágenes, aún cuando éstas se encontraran ocultas, comprimidas o hubieran sido eliminadas.

Enfocándose en el modulo ***EID*** se realizaron diversos tipos de pruebas en las cuales se analizaron a un grupo de archivos y carpetas que comprendieron 10 repertorios por separado, conteniendo 100 imágenes cada uno. Estas pruebas fueron hechas para comprobar la eficiencia en la detección de las ***ImSeEx*** con el ***FTK 3®***.

Con base en los resultados obtenidos de las pruebas, se encontró el grado de efectividad aproximada del sistema, dándole una calificación de eficiencia de un 91%. Utilizando para ello el criterio siguiente: una imagen se consideró sexualmente explícita si los tres perfiles tenían un valor mayor a 60. Es de digno de mencionar que esto puede variar dependiendo del criterio del analista, manejo, interpretación de resultados y el alcance requerido, ya que el software puede tener tanto falsos positivos como falsos negativos.

INTRODUCCIÓN

A través del tiempo la tecnología y las telecomunicaciones han avanzado, permitiendo desarrollar software para una infinidad de actividades y transmisión de datos. Lo que nos permite compartir documentos, presentaciones e imágenes entre otros, siendo estas últimas la base de estudio en el presente proyecto.

Las imágenes en formato de fotografías o videos, que pueden contener figuras sexualmente explícitas hace 20 años se analizaban manualmente, lo cual se llevaba mucho tiempo y un margen de error muy grande, debido al gran número de personas que podían intervenir en el análisis de los archivos o pruebas.

En el Capítulo I se nombran algunos tipos de software que apoyan a desarrollar estos análisis con mayor efectividad y en el menor tiempo posible, y al mismo tiempo se especifica el software que se tomó para el proyecto, así como, una breve definición de filtro e imagen ya que son importantes para la presente investigación.

El Capítulo II detalla el funcionamiento general del software, la creación de diferentes casos, y la adición de evidencias a los casos nuevos y creados previamente.

En el Capítulo III, se lleva a cabo el desarrollo de pruebas con diferentes características, en una red LAN, mediante el sistema Access Data ***FTK 3***® apoyados en su módulo Explicit Image Detection (***EID***),. En estas pruebas se lograron detectar y desarrollar análisis de imágenes sexualmente explícitas, independientemente de donde se encontraran, su tipo de formato, borradas y aun cuando se encontraran comprimidas o con otra extensión diferente a la que se le asigna en su creación.

CAPÍTULO I.

ESTADO DEL ARTE

1.1. Antecedentes

El uso de material pornográfico por parte de la sociedad, ya sea en forma de fotografía o de video, ha existido desde hace mucho tiempo. La creación de dicho material muchas de las veces está ligada a delitos sexuales o venta del mismo, que cometen algunas personas.

El detectar material pornográfico que llevará a la detención de los criminales, anteriormente se llevaba a cabo manualmente, es decir, buscando en sus propiedades: revistas, fotos o videos que los inculparan. La proliferación de los delitos sexuales en nuestra sociedad, así como el uso de la tecnología y herramientas para su edición, manipulación y difusión de todo este material pornográfico, ha llevado al desarrollo de distintos software para detectar dicho material en los equipos de cómputo que son confiscados para un análisis forense.

1.2. Software de detección de imágenes sexuales explícitas

Es de suponer que el software que se encontró basa su funcionamiento en las redes neuronales, utilizando una serie de filtros para determinar si hay imágenes sexualmente explícitas alojadas en el equipo que se está analizando, dado que identifica la cantidad de piel existente en cada una de las imágenes que está analizando, y algunas otras características dependiendo del software que se utilice para la detección de este tipo de imágenes.

Algunos software de detección de imágenes sexualmente explícitas en el mercado son:

- Access Data ***FTK 3***® (módulo Explicit Image Detection)
- Paraben´s (Porn Detection Stick)
- Microsoft (SmutScanner)

Cabe mencionar que la principal causa por la que se seleccionó el software ***FTK 3***® para el desarrollo del presente trabajo, es debido al respaldo que tiene la compañía en el desarrollo de software de análisis forense de alta calidad [2].

1.3. Definición de imagen y filtro.

Una imagen se puede definir como una función bidimensional, f(x, y), donde "x" y "y" son coordenadas espaciales y "f" es la intensidad o nivel de gris de la imagen en esa coordenada, como se muestra en la figura 1.1 [3].

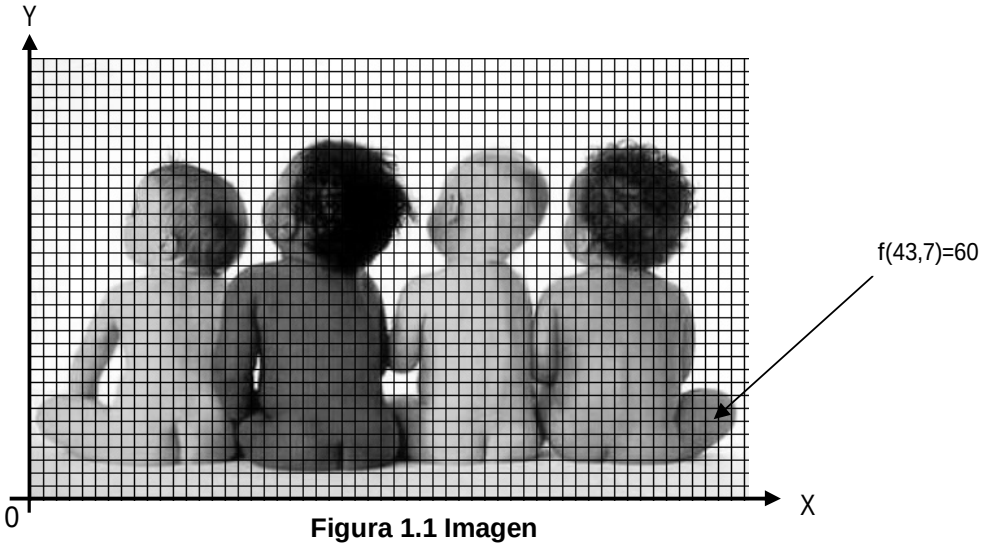
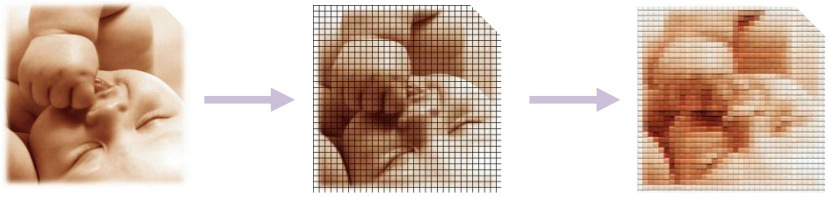


Figura 1.1 Imagen

Un filtro se define como una ecuación matemática que permite modificar el valor de un pixel según los valores de los pixeles contiguos, con coeficientes por cada pixel de la región a la que se le aplica. En la figura 1.2 se muestra un ejemplo de la aplicación de un filtro [4].



Original En pixeles Filtrada

Figura 1.2 Filtro

CAPÍTULO II.

MARCO TEÓRICO

2.1 Generalidades del software ***FTK 3®***

Está hecho bajo las leyes y las normas de seguridad profesionales para llevar a cabo una completa y exhaustiva investigación o dictamen forense a equipos de cómputo.

Tiene características de gran alcance en el análisis y búsqueda de archivos, por lo cual es reconocido como una herramienta líder en el campo forense a nivel mundial.

Está diseñado para ser utilizado por agentes del orden y seguridad corporativa, así como por profesionales de TI (Tecnología de la Información) que necesitan acceder y determinar el valor probatorio de la evidencia en los equipos de cómputo pertenecientes a una red de datos local.

Se puede utilizar para adquirir, preservar, analizar y presentar evidencia digital. Cualquier examen digital forense requiere los pasos básicos mostrados en la figura 2.1.

Figura 2.1 Pasos básicos de un análisis digital forense

La evidencia forense en un equipo de cómputo depende en gran medida de la protección y adquisición de los datos y el garantizar que no se realicen cambios y/o modificaciones en los archivos originales.

En todos los casos, se usa ***FTK 3*** Imager® para adquirir réplicas exactas de las evidencias electrónicas. Los datos que se encuentran en el equipo antes de ser añadidos a ***FTK 3***®, no se modifican, lo que significa que siguen siendo los mismos. Porque el archivo de imagen de disco es una réplica exacta de los datos de prueba, que se usaran como evidencia, pero en otro formato de archivo.

Se les llama ***evidencia estática*** a aquellos datos adquiridos a través de una imagen de disco que es obtenida del equipo que se está analizando, la cual es creada antes de ser agregada al caso.

Se conoce como ***evidencia en vivo*** a los datos que se adquieren de un equipo perteneciente a la red mientras éste se encuentra en funcionamiento, realizando una imagen de disco para mantener la evidencia, sin dañar los datos originales.

La adquisición de ***evidencia remota*** es el proceso de agregar evidencias en vivo a un caso nuevo o existente directamente desde ***FTK 3***®, procedentes de los equipos pertenecientes a la red.

FTK Imager® es una herramienta de adquisición por software, que garantiza crear el archivo de imagen de disco de una evidencia forense, de manera exacta. Hace un duplicado bit por bit de los medios de comunicación, haciendo una imagen de disco forense idéntico en todos los aspectos al original, incluyendo archivos y espacio libre, solo que con otro tipo de formato y extensión.

2.2 Creación de casos

La instalación de ***FTK 3***® se realiza de la misma forma que cualquier otro software, con las particularidades siguientes:

- Solicita crear un administrador proporcionando un nombre de usuario y contraseña, considerando que estos son sensibles entre mayúsculas y minúsculas.

- Para iniciar el ***FTK 3***® en Microsoft Windows Vista y Seven® se debe dar clic derecho en el ícono de ***FTK 3***® y ejecutar como administrador.

Este usuario y contraseña lo solicita cada que se inicia ***FTK 3***® para arrancar su interfaz.

Posteriormente se procede a darle un nombre al caso y si se desea: una referencia que indique a que se refiere y una breve descripción del mismo. Como se muestra en la figura 2.2.

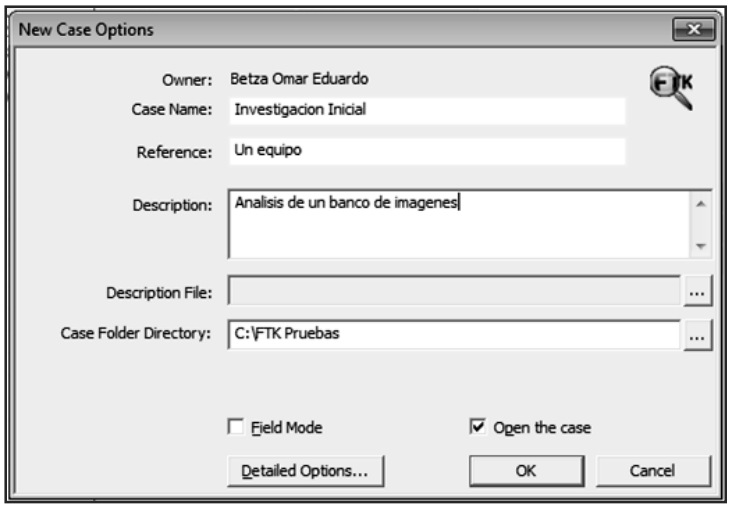


Figura 2.2 Creación de un caso

El análisis de casos permite seleccionar los parámetros requeridos para su desarrollo, la selección utilizada para el presente trabajo se muestra en la figura 2.3.

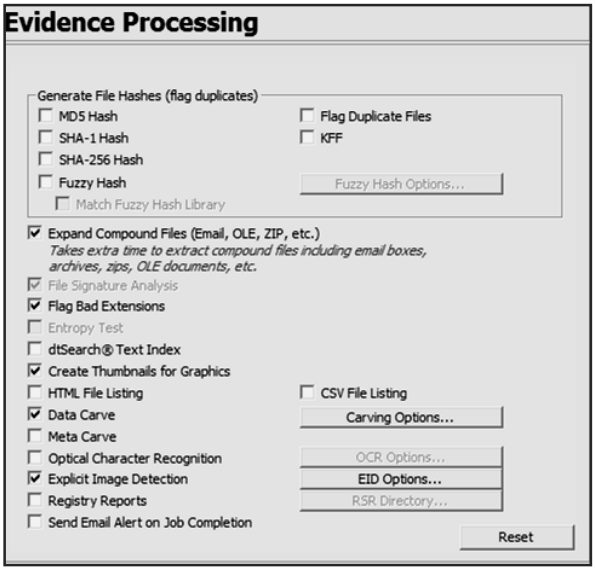


Figura 2.3 Parámetros de procesamiento de la evidencia

A continuación en la tabla 2.1 se muestra la descripción de los parámetros utilizados:

Tabla 2.1 Parámetros de Procesamiento de la Evidencia

Proceso	Descripción
• File Signature Analysis	• Analiza los archivos indicando si sus cabeceras o si las firmas coinciden con sus extensiones. Esta opción se encuentra predeterminada.
• Expand Compound Files	• Se abre automáticamente y procesa el contenido de archivos compuestos como: comprimidos, correo electrónico y los archivos OLE.
• Flag Bad Extensions	• Identifica archivos cuyos tipos no coinciden con sus extensiones, basándose en la información del encabezado del archivo.
• Generate Thumbnails for Graphics	• Crea imágenes en miniatura para todos los gráficos en un caso.

Tabla 2.1 Parámetros de Procesamiento de la Evidencia (continuación)

Proceso	Descripción
• Explicit Image Detection	• Los perfiles del módulo ***EID*** nos permiten identificar las posibles imágenes sexualmente explícitas mediante los valores asignados por cada perfil.
• Data Carve	• Usa el archivo de firmas para identificar archivos eliminados que figuran en la evidencia. Todos los tipos de archivos disponibles son seleccionados por defecto.

Detección de Imágenes Explícitas

En ***FTK 3***® la detección de imágenes explícitas (***EID***) analiza todos los archivos y carpetas en un caso, asignándoles una puntuación basada en la cantidad de piel que detecta de acuerdo a lo que interpreta como posible imagen sexualmente explícita.

En la tabla 2.2 se muestra la interpretación según ***FTK 3***® de los valores ***EID***, en base a lo que detecta en cada imagen.

Tabla 2.2 Valores de *EID* Según *FTK 3*®.

Interpretación de los valores ***EID***
0 a 100 = No se detecta piel o se detecta mucha piel.
-1 = Archivo no encontrado
-2 = Error de licencia
-3 = Formato de archivo incorrecto
-4 = No se encontró coincidencia
-5 = Carpeta no encontrada
-6 = Error desconocido
-7 = No se puede cargar la imagen (ej. Imagen corrupta)

Tabla 2.2 Valores de *EID* Según *FTK 3*® (continuación)

Interpretación de los valores ***EID***
-8 = No hay suficiente información
-9 = El perfil de detección facial es nulo
-10 = No se puede abrir el directorio de detección facial
-11 = Archivo detección facial no encontrado
-12 = Clasificador de entrada no inicializada
-13 = Fallo el inicio de perfil
-14 = Ruta del archivo vacía
-16 = La imagen de datos está vacía
-17 = Emparejamiento nulo
-18 = Recuperación de resultado perdida
-100 = Formato de archivo no soportado
-101 = Imagen en blanco y negro no soportada
-102 = Imagen en escala de grises no soportada
-103 = Imagen monocromática no soportada
-1000 = Error desconocido
-1001 = La puntuación de la función ***EID*** inicio una excepción
-1002 = La puntuación de la función ***EID*** inicio una excepción

Los perfiles de ***EID*** son los tres que se muestran en la figura 2.4.

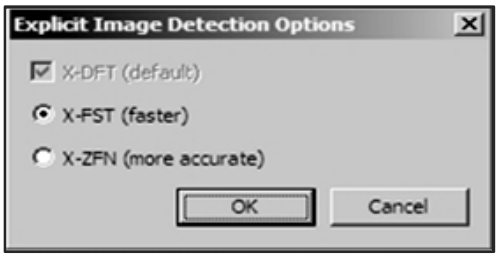


Figura 2.4 Perfiles de *EID*

Se puede elegir entre los perfiles en función de las necesidades, estos se detallan en la tabla 2.3.

Tabla 2.3 Descripción de perfiles *EID*

Nombre	Nivel	Descripción
• X-DFT	• Default (XS1)	• Este es el más preciso en general, es el que la herramienta selecciona automáticamente.
• X-FST	• Fast (XTB)	• Este es el más rápido. Le asigna valores numéricos a los archivos que considera como imágenes. Se basa en una tecnología diferente a la X-DFT. Está diseñado para grandes volúmenes de datos. Su objetivo es reducir rápidamente, la cantidad de archivos o el volumen de datos a un conjunto significativo.
• X-ZFN	• Menos falsos negativos (XT2)	• Se trata de un perfil similar al X-FST, pero con más características y con menos falsos negativos que X-DFT. Aplicar este filtro después de su transformación inicial para todas las pruebas, o para sólo las carpetas con una puntuación más alta con la opción X-FST.

AccessData marca por defecto el perfil default (X-DFT), que es el que detecta la cantidad de piel existente en las imágenes, recomienda ejecutar primero el perfil rápido (X-FST), que identifica las imágenes rapidamente, y posteriormente el de menos falsos negativos (X-ZFN) en las carpetas de alta calificación para lograr un análisis mas profundo y con resultados más precisos, el cual lleva un tiempo mas extenso.

Suponemos que estos perfiles trabajan con la Transformada de Fourier para poder detectar la cantidad de piel en las imágenes existentes en el equipo que se esta analizando.

Nota: Para realizar el análisis por medio de los dos perfiles, una vez que se ha terminado de procesar el caso, se procede como sigue: seleccionar Evidence>Additional Analysis de la barra de menús, marcar la opción Explicit Image Detection, dando clic en ***EID*** Options y seleccionando los tres perfiles (X-DFT, X-FST Y X-ZFN) como se indica en la figura 2.5.

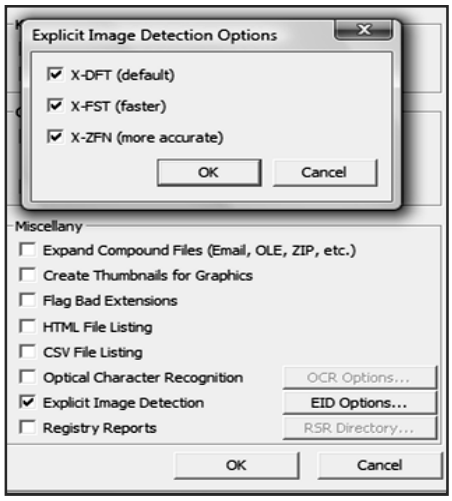


Figura 2.5 Perfiles en el análisis adicional

Después de realizada la selección anterior, se procede a escoger el origen donde se presume que está la evidencia. Para ello se da clic en el botón "Add" en donde podremos seleccionar entre varias opciones la forma de desarrollar el análisis de una manera más específica, como se ilustran en la figura 2.6.

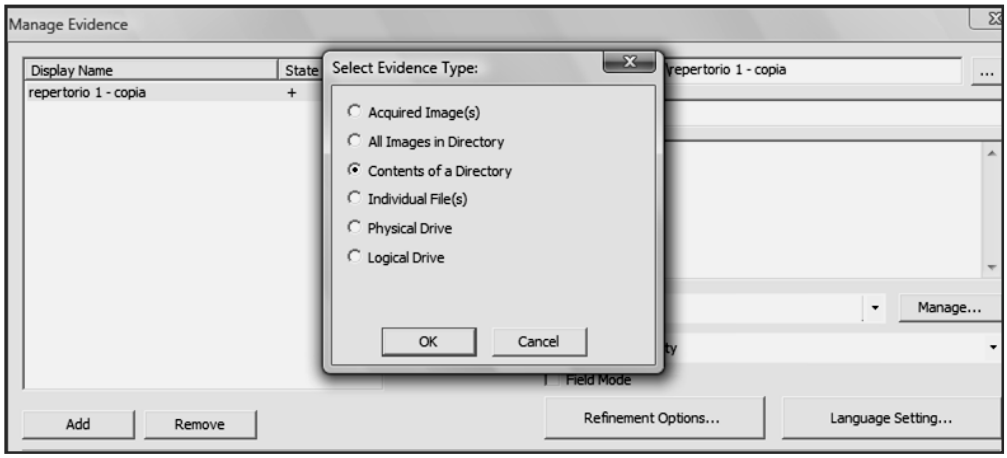


Figura 2.6 Opciones para la procedencia de la evidencia

Al darle "ok" se abre una ventana en donde se seleccionará la carpeta deseada.

Cuando se haya terminado de seleccionar todas las opciones del caso inicial, se procede a crear el caso. Hasta este momento no se han añadido evidencias al caso todavía. Al hacer clic en "ok" se iniciará la creación del caso.

Una vez iniciado el caso, se realiza la creación de una imagen de disco de la evidencia, para trabajar en ella y no en los archivos originales, evitando así un posible daño o pérdida de los mismos. ***FTK 3***® lo solicita como se puede ver en la figura 2.7.

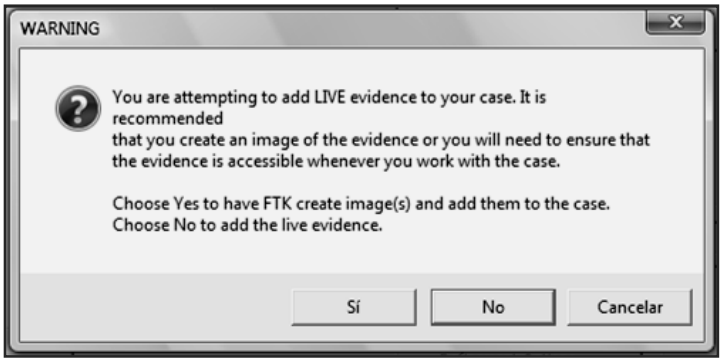


Figura 2.7 Creación de imagen de disco

Para abrir un caso existente en ***FTK 3***®. Se realizan los siguientes pasos:

- Inicie sesión en ***FTK 3***® y
- Dar doble clic en el caso que se quiere abrir.

2.3 Adición de evidencias

Después de crear un caso se pueden importar archivos relevantes cuando sea necesario, verificando la integridad de la imagen de disco deseada, identificando evidencia significativa, para realizar otras tareas.

Cuando la creación de un caso está completa, ***FTK 3***® abre el diálogo del administrador de casos. Los archivos de la evidencia que se agregaron aquí fueron procesados utilizando las opciones seleccionadas anteriormente.

Para añadir evidencia estática a un caso existente, de debe seleccionar: Evidence>Add/Remove de la barra de menús. Un ejemplo se muestra en la figura 2.8.

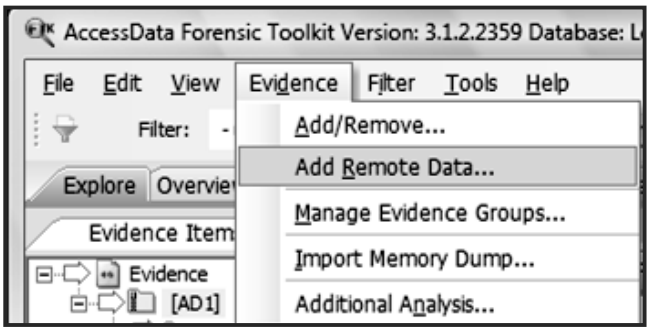


Figura 2.8 Agregar evidencia

Es importante mencionar que las evidencias tomadas de cualquier fuente física que es removible, pasarán a ser inaccesibles para el caso si la unidad cambia de letra o es movida.

FTK 3® puede adquirir evidencia viva de computadoras de la red. Para ello existen dos métodos: La inserción de un agente temporal y el uso de un agente existente [1].

CAPÍTULO III.

PRUEBAS

3.1 En un equipo de cómputo con SO Microsoft Windows®

Para realizar estas pruebas, se conectó la CmStick, que es la llave que permite abrir el ***FTK 3***®.

Las pruebas que se realizaron están organizadas en los siguientes tipos de evidencia mostradas en la figura 3.1.

Figura 3.1 Selección de tipo de evidencia

Archivo de Imagen de disco adquirido

Esta evidencia provenía de una imagen de disco obtenida previamente. Al encontrar dicha imagen el programa añadió la evidencia al caso que se estaba analizando.

Todos los archivos de imagen de disco en un directorio

Al seleccionar esta opción el programa buscó todos los archivos de imagen de disco que se encontraban en la ubicación que se le indicó, lo que permitió obtener las imágenes de disco que se buscaban.

Archivos individuales

Se añadió una evidencia específica de la que se conocía la ruta para analizarla detalladamente.

Unidad física

Está ayudó para analizar una unidad de disco completa, obteniendo datos específicos, como: las particiones y el sistema de archivos, más los archivos contenidos en el disco.

Unidad lógica

Permitió analizar una unidad de disco completa, obteniendo datos específicos, como: el sistema de archivos, y los archivos eliminados, junto con los archivos contenidos en el disco. Un ejemplo del análisis se muestra en la figura 3.2.

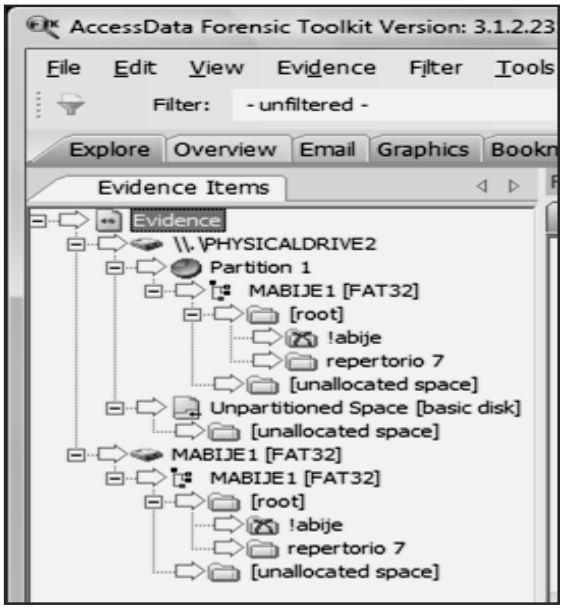


Figura 3.2 Unidad física y lógica

Contenido de un directorio

Aquí se seleccionó un directorio específico indicándole al programa que extrajera la evidencia del mismo. Éste extrajo todos los archivos encontrados y los procesó según el perfil de análisis de ***EID*** que se había determinado.

Una vez que inició el procesamiento de la evidencia el programa mostró una pantalla como la indicada en la figura 3.3.

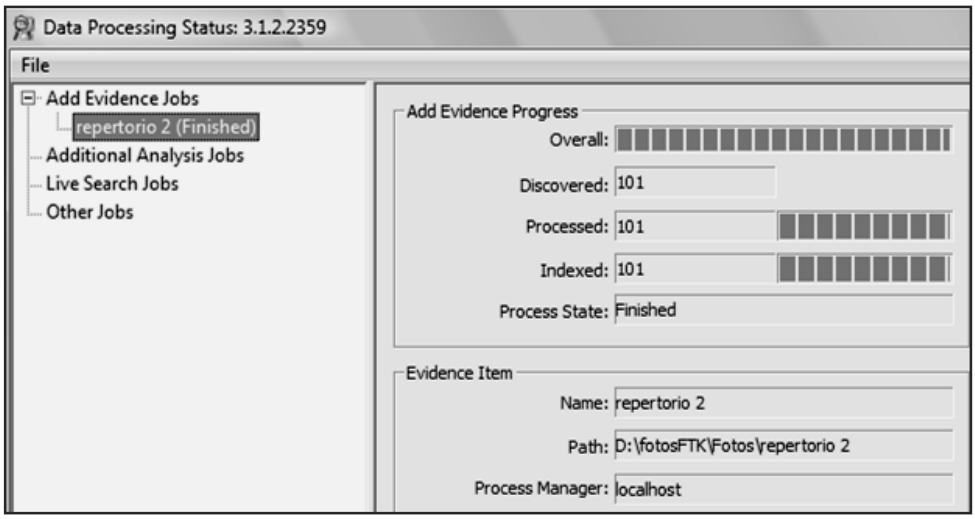


Figura 3.3 Procesamiento de la evidencia

Con este tipo de evidencia se realizaron una serie de pruebas que a continuación se detallan:

Prueba 1.

Se creó una carpeta que contenía archivos de texto, hojas de cálculo, PDF´s y presentaciones con diapositivas. Para determinar si ***FTK 3***® tiene la característica de de detectar imágenes dentro de este tipo de archivos.

Resultados

Se pudo observar que el software encuentra los archivos, sin embargo ***EID*** no le asigna valores a los mismos, dado que no puede ver lo que está dentro del archivo aunque si se puede observar en su explorador, como se observa en la figura 3.4.

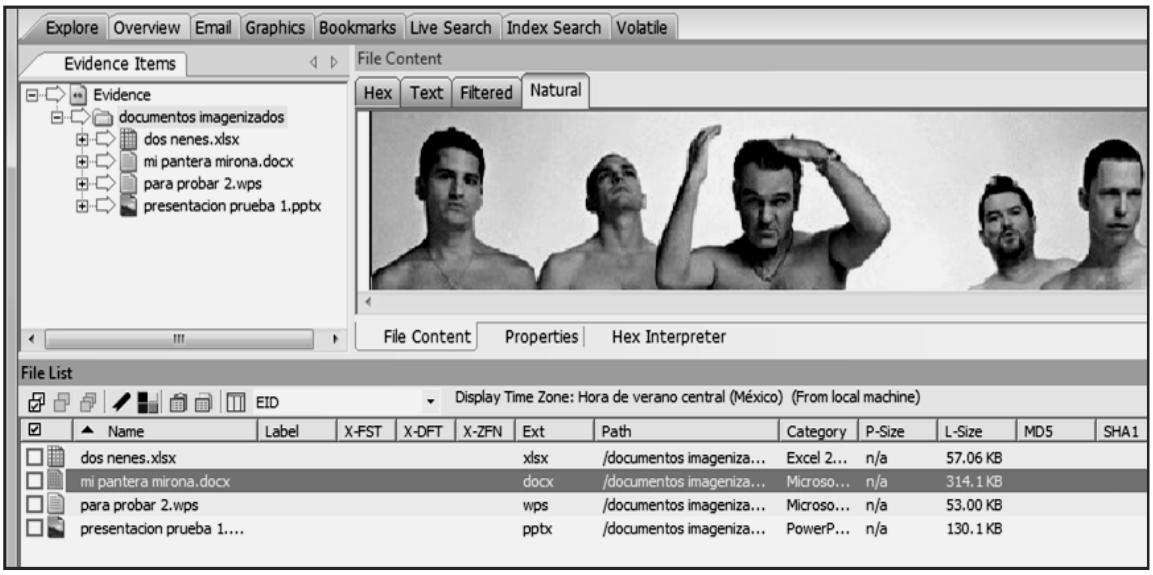


Figura 3.4 Prueba 1 Diferentes tipos de archivo

Prueba 2.

Se creó una carpeta con 100 imágenes de diversos tipos en una unidad USB y otra con las mismas características en el disco duro, posteriormente se le dio formato rápido a la USB y se borró la carpeta del disco duro. Se creó un caso, seleccionando "Physical Drive" en donde el software hizo un análisis físico de las unidades USB y la de disco duro para ver si detectaba los archivos eliminados.

Resultados

Al terminar la prueba se observó que ***FTK 3***® no encuentra los archivos eliminados, pero nos muestra las particiones y el sistema de archivos. Como se observa en la figura 3.5.

Prueba 3.

Se creó una carpeta con 100 imágenes de diversos tipos en una unidad USB y otra con las mismas características en el disco duro, posteriormente se le dio formato rápido a la USB y se borró la carpeta del disco duro. Se creó un caso, seleccionando "Logical Drive" en donde el software hizo un análisis lógico de las unidades para ver si detectaba los archivos eliminados.

Resultados

Al terminar la prueba se constató que efectivamente ***FTK 3***® encontró todos los archivos que habían sido eliminados al formatear la USB y los que habían sido borrados del disco duro. Lo cual se muestra en la figura 3.5.

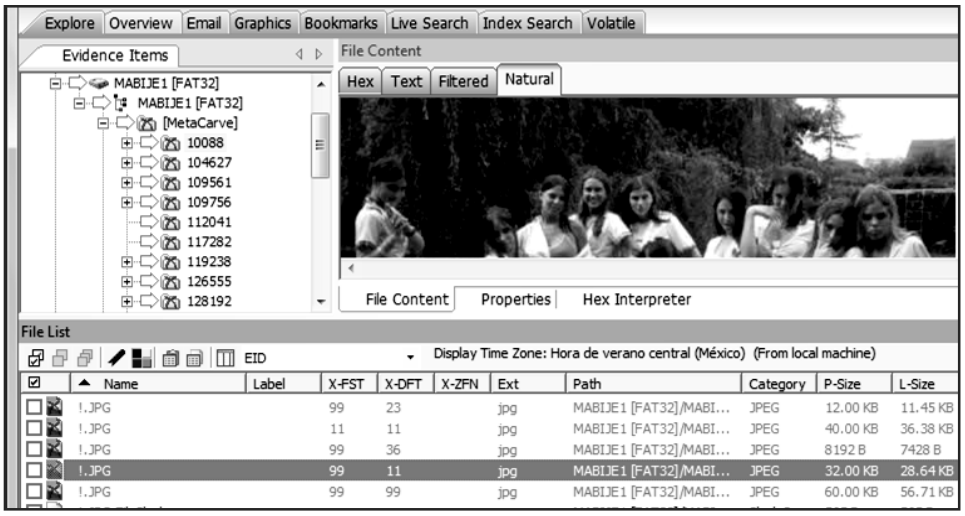


Figura 3.5 Pruebas 2 y 3 Archivos eliminados

Prueba 4.

Se creó una carpeta con 100 imágenes de diversos tipos, la cual después se comprimió. Se creó un caso, seleccionando "Individual Files" para comprobar que el software es capaz de detectar imágenes en este tipo de archivos. Adicionalmente se analizaron un CD de datos y un disco duro externo con las mismas características.

Resultados

Se corroboró que ***FTK 3***® es capaz de detectar eficazmente las imágenes que se encuentran dentro de una carpeta comprimida. Además de lo anterior, muestra la carpeta comprimida asignándole valores ***EID*** para que se pueda decidir si abrirla o no. La imagen obtenida de esta prueba se observa en la figura 3.6.

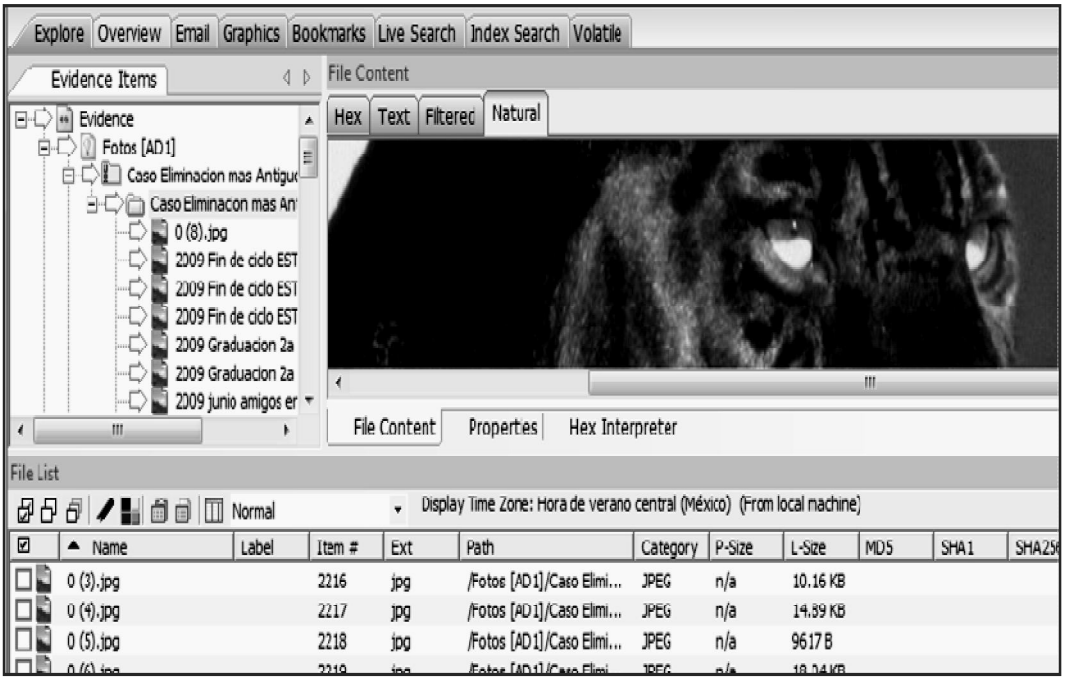


Figura 3.6 Prueba 4 Archivo comprimido

Prueba 5.

Se creó una carpeta con 14 imágenes de diversos tipos y se le cambiaron aleatoriamente las extensiones, se creó un caso para comprobar la función "Flag Bad Extensions" de ***FTK 3***®, que Identifica archivos cuyos tipos no coinciden con sus extensiones.

Resultados

Se observó que efectivamente reconoce las imágenes a pesar del cambio de las extensiones de archivo, mostrando además los valores ***EID*** correspondientes. Así como también muestra la extensión que está cambiada y el tipo de archivo real, como se observar en la figura 3.7.

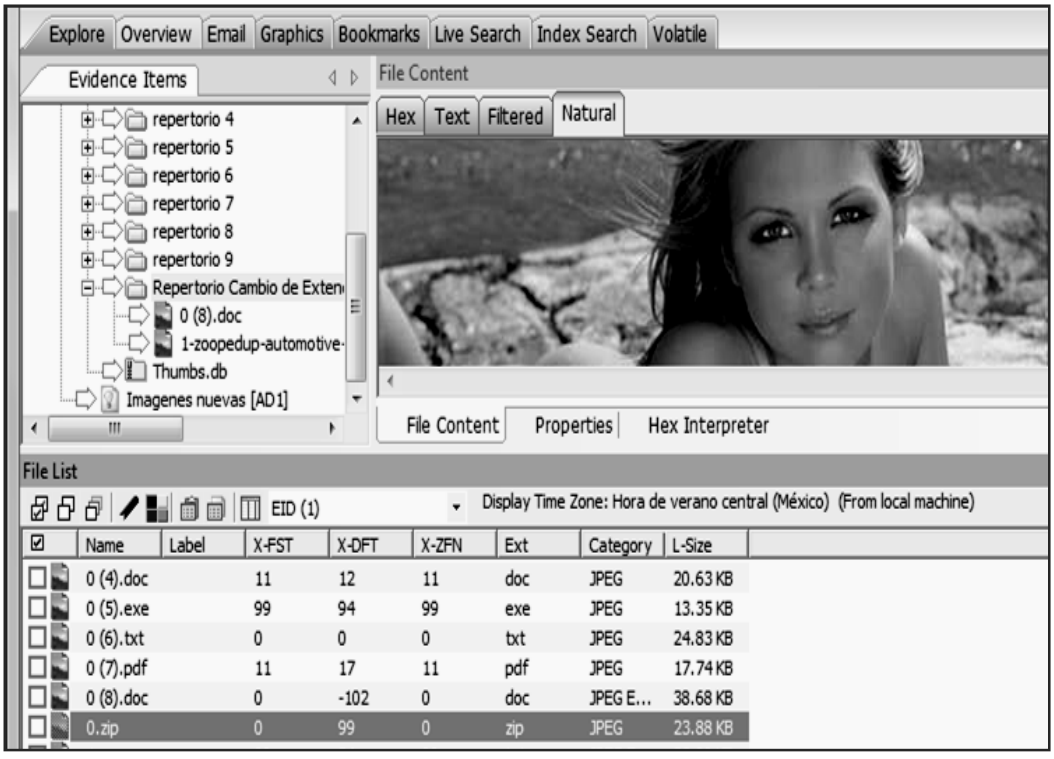


Figura 3.7 Prueba 5 Extensiones falsas

Prueba 6.

- Se creó una cuenta de correo electrónico y se dio de alta en el Outlook 2007®, al que le enviamos 4 correos con imágenes.
- Se abrió el Outlook revisando que se hubieran recibido los correos.
- Se revisaron los correos, comprobando que habían llegado las imágenes.
- Se seleccionó un correo y se eliminó.
- Se creó un caso seleccionando "Contents of a Directory" dirigiéndonos a la carpeta donde el equipo guarda los archivos con extensión "pst". Para comprobar la función que realiza "Expand Compound Files".

Resultados

Se comprobó que detecta todos los correos existentes, inclusive los eliminados, además de los archivos adjuntos que contenían. Donde ***EID*** les asignó una puntuación indicando cuales contenían imágenes. En la figura 3.8 se puede ver cómo mostró los correos y en la 3.9 el correo eliminado y los archivos adjuntos que contenía.

Figura 3.8 Prueba 6 Vista de correo

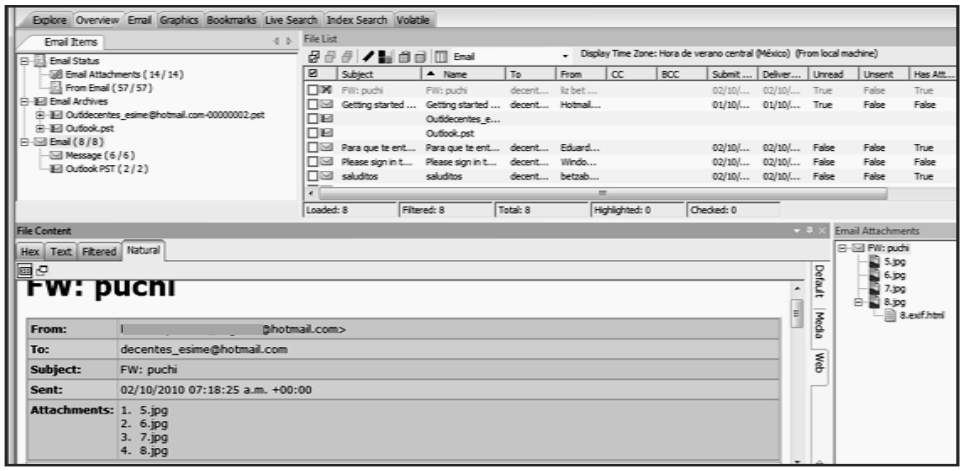


Figura 3.9 Prueba 6 Correo eliminado

Prueba 7.

Se realizó la imagen de disco de 10 repertorios por separado, los cuales contenían 100 imágenes cada uno.

- Se creó un caso para analizar la imagen de disco del repertorio 1, mediante la opción "Acquired Image".

- Utilizando "Add/Remove", se agregó mediante la opción "All Images in Directory" las imágenes de los otros nueve repertorios, que se localizaban en una carpeta específica y aparecen como se muestra en la figura 3.10.

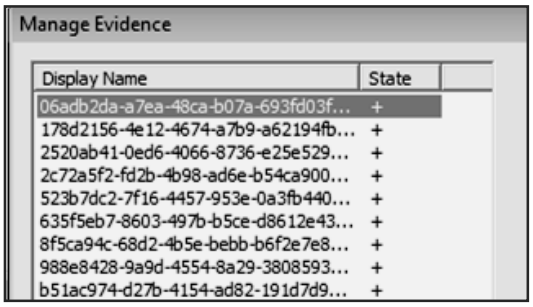


Figura 3.10 Prueba 7 Imágenes en un directorio

Lo anterior fue realizado para determinar la detección correcta de ***ImSeEx*** mediante ***FTK 3***®, considerando los valores ***EID*** de la tabla 2.3.

Resultados

Después de realizado el análisis y aplicando el criterio, de que una imagen sería considerada como sexualmente explícita si los valores ***EID*** eran mayores a 60 en los tres perfiles. Se obtuvieron los falsos positivos, los falsos negativos y la detección correcta de cada repertorio. Resultados que se muestran en la tabla 3.1.

Tabla 3.1 Detección correcta de *ImSeEx*

Caso	Falsos positivos	Falsos negativos	Detección correcta
Repertorio 1	11	1	88
Repertorio 2	12	2	86
Repertorio 3	15	1	84
Repertorio 4	5	4	91
Repertorio 5	5	2	93
Repertorio 6	9	0	91
Repertorio 7	5	3	92
Repertorio 8	6	2	92
Repertorio 9	6	5	89
Repertorio 10	7	1	92

3.2 En equipos dentro de una red de datos local

Para realizar las pruebas en equipos de cómputo dentro de una red de datos local, los cuales son considerados equipos remotos, se realizó previamente el siguiente procedimiento.

Desde el equipo emisor (el que tiene instalado ***FTK 3***®) Se copiaron los siguientes archivos y carpetas que se muestran en la figura 3.11 en una carpeta nueva.

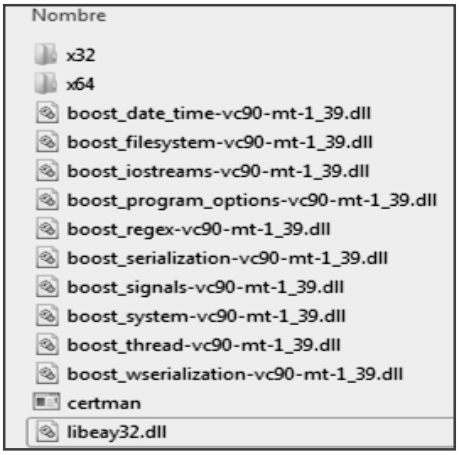


Figura 3.11 Archivos necesarios para la creación de certificados

Los archivos y carpetas se encuentran en las siguientes rutas:

- C:\Archivos de Programa\AccessData\Forensic Toolkit\3.1\bin
- C:\Archivos de Programa\AccessData\Forensic Toolkit\3.1\bin\Agent

Para crear los certificados autofirmados, se abrió una línea de comandos situándose en la carpeta recién creada en donde se escribió la siguiente instrucción:

Certman –n [nombre del equipo emisor] [nombre deseado del certificado], un ejemplo se muestra en la figura 3.12, y se crean el certificado público y privado que se muestran en la figura 3.13.

Figura 3.12 Creación de certificados

Figura 3.13 Certificado público y privado

Posteriormente se copió la versión apropiada del agente FTK (32 o 64) y el certificado público a la USB (el que tiene la extensión "crt").

Una vez copiados el agente y el certificado público en la USB, se procedió a insertarla en el equipo destino.

En éste, se abrió una línea de comandos como administrador y se recorrió la ruta donde se encontraban los archivos, escribiendo el siguiente comando para iniciar el agente existente:

FTKAgent –cert [Nombre del certificado] –port [numero de puerto] –timeout [valor en minutos antes de que se detenga el agente por inactividad]. Un ejemplo se muestra en la figura 3.14.

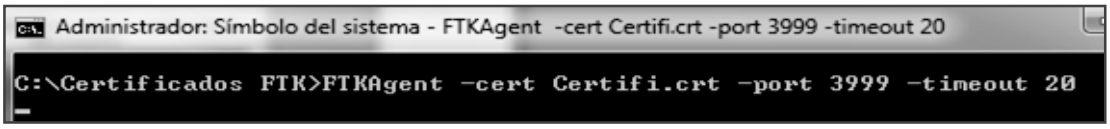


Figura 3.14 Ejecución del Agente existente

Una vez insertado el agente en el equipo destino, en un caso abierto, se añadieron datos remotos, introduciendo la IP del equipo remoto, el puerto especificado y seleccionamos la opción usar un agente existente, como se muestra en la figura 3.15.

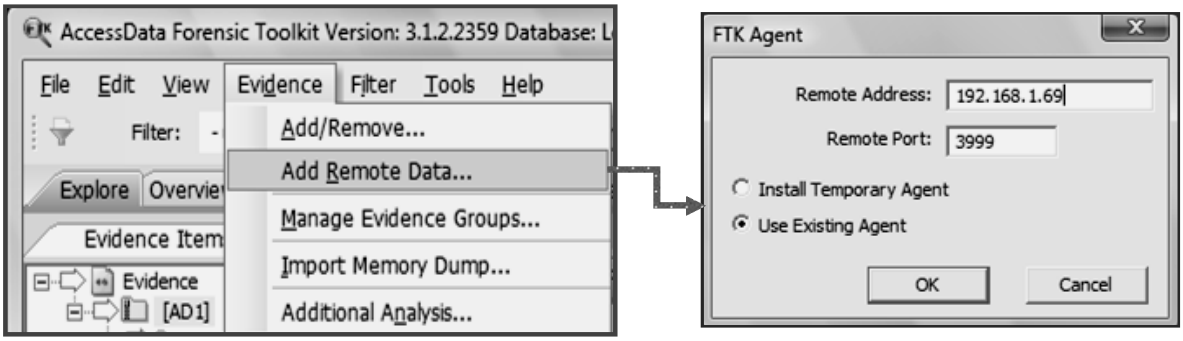


Figura 3.15 Adquisición de evidencia remota

En el equipo emisor se seleccionó el certificado privado, que es el que posee la extensión ".p12". Mostrado en la figura 3.16.

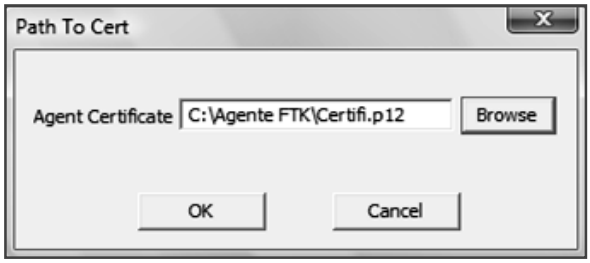


Figura 3.16 Ruta del certificado privado

Prueba 8.

De las opciones que aparecen en la figura 3.17 se seleccionó "Acquire RAM" que permitió analizar los archivos que se encontraban en la RAM del equipo remoto que se analizaba en ese momento.

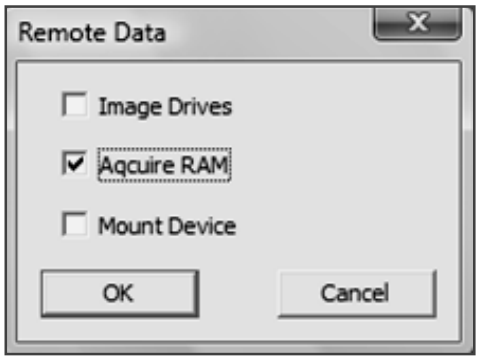


Figura 3.17 Prueba 8 'Selección de adquisición remota'

Posteriormente mostró la pantalla que se observa en la figura 3.18, en donde se seleccionó la ruta donde la imagen de disco de la RAM fue guardada y el formato de tipo de archivo en el que se realizara dicha imagen, que para este caso fue RAW y se solicita que se agregue al caso.

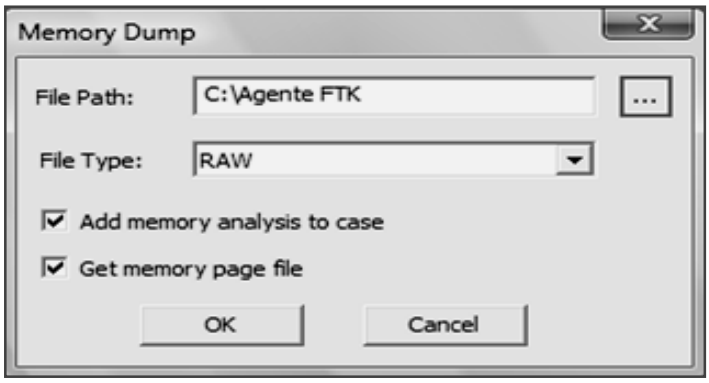


Figura 3.18 Prueba 8 Descarga de análisis de RAM

En la figura 3.19 se muestra la pantalla de proceso de la descarga de la RAM del equipo remoto desde ***FTK 3***®.

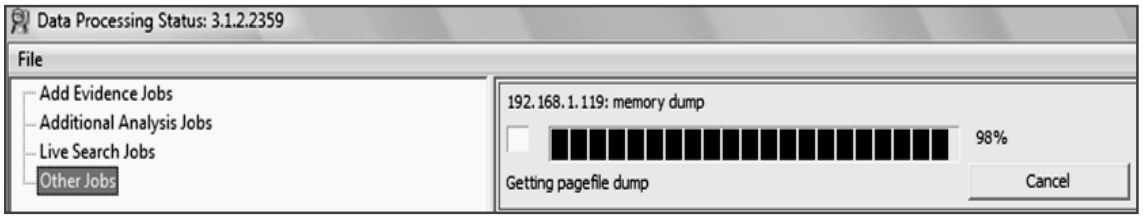


Figura 3.19 Prueba 8 Proceso de la descarga de la RAM

Resultados

En la pestaña "Volatile", que se muestra en el caso que se estaba trabajando, mostró todos los procesos que estaba realizando el equipo remoto en el momento del análisis, por ejemplo los archivos .DLL que se encontraban activos, la lista de los procesos activos, la lista de drivers, los procesadores existentes, etc., lo cual se ejemplifica en la figura 3.20, en la cual también podemos observar la carpeta en la que se encuentra cada uno y la fecha y hora en la que se realizó dicho análisis y cuantos archivos encontró en cada parte analizada de la RAM del equipo remoto.

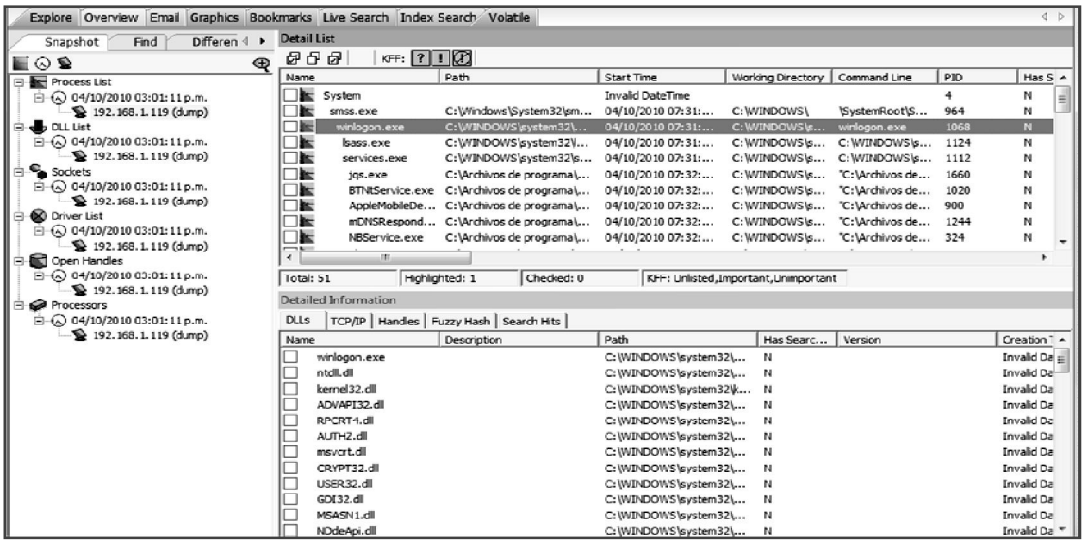


Figura 3.20 Prueba 8 Resultados de la descarga de la RAM

Prueba 9.

Se seleccionó en la pantalla de adquisición remota que se muestra en la figura 3.17 "Image Drives". Posteriormente ***FTK 3***® permite seleccionar la unidad sobre la cual se quiere realizar el análisis como se muestra en la figura 3.21.

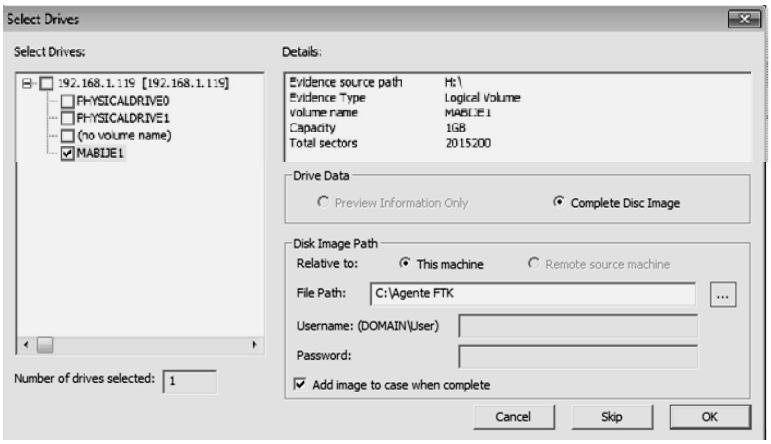


Figura 3.21 Prueba 9 Selección de unidad

En esta prueba se seleccionó específicamente la USB.

Resultados

Se constató que puede hacer un análisis mediante el agente existente a cualquier unidad que se encuentre dentro del equipo remoto o conectado a él. Se detectó que encuentra todos los archivos inclusive los eliminados. Lo anterior se observa en la figura 3.22.

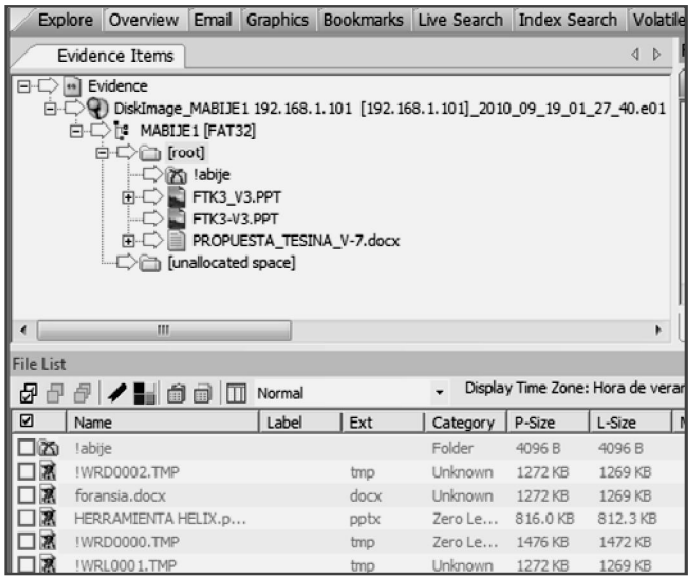


Figura 3.22 Prueba 9 Resultados del análisis de la unidad remota

Prueba 10.

Se analizó una carpeta de un equipo MAC by Apple™ conectado a la red de datos local, mediante las carpetas compartidas.

Resultados

Se comprobó que ***FTK 3***® es capaz de conectarse a un equipo MAC by Apple™ a través de la red de datos local, para analizar las carpetas que estaban compartidas. Lo que se obtuvo se muestra en la figura 3.23.

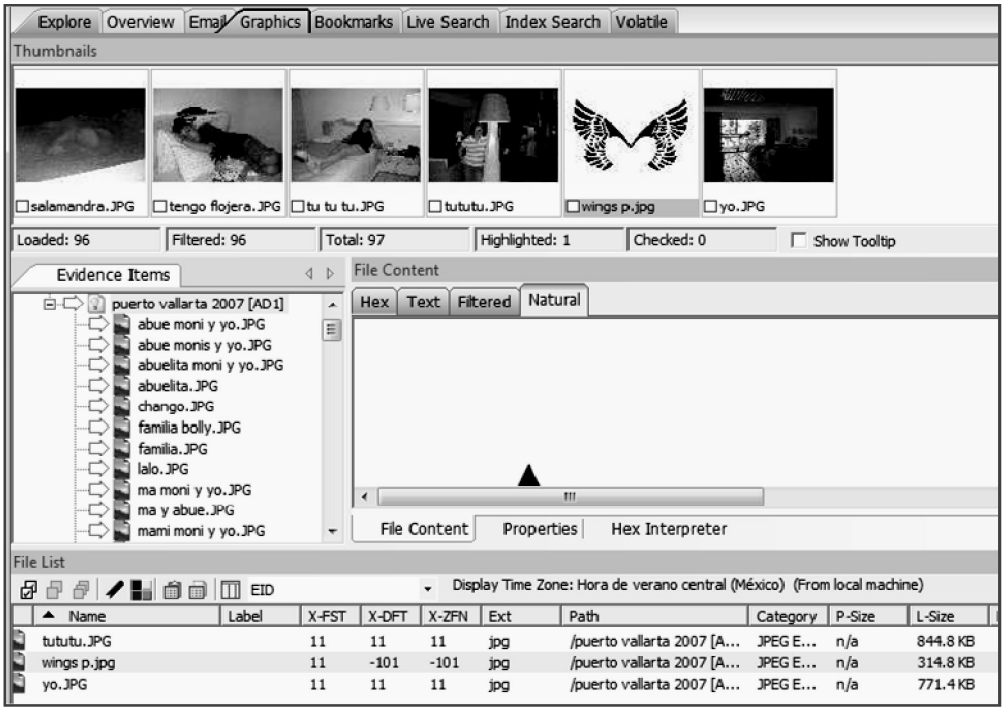


Figura 3.23 Prueba 10 Análisis del equipo MAC

Después de realizadas las pruebas anteriores y con los resultados obtenidos de cada una, se elaboró una tabla y una gráfica donde se muestran los resultados obtenidos en función de los porcentajes de falsos negativos, falsos positivos y detecciones correctas, las cuales se muestran en la figura 3.24 y en la tabla 3.2, en la cual podemos observar el análisis de los 10 repertorios creados y las pruebas de CD, disco externo, archivos comprimidos, archivos eliminados, correo electrónico, y equipos en red, con el porcentaje de falsos positivos, falsos negativos y porcentaje de detección correcta, para lo cual tomamos como estándar el que el valor de ***EID*** en los tres perfiles fuera mayor a 60, indicando que era una probable imagen sexualmente explicita, los falsos positivos son aquellos en donde el valor ***EID***, dice que es una imagen probablemente sexualmente explicita y realmente no lo es, y los falsos negativos son aquellos en donde indica que nos es una probable imagen sexualmente explicita y en realidad si lo es.

.

Tabla 3.2 Análisis de precisión

Caso	Porcentaje de falsos positivos	Porcentaje de falsos negativos	Porcentaje de detección correcta
Repertorio 1	11.00%	1.00%	88.00%
Repertorio 2	12.00%	2.00%	86.00%
Repertorio 3	15.00%	1.00%	84.00%
Repertorio 4	5.00%	4.00%	91.00%
Repertorio 5	5.00%	2.00%	93.00%
Repertorio 6	9.00%	0.00%	91.00%
Repertorio 7	5.00%	3.00%	92.00%
Repertorio 8	6.00%	2.00%	92.00%
Repertorio 9	6.00%	5.00%	89.00%
Repertorio 10	7.00%	1.00%	92.00%
CD de datos	4.00%	0.00%	96.00%
Disco externo	7.00%	2.00%	91.00%
Comprimidos	3.00%	7.00%	90.00%
Eliminados	8.00%	2.00%	90.00%
Correo electrónico	1.00%	1.00%	98.00%
Equipo Windows en red	10.00%	3.00%	87.00%
Equipo MAC en red	0.00%	1.00%	99.00%
	6.71%	**2.18%**	**91.12%**

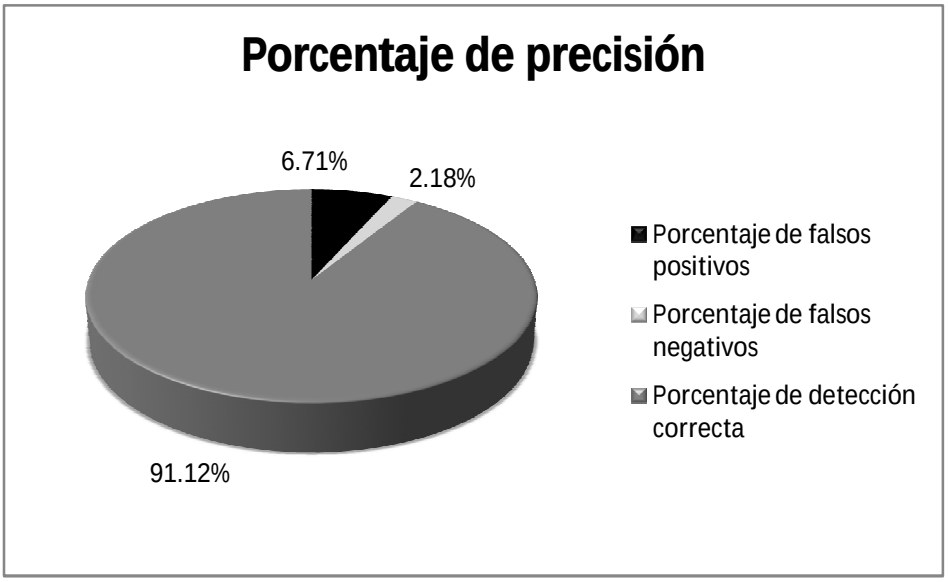


Figura 3.24 Gráfica del porcentaje de precisión

CONCLUSIONES

En la actualidad el desarrollo y procesamiento de la información por medios electrónicos, ha llevado al mal uso de imágenes sexualmente explícitas, por lo que se ha presentado la necesidad de diseñar diversos software que nos apoyen en la identificación de estas imágenes.

En el proceso de investigación del más adecuado, se encontró con el software ***FTK 3***® en su módulo ***EID*** que este permite desarrollar un dictamen detallado de este tipo de archivos. El cual se usó para poder definir, según el criterio antes mencionado (ayudados por los valores ***EID***), si las imágenes encontradas dentro de un equipo de cómputo, eran sexualmente explícitas o no.

El análisis se llevó a cabo sobre imágenes normales, ocultas, comprimidas, archivos de correo electrónico e inclusive, archivos que hubieran sido borrados del equipo o que se les hubiera cambiado de extensión. Así, se pudo comprobar con suma satisfacción que el software ***FTK 3***® tiene aproximadamente un 91% de efectividad en mostrar la evidencia de imágenes sexualmente explícitas.

Estas evidencias pueden servir en un caso forense para tomar las decisiones y acciones correctivas necesarias, o bien para ayudar a proteger a las instituciones de este tipo de material.

Se concluyó que ***FTK 3***® puede ser usado por nuestras instituciones policiacas como una buena herramienta, para analizar y dictaminar toda la información que se genere y transfiera en las redes pudiendo contener imágenes sexualmente explícitas. Esto ayudará a impedir que parte de la población se vea afectada por la pornografía y en la comprobación de los delitos donde se utilizan imágenes sexualmente explícitas. Aportando de esta forma, un medio para sanear nuestra sociedad de estos problemas.

TRABAJOS A FUTURO

Tomando como base el presente trabajo, se considera que algunos de los desarrollos que se pueden realizar a un futuro y que permitirán un conocimiento más amplio del software ***FTK 3***® son los siguientes:

- Comparar el desempeño del ***FTK 3***® con los software: Paraben´s (Porn Detection Stick) y Microsoft (SmutScanner).

- Realizar pruebas para ingresar a computadoras pertenecientes a una red de datos local, por medio del agente temporal.

- Elaborar pruebas para la conexión en red hacia un equipo:
  - MAC sin la compartición de archivos
  - y uno que opera con el sistema operativo Linux.

- Revisar imágenes para ver si existe texto oculto, recomendamos lo anterior basados en que observamos que para algunos archivos, el explorador del ***FTK 3***®, despliega una segunda vista en donde se observan otro tipo de datos que requerirían un análisis más detallado.

- Detectar y revisar archivos cifrados con el ***FTK 3***®.

- Desarrollar pruebas para comprobar el uso ***FTK 3***® para la obtención de las huellas hash de las imágenes de disco que permitan determinar si la evidencia es alterada o no.

GLOSARIO

Bidimensional:	Si tiene dos dimensiones, por ejemplo, ancho y largo pero no profundo.
CmStick:	La llave que nos permite abrir el FTK 3®
EID:	Explicit Image Detection.
Hardware:	Corresponde a todas las partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.
ImSeEx:	Imágenes Sexualmente Explicitas.
LAN:	Red local o LAN es la interconexión de varias computadoras o periféricos.
Monocromático:	Puede indicar que se tiene un solo color que esta encendido o apagado o también que tiene tonos intermedios, por lo que tiene la misma ambigüedad que blanco y negro.
Pixel:	Es la menor unidad homogénea en color que forma parte de una imagen digital, ya sea esta una fotografía, un fotograma de video o un gráfico.
Proliferación:	Multiplicación abundante de alguna cosa.
SO:	Sistema Operativo, es un software que actúa de interfaz entre los dispositivos de hardware y los programas de usuario o el usuario mismo para utilizar un computador.
Software	Se conoce como software al equipamiento lógico o soporte lógico de una computadora digital; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas especificas, en contraposición a los componentes físicos del sistema, llamados hardware.

REFERENCIAS

1.- Access Data Corporation
"*FTK 3*® User Guide"
2010
358 páginas

1.- http://www.accessdata.com/Webinars.html

2.- http://www.accessdata.com/forensictoolkit.html

2.- http://paraben-sticks.com/porn-detection-stick.html

2.- http://www.smutscanner.com

3.- http://www.scribd.com/doc/36581524/Apuntes-de-Procesamiento-Digital-de-Imagenes-1%C2%B0-BORRADOR-Jose-Ramon-Mejia-Vilet

4.- http://es.kioskea.net/contents/video/filtres.php3