UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE CUENCA

CARRERA DE INGENIERIA DE SISTEMAS

TITULO:

"Metodología de la informática forense en la atención de delitos informáticos de cibergrooming"

Tesis previa a la obtención del Título de

Ingeniero de Sistemas

Autor:

Gustavo Xavier Quizhpe Mora

Director:

Ing. Pablo Gallegos

Cuenca – Ecuador

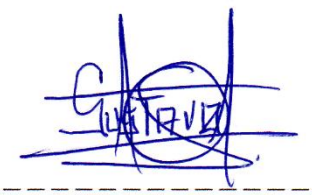
Febrero de 2015

DECLARATORIA DE RESPONSABILIDAD

Yo, Gustavo Xavier Quizhpe Mora declaro bajo juramento que el trabajo aquí descrito es de mi autoría, que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Politécnica Salesiana, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad vigente.

Cuenca, Noviembre 2014



Gustavo Xavier Quizhpe Mora

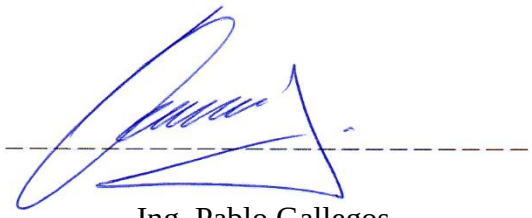
ING. PABLO GALLEGOS

CERTIFICA:

Haber dirigido y revisado cada uno de los capítulos del presente informe realizado por GUSTAVO XAVIER QUIZHPE MORA, así como el cumplimiento y desarrollo de la parte práctica; en base a ello y cumpliendo con todos los requisitos necesarios, autorizo la presentación de la misma.

Ing. Pablo Gallegos, DIRECTOR DE TESIS

Cuenca, Noviembre de 2014



Ing. Pablo Gallegos

DIRECTOR DE TESIS

Dedicatorias

El esfuerzo y el empeño que le puse, fue gracias a la inspiración de mi grandiosa familia, por ello la razón de esta tesis dedicada a mis hijos Alexander y Daniel, que cada día crecen más, son la razón por la que cada día despierto con ganas de luchar en la vida y ser una persona profesional tanto en el entorno laboral como en el hogar. A mi esposa Paola, mi compañera de la vida se la dedico también ya que con su apoyo incondicional y paciencia pone paz, tranquilidad y alegría en mi corazón. Finalmente a mis padres por sus buenos consejos y deseos, no hace falta mencionar que los amo, pero te puedo decir viejita que lo prometido, es cumplido.

Gustavo Xavier Quizhpe Mora

Agradecimientos

Agradezco principalmente a Dios por brindarme vida, salud, capacidad e inteligencia para culminar mis estudios logrando el titulo tanto anhelado, A la Universidad, mis compañeros y docentes que han demostrado ser personas de honra, con su conocimiento y motivación han incentivado a seguir creciendo profesionalmente. A mi familia, que siempre está conmigo, en las buenas y en las malas, gracias por la paciencia, amor y respeto. Finalmente, quiero agradecer todo ese buen ejemplo que recibí en mi vida, todos esos cuidados, atenciones y guías por el buen camino, el camino del triunfo, todo eso me llena de alegría, orgullo que me inspira a aplicarlo en mi hogar ahora con mis hijos, les prometo que hare de la mejor manera posible, queridos papá y mamá, gracias por todo. Sin más palabras a todo el mundo que estuvo conmigo muchas gracias y que Dios los bendiga.

Gustavo Xavier Quizhpe Mora

INDICE

CAPÍTULO 2

CAPÍTULO 3

Figuras

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Tablas

INTRODUCCION

El internet y su mundo de computadoras, ha llegado a ser parte de nuestra vida siendo objeto y principal uso para la comunicación. Inicialmente predestinado para investigación.

Es un mundo donde consultamos y transmitimos información pero, sin restricción alguna, dando posibilidad de cometer fácilmente un delito. La comunicación es reciproca lo cual nos ayuda a contactarnos con cualquier persona que tenga acceso a la red, sea adulto o menor de edad, sea quien dice ser o no.

Los sitios donde se comparte más información y son utilizados para la comunicación son las redes sociales, salas de chat, juegos online, foros, blogs, etc. Estos son una gran ventaja, ya que la distancia no es un obstáculo para este fin, pero, también se convierte en una gran debilidad al momento de cometer un delito, por la misma razón mencionada anteriormente.

De esta gran desventaja nace el cibergrooming, aprovechando su fácil comunicación, su facilidad de anonimato y la factibilidad de información. Este delito va principalmente dirigido a los menores de edad, los cuales su ingenuidad los hace confiar fácilmente en alguien que aparenta ser su amigo, probablemente no toman muy en cuenta que puede tratarse de una falsa identidad y que debe tener el cuidado debido de dar información personal a alguien.

Recuerdo aun cuando mis papas me decían, no hables con desconocidos, no des información a nadie, no abras la puerta de la casa o del carro a nadie pero, qué sucede en internet, si te das cuenta es algo similar, el hecho que sea algo intangible no significa que estemos a salvo de todo peligro. Hagamos de cuenta que al conectarnos abrimos las puertas a todo el mundo dentro de la red exponiendo nuestra integridad personal, información, que puede ser aprovechada por delincuentes para complacerse y en la

mayoría de casos complacer a los demás también. Ahora en este nuevo panorama pregunto yo, como los papás pueden aconsejar a sus hijos de los peligros de la red si no están al tanto de ello.

La informática forense en un buen paso, el cual nos brinda las pautas para prevenir, actuar y aplicar la ley al estar al frente de un caso de cibergrooming. Investigar lo sucedido en la escena del crimen reconstruyendo los sucesos más importantes para comprobar que el delito es real y que hay que castigarlo. Sus fases son muy claras las cuales un investigador forense debe tener muy en cuenta, ya que siendo responsable de un caso similar, tiene la obligación de llevar una información verdadera y valida a manos de las autoridades.

El investigador forense, en estos casos se centra en los equipos que guarden información digital, los cuales son usados para sacar evidencia que sea prueba del crimen cometido, sin alterar la evidencia original. Finalmente después de su recuperación y análisis presentar un informe donde una persona no especializada en informática pueda entender lo encontrado en esta, como el juez miembros de la corte.

Lamentablemente carecemos de una ley que penalice el cibergrooming, existe algo muy parecido implementado en septiembre del 2014 pero, al tener un volumen bien grande de delitos cometidos de este tipo, es necesario estipularlo bien dentro del código penal del Ecuador

Lo que los mostrare a continuación son las fases del cibergrooming y las leyes vigentes en Ecuador referente a este tema. También analizare un caso real de México, aplicando la informática forense según sus fases dando por resultado una información legible la cual podría ser tomada como prueba y evidencia para resolver un caso de Cibergrooming.

Sin más preámbulo y esperando que la información contenida en este sea de su utilidad, prosigo.

ANTECEDENTES

El internet, a través de sus salas de chat, redes sociales y juegos online los cuales son más visitados con frecuencia por los menores de edad, son usados para cometer delitos y el más común es el Cibergrooming.

El Cibergrooming, consiste en una serie de pasos utilizado por los adultos, aplica una estrategia el cual se enfoca en ganar confianza con la victima con fines pedófilos. Seducen a los niños sexualmente aprovechándose de su ingenuidad. Es un delito que se aprovecha del anonimato del internet, su carencia de leyes que castiguen este Cibercrimen en el país y conocimiento para llegar al culpable.

Los menores de edad son usados de una manera que los daña psicológicamente. Este delito llega en forma de amistad hasta obtener confianza, obtienen información personal y comprometedora, según eso los chantajean para provocar al menor temor por su reputación en la sociedad y es obligado a seguir con la extorción y humillación hasta que no de más y comunique a sus padres.

No todos los menores de edad tienen una buena relación con sus papas y esto puede provocar suicidio en algunos casos. Los padres no conocen de este delito y dejan pasar por alto sin saber que sus hijos pueden estar conociendo criminales en vez de buenos amigos.

En Ecuador, no existe policía cibernética ni artículo en el código penal del ecuador que se fije en este delito y lo castigue con todo el peso de la ley, es por ello que debido a lo mencionado y como investigador forense he visto necesario involucrarme y desarrollar su manera de actuar y hacer frente a este delito con la ley a nuestro lado.

JUSTIFICACION

El avance de la tecnología ha dado paso a nuevos medios de comunicación y el medio predominante en este es el Internet, donde comunicarse, intercambiar información y sociabilizar se hace de una manera virtual, asincrónica y rápida utilizando los medios tecnológicos existentes y aun mas con las redes sociales, salas de chat, etc. El acceso a internet inicialmente fue destinado para los adultos pero llego a manos de los menores usándose de forma positiva o negativa.

Todas estas sesiones las podemos tener en nuestros computadores, celulares, tabletas, etc. Estos han llegado a ser parte de nuestros artículos de uso diario dándonos la facilidad de poder conectarnos a la red y mantenernos informados y comunicados. Ocasionalmente todas estas sesiones, guardan en el anonimato su identidad con nombres ficticios, siendo así posible amenazas, acosos, con el fin de seducir a la menor o simplemente chantajearla usando fotografías, videos, filmaciones con escenas de índole sexual y varias cosas más que representa una expresión de la violencia.

La informática forense nos indicara como el Cibercrimen se aplicó, cuál fue su manera de causar daño, herramientas, procesos utilizados, etc. Este nos brindara todo un panorama de todo lo sucedido con el fin aplicar la ley y castigarlo rigiéndonos a los términos legales establecido en nuestro país. También nos ayuda a implementar soluciones y prevenir que ocurran incidentes futuros.

En nuestro marco legal del Ecuador nuevas leyes se han implementado, con nuevas sanciones las cuales estipulan, sus condenas, penas las cuales solo mencionare artículos que tienen que ver con el tema de la información y evidencia digital:

- Art. 178.- Violación de la intimidad
- Art 190.- Apropiación fraudulenta por medios electrónicos

- Art. 191.- Reprogramación o modificación de información de equipos terminales móviles
- Art.- 195 Infraestructura ilícita
- Art.- 229 Revelación ilegal de base de datos
- Art.- 230 Interceptación ilegal de datos
- Art.- 232 Ataque a la integridad de sistemas informáticos
- Art.- 233 Delitos contra la información pública reservada legalmente
- Art.- 234 Acceso no consentido a un sistema informático, telemático o de telecomunicaciones
- Art.- 312 Falsedad de información
- Art.- 456 Cadena de custodia. (a medios digitales)
- Art.- 475 Retención de correspondencia
- Art.- 476 Interceptación de la comunicaciones o datos informáticos
- Art.- 477 Reconocimiento de grabaciones
- Art.- 500 Contenido digital (todo acto que corresponde hechos)

En nuestro País, respecto al cibergrooming no especifica ninguna ley, pena o sanción que se debe cumplir por haber cometido este delito, la que más se asemeja al cibergrooming es el Art 178, que habla de la violación a la intimidad.

En argentina la Cámara de Senadores aprobó una nueva modificación al Código Penal, finalmente consagrada como Ley 26904, por cuyo art. 1° se incorporó dentro del Título correspondiente a los "Delitos contra la integridad sexual" como nuevo Art. 131 el cual dice: Sera penado con prisión de seis meses a cuatro años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

Es importante poder saber que existe este delito, para controlarlo y proteger a nuestros niños que sanamente buscan investigar, sociabilizar y se encuentra con personas que solo quieren satisfacer sus deseos aprovechándose de la ingenuidad de los menores.

OBJETIVOS

OBJETIVO GENERAL

- Desarrollar y aplicar la metodología de la informática forense en la atención de delitos informáticos de cibergrooming

OBJETIVOS ESPECÍFICOS

- Analizar los efectos y formas de cibergrooming
- Investigar aspectos legales en el País a cerca de cibergrooming
- Especificar su forma de actuar de la informática forense en el cibergrooming
- Analizar un caso de Cibergrooming real y desarrollar documentación de la resolución de este

Capítulo 1

Cibergrooming y marco legal en el país

1.1 Concepto de cibergrooming

1.1.1 Concepto

Grooming, es una conducta y acciones tomadas por mayores de edad el cual trata de ganar la amistad y confianza de un niño o un adolecente con la finalidad de abusar sexualmente de él. Esto puede llevar al menor a la pornografía infantil o prostitución.

Cibergrooming, esta conducta y acción se lo hace a través de internet y a lo igual que lo anterior la utilizan adultos catalogados como pederastas aprovechándose del anonimato de la red en salas de chats, redes sociales, blogs, foros, juegos online y así contactar a niños y adolescentes con la finalidad de convencerlos a realizar poses eróticas o aparecer desnudos frente a la webcam generando un material el cual es utilizado como chantaje o seducirlos sexualmente por el pederasta

1.1.2 Medio de comunicación

La utilización del internet va en aumento y son los niños y adolescentes quienes elevan estos indicadores, su uso principalmente fue como fuente de autoaprendizaje para su tarea escolar pero, existen sitios web como Facebook, Instagram, Twitter, etc., que les permite tener un perfil virtual, obtener información de otros usuario y chatear siendo las páginas que son frecuentemente utilizadas por ellos. Estos medios de comunicación son los favoritos para pedófilos quienes utilizan para tener contacto con menores de edad (entre 10 y 15 años) y hacer de las suyas engañándolos y acosándolos sexualmente.

Figura 1.1: Navegando en Internet

La organización “Navega Protegido en Internet” estima que 1 de cada 7 menores que acceden a foros de discusión y chats ha recibido propuestas indebidas o sufrido algún tipo de acoso, y tan solo el 27% de esta dispuesto a informar lo ocurrido a sus padres.[1]

Los medios de comunicación que están expuestos a estas amenazas son:

1) Las salas de Chats que permite tener conversaciones textuales sin filtro alguno de personas.
2) Mensajeros instantáneos dando la posibilidad de tener una lista de contactos para sociabilizar mediante texto y video sea conocido o desconocido.
3) Foto log que nos permite publicar fotografías dando la posibilidad a comentarios por otras personas desconocidas y no.
4) Redes sociales que nos permite tener perfiles virtuales, agregar contactos, publicar fotos, video dando a conocer la vida personal de una persona como edad, dirección, teléfono, etc.

1.1.3 Consecuencias y prevención

Existen consecuencias tanto para las víctimas como a los agresores.

Consecuencias para las víctimas son:

1) Sufren un fuerte trauma el cual obliga a que su personalidad cambien a mal.
2) Asumen conductas autodestructivas, su rendimiento en la escuela comienza a bajar y se llenan de depresiones.
3) Daños psicológicos irreparables y discriminación en la sociedad.
4) Daños físicos con probabilidad de suicidio

Consecuencias para los agresores son:

1) Considerado como delito según el código penal del país en donde este la escena del crimen.

[1] Nota tomada de: http://operacionsafe.blogspot.com/p/acoso-menores-grooming.html

Las amenazas hechas en internet, se aprovechan del anonimato y de la ausencia de control por lo que pueden ser más peligrosas que las hechas personalmente. Estas pueden ocurrir todos los días siendo muy difícil evitarlas, además es muy probable que la víctima no comunique a los padres por temor a quedar sin acceso a la web.

Prevención

Consiste en evitar la obtención del elemento de fuerza, el cual es usado como chantaje por el agresor. Para prevenir es aconsejable:

1) Evitar él envió de fotografías, videos o cualquier información personal
2) Asegurar nuestro dispositivo de navegación en la web y evitar robo de contraseñas
3) Establecer controles de privacidad de cualquier archivo a la web
4) Evitar el uso de páginas para adultos
5) Restringir el uso de las cámaras web

A más de esto unas recomendaciones que podríamos seguir y mejorar que esta amenaza no cause daño a nuestros menores de edad en casa serian:

Figura 1.2: Seguridad en Internet

1) Explorar a menudo el historial de navegación para poder verificar las páginas o sitios que están siendo visitadas por el menor de edad.
2) Revisar su lista de contactos agregados en sus programas de mensajería o servicios.
3) Poner el computador en una zona visible de tal manera que se pueda observar la actividad del niño en internet.

4) Tener una charla amena con sus hijos y poder obtener información acerca de lo que vieron e hicieron en internet.
5) Utilizar software para filtrar contenido o control parental en la sesión, también los ISP pueden ayudar con el control.

1.2 Fases de cibergrooming

1.2.1 Fases

El cibergrooming se comprende de 5 fases principales:

Figura 1.3: Fases de Cibergrooming

Contacto

Es a través de chat, redes sociales, juegos online, donde contactan con niños agregándolos y poder hablar con ellos tranquilamente. El pederasta se hace pasar por un niño o niña y normalmente suelen conseguir más contactos en juegos online de Pocoyo o Pokemon que en chats.

Confianza

Aquí los convencen tratando de ganar la confianza de la víctima con engaños.

Seducción

A través de supuestos juegos tratan de conseguir que el menor se grabe mediante la cámara/webcam llegando a obtener material con índole sexual, es decir desnudos, que realicen tocamientos, con alguna pose erótica, etc.

Amenazas

Aquí empieza la extorsión, donde el menor es chantajeado con la difusión de la foto, reenviando a todas las personas que conoce, familia, profesores, amigos, etc., con la finalidad de obtener más fotografías, imágenes pornográficas del menor. Esta serie de eventos puede conducir al acoso sexual físico del menor.

Difusión

Si la víctima decide dejar de cooperar, el depredador distribuye las conversaciones, imágenes, videos entre sus amigos, familia, etc.

1.2.2 Ejemplo: Caso Colombia

Contacto

El caso implica a una niña menor con tan solo 12 años de edad y una persona mayor entre 20 y 30 años de Miami. El depredador contacto con la menor en un chat público.

Confianza

Logro agregarle al Messenger con perfiles falsos de diferentes chicas y así ir jugando entre ella con la finalidad de ir ganando mucha confianza

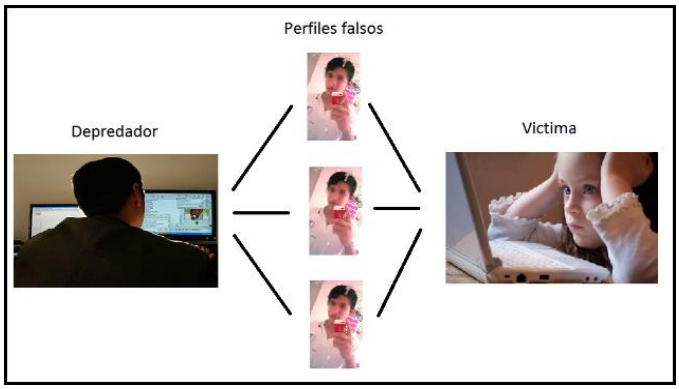


Figura 1.4: Perfiles falsos

Seducción

Aquí es en donde viene el intento de engañarla tratando de obtener una foto en sujetador e interior.

Amenaza

Una vez que accede comienza las amenazas diciendo que si no envía será enviada a la familia, profesor, etc. La niña aguanta dos años de extorción donde envía fotos, pone la webcam, videos, etc.

Difusión

La niña muy deprimida decide dejar de enviar el material y el depredador publica en la red lo que ha obtenido.[2]

1.3 Ciberdepredadores

Estos son los delincuentes informáticos de los cuales tenemos que tener cuidado, pero para poder defendernos es necesario conocerlos e identificarlos. Existe una frase sabia de Sun Tzu que dice: *"Si conocemos a nuestro enemigo, tenemos ganada la mitad de la guerra, si solo nos conocemos, tenemos ganada la mitad de la guerra, pero si nos conocemos y conocemos a nuestro enemigo, tenemos casi segura la victoria."*.[3]

1.3.1 Tipos de Ciberdepredadores

1) Boylovers/Girlovers

   Estas personas tratan de que se dé una aceptación en la sociedad de la atracción por menores de edad como algo natural y tolerable. Frecuentemente se reúnen en foros privados y tienen una adicción por imágenes en la que los menores de edad aparecen en poses eróticas pero en realidad nunca son desnudos.

[2] Entrevista publicada en www.anti-depredadores.com

[3] Nota Tomada de: Sun Tzu 500a.C.

2) Pedófilos

Estos adultos no llegan al acto sexual pero son consumidores de pornografía infantil. Son traficantes de material pedófilo y en ocasiones graban. Frecuentemente se reúnen en chats, foros y webs de temática pedófila. Su movimiento es por las redes sociales y chats donde localizan a sus víctimas.

3) Pederastas

Estos adultos llegan al acto sexual e incluso hasta violaciones. Su objetivo fundamental es contactar a menores mediante técnicas de ingeniería social e incluso hacking logrando extorsionar a los menores para conseguir sus propósitos como la obtención de fotografías, videos y así llegar al contacto.

Su manera de actuar de estos delincuentes está basado en las 3Cs:

- Comunicación: Comparten información en internet mediante servicios o mensajería.
- Comunidad: Comparten experiencias en foros privados, blogs.
- Cooperación: Se ayudan mucho entre ellos.

1.3.2 Simbología utilizada

Sobre todo en los foros utilizan una serie de símbolos para indicar sus gustos de pederastia.

1) Símbolo de la atracción por niños menores, el grosor del símbolo indica si es por los más pequeños o por los más grandes.
2) Símbolo de la atracción por niñas menores.

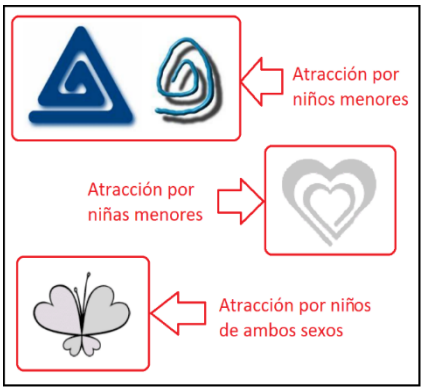


Figura 1.5: Simbología de los Ciberdepredadores

3) Símbolo de la mariposa invertida, atracción de niños menores de ambos sexos

1.3.3 Vocabulario

En foros o en casos periciales, podemos comprender mensajes de lo que esta gente se ha comunicado entre ellos mismos relacionando lo siguiente:

Mensaje	**Significado**
BL	Boylover
GL	Girlover
SYF	Cuando tienen un niño especial que les gusta especialmente
YF	Para referirse a un joven amigo
SGL	Para referirse a la atracción de un niño de su mismo sexo
LBL	Para los que son amantes de niños menores de 8 años
TBL	Para los que son amantes de adolecentes

Tabla 1.1: Mensajes ocultos de los Ciberdepredadores

Eh aquí algunas palabras claves más de los pederastas

Palabras clave para detectarlos				
Preteens	Lolitas	R@ygold	Meninas	y/o
Nifeta	Tits	Menores	Kids	Sexkids
Childrens	Sister	Pedo	Baby j	Brother
Vicky	Reelkidmov	Kiddy porn	Babyshivid	Pedofilia
Niñas	Extreme Child porn	Menores	Sex tenns	Hussyfan
Schoolgirl	Hard Child porn	Crianca	pthc	Kiddy
Yold	Child pornography	Incesto	Child porn	Years old
Childrems	Nude Kids	Kiddy Porn	Kinder sex	Teen raped
Child lovers	Kiddymovis			

Tabla 1.2: Palabras clave para detectar a un Ciberdepredadores

1.3.4 Aprendizaje

Estos delincuentes cada vez van aprendiendo y utilizando sistemas más avanzados de ocultar pornografía como antes era en Emule, de hecho ahora hay menos, ahora están en redes TOR, Gigadrive, dropbox, skydrive, etc.

Utilizan el método anónimo y cifran su contenido pornográfico en sus PCs, aprenden técnicas de esteganografía

1.4 Existe legislación vigente en el Ecuador

El nuevo COIP (Código Orgánico integral penal) rige en su totalidad desde el domingo 10 de agosto del 2014.[4]

1.4.1 COPI relacionado con cibergrooming

Figura 1.6: Código Orgánico Integral Penal

Los artículos a continuación han sido plasmados tal y como han sido escritos por la asamblea nacional de la República del Ecuador, pero solo los referentes a cibergrooming y la informática forense.

CÓDIGO ORGÁNICO INTEGRAL PENAL

CAPÍTULO SEGUNDO

DELITOS CONTRA LOS DERECHOS DE LIBERTAD

SECCIÓN CUARTA

Delitos contra la integridad sexual y reproductiva

Artículo 173.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.- La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona

[4] Nota Tomada de: http://www.asambleanacional.gob.ec/noticia/este-10-de-agosto-entra-en-vigencia-en-su-totalidad-el-codigo

menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años.

Cuando el acercamiento se obtenga mediante coacción o intimidación, será sancionada con pena privativa de libertad de tres a cinco años.

La persona que suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con pena privativa de libertad de tres a cinco años.

Artículo 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos.- La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, foto blogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años.

SECCIÓN SEXTA

Delitos contra el derecho a la intimidad personal y familiar

Artículo 178.- Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por

cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.

Artículo 179.- Revelación de secreto.- La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año.

Artículo 180.- Difusión de información de circulación restringida.- La persona que difunda información de circulación restringida será sancionado con pena privativa de libertad de uno a tres años.

Es información de circulación restringida:

1. La información que está protegida expresamente con una cláusula de reserva previamente prevista en la ley.

2. La información producida por la Fiscalía en el marco de una investigación previa.

3. La información acerca de las niñas, niños y adolescentes que viole sus derechos según lo previsto en el Código Orgánico de la Niñez y Adolescencia.

SECCIÓN SÉPTIMA

Delitos contra el derecho al honor y buen nombre

Artículo 182.- Calumnia.- La persona que, por cualquier medio, realice una falsa imputación de un delito en contra de otra, será sancionado con pena privativa de libertad de seis meses a dos años.

No constituyen calumnia los pronunciamientos vertidos ante autoridades, jueces y tribunales, cuando las imputaciones se hubieren hecho en razón de la defensa de la causa.

No será responsable de calumnias quien probare la veracidad de las imputaciones. Sin embargo, en ningún caso se admitirá prueba sobre la imputación de un delito que hubiere sido objeto de una sentencia ratificatoria de la inocencia del procesado, de sobreseimiento o archivo.

No habrá lugar a responsabilidad penal si el autor de calumnias, se retractare voluntariamente antes de proferirse sentencia ejecutoriada, siempre que la publicación de la retractación se haga a costa del responsable, se cumpla en el mismo medio y con las mismas características en que se difundió la imputación.

La retractación no constituye una forma de aceptación de culpabilidad.

SECCIÓN NOVENA

Delitos contra el derecho de la propiedad

Artículo 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes

electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptados, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.

SECCIÓN DECIMA

Delitos contra el derecho de la identidad

Artículo 212.- Suplantación de identidad.- La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años.

CAPÍTULO SEXTO

DELITOS CONTRA LA ESTRUCTURA DEL ESTADO CONSTITUCIONAL

SECCIÓN ÚNICA

Delitos contra la seguridad pública

Artículo 354.- Espionaje.- La o el servidor militar, policial o de servicios de inteligencia que en tiempo de paz realice uno de estos actos, será sancionado con pena privativa de libertad de siete a diez años, cuando:

2. Intercepte, sustraiga, copie información, archivos, fotografías, filmaciones, grabaciones u otros sobre tropas, equipos, operaciones o misiones de carácter militar o policial.

TÍTULO IV

PRUEBA

CAPÍTULO SEGUNDO

ACTUACIONES Y TÉCNICAS ESPECIALES DE INVESTIGACIÓN

Artículo 470.- Comunicaciones personales.- No podrán grabar o registrar por cualquier medio las comunicaciones personales de terceros sin que ellos hayan conocido y autorizado dicha grabación o registro, salvo los casos expresamente señalados en la ley.

La información obtenida ilegalmente carece de todo valor jurídico. Los riesgos, daños y perjuicios que genere para las personas involucradas, serán imputables a quien forzó la revelación de la información, quedando obligada a efectuar la reparación integral de los daños.

SECCIÓN PRIMERA

Actuaciones especiales de investigación

Artículo 476.- Interceptación de las comunicaciones o datos informáticos.- La o el juzgador ordenará la interceptación de las

comunicaciones o datos informáticos previa solicitud fundamentada de la o el fiscal cuando existan indicios que resulten relevantes a los fines de la investigación, de conformidad con las siguientes reglas:

1. La o el juzgador determinará la comunicación interceptada y el tiempo de intercepción, que no podrá ser mayor a un plazo de noventa días. Transcurrido el tiempo autorizado se podrá solicitar motivadamente por una sola vez una prórroga hasta por un plazo de noventa días.

Cuando sean investigaciones de delincuencia organizada y sus delitos relacionados, la interceptación podrá realizarse hasta por un plazo de seis meses.

Transcurrido el tiempo autorizado se podrá solicitar motivadamente por una sola vez una prórroga hasta por un plazo de seis meses.

2. La información relacionada con la infracción que se obtenga de las comunicaciones que se intercepten durante la investigación serán utilizadas en el proceso para el cual se las autoriza y con la obligación de guardar secreto de los asuntos ajenos al hecho que motive su examen.

3. Cuando, en el transcurso de una interceptación se conozca del cometimiento de otra infracción, se comunicará inmediatamente a la o al fiscal para el inicio de la investigación correspondiente. En el caso de delitos flagrantes, se procederá conforme con lo establecido en este Código.

4. Previa autorización de la o el juzgador, la o el fiscal, realizará la interceptación y registro de los datos informáticos en transmisión a través de los servicios de telecomunicaciones como: telefonía fija, satelital, móvil e

inalámbrica, con sus servicios de llamadas de voz, mensajes SMS, mensajes MMS, transmisión de datos y voz sobre IP, correo electrónico, redes sociales, videoconferencias, multimedia, entre otros, cuando la o el fiscal lo considere indispensable para comprobar la existencia de una infracción o la responsabilidad de los partícipes.

5. Está prohibida la interceptación de cualquier comunicación protegida por el derecho a preservar el secreto profesional y religioso. Las actuaciones procesales que violenten esta garantía carecen de eficacia probatoria, sin perjuicio de las respectivas sanciones.

6. Al proceso solo se introducirá de manera textual la transcripción de aquellas conversaciones o parte de ellas que se estimen útiles o relevantes para los fines de la investigación. No obstante, la persona procesada podrá solicitar la audición de todas sus grabaciones, cuando lo considere apropiado para su defensa.

7. El personal de las prestadoras de servicios de telecomunicaciones, así como las personas encargadas de interceptar, grabar y transcribir las comunicaciones o datos informáticos tendrán la obligación de guardar reserva sobre su contenido, salvo cuando se las llame a declarar en juicio.

8. El medio de almacenamiento de la información obtenida durante la interceptación deberá ser conservado por la o el fiscal en un centro de acopio especializado para el efecto, hasta que sea presentado en juicio.

9. Quedan prohibidas la interceptación, grabación y transcripción de comunicaciones que vulneren los derechos de los niños, niñas y adolescentes, especialmente en aquellos casos que generen la re

victimización en infracciones de violencia contra la mujer o miembros del núcleo familiar, sexual, física, sicológica y otros.

CAPÍTULO TERCERO

MEDIOS DE PRUEBA

SECCIÓN PRIMERA

El documento

Artículo 500.- Contenido digital.- El contenido digital es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí.

En la investigación se seguirán las siguientes reglas:

1. El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses.

2. Cuando el contenido digital se encuentre almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura critica del sector público o privado, se realizará su recolección, en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.

3. Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.

4. Cuando se recolecte cualquier medio físico que almacene, procese o transmita contenido digital durante una investigación, registro o allanamiento, se deberá identificar e inventariar cada objeto individualmente, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante cadena de custodia a un centro de acopio especializado para este efecto.

1.5 Marco Lega de este crimen en otros países

Este delito es aplicado en diversos países del mundo como México, Costa Rica, España, Alemania, Argentina, etc.

1.5.1 México

Su cámara de diputados aprobó el dictamen de proyecto para reformar su Código Penal Federal que castiga el Grooming, ya que estos delitos generan pérdidas que redondean los 2 mil millones de dólares anualmente. El país ocupa el tercer lugar en comisión de Cibercrimen.[5]

Su Secretaria de Seguridad Pública Federal recibió a través de la Policía Cibernética 5mil 582 denuncias de Ciberdelitos entre septiembre de 2010 y julio de 2011. Entre estas están incluidas hackeo de cuentas personales de servicios en línea, fraudes y ataques a sistemas privados y gubernamentales.[6]

[5] Nota expuesta por el diputado Rodrigo Pérez Alonso
[6] Nota tomada de: http://www.elgolfo.info/nota/109702-contra-phishing-y-grooming/

El artículo relacionado a Grooming fue adicionado, mediante decreto publicado en el diario oficial de la federación el 19 de Agosto de 2010

CAPÍTULO VIII

PEDERASTIA

"Artículo 209 bis.- se aplicara de nueve a dieciocho años de prisión y de setecientos cincuenta a dos mil doscientos cincuenta días multa, a quien se aproveche de la confianza, subordinación o superioridad que tiene sobre un menor de dieciocho años, derivada de su parentesco en cualquier grado, tutela, curatela, guarda o custodia, relación docente, religiosa, laboral, medica, cultural, doméstica o de cualquier índole y ejecute, obligue, induzca o convenza a ejecutar cualquier acto sexual, con o sin su consentimiento.

La misma pena se aplicara a quien cometa la conducta descrita del párrafo anterior, en contra de la persona que no tenga la capacidad de comprender el significado del hecho o para resistirlo. Si el agente hace uso de violencia física, las penas se aumentaran en una mitad más.

El autor del delito podrá ser sujeto a tratamiento médico integral el tiempo que se requiera, mismo que no podrá exceder el tiempo que dure la pena de prisión impuesta.

Además de las anteriores penas, el autor del delito perderá, en su caso, la patria potestad, la tutela, la curatela, la adopción, el derecho de alimentos y el derecho que pudiera tener respecto de los bienes de la víctima, en términos de la legislación civil.

Cuando el delito fuere cometido por un servidor público o un profesionista en ejercicio de sus funciones o con motivo de ellas, además de la pena de

prisión antes señalada, será inhabilitado, destituido o suspendido, de su empleo público o profesión por un término igual a la pena impuesta." [7]

1.5.2 Costa Rica

El miércoles 17 de abril del 2013, adicionaron en el Código Penal el articulo167 bis, que castiga el hecho de seducir un niño o persona incapaz por medios electrónicos.[8]

"**Artículo 167 bis**.- Seducción o encuentros con menores por medios electrónicos.

Será reprimido con prisión de uno a tres años a quien, por cualquier medio, establezca comunicaciones de contenido sexual o erótico, ya sea que incluyan o no imágenes, videos, textos o audios, con una persona menor de quince años o incapaz.
La misma pena se impondrá a quien suplantando la identidad de un tercero o mediante el uso de una identidad falsa, por cualquier medio, procure establecer comunicaciones de contenido sexual o erótico, ya sea que se incluyan o no imágenes, videos, textos o audios, con una persona menor de edad o incapaz.

La pena será de dos a cuatro años, en las conductas descritas en los dos párrafos anteriores, cuando el actor procure un encuentro personal en algún lugar físico con una persona menor de edad o incapaz."[9]

1.5.3 España

En el Código Penal español (CP), el artículo 183 bis se encarga de criminalizar el Grooming

[7] Articulo tomado de: http://info4.juridicas.unam.mx/ijure/fed/8/252.htm?s=
[8] Nota tomada de: http://www.canara.org/panorama-14/comentarios/3615-grooming.html
[9] Articulo tomado de: ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA

“Artículo 183 bis.- El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de trece años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 178 a 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño”[10]

1.5.4 Alemania

En su código Penal sanciona el delito de Grooming con el artículo 176

§ 176. Abuso sexual de niños

(1) Quien practique acciones sexuales en una persona menor de 14 años (niño) o permita que se practiquen en él por el niño, será castigado con pena privativa de la libertad de seis meses hasta diez años. En casos menos graves con pena privativa de la libertad hasta cinco años o con multa.

(2) En la misma forma será castigado quien disponga a un niño, para que practique acciones sexuales con un tercero o para que permita que un tercero los practique en él.

(3) Será castigado con pena privativa de la libertad de hasta de cinco años o con multa, quien

1. practique acciones sexuales ante un niño
2. determine a un niño a que practique acciones sexuales consigo mismo, o,
3. influya sobre un niño por medio de la presentación de ilustraciones o representaciones pornográficas o por dispositivos sonoros de contenido pornográfico o por conversaciones en el mismo sentido.

[10] Articulo tomado de: Código Penal Español (CP)

(4) La tentativa es punible; esto no rige para hechos según el inciso 3 numeral 3.[11]

1.5.5 Argentina

En diciembre del 2013, incorporan el delito de Grooming al Código Penal.

"**Art. 131.-** Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma."

También está el Artículo 128 el cual sanciona la publicación en internet cualquier representación del menor dedicado a actividades sexuales.

"Artículo 128.- Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) 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 (4) meses a dos (2) 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 (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años."

[11] Articulo tomado de: Código Penal Alemán

Capítulo 2

La informática Forense

2.1 Concepto de informática forense

2.1.1 Principios

La informática Forense toma como base el principio de Locard, (Edmond Locard), quien fue un criminalista francés, pionero y creador de teorías en el ámbito forense, fue también fundador del instituto de criminalística de la universidad de Lyon.

Figura 2.1: Manual de Técnica policiaca por Edmond Locard

Compartió sus teorías y frases las cuales han transcendido hasta que ahora es la ciencia forense. Una de las frases más destacadas que compartió fue:

"Los restos microscópicos que cubren nuestra ropa y nuestros cuerpos, son testigos mudos, seguros y fieles de nuestros movimientos y de nuestros encuentros"[12]

Siendo un experto muy hábil para resolver crímenes, era conocido como el Sherlock Francés y menciona tres entidades importantes relacionadas entre sí el cual nos ayuda al desarrollo de la investigación de un crimen:

1) Escena del crimen
2) Sospechoso
3) Victima

Este principio indica que cualquiera o cualquier objeto que entra en la escena del crimen, deja un rastro en la escena o en la víctima y viceversa. *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias*

[12] Frase tomada de: Libro, manual de técnica policiaca de Edmond Locard

ocasionadas Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas Este tipo de material es restringido.

Tomando en cuenta el principio de Locard mencionado, se puede determinar que tanto en la escena como el dispositivo que se va a analizar (computadora, disco duro, memoria USB, Celulares, etc.), nos aportara pruebas de acciones y manipulación que se hayan realizado. También a identificar posibles involucrados como pueden ser víctima o víctimas, usuario, testigos o posibles culpables entre otras pruebas que pueden ser útiles dando evidencia para el desarrollo de la investigación.

2.1.2 Conceptos y objetivos principales

La informática forense es la aplicación de técnicas científicas y analíticas especializadas a infraestructuras tecnológicas que *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas Este tipo de material es restringido* la evidencia o evidencias obtenidas son legítimas y que estas no han sufrido ningún tipo de alteración siendo cien por ciento confiables y puedan ser presentados en un litigio legal. El caso va a depender del conocimiento, experiencia y versatilidad de cada uno de los investigadores.

Los objetivos de informática forense son:

1) Saber qué tipo de incidente o incidentes han ocurrido

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas.

2) Cuantificar y determinar la magnitud del incidente en:

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas Este tipo de

3) Determinar entidades implicadas en el incidente como

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas Este tipo de

4) Prevenir y prepararnos para incidentes futuros

5) Determinar y deslindar responsabilidades

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas Este tipo de material es restringido.

Incidentes y entidades donde se involucra la informática forense:

En la actualidad se ha vuelto indispensable el uso de la informática forense en los delitos informáticos y otros incidentes que son de la vida diaria que no están relacionados con la informática como por ejemplo:

Prosecución criminal *Este tipo de material es restringido, pedimos disculpas*

Temas corporativos: *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas Este tipo de material es restringido.*

Litigación civil: *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas*

Estos diferentes campos son los que se pueden verse involucrado la informática forense siempre y cuando esté involucrado un dispositivo digital sobre el cual se puede aplicar esta ciencia para obtener evidencia digital.

Las evidencias potenciales son entidades que pertenecen a la escena del crimen como por ejemplo:

Trafico de red: Direcciones IP, registros de conexión de red, procesos y servicios que se encuentran a la escucha, etc.

Base de Datos: Aplicaciones web, sistemas internos o externos de la empresa

Testimonio humano: sirve de referencia para integrar en la investigación a otros presuntos involucrados ya sean personas, dispositivos, software, etc.

Sistemas operativos: esta es una de las evidencias donde aloja la mayoría de la información

Aplicaciones de software *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas*

Unidades de almacenamiento: Discos duros, memorias USB, celulares, agendas electrónicas, dispositivos GPS y además impresoras, dispositivos multimedia, cámaras digitales, etc.

2.2 Fases de la informática forense

Para lograr buenos resultado, es necesario seguir ciertas metodologías fijados por un procedimiento, es por ello que al realizar una investigación forense, es fundamental seguir ciertas fases.

Figura 2.2: Fases de la Informática Forense

Cumpliéndose este ciclo, el proceso y la investigación, terminara con éxito pero, una falla en cualquiera de estas, toda la investigación se verá afectada y por ellos fracasara.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

2.2.1 Identificación del incidente

En esta fase es en donde se recolecta toda la información posible del incidente el cual nos tendrá que resolver las interrogantes como *Este tipo de*

material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Estas preguntas nos van a permitir identificar los antecedentes desde antes, durante y *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas* se debe documentar absolutamente todos los resultados obtenidos en esta fase ya que influenciara para la toma de decisiones y reacciones que se deban tomar con respecto al incidente.

Las fotografías también son muy importantes ya que deberíamos indicar en el informe momentos y circunstancias del hallazgo, obtener todo el hardware que se vea afectado en el incidente.

Figura 2.3: En la escena del crimen, identificación del incidente

Hay que clasificar toda la evidencia obtenida por categorías como por ejemplo:

- Evidencia digital (memoria RAM, cache, base de datos, etc.)
- Evidencia lógica (Sistemas operativos, aplicaciones de software, etc.)
- Evidencia física (discos duros, cintas magnéticas, etc.)
- Dispositivos electrónicos (Celulares, agendas magnéticas, etc.)
- Dispositivos de red (switchs, routers, etc.).

Si no se está seguro de cómo actuar en el incidente es mejor no tocar ni hacer nada *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas*

La obligación del investigador forense consiste en asegurar la evidencia y garantizar la cadena de custodia, *Este tipo de material es restringido,*

pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

2.2.2 Obtención de la evidencia

Para la obtención de la evidencia, se debe de hacer una imagen forense bit a bit del dispositivo a investigar del cual se obtuvo de la escena del crimen. En esta copia idéntica de la evidencia es en donde se va a realizar las prácticas de los análisis para recuperar archivos eliminados, archivos ocultos, archivos encriptados, etc.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Figura 2.4: Generando Copia Forense

Hay que tomar muy en cuenta las herramientas de software o hardware con las cuales se va a realizar la imagen forense, ya que estas junto con los métodos del investigador deberán ser conocido y aceptados por los profesionales de su sector. Trabajar con tecnologías innovadoras no siempre es lo mejor, lo ideal es que otros investigadores hubieran trabajado previamente con esos procedimientos dando como resultado informes positivos.

Es de vital importancia salvaguardar la integridad de la evidencia, estas pruebas no deben sufrir alteraciones de ningún tipo. Generalmente el medio

(disco duro, pendrive, etc.) se precinta después de haber obtenido tres copias cuyos hashes van a coincidir con las copias realizadas.

Un hash viene a ser una huella digital de un archivo o un dispositivo de almacenamiento el cual nos brinda la seguridad y confianza de que la copia forense bit a bit de la evidencia original no ha sido alterada.

Figura 2.5: Comparación de código HASH con la evidencia

Al momento de obtener la evidencia, existen ciertos factores a tomar en cuenta y uno de los más importantes es la volatilidad de los datos, esto datos son los que se perderán al apagar el equipo.

Generalmente en una escena del crimen donde los ordenadores se encuentran encendidos y cumpliendo sus funciones, y su red ha sido atacada, surge un dilema de que acción debemos utilizar. Si apagamos los ordenadores con la idea de detener el ataque, lo vamos a lograr pero en realidad perderemos información importante, se podría eliminar archivos temporales que se eliminan automáticamente al detenerse el sistema operativo perdiéndose elementos potenciales de la evidencia o quedando alterada la prueba del delito, y si dejamos encendidos los ordenadores, el ataque seguirá en ejecución causando daños.[13]

[13] Basado en: Análisis Forense Digital, por Miguel López Delgado

Una de las alternativas emergentes a utilizar es desconectar los ordenadores de la red, quizá perderemos información pero no de la misma manera de como si lo hubiésemos apagado.

Esta alternativa depende mucho del investigador, circunstancias e incidentes ocurridos mas no significa que sea la mejor opción.

Otra alternativa es realizar un análisis en caliente, que consiste en utilizar herramientas de software forense especializadas para hacer un rápido análisis de la evidencia, no es muy aconsejable dado a que se podría alterar nuestra evidencia original.

Lo recomendable es *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas*

2.2.3 Preservación de la evidencia

La preservación de la evidencia está dirigida a la protección de los objetos que tenga información como evidencia quedando completos, verificables y claras. Cualquier examen llevado a cabo sobre la evidencia no debe genere cambios ya que de ser así y generar un cambio inevitable, es muy importante que se presente la razón detallando todo su suceso, registrarlo y justificarlo.

Recomendaciones para la preservación de la evidencia para que en caso de un proceso legal sea admisible

Manipulación de la evidencia digital

1) Los medios forenses a utilizar en las copias de información deben estar esterilizados
2) Realizar acciones para recolectar información de la evidencia digital sin cambiar la original, manteniendo y controlando su integridad
3) Solo un profesional forense debe tener acceso a la evidencia digital forense
4) Las copias de resultados forenses disponibles, deben de estar marcadas, controladas y preservadas
5) El individuo que este empoderado de la evidencia digital forense será responsable de las acciones tomadas en ella
6) Actualizar cadena de custodia (Nombre de la persona que examina la evidencia, fecha, tiempo de disposición de la evidencia, hora de devolución, etc.)
7) Evidencia protegida digital y físicamente

Cadena de custodia

Es un sistema que nos ayuda a preservar las evidencias garantizando la integridad, conservación, inalterabilidad de un espécimen o evidencia desde su obtención. Estos serán presentados y servirá como medios de prueba en los estados judiciales.

Está constituida por la siguiente información:

1) Quien o quienes obtuvieron a la evidencia *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas*

2) Donde y cuando fue obtenida la evidencia *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas*

3) Quien protegió la evidencia *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas*

4) Quien ha tenido acceso a la evidencia *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas*.

Es necesario llenar una ficha que pruebe y responsabilice lo mencionado[14].

[14] Cadena de custodia: Tomada del Libro, Introducción a la informática forense, Francisco Lázaro Domínguez

Hoja de control de medios probatorios				Caso:
Fecha:	Lugar de los hechos:			Nr.Id.:
Hora:				
Investigador:		Testigo:		
Firma:		Firma:		
Objetivo:	Número:	Descripción (tipo, fabricante, numero de serie, caracteristicas, etc.):		
Control de accesos:				
Objeto:	**Fecha/Hora:**	**Entregado por:**	**Recibido por:**	**Motivo:**
		Nombre:	Nombre:	
		Organización:	Organización:	
		Firma:	Firma:	
		Nombre:	Nombre:	
		Organización:	Organización:	
		Firma:	Firma:	
		Nombre:	Nombre:	
		Organización:	Organización:	
		Firma:	Firma:	
		Nombre:	Nombre:	
		Organización:	Organización:	
		Firma:	Firma:	
		Nombre:	Nombre:	
		Organización:	Organización:	
		Firma:	Firma:	
Protocolo de entrega de entrega final				
		Destinatario de entrega, testigo(s):		
Operaciones (devolución al propietario, archivado, destrucción, etc.)		Nombre y apellido:	Firma:	Fecha:
		1)		
		2)		
		3)		
		4)		

Figura 2.6: Modelo de la hoja para control de acceso a la evidencia, Cadena de custodia

2.2.4 Recuperación y análisis de la evidencia

Recuperación

Para recuperar la evidencia, el investigador utilizara técnicas y software forense que le ayuden a obtener archivos los cuales serán de gran importancia para la resolución del caso. Hay que dar por hecho que en varias ocasiones el criminal hará lo posible para eliminar información incriminatoria y evidencias de su presencia

La información recuperada pasara a la fase de análisis donde nos dará un veredicto de quien o quienes fueron los atacantes. Además las actividades ilícitas a las cuales se dedican.

Obteniendo el equipo del sospechoso podemos recuperar documentos, correos, logs, datos encriptados, datos ocultos, todos estos aun así hayan sido eliminados, dejando por resultado las actividades ilícitas realizadas.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Análisis

Ya con la disposición de las evidencias almacenadas y ordenadas, empieza lo más importante que es el análisis forense de los archivos que conforman la evidencia.

Con el análisis se pretende reconstruir la línea temporal del incidente, esta determina los acontecimientos que tuvieron lugar desde *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas*

En esta fase es donde se analiza áreas y archivos específicos del sistema operativo como:

1) Análisis de datos

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

2) Información de sistema operativo

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

3) Análisis de logs

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

4) Análisis de log

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

2.2.5 Documentación y presentación de la evidencia

Una vez concluido la fase de análisis forense de la evidencia, ya tendremos los resultados y a su vez el conocimiento del tipo y magnitud de ataque e incidente ocurrido, daños ocasionados, culpables y toda la información necesaria para la resolución y culminación del proceso de investigación.

El investigador forense deberá documentar mediante un informe detallado todo el proceso realizado, como metodologías, software forense utilizado, técnicas aplicadas desde que se obtuvieron las evidencias hasta la fase del análisis.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Existen dos tipos de informes:

Informe Técnico

En este informe el investigador forense deberá detallar de manera general el análisis efectuado, dando a conocer metodologías, herramientas, tipos de ataques y programas que fueron utilizados para dicho propósito. Además la cronología de las actividades realizadas en la evidencia.

También se debe proporcionar toda la información de las actividades técnicas que fueron utilizadas en la investigación.

Este informe debe contener[15]:

1) Exposición
    a. Antecedentes
    b. Objetivo
    c. Descripción de la evidencia
2) Entorno y recolección
    a. Herramientas utilizadas
    b. Recolección de datos
3) Análisis
    a. Integridad de la evidencia
    b. Identificación de la evidencia
    c. Servicios y procesos activos
    d. Programas ejecutándose en el sistema
4) Metodología
5) Descripción de hallazgo
6) Huellas de comportamiento, Actividades y Rastros del sospechoso
7) Cronología de Actividades
8) Posibles víctimas del sospechoso
9) Posibles cómplices del sospechoso
10) Conclusiones
11) Recomendaciones a los padres
12) Referencias

[15] Tomado de un informe real de la comunidad Dragonjar, reto forense

Informe Ejecutivo

Este detalla la misma información que contiene el informe técnico con la diferencia de que en el informe ejecutivo se emplea una explicación no técnica y con lenguaje común el cual va dirigido a la persona no especializada en informática como lo pueden ser: Abogados, Recursos humanos de la entidad afectada, integrantes del juzgado, etc.

Este informe debe contener[16]:

1) Introducción
2) Análisis
3) Resumen de hechos
4) Conclusiones
5) Recomendaciones

2.3 Esteganografía y Estegoanálisis

En la informática, es la disciplina dedicada al estudio del conjunto de técnicas que tiene por objetivo ocultar la información sensible, mensajes u objetos dentro de otros ficheros denominados contenedores o portadores como: archivos ejecutables, multimedia, imágenes digitales, videos, audio, siendo transparente a terceros y recuperada por un usuario legítimo.

Figura 2.7: Esteganografía, imagen con mensaje oculto

[16] Tomado de un informe real de la comunidad Dragonjar, reto forense

Es la ciencia y el arte dedicada al estudio de la detección de mensajes ocultos aplicados por la esteganografía. Pueden estar en medio como imágenes, video, audio o incluso un simple texto plano.[17]

2.3.1 Técnicas de esteganografía

PoC (Inserción de bits en el objeto contenedor)

A partir de una marca estructural del fichero contenedor (fin de fichero, espacios de padding o alineamiento, etc.) se añaden los bits a ocultar. El problema es que se incrementa el tamaño del fichero contenedor siendo un poco indiscreto ante terceros.

Por ejemplo:

En una imagen BMP, los primeros 54 bytes contienen los metadatos de la imagen divididos de la siguiente manera:

BYTES	CONTENIDO
2	Contiene la cadena BM, revelando que se trata de un BMP
4	Tamaño en bytes
4	Contiene ceros (reservados para usos futuros)
4	Offset, distancia entre cabecera y primer pixel de la imagen
4	Tamaño de los metadatos
4	Ancho (número de pixeles horizontales)
4	Alto (número de pixeles verticales)
2	Número de planos de color
2	Profundidad de color
4	Tipo de compresión (valor cero porque BMP no es comprimido)
4	Tamaño de la estructura de la imagen
4	Pixeles por metro horizontal
4	Pixeles por metro vertical
4	Cantidad de colores usados

[17] Basado en: http://www.expresionbinaria.com/el-arte-de-ocultar-informacion-esteganografia/

4	Cantidad de colores de importancia

Tabla 2.1: Estructura de bytes de una imagen BMP. [18]

La ocultación de los datos se lo hace justo después de los metadatos, quedando así entre los metadatos y los datos de la imagen modificando el campo offset (distancia entre los metadatos y pixeles de la imagen). Pudiendo así insertar todo el contenido que queramos.

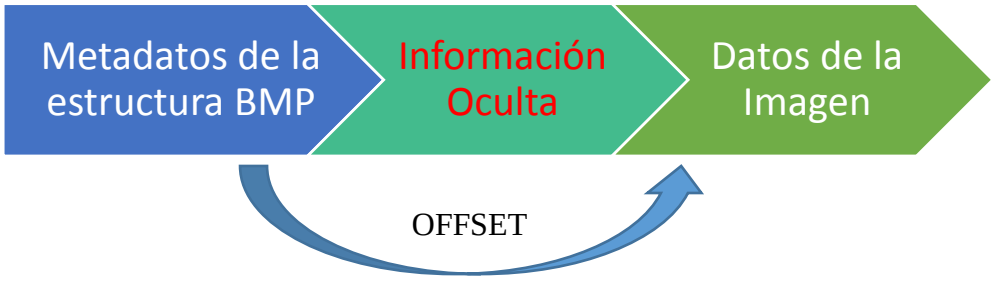


Figura 2.8: Estructura de la imagen con mensaje oculto

LBS (Least Significant bit / Inserción en el bits menos significativo)

Llamado también método de sustitución, el cual remplaza el bit menos significativo de los pixeles de una imagen digital (contenedor), por otros bits del mensaje a ocultar.

El tamaño del archivo no cambia y su calidad no se ve mermada ya que podríamos remplazar por ejemplo, en un archivo de audio, remplazar los bits que no son audibles por el ser humano por los bits del mensaje a ocultar.

El bit menos significativo se encuentra al lado derecho de este: 1 1 0 0 1 0 0 1

Un pixel es la menor unidad homogénea en color que forma parte de una imagen digital. Cada pixel está formado por 3 bytes que almacenan un color

[18] Tabla tomada de INTECO

primario Rojo, Verde y Azul. Su variación forman los distintos colores que se puede observar en cada pixel.

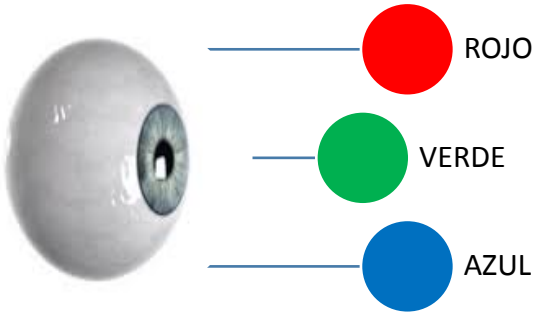


Figura 2.9: Pixeles visualizados por el ojo humano

Por ejemplo:

Si queremos esconder la letra A=01000001 que consta de 8 bits, necesitamos utilizar 3 pixeles de la imagen que contiene 3 bytes cada uno y así sustituir el LSB (bit menos significativo) de cada número binario por cada bit de la letra A (el mensaje a ocultar).[19]

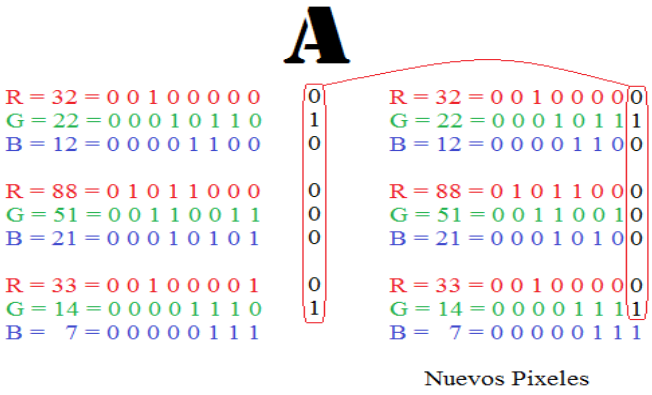


Figura 2.10: Esteganografía en el bit menos significativo

EoF (End of File / Fin del archivo)

Este es el método más fácil, el cual consiste en añadir el mensaje a ocultar al final del archivo contenedor *Este tipo de material es restringido, pedimos*

[19] Tomado de INTECO

disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Por ejemplo:

Si queremos esconder un imagen .JPG dentro de una imagen JPEG, esta es la siguiente estructura.

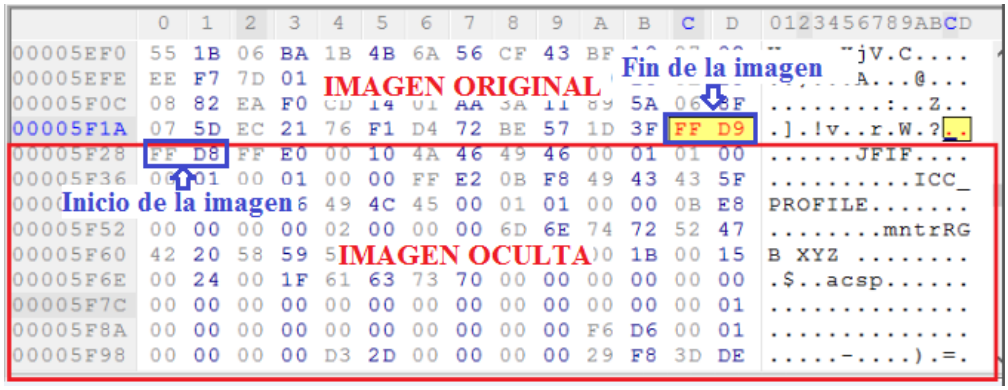


Figura 2.11: Imagen oculta dentro de otra

2.4 Herramientas de la informática forense

Las herramientas que nombrar a continuación, son muy útiles, ya que, en caso de estar al frente de un caso de Cibercrimen, nos ayudaran a resolverlo y a probarlo de una manera legal.

2.4.1 Herramientas para la adquisición de la imagen forense

DEFT

Digital Evidence & Forensics Toolkit, en septiembre del 2012 se convirtió en una asociación sin fines de lucro, permitiendo diseño, desarrollo y algunas aplicaciones incluidas en el sistema a la distribución GNU Linux. Su distribución es de forma gratuita. Contiene diferentes herramientas que nos ayudan a llevar un caso de informática forense. Se puede cargar su Live CD

dentro de cualquier maquina a analizar y así no dañar la evidencia del disco duro.[20]

Dentro de este sistema operativo podemos encontrar las herramientas dd, dc3dd y dcfldd para realizar la imagen forense del disco duro y la memoria RAM que son primordiales para llevar a nuestro laboratorio forense para analizarla. Más adelante veremos el porqué de las imágenes forenses.

DD (Dataset Definition)

Esta herramienta nos ayuda a realizar la copia del disco entero para no alterar la evidencia original. Es una herramienta de los sistemas operativos Unix el cuan nos ayuda a realizar una copia forense bit a bit de un dispositivo digital. El sistema operativo se puede ejecutar en modo Live, de esta manera no es necesario desconectar el disco a copiar. Es necesario tener otro disco con suficiente espacio y esterilizado el cual contendrá la imagen a respaldar.

Sintaxis: sudo dd if=origen of=destino. [21]

Para utilizar este comando es necesario tener muy en claro el nombre de las particiones a utilizar, el comando fdisk –I o el programa grafico gparted nos ayudan con lo mencionado.

Parámetros que nos ayudaran a mejorar el uso de esta herramienta

Parámetros	**Sintaxis**	**Detalle**
Pv	dd if=origen |pv|dd of=destino	Nos presenta información del proceso de copiado como, bits transferidos, tiempo que lleva

[20] Tomado de: http://www.deftlinux.net/
[21] Tomado de: http://blog.desdelinux.net/uso-del-comando-dd/

		ejecutándose y la tasa de trasferencia
Bs	dd if=origen |pv|dd of=destino bs=1M	Con este parámetro indicamos que la lectura y escritura se realice en bloques de 1MB (menos sería más lento pero más seguro, más nos arriesgaríamos a perder datos por el camino)
hda1	dd if=/dev/hda1 |pv|dd of=/dev/hdb bs=1M	Graba solo la primera partición del disco de origen hda1 en el destino hdb
Hda	dd if=/dev/hda |pv|dd of=/dev/hdb1 bs=1M	Grabar el disco completo (hda) en la primera partición (hdb1) del destino
bin o iso	dd if=/dev/hda |pv|dd of=/home/hda.bin	Crea una imagen iso del disco duro (hda) en el directorio /home
For n in {1..5}	For n in {1..5}; do dd if=/dev/urandom |pv|dd of=/devhda bs=8b conv=notrunc;	Borra totalmente la información de un disco, llenando el disco con caracteres aleatorios cinco veces.
X	dd if=/dev/zero |pv|dd of=/dev/sdx	Borra el disco completo de cualquier dispositivo
A	Dd if=/dev/zero |pv|dd of=/dev/sdxa	Borra la partición del disco de cualquier dispositivo
conv=noerror,sync	Dd if=/dev/dcrom |pv|dd of=/home/dvd_recuperado.iso conv=noerror,sync	Recupera solo los sectores legibles de un DVD o de un disco duro (noerror ignora los errores de lectura en cualquier situación)

Men	Dd if=/dev/men of=/dev/sde1/men_dump. dd bs=1MB count=10	Este realiza una imagen de lo que se carga en la memoria RAM de la evidencia.

Tabla 2.2: Parámetros para el uso de DD

DC3DD

Es una modificación de dd que incluye ciertas características que facilitan la adquisición de las imágenes forenses. [22]

Sintaxis: sudo dc3dd if=/dev/sdb hofs=/media/dev/dm-0/dc3dd/imagen.dd.000 ofsz=500M hash=md5 log=/media/dev/dm-0/dc3dd/imagen.txt

Descripción de parámetros:

- If=/dev/sdb (disco a copiar)
- Hofs=/media/ …/imagen.dd.000 (destino donde guardar la imagen) Podría haberse utilizado of pero hofs permite dividir la salida en distintos archivos con extensión secuencial imagen.dd.000, imagen.dd.001, etc. Calcula el hash para cada archivo comparando contra el disco de origen.
- Ofsz=500M (tamaño de cada uno de los archivos)
- Hash=md5 (el algoritmo a utilizar puede ser: md5, sha1, sha256 o sha512)
- Log=/media/ …/imagen.txt (ruta donde se guardara las estadísticas del proceso)

[22] Tomado de: http://www.welivesecurity.com/la-es/2013/07/17/herramienta-adquisicion-imagenes-forenses-elegir/

Durante la ejecución se ofrece una cantidad importante de información donde muestra la cantidad de los bytes copiados.

DCFLDD

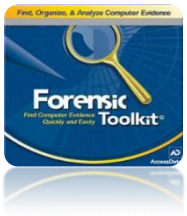
Esta herramienta también es basada en dd con la diferencia de dc3dd en que es una bifurcación de dd más no actualización.

Sintaxis: sudo dcfldd if=/dev/sdb Split=500M splitformat=000 of=/media/dev/dm-0/dcfldd/imagen.dd hash=md5 errlog=/media/dev/dm-0/dcfldd/error.txt hashwindow=500M hashlog=/media/dev/dm-0/dcfldd/hash.txt

La diferencia es que se especifica un archivo donde almacenar el log con los errores durante el proceso, y otro donde almacenar los hash. Hashwindows indica cada cuantos bytes calcular el hash. Si hash Windows coincide con Split, el proceso de verificación de hash es por comparación directa.[23]

Finalmente, la información que dcfldd muestra en pantalla es muy poca, solamente indica la cantidad de bits copiados y la velocidad de copia es baja.

FTK IMAGER



Es una herramienta para pre visualizar datos, realizar copias o imágenes, permitiéndonos examinar de una manera rápida evidencia digital y así determinar si se requiere realizar un análisis más profundo o no.

Este nos ayuda a crear imágenes forenses perfectas sin alterar la evidencia original.

Con FTK Imager podemos:

[23] Tomado de: http://www.sahw.com/wp/archivos/2010/09/25/obtencion-de-imagenes-forenses-mediante-derivados-mejorados-de-dd-dcfldd-y-dc3dd/

- 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 desde las imágenes forenses
- Recuperar archivos o carpetas desde las imágenes forenses
- Recuperar archivos borrados desde la papelera de reciclaje
- Crear hashes de archivos utilizando MD5 o SHA-1
- Generar reportes de hashes para archivos regulares e imágenes

FTK Imager fue desarrollado por AccessData Forensics Toolkit que es una plataforma donde podemos realizar investigaciones forenses digitales de una manera rápida, estable y muy fácil de usar.[24]

FTK IMAGER PARA LINUX

Es una herramienta comercial, pero que se puede utilizar en forma gratuita.

Sintaxis: sudo ftkimager /dev/sdb /mediadev/dm-0/ftkimager/imagen –ver ify –e01 –frag 500M –compress 5

Este ofrece mayo información que dc3dd, y al terminar el cálculo se realiza la verificación. Esta ofrece la posibilidad de comprimir los archivos de salida, es decir, de un disco de 100GB se obtuvo una imagen de menos de 40GB, casi sin reducir la velocidad de copia.[25]

2.4.2 Herramientas para cálculo de hash

[24] Tomado de: http://accessdata.com/product-download
[25] Tomado de: http://www.reydes.com

SLAVASOFT HASHCALC

Este es un software que calcula HASH, CRC y HMAC muy fácil y rápido de usar. Este se puede usar en archivos, cadenas de texto y cadenas hexagonales. Tiene a disposición 13 algoritmos hash y checksum más populares. [26]

Características:

- Trabaja con archivos de gran tamaño
- Calculo para cualquier tipo de archivo
- Instalación rápida y sencilla
- Arrastra y soltar
- Soporte de dos modos de cálculo HASH y HMAC

2.4.3 Herramientas para análisis de imágenes forenses y registros de Windows

Herramienta Open Source que extrae e interpreta información como llaves, valores y datos desde el registro de Windows, también ofrece la posibilidad de personalizar a cada una de las necesidades del examinador con diferentes plugins.

Para ejecutarla debemos ya tener generado los Hive File (registro de Windows) como imagen forense que contiene todos los movimientos del sistema hechos hasta esa hora. [27]

Esta herramienta permite recuperar información de un dispositivo externo proveyendo al examinador forense la recolección eficiente de evidencia. Esta permite[28]:

[26] Tomado de: http://www.slavasoft.com/hashcalc/

[27] Tomado de: http://www.reydes.com/d/?q=Extraer_Informacion_del_Registro_de_Windows_con_RegRipper

[28] Tomado de: http://recorriendo-los-caminos-de-encase.blogspot.com/search/label/EnCase%20Forensic

- Adquirir datos de diferentes dispositivos
- Desenterrar las posibles pruebas con el análisis forense a nivel de disco
- Realización de reportes detallados sobre sus hallazgos
- Mantener la integridad de la evidencia en un formato que los tribunales han llegado a confiar
- Presenta una vista previa de los resultados pudiendo de forma simultánea ir analizando y buscando archivos y medios

Es una plataforma para análisis forense digital. Esta comúnmente es utilizada por la policía cibernética, ejército y examinadores corporativos con el objetivo de investigar lo ocurrido en un ordenador. También recupera archivos del dispositivo a analizar.

Autopsy ejecuta tareas en segundo plano, en paralelo con múltiples núcleos para ofrecer resultados de una manera rápida. Puede tomar horas en analizar todo un disco per en cuestión de minutos se podrá saber si se encontraron palabras clave en la carpeta de inicio de usuario.

Antopsy es gratuito y ofrece otras características esenciales, como el análisis de artefactos web y análisis del registro que otras herramientas comerciales no ofrecen.[29]

2.4.4 Herramientas para recuperación de archivos

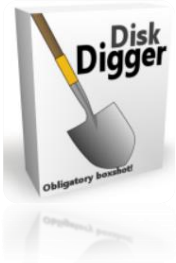
TestDisk, es una potente herramienta de recuperación de datos desarrollado por CGSecurity para Windows, Mac y Linux.

[29] Tomado de: http://www.sleuthkit.org/autopsy/

Permite recuperar particiones perdidas de diferentes sistemas de archivos incluyendo FAT12/ 16/ 32, FEB, CramFS, Linux RAID, NTFS, HSF, BSD, etc. También recuperar particiones eliminadas, así como la tabla de particiones fix.

Diseñado para filtrar tableas FAT, FAT32 y hacer copiar de seguridad, recuperar y reconstruir sectores de arranque NTFS y FAT32

Esta herramienta no tiene costo y es muy fácil de usar.[30]



DiskDigger, esta herramienta permite deshacer la eliminación y recupera archivos perdidos de su disco duro, tarjetas de memoria, USB, etc.

Cuando se elimina un archivo en realidad no queda limpiada desde el disco, el sistema de archivos lo marca como eliminado y de esta manera no muestra el archivo cuando se explora el contenido del disco.

DiskDigger escanea el sistema de archivos en busca de archivos eliminados, los expone al examinador y permite traer de vuelta.

Solamente es compatible con FAT, FAT32, NTFS y exFAT.[31]

2.4.5 Herramientas para escavar en caches históricos

Es una herramienta que analiza un archivo de funciones de Windows proporcionando información sobre el uso de este en base a los archivos Thumbs.DB, Prefetch, index.dat, archivos de acceso directo.

[30] Tomado de: http://www.tomsguide.com/us/download/TestDisk,0301-4874.html

[31] Tomado de: http://diskdigger.org/

Los archivos Prefetch están ubicados en C:\Windows\Prefetch y tiene el nombre del archivo ejecutable del programa .exe seguido de un hash de la ruta (información del directorio) y con extensión .pf

Este lee el archivo .pf y nos muestra información sobre fechas de ejecución, número de ejecuciones, etc. Todo esto referente a un programa que haya sido ejecutado en el sistema operativo Windows.[32]

Las Siguientes son para análisis en caliente[33]:

UserAssistView

Utilidad freeware que descifra y muestra una lista de todas las entradas guardadas bajo la llave UserAssist HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \Explorer \UserAssist en el registro del sistema. Esta contiene información sobre los archivos .exe y enlaces que se abren con frecuencia. Pueden guardar la lista en archivos de texto html, xml, csv y también podemos eliminar archivos no deseados.

WinLogOnView

Es una herramienta para Windows, que analiza el registro de sucesos de seguridad del sistema operativo detectando la fecha, hora de inicio y cierre de sesión.

Por cada usuario que inicie sesión nos muestra la siguiente información.

- ID de inicio de sesión
- Nombre de usuario
- Dominio
- Ordenador
- Tiempo de inicio de sesión
- Hora de cierre de sesión
- Duración
- IP (Dirección de red)

[32] Tomado de: http://www.mitec.cz/wfa.html

[33] Tomado de: http://www.nirsoft.net

También permite exportar la información obtenida en HTML, XML. La exactitud de esta información depende de la disponibilidad y exactitud de los datos almacenados en el registro de eventos de seguridad.

LastActivityView

Es una herramienta que recopila información de diferentes fuentes mostrando un registro de las acciones realizadas por el usuario y los eventos ocurridos en ese tiempo en el equipo.

La actividad que nos muestra es:

- Ejecución del archivo .exe
- Apertura del archivo
- Carpeta de apertura desde el explorador o cualquier otro software
- Instalación de software
- Apagado e inicio del sistema
- Conexión y desconexión de red
- etc.

También permite exportar la información obtenida en HTML, XML.

FolderChangesView

Es una herramienta lo cual supervisa la unidad de disco o carpeta, listando de cada archivo o carpeta encontrados todos los cambios efectuados en esta. Es decir, monitorea que se está ejecutando, cambios que se están haciendo, monitorea actividades que se hacen en ciertas selección, etc.

JumpListsView

Es una herramienta que muestra la información almacenada por las características de Windows 7/8. Cada registro que se encuentre en la Jump List se muestra:

- Nombre del archivo abierto por el usuario
- Fecha
- Hora en que se abrió el archivo

- ID del aplicativo utilizado para abrir el archivo
- Tamaño
- Tiempo
- Etc.

También permite exportar la información obtenida en HTML, XML.

ChromeCacheView

Esta herramienta lee la carpeta de cache del navegador web Google Chrome mostrando en forma de lista todos los archivos alojados en la memoria caché. La información mostrada para cada registro encontrado es:

- URL
- Tipo de contenido
- Tamaño del archivo
- Última visita
- Tiempo de caducidad
- Servidor
- Respuesta del servidor
- Etc.

El Path de la carpeta caché de Google Chrome es usuario\Configuración local\datos de programa\google\chrome\user data\default\cache. También permite exportar la información obtenida en HTML, XML, texto.

ChromeHistoryView

Es una herramienta la cual lee el archivo de datos de la historia de Google Chrome mostrando todas las páginas web visitadas en los últimos días, donde su información para cada página web es:

- URL
- Titulo
- Fecha y hora de visita
- Número de visitas
- Número de veces donde el usuario a escrito esta dirección

- Etc.

También permite exportar la información obtenida en HTML, XML, texto.

MyLastSearch

Es una herramienta que escanea los archivos de cache y el historial del navegador web, también localiza todas las búsquedas que se han realizado con los motores de búsqueda más populares (Google, Yahoo y MSN) y redes sociales como (Twitter, Facebook, MySpace). La información mostrada es la siguiente:

- Texto de búsqueda
- Búsqueda por tiempo
- Tipo de búsqueda (Video, imágenes, etc.)
- Navegador web
- URL
- Etc.

También permite exportar la información obtenida en HTML, XML, texto.

Thumbnail Database Viewer

Permite ver cache de miniaturas que se utiliza por Windows con el objetivo de acelerar la visualización e imágenes en miniatura en carpetas (thumbs.db, ehthumbs.db, thumbcache.db, etc.). La cache almacena todo en una carpeta incluso si ha sido borrada la imagen original.

Database Viwer en miniatura se puede utilizar para analizar archivos que thumbs.db que proporcionan detalles de cuando se guardan las imágenes, sus nombres y lugares de almacenamiento. Esta herramienta no tiene costo y es de libre uso y distribución.

2.4.6 Herramientas para el uso de esteganografía y Estegoanálisis

HEXWORKSHOP

Desarrollado por BreakPoint Software, este contiene herramientas de desarrollo hexadecimal para Windows. Permite la edición y la interpretación avanzada de datos binarios siendo fácil su visibilidad y flexibilidad con un procesador de textos moderno.

Características:

- Ubicación del sector y editor
- Buscar y remplazar datos
- Realizar operaciones aritméticas
- Bit a bit
- Operaciones lógicas
- Comparar archivos binarios
- Distribuciones de caracteres
- Editor de sectores con herramientas de imagen de disco
- Convertidor entre hexadecimal, decimal y tipos de datos binarios
- Visualizador de datos (Este ayuda a identificar visualmente los patrones y datos interesantes de las imágenes rende rizadas)

No es software libre por lo que tiene un costo. Adicionalmente permite dar color a las secuencias de datos, edición de datos binarios, importación y exportación de bloques de datos, búsqueda de datos por cadenas hexagonales, texto, Unicode, mascara de bits o valores decimales, ediciones de sectores, entre otros. Su interfaz se puede personalizar a gusto de cada usuario y definir cómo y qué datos se va a mostrar.[34]

STEGANOGRAPHY ANALYZER FIELD SCANNER

StegAlyzerFS, es una herramienta de Estegoanálisis diseñado para realizar una rápida exploración de medios en busca de información oculta de esteganografía.

[34] Tomado de: http://www.hexworkshop.com/overview.html

Un ordenador sospechoso se puede arrancar desde el dispositivo StegAlyzerFS capturando resultados en cuestión de minutos. Detecta más de 55 patrones de bytes singularmente identificables, o firmas conocidas dejado dentro de los archivos originales donde se ha ocultado la información.

Características:

- Software exclusivamente desde un dispositivo USB
- No requiere instalación ni configuración
- No cambia los medios de almacenamiento de destino, conservando la integridad de la informática forense
- Escaneo automático de todo dispositivo
- Escaneo de sistemas de archivos más populares como ext2, ext3, ReiserFS, XFS, FAT, FAT32, NTFS, ISO y otras soportadas por el Kernel de Linux 2.6.32
- Automática descompresión y extracción de tipos de archivos como: zip, iso, tar, gz, gz2, bz, bz2, rar, cab, pax, cpio, xar, lha, ar, mtree
- Generación de reportes en formato HTML

Tiene un costo de licencia y se lo puede obtener de SARC (Steganography Analysis and Research Center. [35]

STEGANOGRAPHY ANALYZER ARTIFACT SCANNER

StegAlyzerAS, es una herramienta que permite al examinador escanear medios sospechosos o imágenes forenses de medios de comunicación.

Permite la identificación de archivos mediante valores hash, aplicación de huellas digitales.

Características:

- Versiones disponibles para 32 y 64 bits
- Generación y gestión de casos

[35] Tomado de: https://www.sarc-wv.com/products/stegalyzerfs/learn_more.aspx

- Monta y escanea imágenes forenses de medios de almacenamiento en EnCase, ISO, RAW (dd), SMART, SafeBack, paraben Forensic Replicator
- Exploración automatizada de todo un sistema de archivos, directorios individuales o archivos individuales en medios sospechosos
- Análisis automatizado del registro de Windows
- Permite un resumen estadístico de cualquier análisis anterior ya terminado durante el proceso de examinado
- Reportes en formato HTML

Tiene un costo de licencia y se lo puede obtener de SARC (Steganography Analysis and Research Center. [36]

STEGANOGRAPHY ANALYZER REAL-TIME SCANNER

StegAlyzerRTS, es un dispositivo de red que ofrece seguridad siendo capaz de detectar en tiempo real aplicaciones de estenografía. Compara los hash de los archivos bajados para verificar autenticidad.

Detecta también escaneando archivos de entrada y salida de la red, robo de información oculta dentro de un archivo portador que puede ser enviada por correo electrónico. [37]

Características:

- Envía alertas a los administradores de red
- Realiza copias de los archivos sospechosos para su análisis
- No afecta el rendimiento de la red

[36] Tomado de: https://www.sarc-wv.com/products/stegalyzeras/learn_more.aspx
[37] Tomado de: https://www.sarc-wv.com/products/stegalyzerrts/learn_more.aspx

STEGANOGRAPHY ANALYZER SIGNATURE SCANNER

StegAlyzerSS, esta herramienta permite examinar cualquier dispositivo o imágenes forenses en busca archivos sospechosos que hayan sido aplicados estenografía, archivos con información oculta en su interior. Dispone de algoritmos de extracción únicas para recuperar información.

Este fue diseñado para ser eficaz e identificar los archivos ocultos estenográficos por el instituto de Defensa de Delito Cibernético (DCCI) y el Laboratorio Cyberscience (CSL). [38]

Características:

- Versiones disponibles para 32 y 64 bits
- Generación y gestión de casos
- Monta y escanea imágenes forenses de medios de almacenamiento en EnCase, ISO, RAW (dd), SMART, SafeBack, paraben Forensic Replicator
- Exploración automática de todo un sistema de archivos, directorios o archivos individuales
- Identificar archivos que se adjuntan más allá del marcador de un archivo, al final de su archivo con la función de analizar datos anexados y visualizar en un editor hexadecimal para determinar la naturaleza de la información oculta.
- Identificar, extraer y reorganizar archivos donde se ha aplicado esteganografía utilizando la técnica del bit menos significativo (LSB)

MP3Stego

Esta herramienta oculta información en archivos MP3 durante el proceso de compresión, es decir, los datos se comprimen primero, se encripta y luego se oculta en el flujo de bits de MP3.

[38] Tomado de: https://www.sarc-wv.com/products/stegalyzerss/learn_more.aspx

Inicialmente ha sido escrito con aplicaciones esteganografía con la finalidad de marcar los derechos de autor para los archivos MP3. Se puede volver a descomprimir y volverlo a comprimir, esto borrara el mensaje pero a costa de la perdida de la calidad del archivo MP3. [39]

JPHide y JPSeek

Esta herramienta permite ocultar un archivo dentro de una imagen .jpeg teniendo como objetivo principal es imposibilitar demostrar que el archivo contenedor contiene un archivo oculto. Esto se debe a una baja tasa de inserción (por debajo del 5%) y la ausencia del archivo original. La inserción por encima del 15% comienza a ser visible a simple vista. Algunas imágenes son mejores portadores que otras tomando en cuenta algunos detalles como:[40]

- Buen portador: Imagen de una cascada en un bosque
- Mal portador: Cielo azul con una montaña de nieve

WbStego

wbStego4open, es una aplicación de código abierto para Windows y Linux. Este puede ocultar cualquier tipo de archivo en los siguientes archivos contenedores: [41]

- Mapas de bits de Windows con 16, 256 o 16.7M de colores
- Archivos de texto ASCII o ANSI
- Archivos HTML
- Archivos de Adobe PDF

MSU StegoVideo

[39] Tomado de: http://www.petitcolas.net/fabien/steganography/mp3stego/
[40] Tomado de: http://linux01.gwdg.de/~alatham/stego.html
[41] Tomado de: http://wbstego.wbailer.com/

Permite ocultar cualquier archivo en una secuencia de video. Esta herramienta sobre la cual se han hecho análisis de diferentes codecs populares y un algoritmo, que proporciona la pérdida de datos más pequeña después de la compresión. La decodificación de Viterbi es utilizada para corregir errores ocurridos.

Características:

- Pequeñas distorsiones de video después de ocultar información
- Es posible extraer información después de la compresión de video
- La información está protegida por contraseña

MSU StegoVideo puede utilizarse como filtro VirtualDub o como programa.[42]

Stegdetect / Stegbreak

Stegdetect es una herramienta automatizada para detectar contenido steganografico en imágenes. Este es capaz de detectar varios métodos estenográficos diferentes para incrustar información en imágenes JPEG. Disponible para sistemas operativos Linux.

Los Stegbreak son ataques de diccionarios de fuerza bruta contra las imágenes JPG específicas. Estas dos herramientas han sido desarrolladas por Niels Provos.[43]

[42] Tomado de: http://compression.ru/video/stego_video/index_en.html
[43] Tomado de: http://ambitwire.com/apps/cats/steganography/stegdetectstegbreak

ALTERNATE DATA STREAM

ADS, esta técnica de esteganografía funciona en sistemas de archivos NTFS, como Windows. Este consiste en asociar información a un archivo o directorio, de tal forma que podemos asociar un archivo1 a un arhivos2, de tal manera que el archivo 1 contendrá al archivo2 sin presentar modificación alguna siendo invisible para el sistema operativo y visible solo para el que sabe que está ahí.[44]

[44] Tomado de: http://jonathanmelgoza.com/blog/esteganografia-ocultacion-de-datos/

Capítulo 3

Metodología de la informática forense en cibergrooming

3.1 Análisis y exposición de un caso real de Cibergrooming

Hoy en día, la delincuencia es creciente, y sobre todo en la red donde su identidad permanece en el anonimato, se hace más fácil y rápido cometer esta especie de extorciones, como las que hablare en este caso la de Cibergrooming.

Siendo una adolecente, quien su identidad no es revelada, se encuentra desesperada, con miedo, pero se arma de valor para indicar a sus padres de que ha sido víctima de Cibergrooming (Acoso Sexual). Llega al acuerdo de que esto no puede continuar y que no debería quedar así, entonces deciden acudir a la fiscalía, donde indican y exponen su tema a las autoridades.

Levantan una denuncia contra un posible agresor, quien es denunciado por publicar fotos de ella intimas en internet, utilizar una identidad falsa y de amenazarla con la publicación de este material para humillarla. Lo acusan de practicar Cibergrooming.

El fiscal a cargo, con miembros de la policía, entre ellos uno de la policía cibernética por tratarse de Cibercrimen, van al lugar donde empezaron los hechos, inspeccionan y llegan al equipo de la niña, ella les brinda acceso total e indica que mediante el computador, a través de la aplicación de Messenger, Facebook, envió fotos a un contacto, quien creía conocer. Poco después este exigió fotos mucho más íntimas la cual causaron susto, generando muchas interrogantes sobre, quien en verdad puede ser y que es lo que busca de ella.

Finalmente indica que recibe una amenaza donde indica que sus fotos van a ser publicadas en la red si es que no enviaba más. El chantaje comienza pero ella no sede y busca ayuda en sus papás.

El fiscal, cuerpo de policías y sus padres junto con la niña, aguardan a tener nuevamente contacto con el posible agresor, la cual se dio, se procedió a rastrear el equipo del sospechoso obteniendo su dirección IP con la que

usaba para tener contacto con la víctima y dirección geográfica. Con la información entregada por la niña y el rastreo, el fiscal solicita al juez la incautación del equipo sospechoso. El juez emite una orden para 48 horas de incautación de los equipos que han tenido acceso con esa dirección IP por el fiscal, teniendo en cuanta que si se pasa de este tiempo es necesario averiguar por qué lo hizo y no realizo la incautación, esto para volver a generar nuevamente la orden.

El fiscal con el cuerpo de policías involucrados en el crimen, se dirigen a la escena del crimen, llegan a la ubicación obtenida, el fiscal toca su puerta, muestra sus credenciales y le informa el motivo de su presencia, muestra la orden emitida por el juez para obtener acceso a los equipos y al lugar de donde se encuentran. Le hace una serie de preguntas como: sus nombres y apellidos, los equipos que tienen acceso a internet, si conoce a la víctima, que relación tenia, en fin, simultáneamente el policía cibernético, entra en acción, tomando fotos de toda la escena del crimen, de los equipos, y lugares sospechosos. Toma notas de todos los acontecimientos e interroga a posibles testigos o cómplices.

Ahora, se acerca a los equipos y saca fotografías del estado en la que se encuentran, en este caso el equipo de cómputo estaba apagado, pero al parecer un poco caliente, encendió el equipo y realizo la virtualización de este, toda la evidencia recogida en la escena del crimen, el fiscal incauta y lleva a ponerla bajo cadena de custodia.

De igual manera hace con los demás dispositivos encontrados ahí, terminando su proceso y abandonando la escena del crimen junto con los demás miembros. También detienen al sospechoso por unas horas para una profunda interrogación y probar que el sospechoso es quien dice ser en la denuncia emitida por la víctima analizar su caso.

Es necesario conocer también que de ser necesario incautar los equipos de forma provisional, el fiscal lo puede hacer durante unas horas estableciendo por escrito el tiempo y dispositivo incautado para, futuramente pedir su

orden al juez indicando lo encontrado y que es necesario incautarlos por más tiempo para continuar con el análisis.

Mi misión será seguir y aplicar las fases de la informática forense para encontrar información valiosa, que delate y sea prueba del delito infringido por el sospechoso de Cibergrooming. Obtener la máquina virtual la cual voy a analizar llenando su hoja de control de medios probatorios para llevar todo de forma legal y finalmente emitir un reporte donde explique y detalle la forma de uso del equipo de cómputo por el usuario al que se le incauto y es sospechoso de Cibergrooming.

3.1.1 Identificación del incidente

El investigador forense saco varias fotografías de la escena del crimen, detallando todo lo encontrado referente a circunstancias de los hallazgos, incautaciones del cesto de basura, agendas, celulares, agendas electrónicas, equipo de cómputo, etc. Con el fin de obtener la mayor información posible para llegar a obtener más información de los hechos.

La policía cibernética guardo todo el material obtenido y puso bajo cadena de custodia todo aquello que puede ser prueba y evidencia de este delito mediante imágenes virtuales de los equipos encontrados y equipos físicos.

En mi caso, como investigador forense voy a analizar la copia exacta del equipo de cómputo, la cual es una máquina virtual. Para ello, procedí a llenar la hoja de control de cadena de custodia indicando que voy a obtener acceso a esta evidencia virtualizada con el fin de analizarla y entregar los resultados. Esta evidencia está custodiada por el director del departamento de delitos informáticos de *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas*

Hoja de control de medios probatorios				Caso:01
Fecha: 04/12/2014	Lugar de los hechos: Departamento de delitos informaticos de Mexico			Nr.Id.:001
Hora: 11:49:32				
Investigador: CFI-IR. Gustavo Quizhpe		Testigo: ISC. Edgar Justo Dominguez		
Firma: CFI-IR. Gustavo Quizhpe		Firma: ISC. Edgar Justo Dominguez		
Objetivo: Equipo de computo Virtualizado	Número: 1	Descripción (tipo, fabricante, numero de serie, caracteristicas, etc.): Imagen virtual .wmdk que representas las caracteristicas de una maquina, Intel core i7-4500U, con numero de serie del producto: 55274-649-9930016-23187, tiene 512MB de RAM, Sistema operativo Microsoft Windows XP Professional SP3		
Control de accesos:				
Objeto:	**Fecha/Hora:**	**Entregado por:**	**Recibido por:**	**Motivo:**
Maquina virtual del Equipo de Computo	04/12/2014	Nombre: ISC. Edgar Justo Dominguez	Nombre: CFI-IR. Gustavo Quizhpe	Analisis Forense, para comprobar el delito denunciado
		Organización: Policia Cibernetica de Mexico	Organización: GTV	
		Firma: GTV	Firma: Gustavo	
		Nombre:	Nombre:	
		Organización:	Organización:	
		Firma:	Firma:	
		Nombre:	Nombre:	
		Organización:	Organización:	
		Firma:	Firma:	
		Nombre:	Nombre:	
		Organización:	Organización:	
		Firma:	Firma:	
		Nombre:	Nombre:	
		Organización:	Organización:	
		Firma:	Firma:	
Protocolo de entrega final				
		Destinatario de entrega, testigo(s):		
Operaciones (devolución al propietario, archivado, destrucción, etc.)		Nombre y apellido:	Firma:	Fecha:
		1)		
		2)		
		3)		
		4)		

Figura 3.1: Control de cadena de custodio, Obtención de la máquina virtual

Una vez obtenido acceso a esta aplico mis herramientas, las cuales voy a utilizar para dar solución a este caso. La imagen virtual es montada en el Software VMware Workstation.

Enciendo la máquina y lo primero que hago es identificar todo el incidente clasificando la evidencia como:

Evidencia digital

- Memoria RAM
- Memoria Cache
- Disco Duro

Evidencia lógica

- Sistema Operativo
- Aplicaciones de software
- Archivos
- Carpetas

Especificaciones:

- Puertos TCP y UDP abiertos y sus aplicaciones asociadas, para ello utilizo el comando netstat –anb

  Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

- Usuarios conectados al sistema localmente y remotamente, para ello utilizo el comando net user (usuario locales) y nbtstat –s (usuarios remotos)

  Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

- Fecha y hora del sistema operativo, para ello utilizo el comando date /T y time /T. También de manera más general el comando systeminfo

  Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

- Procesos activos, recursos que utilizan usuarios o aplicaciones los veo en el administrador de tareas

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

- Direcciones IP del sistema, para ello utilizo el comando netstat –an

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

- Configuración de seguridad del sistema lo veo en el Centro de seguridad de Windows

Figura 3.2: Configuración de Seguridad del Sistema

- Programas instalados del Sistema Operativo en las configuraciones de Windows donde permite agregar o quitar programas

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

- Programas que arranca al inicio del sistema utilizando msconfig

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

3.2 Aplicación de la metodología de la informática forense en un caso real

3.2.1 Obtención de la evidencia

Como investigador forense, tengo que tener todos mis medios esterilizados que en donde manipulare la información, esto quiere decir formateado a bajo nivel. Este dispositivo utilizare solo para este caso e información que pertenezca a ello.

Para navegar por las carpetas, abrir archivos, analizarlos y recuperar información, es necesario sacar imágenes forenses y proseguir con un análisis en frio, de esta manera no alterare información valiosa como por ejemplo, veces abiertas un archivo, programa, etc.

Así evitare el remplazo de información en la memoria RAM ya que si bien sabemos, cada archivo, programa, etc., que abrimos es primero cargado en memoria y esto dañara rotundamente la información que haya podido recuperar de ella, como por ejemplo, mensajes de Facebook, Messenger, contactos, correos, etc.

Para realizar la copia bit a bit utilizare la herramienta AccessData FTK Imager, que necesariamente tendré que instalarla en la máquina del sospechoso, esta herramienta no consume muchos recursos y es aconsejada por investigadores forenses ya que de esta se ha obtenido buenos resultados que han sido validos ante un juzgado.

Empiezo generando la imagen forense de la memoria RAM ya que es la más delicada por ser una memoria volátil y que cualquier proceso puede generar cambios en esta fácilmente.

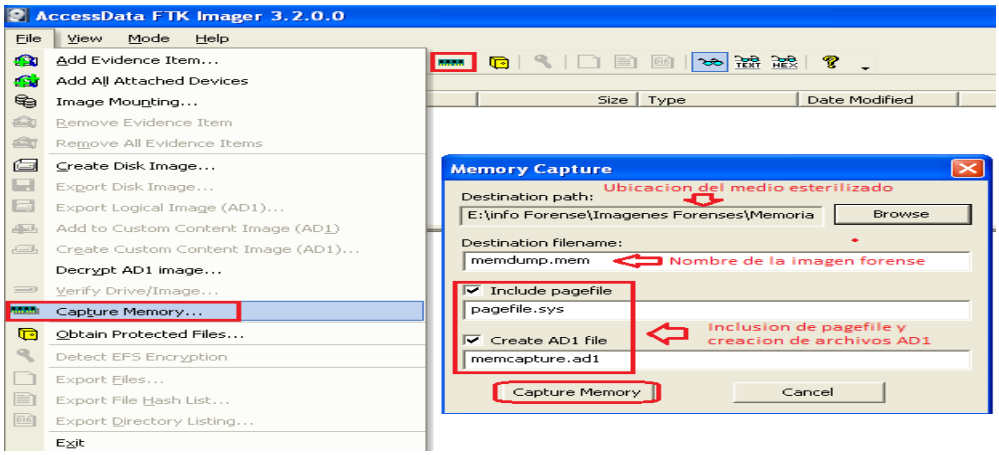


Figura 3.3: Generación de la Imagen Forense de la RAM

Una vez obtenida la imagen forense de la memoria RAM procedo con el Disco Duro, pudiendo hacer todo el disco y hacer una imagen física o simplemente por partición siendo esta una imagen Lógica.

Yo hare la imagen forense lógica, en este caso de la partición C, que es en donde está el sistema operativo el cual almacena toda la información y evidencia que me servirá para resolver este caso.

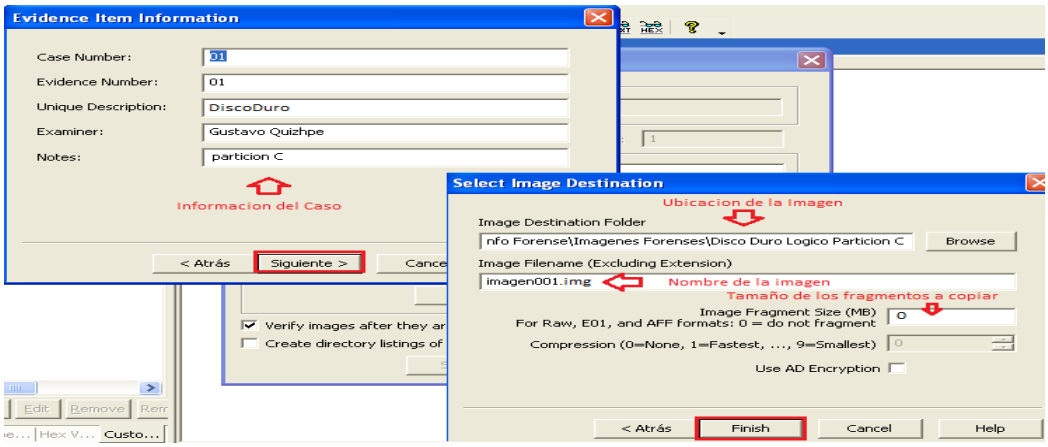


Figura 3.4: Generación de la Imagen Forense del Disco Duro

Para las imágenes forenses obtenidas, generare tres copias de cada una donde poseerán un código hash cada copia coincidiendo entre si su código.

Así aseguro que la información que estoy analizando es real y no ha sido manipulada o afectada por terceros. Las imágenes forenses hay que facilitarlas y ponerlas en cadena de custodia, de igual manera que la máquina virtual es necesario que aquel que tenga acceso a la evidencia llene la hoja de control de medios probatorios. Más adelante veremos un ejemplo.

La primera copia de la imagen forense es dada a la policía cibernética, para su comprobación y autorización de que la copia es correcta, la segunda copia a la fiscalía en caso de que se requiera comprobar la evidencia obtenida y la tercera, me la quedo para analizar más a fondo sobre el incidente denunciado por la victima menor de edad.

Eh montado una máquina virtual con las herramientas forenses necesarias para analizar información oculta, recuperar información, crackear contraseñas de archivos, etc. Esta máquina es utilizada específicamente y solo para resolver delitos informáticos. Su sistema operativo es Windows 8.1 de 64 bits.

3.2.2 Preservación de la evidencia

Al estar dirigida a la protección de los objetos catalogados como evidencia, trata de proteger que estos queden completos, verificables y claras. Los exámenes que se hagan, no deben generar cambios y de ser así presentar la razón, registrarlo y justificarlo.

Los medios forenses donde se va almacenar las imágenes forenses deben de estar esterilizados por lo que podríamos realizar un proceso de wipeo y copiarlas dentro del dispositivo.

Los únicos que tienen acceso a la evidencia somos los investigadores forenses, cuando necesitemos una copia para el análisis deben estar correctamente marcadas y preservadas, de esta manera somos responsables de las acciones tomadas en ellas.

Después de asegurarnos que estén correctamente marcadas y preservadas, tenemos que llenar la cadena de custodia, de tal manera que quede de la siguiente manera:

Hoja de control de medios probatorios				Caso:01
Fecha: 04/12/2014 Hora: 11:49:32	Lugar de los hechos: Departamento de delitos informaticos de Mexico			Nr.Id.:001
Investigador: CFI-IR. Gustavo Quizhpe	Testigo: ISC. Edgar Justo Dominguez			
Firma: CFI-IR. Gustavo Quizhpe	Firma: ISC. Edgar Justo Dominguez			
Objetivo: Imagen Forense de la memoria RAM y Disco Duro	Número: 1	Descripción (tipo, fabricante, numero de serie, caracteristicas, etc.): Imagen forense de la memoria RAM con un tamaño de 512MB, Mark Vision y Imagen forense del Disco Duro Logico, particion C, con un tamaño de 8GB, Maxtor.		
Control de accesos:				
Objeto:	**Fecha/Hora:**	**Entregado por:**	**Recibido por:**	**Motivo:**
Imagen Forense de la memoria RAM y Disco Duro	15/12/2014	Nombre: ISC. Edgar Justo Dominguez Organización: Policia Cibernetica de Mexico Firma: Edger	Nombre: CFI-IR. Gustavo Quizhpe Organización: GTV Firma: Gustavo	Analisis Forense, para recuperar archivos sospechosos
		Nombre: Organización: Firma:	Nombre: Organización: Firma:	
		Nombre: Organización: Firma:	Nombre: Organización: Firma:	
		Nombre: Organización: Firma:	Nombre: Organización: Firma:	
		Nombre: Organización: Firma:	Nombre: Organización: Firma:	
Protocolo de entrega final				
		Destinatario de entrega, testigo(s):		
Operaciones (devolución al propietario, archivado, destrucción, etc.)		Nombre y apellido: 1) 2) 3) 4)	Firma:	Fecha:

Figura 3.5: Hoja de control de medios probatorios, Imágenes Forenses

3.2.3 Recuperación y análisis de la evidencia

Una vez pasada las imágenes forenses a mi maquina donde comenzare con el análisis, montada la máquina virtual del sospechoso, procedo a utilizar técnicas y herramientas adecuadas para recuperar archivos e información que nos servirá como medio probatorio de lo ocurrido en la máquina.

Recuperación

Para recuperar archivos y luego hacer el análisis sobre este, es necesario examinar ciertos registros del sistema, archivos borrados, historial de navegación visitado, etc. De tal manera de obtener rutas sospechosas y recuperar los archivos dentro de estas.

Con la herramienta LADS, el cual verifica si existen archivos ocultos con esta técnica, copio al escritorio y desde la línea de comando ejecuto: lads c:\ /s > resultado.txt, así analizo todo el disco en busca de información oculta.

Figura 3.6: Búsqueda con LADS

El resultado es grabado en un archivo de texto con el nombre indicado en el comando anterior e indica que no existe información oculta pero si ciertos archivos cifrados en ciertos directorios sospechosos.

Estos directorios posiblemente es en donde se encuentra información que contiene otra información oculta dentro. Esta es la primera pista.

Directorios sospechosos:

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Con la herramienta Autopsy procedo a recuperar los archivos en los directorios sospechosos para su posterior análisis.

Creo un caso, selecciono la imagen forense del disco duro que es en donde se encuentran estos directorios, configuro y busco los directorios. Una vez encontrados extraigo toda la información contenida en estas rutas:

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedi

También, para tener mayor información de los movimientos del usuario en el sistema operativos, es necesario recuperar algunos archivos importantes:

- HIVE FILE: Este contiene los registros de Windows, en especial el archivo SAM que indica última sesión iniciada, número de veces, tipo de sesión, etc.
- PREFETCH: Este archivo contiene información de los programas ejecutados como número de veces, fechas, etc.
- NTUSER.DAT: este archivo es único para cada usuario, contiene todos los movimientos realizados en el sistema

Con la herramienta FTK Imager, desde la máquina virtual incautada, obtengo los registros de Windows exportándolos a mi dispositivo esterilizado para su análisis en mi maquina con FTK Imager las herramientas forenses.

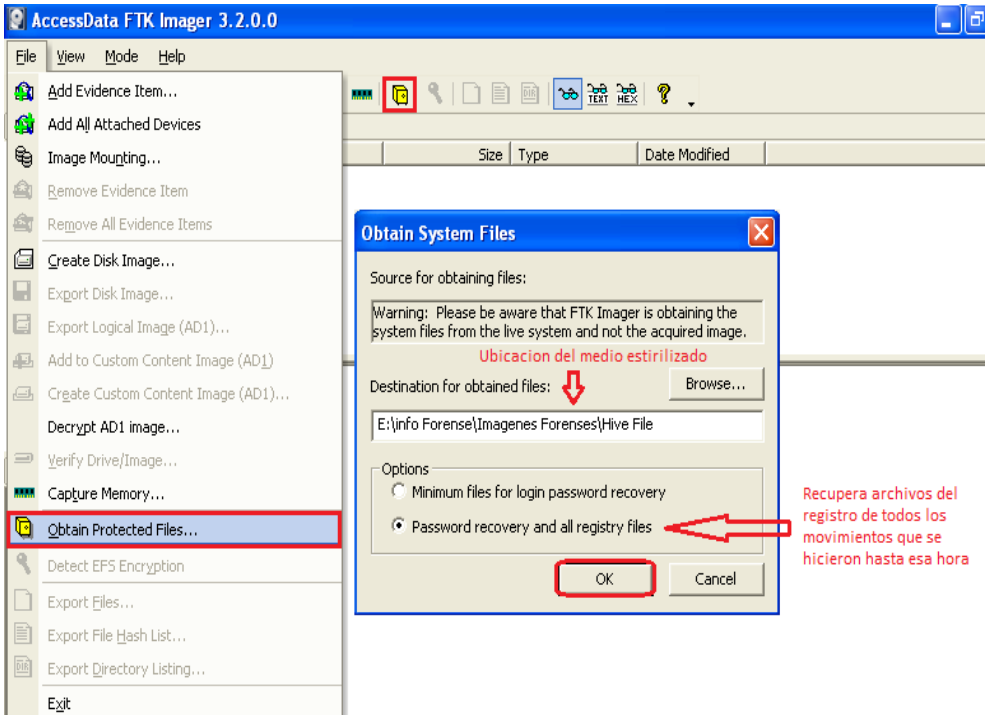


Figura 3.7: Adquisición de Hive File

Con la herramienta FTK Imager de mi maquina con las herramientas forenses, monto la imagen forense del Disco duro de manera física y lógica.

Navego con el programa hacia el directorio: C:\Windows\ y exporto la carpeta Prefetch con todos sus archivos.

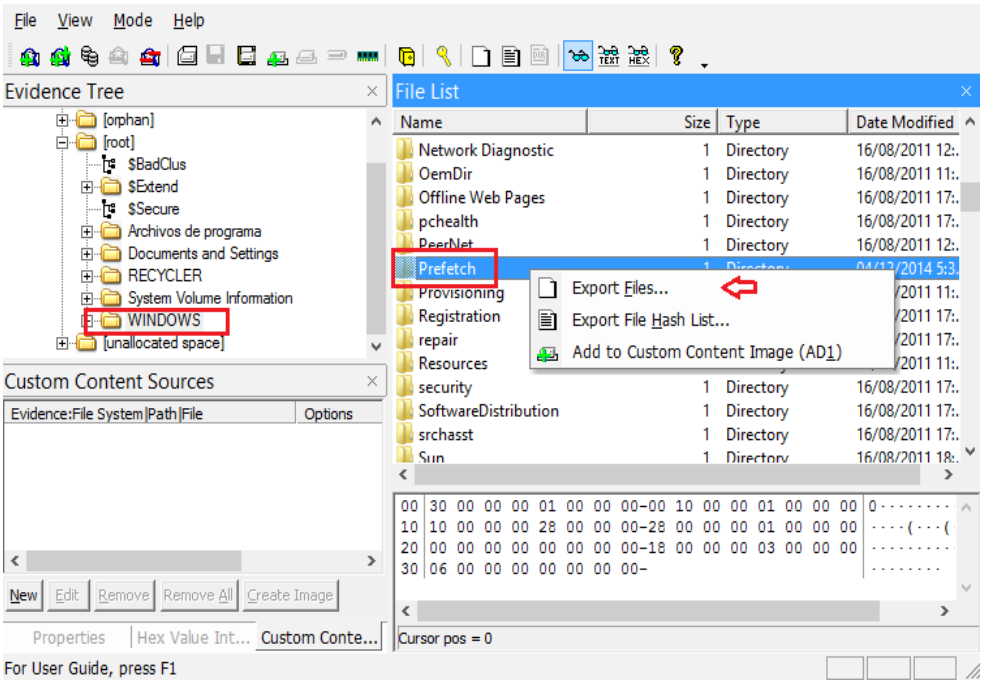


Figura 3.8: Recuperando Archivos Prefetch

De igual manera en el directorio C:\Documents and Settings\Administrador\ exporto el archivo NTUSER.DAT.

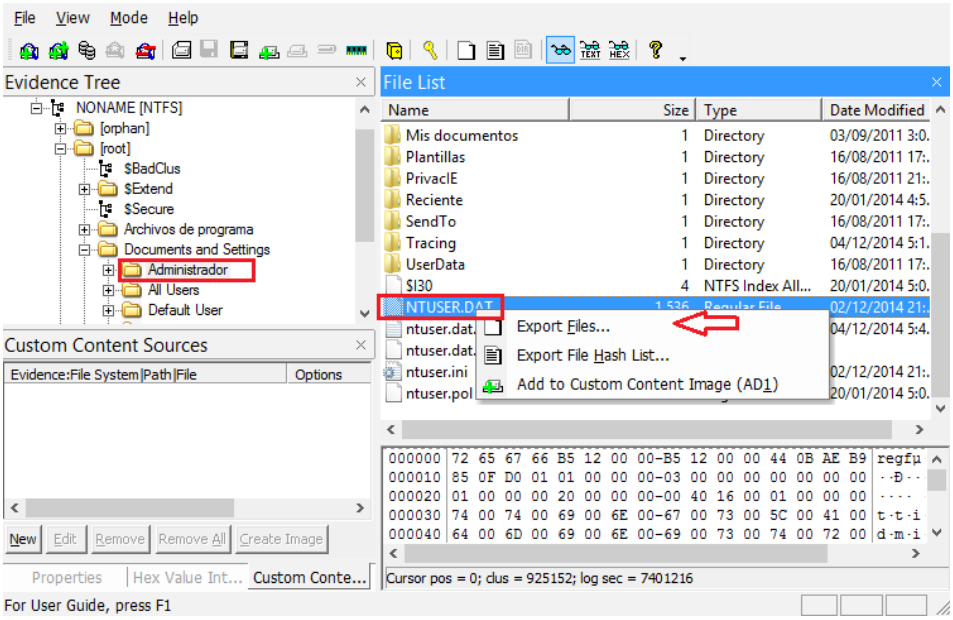


Figura 3.9: Recuperando Archivo NTUSER.DAT

Análisis

Una vez obtenido todos los archivos para su análisis, empezare por los registros de Windows que me indicaran los movimientos de la sesión del usuario, en este caso el usuario utilizado es Administrador.

Con la herramienta AccessData Registry Viwer, leo el archivo SAM (Administrador de cuentas de seguridad) el cual me da la siguiente información:

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Con la herramienta Prefetch Forensics leo el archivo prefetch y obtengo información acerca de los programas ejecutados en el sistema operativos. También el número de ejecuciones, fecha de creación, modificación, etc.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Ahora el archivo NTUSER.DAT me proporcionara información más amplia a cerca de todos los movimientos y acciones del usuario en el sistema

operativo. Este archivo lo leo con la herramienta Regripper el cual me da un reporte en bloc de notas.
El reporte indica y confirma programas, rutas sospechosas como las son:

Programas sospechosos:

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Directorios sospechosos

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Eh encontrado archivos que al parecer han sido modificados por ciertos aplicativos señalados en la siguiente imagen. También se observa ciertos archivos dentro de carpetas que no están ahora donde se muestra.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Imágenes jpeg y jpg sospechosos de igual manera encontrados, sobre todo un nombre de una carpeta que contienen algunos de estos archivos, esta se llama *Este tipo de material es restringido*

Archivos mp3 y rar sospechosos que aparentemente estaba dentro de una carpeta *Este tipo de material es restringido.* Me llama la atención los nombres de los archivos *Este tipo de material es restringido.* que fueron comprimidos en un formato .rar
Archivos avi y mp3 sospechosos.

Eh encontrado usuarios de Messenger que fueron logueados desde este usuario. Este pertenece al sospechoso ya que se a tenido acceso a las cuentas, y para esto significa que se sabe la contraseña de las mismas.

Finalmente este reporte me provee de URL que han sido visitadas con su última apertura de las cuantas ya encontradas. Las URL me indicaran que temas han sido de interés y en donde ha estado en internet.

Con la herramienta Autopsy recupere más historial de navegación, el rango sospechoso va desde *Este tipo de material es restringido.*

Éste historia me da páginas muy sospechosas, especialmente las que tienen el número:

- #4: Al parecer es un foro donde se publican fotos de alguien, e indican que existen fotos maquilladas y no.
- #5,6,15,17: Algunos servidores gratuitos donde permiten subir información para compartirla
- #23,26: Paginas de pornografía pedófila

Ahora, es hora de analizar los archivos extraídos en los directorios sospechosos. Por lo encontrado hasta el momento, es posible que el sospechoso haya utilizado técnicas de esteganografía para ocultar la información por lo que tengo que ser sumamente cuidadosos con esto.

Archivos examinado y en los que encontré evidencia para este caso.

Este tipo de material es restringido.

Aquí se encuentran varias imágenes, también un archivo Thumbs.db, este archivo Thumbs.db almacena una vista previa de las imágenes que están dentro de la carpeta como también las que hayan sido eliminadas. Eh notado dos imágenes con un tamaño en comparación a las demás, podría contener información oculta.

Este tipo de material es restringido.

Examinando las imágenes encontré que habían sido retocadas con Adobe Photoshop 3.0.8 e información de marca de la cámara, ángulo de la foto, etc. Es por ello el tamaño de estas. Con el archivo Thumbs.db me asegure de que no existan archivos borrados en la carpeta actual por la que no encontré nada sospechoso.

Este tipo de material es restringido.

Examinando su configuración comparando con la tabla de estructuras hexadecimales de los archivos,[45] encontré una imagen oculta posiblemente de una victima

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas.

Encontré un archivo .rar oculto el cual tenía contraseña, procedí a crackear el archivo y obtener la contraseña. Al descomprimir el archivo se obtuvo una carpeta llamada *Este tipo de material es restringido.* con imágenes de otra posible víctima. En el archivo Thumbs.db fue examinado y encontrado que una carpeta fue eliminada.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Encontré información que fue retocada con Adobe Photoshop y que tenía una imagen oculta dentro.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

[45] FILE SIGNATURES TABLE, se adjuntara en los anexos al final

Encontré un archivo .zip oculto, de igual manera con contraseña. Procedí a crackear la contraseña. Dentro de este dos archivos .rar protegidos por contraseña. El mismo procedimiento dando como resultado aplicaciones de esteganografía llamados mp3stegz y MSU StegoVideo los cuales sirven para ocultar dentro de archivos de audio y video.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Encontré un archivo zip oculto y protegido por contraseña, el mismo procedimiento dando por resultado un archivo de texto llamado *Este tipo de material es restringido,* conteniendo contraseñas de los archivos mp3 y algunos videos.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

En la carpeta *Este tipo de material es restringido* se encontraron diferentes archivos de audio y con la contraseña obtenida en el anterior archivo obtengo la información oculta de estos.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Encontré imágenes ocultas de victimas utilizando la aplicación mp3stegz

Este tipo de material es restringido

Esta carpeta contiene varias imágenes dentro de la ruta *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas*

Encontré videos ocultos, grabados posiblemente con Camtasia Studio, estas grabaciones son de video conferencias de Messenger, estas imágenes tienen contenido sexual.

Con las claves que encontré *Este tipo de material es restringido*, obtuve con el programa MSU StegoVideo un archivo de texto plano con usuarios y contraseñas. El video contenedor se llama *Este tipo de material es restringido.*

Ahora tengo evidencia donde delata totalmente al sospechoso.

Para llegar un poco más allá con la investigación, analizare su Messenger que se ejecuta al iniciar el sistema. Esto con fines de encontrar conversaciones, archivos recibidos, contactos, movimientos de las cuentas encontradas hasta el momento donde parecen ser usadas continuamente por el sospechoso.

Con la herramienta autopsy, buscando en la ruta *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas.* encontré los contactos activos y su log de movimientos, lastimosamente no pude encontrar archivos ni mensajes recibidos.

Una archivo interesante es el contactsLog.txt, que me da indica todo el movimientos del uso de Messenger

Su log de movimientos indica:

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Cuentas con las que se tuvo contacto:

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Al no encontrar mensajes, lo que me queda es analizar la memoria RAM en busca de ello.

La información que encontrare en la imagen forense de la memoria RAM no va a ser 100% clara, es decir, un texto con una información informal. Por ejemplo, si queremos examinar los mensajes de Facebook, nos basamos en el protocolo de este para encontrar los mensajes de texto un poco descoordinados.

Estas conversaciones si pueden ser tomadas en cuenta en un proceso legal pero, siempre y cuando encontremos ¿de quién?, ¿para quién?, la fecha y el mensaje.

Lo primero es montar la imagen forense de la memoria RAM en el FTK Imager y según el protocolo de búsqueda, en este caso la cadena con la que quiero encontrar los mensajes simplemente la escribo en el filtro y aplico. Una de las cadenas que siempre suelen tener los protocolos de mensajes como facebook, correos electrónicos y algunos más, es la caden (“text”:), aplicando la cadena mencionada de la siguiente manera, a continuación encontré los siguientes mensajes.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias

Estos mensajes son muy claros y válidos. También encontré al parecer uno que otro correo electrónico.

El formato de fecha de la mayoría de los mensajes esta con un formato diferente, por lo que es un numero tomado en segundos que han transcurrido desde 1 de enero 1970 a las 00:00:00 GMT (1970-01-01 00:00:00 GMT), dependiendo el formato de cada País, es este caso utilizare un conversor el cual a partir de esta serie de números nos devuelve la fecha a la que pertenece. Utilice un conversor online de www.freeformatter.com. La conversión de las fechas las pondré en el informe técnico para el juez.

Su medio de publicación en la red es a través de un foro, el cual anteriormente encontré su cuenta y su contraseña. Entrando a este blog encontré lo siguiente:

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Comparando con las imágenes encontradas, el nombre parece ser *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas.*

Con esto confirmo que es una menor de edad de *Este tipo de material es restringido* según el texto indica que fue enamorada haciéndose pasar por otra persona para obtener el material de fuerza para el acoso.

Las fotos *Este tipo de material es restringido.* nos mandan a descargar en el servidor de megaupload el cual, el enlace ya no funciona pero, tengo una pista, al parecer es una foto donde se encuentra el nombre *Este tipo de material es restringido*

Finalmente después de un largo trabajo, tengo la suficiente evidencia para detallar en los informes y presentar los resultados.

Capítulo 4

Informes y presentación de los resultados

4.1 Documentación y presentación de la evidencia

Ya en la última fase de la informática forense, comienzo a desarrollar los informes que serán leídos por los miembros de la corte, fiscales y juez. No hace falta tener un perito ya que estos no serán sobrecargados de tecnicismos siendo de fácil lectura para cualquier persona no especializada en informática. En caso de que se requiera analizar y comprobar estos resultados, se podría buscar la ayuda de uno

Estos informes contendrán todo el proceso realizado, metodologías, software forense, técnicas aplicadas, desde la obtención de la evidencia hasta la recuperación y análisis de la evidencia siendo válidos en el proceso legal respectivo.

Los informes contienen su estructura propia como vimos anteriormente, es necesario llevarlo tal y cual su estructura para tener un correcto ejemplo de cómo pudiéramos hacer y aplicar en Ecuador.

4.1.1 Informe técnico del análisis de la evidencia

Para este informe no es necesario etiquetar imágenes ni tablas, pero si un índice donde se encuentra los puntos globales y de importancia.

Lleva su respectiva caratula indicando el motivo y su investigador forense. E aquí lo mencionado:

Análisis forense, caso Cibergrooming

Informe Técnico

CFI-IR Gustavo Quizhpe

gatogtv11@hotmail.com

29/12/14

INDICE

1. Exposición

1.1. Antecedentes

Como estudio resultante por tema de tesis propuesto a la Universidad Politécnica Salesiana, se pretende detallar un informe técnico realizado a una maquina incautada, la cual, su copia exacta virtualizada de toda la maquina ha sido obtenido y dada la autorización correspondiente por *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas* propiedad de un usuario que es acusado de un delito considerado como cibergrooming y distribución de imágenes de contenido sexual de las víctimas en internet.

1.2. Objetivo

Obtener todas las pruebas necesarias para demostrar que el sistema analizado es utilizado para acoso sexual cibernético y distribución de imágenes sin permiso por parte de la víctima en internet

1.3. Descripción de la evidencia

Es facilitado una imagen de la máquina virtual del sospechoso en formato ".wmdk" (Virtual Machine Disk). Son hechas imágenes forenses del disco y la memoria RAM, puestas en custodia y autorizadas para el análisis.

2. Entorno y recolección

Utilizando el programa VMware Workstation, cargo la imagen adquirida y con la ayuda de un dispositivo USB con herramientas para realizar el análisis

forense, obtendré datos e información importantes respaldándolas en el mismo dispositivo para su análisis.

2.1. Herramientas utilizadas

#	Aplicación	Funcionalidad	Licencia
1	VMware Workstation	Emulador de máquinas virtuales	Comercial
2	FTK Imager	Adquisición y tratamiento de imágenes forenses	Free
3	Autopsy	Extraer archivos de las imágenes forenses	Free
4	HashCalc	Calcular código hash para imágenes	Free
5	Hex Workshop	Editor hexadecimal para verificar estructura de archivos	Comercial
6	AAPR	Recuperación avanzada de contraseña en archivos	Comercial
7	Thumbviewer	Muestra imágenes en miniatura almacenadas en Explorador de Windows en archivos Thumbs.db	Free
8	Lads	Búsqueda de Alternate data Stream (ADS)	Free

2.2. Recolección de datos

Los datos y rastros a recoger son:

- Procesos en ejecución
- Servicios Activos
- Programas Instalados
- Temporales de internet
- Historial de Carpetas de Mensajería instantánea (MSN)
- Clúster no asignado del Disco Duro
- Archivos borrados

3. Análisis

3.1. Integridad de la evidencia

Una vez llenado la ficha de control de evidencia, con la fecha y hora de la adquisición, es necesario hacer una comparación de código hash y así comprobar autenticidad del material que se va analizar.

3.2. Identificación de la evidencia

Una vez montada la imagen en VMWare Workstation, observo el sistema operativo y toda la información de la maquina como:

Sistema Operativo: *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas.*

Usuario: *Este tipo de material es restringido.*

Fecha y hora de instalación del SO: *Este tipo de material es restringido.*

Idioma: *Este tipo de material es restringido*

Usuarios locales y activos: *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas*

Programas instalados a tomar muy en cuenta: *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas*

3.3. Servicios y procesos activos

Estos aparentemente parecen estar en orden, Windows Live Messenger, es arrancado al iniciar el Sistema Operativo.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

3.4. Programas ejecutándose en el sistema

Analizando el archivo prefetch detallo los programas con más veces ejecutados y un poco sospechosos.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

3.5. Imágenes forenses

Las imágenes forenses del Disco Duro y la memoria RAM, fueron generadas y aprobadas para trabajar en ello. Cada una con su código Hash la cual coincide con las copias de la policía cibernética y fiscalía.
Código hash de la Memoria RAM:

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Código Hash del Disco Duro, disco local C:

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

4. Metodología

La metodología utilizada es, primero hacer un análisis en caliente y buscar archivos sospechosos con la herramienta Lads, después, un análisis en frio, la cual en mi laboratorio examino las imágenes forenses obtenidas de la máquina virtual y analizando los resultados de la herramienta Lads, busco los directorios y archivos sospechosos.

4.1. Búsqueda de “Alternate Data Streams”

Utilizando la herramienta Lads en búsqueda de archivos ocultos por esta técnica en el disco duro, no encontré archivos ocultos más que algunos encriptados, al parecer con otra técnica de esteganografía.

Para analizar el disco completo, desde la línea de comandos ejecuto:

```
C:\Documents and Settings\Administrador\Escritorio\lads>lads c:\ /s > resultado.
txt
```

El resultado es grabado en un archivo de texto llamado resultado.txt el cual daré su descripción en el punto 5.1.

4.2. Búsqueda de movimientos del sistema operativo

Movimientos realizados (NTUSER.DAT)

El archivo fue extraído con Autopsy de la imagen forense del disco duro.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Leído con Regripper.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Su archivo de resultados indico ciertos movimientos y acciones realizados por el usuario del equipo, Administrador. Los cuales son detallados en el punto 5.2

4.3. Búsqueda de archivos y URL de interés

Los archivos sospechosos de los directorios como *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas* son recuperados con Autopsy. Su análisis esta detallado en el punto 5.3

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

4.4. Búsqueda de mensajes

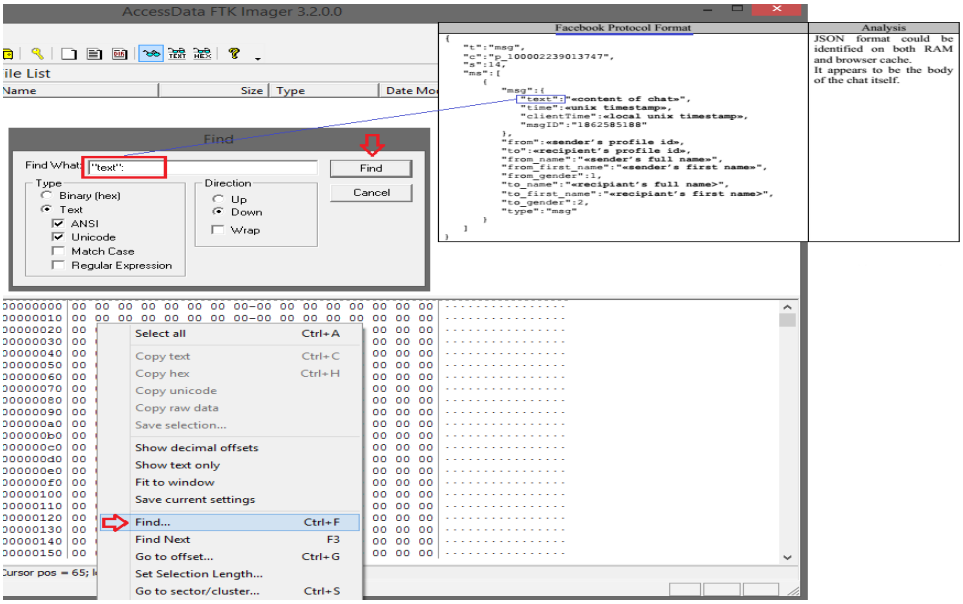
Los mensajes son parte vital de la evidencia, ya que señala directamente si un sospechoso es culpable o no.

Con Autopsy recupero los logs de los contactos de Messenger, un archivo llamado ContactsLog.txt, lamentablemente no se encuentran archivos ni mensajes recibidos. El log encontrado esta descrito en el punto 5.4.

4.5. Búsqueda de mensajes en la memoria RAM

Ya que los mensajes en la carpeta de configuración de Messenger no estaban, procedo a analizar la imagen forense de la RAM, cabe recordar que la información encontrada en esta no va a ser 100% clara, es decir, un texto con una información informal.

Yo utilizare la cadena (“text”:) como filtro para buscar dichos mensajes ya que la mayoría de protocolos de mensajería suelen tener esta cadena que indica el texto escrito por los usuarios. Los mensajes encontrados están descritos en el punto 5.5.



5. Descripción de hallazgo

5.1. Descripción de hallazgos de “Alternate Data streams”

El resultado de este análisis dio 2 directorios y algunos archivos sospechosos. Pero nada oculto con esta técnica.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

5.2. Descripción de hallazgos de movimientos del sistema operativo

Directorios escritos varias veces y sospechosos:

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Herramientas sospechosas

- MSU_stego_video
- Mp3stegz
- Msnmsgr

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Archivos y carpetas sospechosos

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Usuarios Messenger encontrados

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Historia de navegación y últimas aperturas de las cuentas encontradas

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

5.3. Descripción de hallazgos de los archivos y URL recuperados.

Los archivos examinados dieron los siguientes resultados:

Este tipo de material es restringido

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

5.4. Descripción de hallazgos de mensajes

El archivo ContactsLog.txt me da información de cuantas con las que se tuvo contacto, estas son:

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Su historial de movimientos son los siguientes:

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

5.5. Descripción de hallazgos de mensajes en la RAM

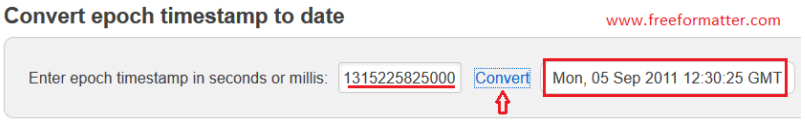
Los mensajes encontrados los describiré a continuación, pero es necesario aclarar que su fecha esta con un formato diferente, lo cual iré convirtiendo su fecha en un formato el cual dominamos a diario (dd/mm/yyyy).

El formato actual de los mensajes es un numero tomado en segundos que han transcurrido desde 1 de enero 1970 a las 00:00:00 GMT (1970-01-01 00:00:00 GMT), dependiendo el formato de cada País.

Conversor online utilizado es: www.freeformatter.com

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

Conversión de formato de fecha:



Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias

6. Huellas, Actividades y Rastros del sospechoso

Las huellas que se puede observar del sospechoso, como resumen de los puntos anteriores son:

- Historial de navegación: Actividades en internet
- Historial de Microsoft Messenger: Actividad y cuentas existentes
- Historial de archivos abiertos: Rastros de ubicaciones sospechosas donde se habían guardado las imágenes
- Historial de aplicativos ejecutados: Software utilizado para esteganografía

7. Cronología de Actividades

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

8. Posibles víctimas del sospechoso

De acuerdo a las evidencias encontradas, nombres de archivos, cuentas y mensajes recuperados. Las posibles víctimas son:

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

9. Posibles cómplices del sospechoso

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas

10. Conclusiones

Tomando como base los datos y rastros encontrados de la evidencia la cual se estudió y analizo, de acuerdo a los puntos anteriores puedo afirmar:

- Se puede afirmar que el usuario del sistema ha estado usando el equipo de cómputo para aplicar delitos informáticos, especialmente de cibergrooming, el cual engancha a las niñas menores de edad haciéndose pasar por alguien más, enamorándolas para obtener el material de fuerza y extorsionarla. Todo esto expuesto en el punto 5.3
- Se puede afirmar que el usuario conoce técnicas de esteganografía para ocultar información dentro de otra con la finalidad de despistar toda evidencia que le pudiera comprometer e incriminar ante un ilícito penal. Todo esto expuesto al punto 5.2

- Se puede afirmar que el usuario contenía fotografías y videos de contenido pedófilo, no solo en el disco duro, sino también en internet. Todo esto expuesto en el punto 5.3
- Se puede afirmar que las imágenes y videos eran solicitadas por engaños, es decir haciéndose pasar por otra persona, de la que puedo confirmar es de *Este tipo de material es restringido.* según lo expuesto en el punto 5.3 y 5.5
- Se puede afirmar que el usuario del sistema distribuía por internet imágenes descritas en el punto anterior. Todo esto expuesto en el punto 5.3 y 5.5

11. Recomendaciones a los padres
    - El computador debe de estar en una zona visible por todos, especialmente por los responsables del menor, de tal manera que podemos controlar las horas de uso y su actividad pero sin violar la intimidad de este.
    - Indicar y explicar los riesgos que corren los hijos en internet mediante conversaciones intimas o personales con otras personas incluso con quienes se los cree conocer, revelar datos personales o familiares y enviar fotografías íntimas.
    - Controlar el uso de la webcam, ya que un punto a favor de los delincuentes, en lo posible no tenerlo cerca de ellos.
    - En situaciones de cibergrooming, no tomarse la justicia por sus manos y denunciar en seguida, conversar con el menor y darle el total apoyo y confianza.
    - De conocer algún menor que le sucede lo mismo o sucedió, animarla para que comunique a sus papas cuanto antes.
    - Una vez afectada una cuenta de correo y usuario por delitos de ciber acosos, dejar de utilizarla y perder contacto con ella.
12. Referencias

VMWare Workstation: http://www.vmware.com

FTK Imager: http://www.accessdata.com

Aplicaciones Sysinternals: http://technet.microsoft.com/es-es/sysinternals/

Lads: http://www.heysoft.de

Autopsy: http://www.sleuthkit.org

Thumbnail Database Viewer: http://www.itsamples.com

4.1.2 Informe ejecutivo del análisis de la evidencia

Análisis forense, caso Cibergrooming

Informe Ejecutivo

CFI-IR Gustavo Quizhpe

gatogtv11@hotmail.com

29/12/14

Introducción

Como análisis y estudio de una máquina virtual incautada, que presuntamente cometió cibergrooming, y distribución de imágenes y videos privados por internet, se pretende describir un resumen ejecutivo el cual describa el informe técnico realizado sobre este.

Para lograr mi objetivo es facilitada la máquina virtual en formato ".wmdk" (Virtual Machine Disk).

Análisis

Para su respectivo análisis, fue montada sobre la aplicación VMWare Workstation donde utilice herramientas forenses estando la mayoría en sus versiones free.

En el informe técnico fue descrito los pasos y evidencias encontradas en la máquina de manera clara y precisa.

Resumen de Hechos

Con las pruebas encontradas, su manera de usar el computador por parte del usuario sospechoso y de acuerdo a la cronología de los hechos, los resultados son:

- El sistema operativo es *Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas. Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas*

- Un acontecimiento a tomar muy en cuenta es la presencia de aplicaciones como Mp3Stegz y MSU_stego_video que utilizan una técnica de esteganografía, donde su objetivo es ocular información en audio y video. Esto ayudo a pensar que existen posibles archivos ocultos dentro de otros.
- Se encuentra fotos de menores de edad en paños menores ocultos dentro de imágenes descargadas de internet. También videos conferencias, archivos comprimidos y archivos de texto con notas importantes como: usuarios y contraseñas de cuentas que fueron usadas para causar daño y cometer un ilícito penal.
- Se localiza historial de movimientos de Messenger al igual que las cuantas que han tenido un inicio de sesión en esta aplicación. Además algunos contactos removidos como lo son floresita.13.05@hotmail.com y yessenia.love@live.com.mx. *Este tipo de material es restringido.*
- Se encuentran conversaciones que tratan el tema de acoso a menores de edad utilizando una identidad falsa con el fin de obtener fotografías, videos de usuarias conectadas a Microsoft Messenger enamorándolas y después amenazándolas para él envió de las mismas.
- Existen rastros de apertura a una cuenta *Este tipo de material es restringido.* donde es utilizado para el tráfico de imágenes, videos de contenido pedófilo que son de las menores extorsionadas. Contiene un link llamado *Este tipo de material es restringido.* donde, publica un comentario sobre la víctima, próxima víctima y fotografías de esta.
- Existe también evidencia de cómplices que al parecer son gente conocida, estos gozan de la información, difunden por internet y ayudan a protegerla con técnicas para ocultar información.

Conclusiones

- Varias herramientas para ocultar información dentro de otros archivos han sido utilizadas
- Se han eliminado evidencias incriminatorias con la finalidad de estar al margen de cualquier delito
- Existen conversaciones a través de Messenger con los presuntos cómplices y consumidores de material pedófilo, también mensajes con el cual indican las víctimas, próximas víctimas y distribución a través de internet.
- Se puede afirmar que el usuario del sistema operativo, el cual ha sido puesto para el análisis posee imágenes de contenido pedófilo y que las comparte con otros usuarios de internet.
- Se puede afirmar que el usuario se hace pasar por otra persona para engatusar a menores de edad, con la finalidad de entrar en confianza, enamorarlas y aprovechar de la ingenuidad del menor con el propósito de obtener fotografías, videos de contenido pedófilo.

Recomendaciones

- De conocer a una persona afectado por este incidente, contacta a los padres o tutores y ponerlos al tanto de lo sucedido.
- Informar a los menores de edad lo peligroso que resulta compartir fotografías e información de carácter íntimo o personal, en especial con personas que se creía conocer.
- Ante una situación similar, respaldar toda conversación e información de tal manera de poder ayudar a las autoridades y facilitar el trabajo de investigación que se lleva a cabo.
- Compartir con los padres o tutores cualquier incidente presentado en internet o que se crea que puede ser tomado como un ilícito penal.
- A los padres, no actuar por su propia voluntad ante una situación similar, más bien demandar y poner al tanto a la policía.
- Cuando una cuenta de correo ha sido víctima de este incidente, es fundamental perder todo contacto dejando de utilizar esta

CONCLUSIONES

Es indispensable llegar a tomar acciones preventivas sobre el ciberacoso, siendo necesario emprender un proyecto en base a este trabajo investigativo, en el cual intervengan la trilogía educativa, padres, hijos y docentes, como también los directivos de las instituciones educativas para que gestionen y designen recursos para afrontar esta nueva forma de cometer delitos criminales y sobre todo es muy necesario realizarlo en nuestro país, que todavía no cuenta con una legislación para sancionar esta seria amenaza.

El cibergrooming provoca en el niña(o) y adolecente, cambios drásticos en su personalidad provocando la discriminación en la sociedad. Al recibir la noticia que ha sido engañado a través de la Internet, el agresor le obliga a realizar actos en contra de su voluntad mediante el chantaje y la amenaza, intimidándole a que si no accede a lo que el disponga publicara información lesiva contra su persona. Este tipo de extorción provocaría en el niña(o) y adolecente un daño irreparable en su personalidad perdiendo el desarrollo normal de su infancia y el sentido de la vida. Para este problema es fundamental la comunicación con los padres ya que ellos podrían evitar mayores incidencias fatales que inclusive podrían llegar al suicidio.

Las redes sociales son medio de comunicación masiva que la tecnología y la Internet nos brindan, pero al no contar con un control adecuado de los niñas(os) y adolescentes, como también adultos pueden ser las vías para que personas inescrupulosas las usen para causar daños irreparables en personas vulnerables. Referente a esto es necesario se implementen mecanismos de control utilizando programas especializados y con restricciones para los usuarios.

En nuestro país no existen casos documentados de este tipo de crímenes, pues tampoco contamos con leyes que la castiguen, por ello es necesario sociabilizar la existencia de estos actos criminales dando a conocer el daño que pueden ocasionar, pues sin prevención no hay sanción.

Una gestión imperiosa que se debe realizar, es el apoyo y la iniciativa a que existan leyes y reglamentos claros en el código penal del Ecuador en relación al cibergrooming, para sancionar acorde a las faltas cometidas especificando en cada caso la manera de cómo proceder en la respectiva falta y no dejar en la impunidad los crímenes cometidos.

Una de la funciones de un investigador forense, sería la de controlar los delitos que aparecen en internet, en el cibergrooming protegería a nuestros niñas(os) y adolescentes vulnerables, como también encontraría a los culpables para castigarlos según lo especifique el código penal imponiéndoles todo el peso de la ley.

Cuando el delito ha sido cometido, se debe llevar a cabo el debido proceso en presencia del fiscal y del perito forense. El deber del investigador forense es obtener todos los sucesos de lo ocurrido, evidenciando todas las pruebas para así demostrar que el acusado es inocente o culpable sirviendo estas evidencias como pruebas validas en un litigio legal.

Es necesario mencionar que la información no siempre está disponible o su extracción es muy complicada ya que, las pruebas y evidencias incriminatorias pueden estar ocultas con técnicas y software dentro del sistema operativo o en archivos contenedores como audio, video, etc. Esto debido a que los delincuentes actualmente protegen toda información que delate su transgresión. Seguramente el investigador forense en la mayoría de casos tenga que realizar un estegoanálisis de archivos para que según su criterio encuentre sospechosos.

Al finalizar esta investigación de actualidad, es necesario tomar en cuenta la relevancia del respeto a las fases del análisis forense, con un proceso trasparente y valido en cualquier litigio penal para que puede ser tomado como referencia en caso de naturaleza similar, debo manifestar que a la culminación de esta tesis se alcanzaron los objetivos planteados, además de cumplir con mis anhelos profesionales.

RECOMENDACIONES

A todos los sujetos vulnerables en especial a las niñas(os) y adolescentes se recomienda:

No creer en todo lo que vemos y escuchamos en internet, ya que pueden ser objeto de burlas o simplemente mentiras, dañando la reputación de alguna persona.

Navegar con prudencia en internet y evitar páginas pornográficas para no dañar sus mentes y conservar la integridad en sus pensamientos.

No aceptar solicitudes desconocidas en redes sociales, ni hacer uso del chat con personas que jamás han tenido contacto.

Conversar con sus padres y pedir explicación de temas nuevos que puedan confundirlos, ya que la experiencia es lo que más fuerte hace al ser humano.

No difundir ni publicar información personal como: edad, dirección, teléfonos, etc. Esta información podría ser clave para los criminales, dándoles un conocimiento más amplio de como manipular sus técnicas para convencerlos y chantajearlos.

A todos los padres de familia y tutores:

Tener comunicación con los hijos a cerca de la tecnología y la navegación en internet, instruyéndolos sobre el peligro de confiar en un extraño.

Instalar software de control parental que pueda brindar un mejor control sobre las consultas que realizan vuestros hijos.

Explorar historiales de navegación en internet para, poder saber cuáles son los sitios de internet de vuestros hijos frecuentan y así poder llevar un mayor control.

Explorar los dispositivos digitales para verificar acerca de la comunicación con otras personas, sobre todo aquellos que poseen conexión a internet y aplicaciones que conectan fácilmente a redes sociales, juegos online, chats, etc.

Identificar contactos y amigos con los que se comunica frecuentemente, ya que atrás de alguno de ellos puede estar alguna persona que trata de engañar con mentirías a vuestros hijos.

Acudir a expertos para obtener una ayuda profesional e implementar software de control a los medios de comunicación que poseen.

A los investigadores forenses

Tener un criterio más amplio de evaluación en un incidente, es decir, no solo centrarse en el dispositivo digital si no en todo lo ocurrido en la escena del crimen.

No caer en la desesperación por llegar a obtener información, analizar paso por paso para reconstruir todos los sucesos en orden según hayan sido cometidos por el acusado.

Ampliar los conocimientos para obtener una mayor capacidad de intuición, respecto a las evidencias encontradas y su correcto proceso del análisis a realizarse.

Utilizar técnicas y herramientas forenses adecuadas, para tener buenos resultados brindando confianza al juez y miembros de la corte.

A las Instituciones Educativas

Tener una política de prevención en escuelas y colegios evitando que los niños y adolescentes caigan fácilmente en ciberacoso.

A los docentes, instruir a sus estudiantes indicándoles que las redes sociales se han convertido en un vector de ataque de personas sin ningún tipo de moral aprovechándose de la inocencia preferentemente de niños y adolescentes.

Y por último, al existir un creciente grado de delincuencia en el país que va en aumento, se debería fomentar el cuidado e incentivar a denunciar a los cibercriminales para que se implementen leyes de penalización en el código penal del Ecuador en el que existan artículos específicos que sancionen drásticamente las faltas cometidas mediante el cibergrooming.

GLOSARIO DE TERMINOS

Cibergrooming: Acoso sexual cibernético

Cifrar: digitar un mensaje en clave formado por números, letras, símbolos, etc.

Hacker: Persona apasionado en la seguridad informática

IP: Internet Protocol, es un número usado para identificar un dispositivo en la red

ISP: Proveedor de servicios de internet

N3XAsec: Empresa Mexicana que brinda certificaciones avaladas por la NSA

Logs: Es una bitácora donde se guarda un registro de actividad de un sistema

Policía cibernética: Policía dedicada al patrullaje en la red, sitios, procesos, y responsables de actos delictivos en medios informáticos y electrónicos

TCP y UDP: protocolo orientado a la conexión, este recibe confirmación del emisor y no orientado a la conexión, sin confirmación del emisor

URL: Localizador uniforme de recurso, sirve para nombrar recursos en internet

Wipear: formateo a bajo nivel el cual remplaza todos los datos escritos e el disco con los caracteres que indiquemos. Borra toda la información lo cual es conocido como una técnica anti forense

REFERENCIAS BIBLIOGRAFICAS

Aviles, Á. P. (2013). *Por una red mas segura. Informando y educando.* España: x1RED+SEGURA.

Boston, R. (s.f.). *infobae*. Obtenido de http://www.infobae.com/2012/02/01/629718-cuales-son-los-paises-mejor-preparados-recibir-un-ciber-ataque

Ciudadana, D. G. (s.f.). *slideshare.* Obtenido de http://es.slideshare.net/EycaSoluciones/guia-del-taller-prevencion-delito-cibernetico

Control, F. (s.f.). *Computer forensics*. Obtenido de https://forensiccontrol.com

deft. (25 de 1 de 2015). *DEFT*. Obtenido de http://www.deftlinux.net/

Domínguez, F. L. (2013). *Introduccion a la informatica rofense.* Madrid: RA-MA EDITORIAL.

DragoN. (s.f.). *Dragonjar*. Obtenido de www.dragonjar.org

Ecuador, A. N. (12 de 2014). *Asamblea Nacional República del Ecuador*. Obtenido de http://www.asambleanacional.gob.ec/

Locard, E. (2010). *Manual de Tecnica Policiaca.* Málaga: MAXTOR.

MiTeC. (2014). *MiTeC*. Obtenido de http://www.mitec.cz/

Muñoz, A. (12 de 2007). *StegSecret. A simple steganalysis tool ;)*. Obtenido de http://stegsecret.sourceforge.net/

N3XAsec. (s.f.). *N3XAsec*. Obtenido de Introducción al taller de informática forense: http://www.n3xasec.com/

N3XAsec. (s.f.). *N3XAsec*. Obtenido de Esteganografía y Estegoanálisis: http://www.n3xasec.com/contacto.html

NirSoft. (2014). *NirSoft*. Obtenido de http://www.nirsoft.net/

Olaya, R. (09 de 12 de 2014). Pedófilos usan Facebook para abusar de niños en Ecuador. (B. Granja, Entrevistador)

OperacionSAFE. (s.f.). *OperacionSafe*. Obtenido de https://twitter.com/operacionsafe

Quezada, A. E. (12 de 2013). *Autopsy3.* Obtenido de ReYDeS: www.reydes.com

Rambla, J. L. (2012). *Un Forense Llevado A Juicio.* España: Creative Commons.

Riquert, M. A. (2014). *El cibergrooming.* Buenos Aires.

SARC. (2014). *Welcome to the Steganography Analysis and Research Center*. Obtenido de https://www.sarc-wv.com/

Software, B. (2014). *HexWorkshop*. Obtenido de http://www.hexworkshop.com/

ANEXOS

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas.

Este tipo de material es restringido, pedimos disculpas por las molestias ocasionadas