Como obtener y presentar evidencia Digital

Publicado en el III Congreso Mundial de Derecho e Informatica
29 de septiembre hasta el 3 de octubre 2003

Guillermo Buriticá Tobón

E-Mail buriticag@supercabletv.net.co

Resumen: En este corto paper se pretende mostrar los procedimientos para la presentación de evidencia digital en las cortes de habla hispana, No es del alcance del paper mostrar las técnicas utilizadas por los investigadores forenses en materia de recolección, clasificación y presentación de evidencia digital sino mas bien mostrar un procedimiento aceptable a fin de evitar la improcedencia de la evidencia por vicios en las diferentes legislaciones.

Palabras Clave: Evidencia digital, computación forense, derecho informático.

Introducción: Desde el momento en que la tecnología de información se popularizo a inicios de los años 80 con la aparición del IBM-PC y llego primero a las compañías grandes, medianas, pequeñas y se introdujo en nuestros hogares, el computador se ha usado en una gran cantidad de actividades que ayudaron a las organizaciones a convertirse en competitivas y eficientes. Pero no todo fue bueno en la aparición del computador este también llego a las manos de los delincuentes quienes los han utilizado como una herramienta para delinquir.

En esta corta historia de 20 años de en que se masificaron los sistemas de computo y se interconectaron con la proliferación de las redes de computador cada día se ven mas y mas casos de abusos y utilización ilegal de los sistemas de computo es común ver los diferentes gobiernos emprenden una carrera contra el tiempo intentando tipificar delitos informáticos los cuales convierten en sofisticados y rápidos a medida que los sistemas avanzan.

Por ejemplo la pornografía infantil y el abuso sexual a menores esta tipificada como un delito en casi todos los países del mundo diferenciándose de un país a otro la edad contemplada como máxima para considerarse un delito y normal mente condensado como delitos contra la libertad, integridad y formación sexual. La pornografía infantil incursiono en la red global de información Internet a mediados de los años 90 en los cuales diferentes magazines (ilegales) incursionaron en la red mundial de información utilizando la red para divulgar sus contenidos y amparados por el anonimato que la red ofrece en los pocos casos que se han podido procesar los implicados han sido exonerados debido a errores procedí mentales en la recopilación, y presentación de pruebas ya que la normatividad mundial no ofrece un mecanismo efectivo para la presentación de evidencia digital.

Otros casos comunes de crímenes informáticos corresponden a la instrucción o el hacking, abuso del recurso tecnológico en las empresas, abuso de los sistemas de información, estafas informáticas, abusos en derechos de autor, y en general en cada categoría de delito es posible usar un sistema automatizado para cometer el delito.

Mediante este paper pretendo mostrar un procedimiento general a fin de llenar el vació existente en todo el mundo y en especial en los países de habla hispana para obtener, clasificar y presentar evidencia digital. De tal forma que se mantengan las características básicas de las pruebas y puedan ser utilizadas en una corte de esta manera la evidencia digital debe ser confiable, completa y autentica [1] tomando diversas formas como podrían ser Registros, Imágenes (Archivos de Matriz bits), Documentos digitales, Correo Electrónico, Archivos temporales o de cache, Archivos eliminados, y archivos de intercambio SWAP entre muchos otros mas. Este tipo de evidencia digital tiene características especiales

[1] Casey 2000 Pagina 47

como su fácil duplicidad de manera exacta y confiable tal como si fuese el original, Con herramientas especiales es relativamente fácil demostrar si integridad (Garantizar que no se ha modificado en algunos casos), Si es eliminada mediante técnicas especiales de computación forense es posible en la mayoría de los casos recuperar la información, Cuando los criminales intentan destruir la información general mente existen copias en otros sitios.

Aunque también presenta sus problemas característicos como seria la falta de conocimiento de los legisladores para identificar, valorar y revisar la evidencia digital presentada, la facilidad de alteración y su dificultad para corroborarla con el original, almacenamiento y persistencia del medio electrónico, identificación del autor de los documentos, problemas en el transporte que podrían alterar la evidencia recolectada, e incluso la evidencia podría encontrarse con algún tipo de cifra lo que hace que no se pueda conocer su contenido y por ultimo las desconocimiento de las técnicas utilizadas para intrusión en sistemas de información o encripcion de datos.

Contenido

Búsqueda y Recolección de pruebas electrónicas

En la normatividad consultada en la mayoría de los países de habla hispana se defiende la privacidad y se tipifica como “DELITOS CONTRA VIOLACION A LA INTIMIDAD, RESERVA E INTERCEPTACION DE TELECOMUNICACIONES” protegiendo tanto a las personas de bien como a los delincuentes esta normatividad hace que la captura de evidencia digital mediante interceptaciones, uso de sniffers y demás herramientas para la captura de paquetes sean descartadas en una corte no obstante se prevén los mecanismos jurídicos para poder obtener mediante orden judicial la potestad de interceptación de telecomunicaciones; los delincuentes conocen bien estas normas de protección a la intimidad y en la mayoría de los casos exigen que las pruebas recolectadas sin una orden sean descartadas en las cortes por esta razón si se presume que alguien esta transmitiendo información electrónica por intermedio de las redes de telecomunicaciones es necesario obtener una orden que permita realizar el seguimiento, captura y almacenamiento de la información transmitida electrónicamente garantizando que estas pruebas incluyan una forma de reconocimiento tanto del emisor como del receptor (Hardware o Individuo), Asegurar que se preserven en la forma en que fueron transmitidas mediante un archivo de datos o registro de actividad mas conocido como LOG, Se debe presentar clasificada en orden cronológico de transmisión, contenido y forma y garantizar su reconstrucción en un futuro. A fin de garantizar la confiabilidad, autenticidad y su integridad es deseable que esta recolección de información se realice desde diferentes sistemas de computo simultáneamente con presencia de 2 investigadores forenses cada uno responsable de su propio sistema de intercepción.

No obstante la ley no protege el archivo de direcciones IP direcciones MAC o números de teléfono en los dispositivos electrónicos en este caso se puede presentar como evidencia digital los registros de actividad del sistema de telecomunicaciones utilizado a fin de conservar estos registros es importante mantener los datos de sincronización horaria en los dispositivos de red y telecomunicaciones esta evidencia digital obtenida de esta manera probaría únicamente la interconexión de dos sistemas. Para la presentación de esta evidencia digital es deseable almacenar el registro integro de la comunicación entre sistemas de tal forma que se refleje la dirección IP o MAC del dispositivo que origina la comunicación (transmisor) como del dispositivo que recibe la comunicación (RECEPTOR)

Para obtener esta información las técnicas propias de la informática forense pueden optar por un recurso adicional a fin de exigir que la evidencia digital se apruebe como valida en un proceso judicial. Cuando se presume un acto antijurídico en el cual ha intervenido un sistema electrónico de transmisión de datos se puede recurrir a una orden de allanamiento por parte de un juez a fin de recopilar la información contenida en el ordenador desde el cual se origino el mensaje esta información puede ser copiada, recuperada de un archivo eliminado, extractado de

archivos temporales, o logs del sistema a fin de obtener el mensaje o transmisión deseada en algunos casos esta información se puede recopilar de dispositivos de almacenamiento temporal que se usaron durante la transmisión recurriendo mediante orden judicial al ISP o carrier.

En algunos países como en EEUU la protección de interceptación de datos no aplica en los siguientes casos cuando se presume la utilización de equipos de telecomunicaciones para efectuar acciones de contrabando, o como medio para planear o ejecutar un crimen., cuando se presume muerte o daño físico a las personas, o cuando se presume el almacenaje o transmisión de datos que constituyan un riesgo para la seguridad nacional como materiales protegidos, secretos de estado o la posesión de pornografía infantil. En estos casos se debe presentar la información en la forma en que se obtiene.

De esta forma se tienen dos preguntas que resolver antes de interceptar alguna comunicación de datos electrónicos a fin de evitar que las pruebas recolectadas sean rechazadas por las cortes

Esta el sistema de gobierno involucrado?
El procedimiento puede afectar la privacidad de la persona investigada?

Por ejemplo si en un departamento de reparaciones se descubre un archivo relacionado con contrabando el empleado puede informar y liberar la información al departamento de justicia correspondiente en este caso se faculta para la obtención de la evidencia digital sin una orden judicial.

Una forma segura de obtener evidencia digital cuando no se tiene una orden judicial es aislar el dispositivo en el cual se presume la existencia de evidencia digital en un compartimiento cerrado hasta tanto la corte determine autorizar el escrutinio y análisis de la información.

Como mecanismo de prevención algunas organizaciones pueden determinar la recolección de información en los sistemas de computo mediante un consentimiento en el cual el empleado autoriza al empleador para obtener información de su sistema de computo y grabar, almacenar información estos consentimientos de indagación se pueden encontrar limitados en materia de tiempo, duración de la información este documento escrito puede ser en un momento dado la mejor herramienta para un investigador caro que esto aplica en el sector privado ya que en el sector gubernamental estas reglas podrían estar un poco alejadas de ser procedimentalmente correctas.

A fin de evitar la destrucción de evidencia digital es recomendable extraer una copia de seguridad integra del sistema mediante medios como imágenes de disco, backups en citas o cdroms, etc.

Se recomienda preservar los dispositivos involucrados en actos criminales mediante un inventario y clasificación de los activos electrónicos involucrados mediante fotografías, números seriales, y demás información relevante esto hace que en el futuro la evidencia digital sea corroborada y sustentada mediante evidencia física adicionalmente el inventario pretende proteger la propiedad de una persona contra daño o perdida permitiendo a los investigadores obtener la evidencia digital contenida ya que los elementos se encuentran en custodia.

Planificar la búsqueda de la evidencia digital es un factor critico del éxito mediante objetivos concretos e hipótesis planificadas se pretende demostrar mediante técnicas computacionales el hallazgo de evidencia formal.

Para garantizar que la evidencia digital sea tenida en cuenta por la corte se debe describir la propiedad con lujo de detalles incluyendo sus componentes internos en el caso del hardware como instrumento del crimen,

Documentar y buscar garantías de propiedad y autoría como passwords, o llaves de encripcion en algunos casos se hace imposible acceder al sistema si este se encuentra protegido mediante contraseñas o sus datos son encriptados no obstante se pueden usar herramientas de cracking de contraseñas como Adivinación de contraseñas, Fuerza bruta, Borrado de Bios, Acceso forzado al File System, etc si estas técnicas son utilizadas se debe documentar su utilización y describir la técnica utilizada.

Para llevar a cabo la búsqueda de evidencia digital en dispositivos electrónicos se puede requerir conocimientos técnicos avanzados que garanticen la obtención de la evidencia buscada en el caso de que durante esta búsqueda de hipótesis revelen evidencia no contemplada se deben emitir nuevas hipótesis y aumentar el alcance de la búsqueda digital a fin de ajustarla a las nuevas hipótesis.

Si es imposible realizar la búsqueda de evidencia digital en el sitio en el cual se encuentra se debe justificar y documentar la razones para el retiro de los elemento que se presume contienen evidencia si el elemento es removido del lugar del la búsqueda de evidencia debe hacerse lo mas eficientemente posible garantizando la obtención de copias a fin de reflejar la información en el estado original.

Si por alguna razón el elemento propio de estudio contiene información privilegiada, o clasificada como confidencial como por ejemplo cuando se realizan búsquedas de evidencia en oficinas legales, centros médicos, entidades religiosas, o embajadas o consulados antes de iniciar la búsqueda de la información la el investigador debe identificar las limitaciones legales y cumplir con esas limitaciones.

Integridad De la evidencia digital

Mantener la integridad de la evidencia digital a lo largo de un proceso presenta diferentes problemas desde el manejo de los tradicionales documentos físicos, equipos de hardware y sus correspondientes archivos de datos, Algunos de estos problemas son la extremada complejidad de las redes de computo, el alarmante tamaño de los archivos de computo tanto de datos como multimedia así como las bases de datos.

En estos procedimientos se asume que se cuenta con los recursos necesarios para almacenar la información relevante a la investigación y mantenerla en custodia sin alteración alguna almacenar el tamaño de los datos no es suficiente para determinar la integridad de la información obtenida en un estudio de ciencias forenses.

Mediante la utilización de herramientas de computación forense previamente reconocida por la comunidad forense y avaladas como mejores practicas en recuperación de evidencia digital se debe proceder a realizar una copia de seguridad de los datos obtenidos como evidencia se recomienda sacar un código de chequeo como md5 al contenido de la evidencia a fin de demostrar que no se altero durante el proceso de copia adicionalmente se requiere autenticar la maquina que contiene la información propia de la investigación. Se ha visto casos en que se ha alterado la información de la maquina portadora después de que se ha obtenido la evidencia por los representantes de la ley en estos casos se genera una intrusión en la evidencia generándose una causal de agravamiento del delito para demostrar este echo es necesario contar con las herramientas necesarias como la firma MD5 que demuestren la alteración de la evidencia digital en su origen a fin de ser comparada con la copia obtenida durante el proceso de recolección de información y evidencia digital.

Adicionalmente un investigador debe cuestionarse acerca de los siguientes hechos antes durante y después de la recolección de la evidencia forense

a. Que evidencia se tiene para creer que es una victima?
b. Cual es el orden cronológico en que ocurrieron los hechos de alteración, transmisión o acceso?
c. Cuales son los daños ocurridos?
d. A quienes se puede hacer responsable por el incidente?
e. Que personas son sospechosas del suceso?
f. Cual es el impacto de esta información en el negocio o suceso a investigar?
g. Estos equipos son requeridos para la operación normal del negocio?
h. Como se descubrió el incidente, perdida de datos o delito?
i. Cuando pudo ocurrir el incidente por primera ves?
j. Quien ha investigado el incidente, que acciones ha tomado para preservar, identificar, recolectar y analizar los datos de los dispositivos involucrados?[2]

[2] Electronic Crime Scene Investigation: A guide for first responders and A Guide for forensic Examination of Digital Evidence

La respuesta de estas preguntas garantiza que la evidencia recolectada pueda ser admitida en una corte ya que asegura que:

a. Que es un acto humano (Acción u omisión) Definición de delito
b. Dicho acto humano se presume antijurídico, Lesiona o pone en peligro un interés jurídicamente protegido
c. Permite identificar la tipicidad del delito.

El investigador debe estar en capacidad de demostrar in una corte que la información obtenida desde el medio de almacenamiento y/o transmisión es verdadera de acuerdo a la forma en que la información fue obtenida originalmente como herramientas para lograr estos objetivos se tiene el recurso de la custodia de pruebas judiciales la cual debe garantizar los procedimientos para el manejo y almacenaje de pruebas físicas y que la recolección de datos se han realizado con las mejores practicas mediante la custodia de una imagen exacta de la evidencia original.

El investigador debe identificar que clase de evidencia digital va a conservar debido a su relevancia como conversaciones electrónicas, copias impresas de correos electrónicos, Se tienen copias electrónicas? estas contienen los encabezados completos?

Para identificar la evidencia digital se debe conservar y documentar nombre y cargo de la persona que se involucra con la evidencia recolectada conservando el control aplicado y la relación que tuvo con la evidencia digital justificando el porque logro tener acceso a la evidencia.

Documentar el procedimiento empleado para recolectar la evidencia digital como se obtuvo, quien la obtuvo y quienes han tenido contacto con la evidencia después de ser recopilada todas estas personas hacen parte de la cadena de custodia.

Documentar cuando se obtuvo la evidencia almacenando Hora y fecha en que se obtuvo la información incluyendo las referencias de zona horaria si es pertinente

Documentar donde se obtuvo la información
a. relacionando datos geográficos Ciudad, cuarto, escritorios, etc
b. Hardware
    a. Tipo de Hardware
    b. Quien tuvo acceso al elemento
    c. Propietario de la maquina
    d. Números de identificación serial numero de inventario
    e. El elemento es compartido
    f. Opera en entorno de red?
    g. La información esta protegida con Passwords o claves
    h. Quien tiene acceso al password de la maquina
c. Fuera del sitio
    a. Servidores
    b. Correo remoto
    c. Paginas Web
    d. Accesos remotos

Presentación de la Evidencia Digital

a. Para presentar la evidencia digital se debe presentar a la corte la forma en que se busco la presencia de evidencia digital garantizando que no se violo ninguna norma de protección de datos, privacidad, o derechos constitucionales, códigos de procedimiento, leyes, decretos, etc en la búsqueda de la evidencia digital.
b. Mostrar el procedimiento empleado para la copia y recolección de datos
c. Mostrar el procedimiento empleado para el análisis de los datos recolectados
d. Mostrar el procedimiento empleado para el almacenamiento de los datos
e. Demostrar la competencia de investigador como experiencia, certificaciones, etc.
f. Presentar las notas forenses
    a. Se deben preparar la notas forenses y almacenarlas según lo estipulado por cada país
    b. Mantenerlas ordenadas según cada hallazgo
g. Reportes
    a. Se deben presentar los reportes solicitados por la corte según se

ajusten a procedimientos civiles o criminales

b. Incluir en los reportes de evidencia forense
    i. Las opiniones relevantes que el experto emita
    ii. La bases teóricas o practicas para emitir el concepto
    iii. Incluir una hoja de vida que demuestre su experiencia
    iv. Instancias en las cuales el examinador es considerado como experto

Las pruebas sustantivas presentadas a la corte deben ser relevantes para el caso mostrando las partes técnicas correspondientes

Consideraciones Adicionales

Siempre se debe ofrecer un copia exacta a la otra parte del conflicto legal a fin de garantizar el debido proceso, garantizando que la defensa tenga acceso a un computador limpio de características iguales al dispositivo original y un espacio de trabajo apropiado para realizar sus propios exámenes forenses.

Documente siempre que sea posible los tiempos de retención de la información en algunas legislaciones se puede argumentar la irrelevancia de la información por caducidad en el tiempo

Asegúrese de mantener acreditaciones, ejecutar los procedimientos de punta o el estado del arte en materia de recolección de información digital

Asegurarse de mantener el material de trabajo suficiente y necesario para adelantar la investigación y la recolección de información como Cuadernos de notas, Cintas, grabadores de datos, equipos de computo, correo electrónico etc.

Identifique la idoneidad de los investigadores en materia informática.

Resultados

Se espera que esta aproximación genérica sea un modelo de presentación jurídica para mostrar información relevante contenida en medios digitales, como archivos, fotos, documentos, logs de sistema, etc espero que pueda ser aplicable a todas las cortes de habla hispana.

Este paper no pretende ser euxastivo en el procedimiento técnico si no que intenta mostrar a todos aquellos detalles conceptúales en los que los investigadores forenses presentan fallas jurídicas al momento de presentar un caso que involucre evidencia digital.

Conclusiones

En América latina el termino de Computación Forense es todavía un termino desconocido y mas aun las técnicas de recolección de evidencia digital aunque en algunos países como España, Argentina y Chile se han logrado avances significativos en materia de derecho probatorio informático el camino que falta por recorrer es todavía largo.

En el tema de investigación forense informática debemos generar las pautas de credibilidad, manejo y pertinencia de la información recolectada a fin de impulsar el desarrollo de esta ciencia moderna que si bien es requerida por todos aquellos que incursionan el campo del comercio electrónico también es una herramienta imprescindible en el campo del procedimiento penal, procedimiento comercial, y a lo largo y ancho del derecho ya que con varios cientos millones de usuarios de computadores en el mundo los delitos informativos han venido creciendo en forma exponencial exigiéndole a los gobiernos la generación de normas que regulen la información digital, los delitos informáticos y en especial el procedimiento probatorio de la evidencia digital.

Referencias

Corte suprema de Justicia Colombia
National Center for Forensic Science
High Tech Crime Task Forces
NLETCs
SEARCH
NW3C

Los Alamos Lab
Search and Seizure Guidelines
NCTP
NAAG
NAC
HTCIA
FACT, Forensic Association of Computer Technologist
Casey 2000 Digital Evidence and Computer Crime

Autor

Guillermo Buritica Tobón.
Email:buriticag@supercabletv.net.co
Ingeniero de Sistemas
Escuela Colombiana de Ingeniería
Especialista en Auditoria de Sistemas Universidad Santo Tomas.
Aspirante al titulo de Magíster en Ingeniería de sistemas Universidad Nacional de Colombia
Miembro activo ISACA Information System Audit. And Control Asociation
Consultor en Gerencia Estratégica de Sistemas de Información, Consultor en seguridad Informática. Auditor Certificado Iso-9000:2000.
Profesor retirado de la Pontificia Universidad Javeriana de Bogota.
Profesor de Cátedra Fundación Universitaria Konrad Lorez Bogota
Profesor de Cátedra Universidad Nacional de Colombia.