Webinar Gratuito
Informática Forense

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Cómputo Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Jueves 15 de Agosto del 2013

¿Quién Soy?

- Consultor e Instructor Independiente en Hacking Ético, Cómputo Forense y GNU/Linux.

- Ex Integrante de RareGaZz y actual integrante de PeruSEC.

- Ex Redactor en la Revista Linux+ DVD (ES).

- Creador del II Reto Forense Digital Sudamericano - Chavin de Huantar 2012.

- Brainbench Certified Network Security, Brainbench Certified Computer Forensics (U.S.) & Brainbench Certified Linux Administration (General). CNHE, CNCF, CNHAW.

- Más de 10 años de experiencia en el área.

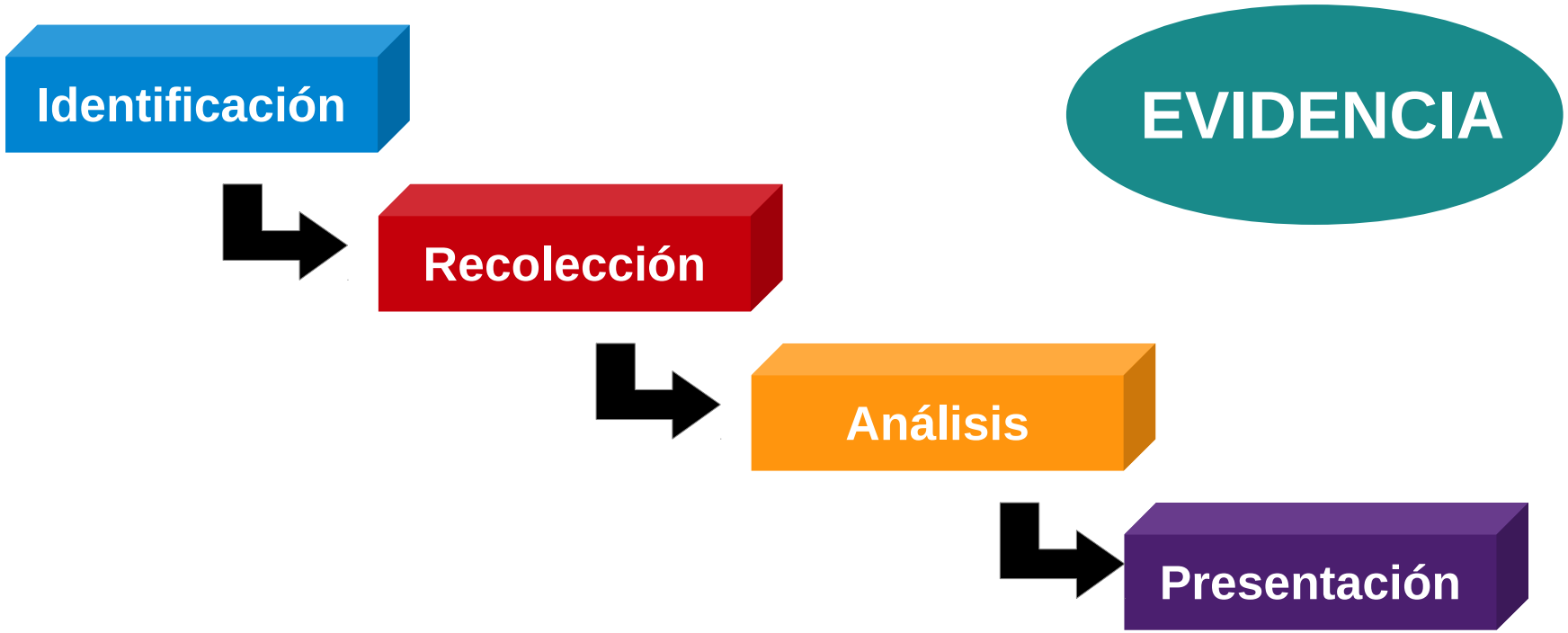
- Twitter: @Alonso_ReYDeS

- LinkedIn: pe.linkedin.com/in/alonsocaballeroquezada/

Introducción

La Informática Forense es la preservación, identificación, extracción, interpretación, y documentación de evidencia de computadora.

Forense Digital también se denomina como “La adquisición, análisis y preservación científica de los datos contenidos en medios electrónicos cuya información puede ser utilizada como evidencia en una juzgado”.



Objetivos de la Informática Forense

La actividad relacionada a las computadoras es una parte importante de nuestra vida diaria. Desde algo tan simple como utilizar nuestra computadora personal, hasta utilizar otro dispositivo como un blackberry.

El examen de evidencia digital (medios) proporciona un mecanismo para que los investigadores forenses determinen la naturaleza y eventos relacionados a un hecho, y ubicar al perpetrador siguiendo un procedimiento de investigación estructurada.

¿Qué es la Informática Forense?

Una serie metódica de técnicas y procedimientos para obtener evidencia de equipos de cómputo, desde diferentes dispositivos de almacenamiento y medios digitales que pueden ser presentados en una corte con un formato coherente y significativo.

1001 1110 1010 1010

Crímenes Facilitados por Computadoras

Nuestra dependencia de las computadoras proporciona nuevas oportunidades para los criminales. En consecuencia se elevan los crímenes.

1. La proliferación de acceso a internet y las computadoras hacen que el intercambio de información sea rápido y barato.

2. La utilización de herramientas sencillas de “Hacking” y la proliferación de grupos “Underground” facilitan la comisión de crímenes.

3. Internet permite ocultar la identidad mientras se comete un crimen.

4. La falsificación de correos electrónicos, creación de perfiles falsos, y robo de identidad son incidentes difíciles de detener, complicando su investigación.

5. En estos crímenes no existe evidencia colateral o forense, como testigos oculares, huellas, DNA, haciéndolos difíciles de perseguir.

Razones para los Ataques

Estos crímenes se cometen por individuos más organizados. La mayoría de nosotros equipara los ataques cibernéticos con lo que muestra la televisión y las noticias; pornografía, “Hackers” ganando acceso a información sensible del gobierno, robo de identidad, robo de contraseñas, etc.

Pero esto va más lejos de todo esto; como el robo de propiedad intelectual, daño en el servicio de las redes, malversación, piratería (software, películas, música), pornografía infantil, sembrar malware, tráfico de contraseñas, spam, y un largo etc.

Los criminales aprenden técnicas más avanzadas en comparación a las agencias que luchan en contra de ellos.

Un crimen de computadora es cualquier acto ilegal que se relaciona con una computadora, un sistema o aplicación.

Un crimen de computadora es intencional,
no accidental.
(Esto requiere un tema legal.)

Etapas de una Investigación Forense

Un investigador forense debe seguir ciertos pasos y procedimientos cuando trabaja en un caso.

Primero se procede a identificar el tipo de crimen, con la computadora o la herramienta con la cual se cometió.

Entonces se obtiene la evidencia digital y construye una cadena de custodia. Para esto, se debe seguir los siguientes procedimientos:

A. Debe realizar una copia espejo (copia bit a bit), y replicarla, para luego proceder a realizar el análisis con las herramientas forenses adecuadas.

B. Después de analizar la evidencia digital se debe presentar y testificar la evidencia en un juzgado.

C. El investigador se convierte en la “herramienta”, que utilizan las fuerzas legales para rastrear y perseguir a los criminales.

Etapas de una Investigación Forense (Cont.)

1. El personal llama al abogado para asesoría del caso.

2. El Investigador Forense prepara el Procedimiento de Primera Respuesta.

3. El investigador Forense captura la evidencia en la escena del crimen y lo transporta al laboratorio forense.

4. El Investigador Forense prepara una réplica de flujo de bits (Copia Bit a Bit) de los dispositivos y crea un Hash MD5 y SHA-1 (como mínimo) de ellos.

5. El Investigador Forense examina la evidencia para probar un crimen, y prepara un reporte de investigación antes de concluir la investigación.

6. El Investigador Forense presenta el reporte con información sensible al cliente, quien lo revisa para ver la factibilidad de proceder con los cargos.

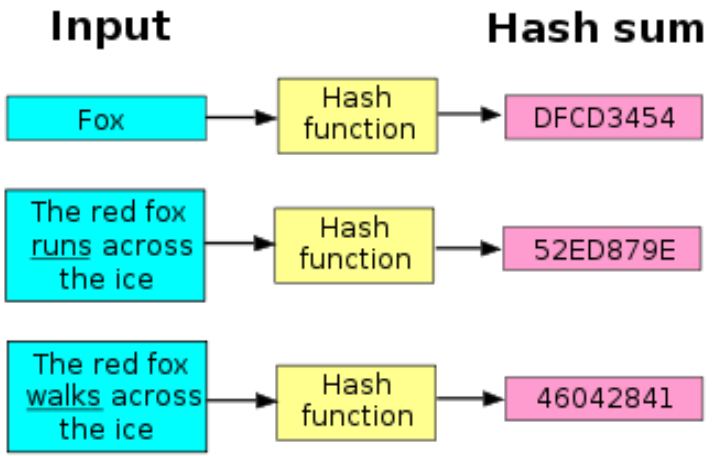
7. El Investigador Forense destruye cualquier dato sensible.

Etapas de una Investigación Forense (Cont.)

Es muy importante que el Investigador Forense siga todos estos pasos y que el proceso no contenga información inexacta que pueda arruinar su reputación o la reputación de la organización.

¿Qué es un Hash?

En informática, hash se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. Un hash es el resultado de dicha función o algoritmo.



Reglas, Procedimientos y Leyes

Un buen investigador forense siempre debe seguir las siguientes reglas:

1. Examinar la evidencia original lo menos posible, siempre se debe examinar el duplicado.

2. Seguir las reglas sobre manejo de la evidencia y no dañarla.

3. Preparar siempre una Cadena de Custodia, y manejar la evidencia con extremo cuidado.

4. Nunca exceder los conocimientos básicos que se poseen.

5. Asegurarse de documentar cualquier cambio sobre la evidencia.

6. Si todo se mantiene dentro de estos parámetros, el caso será de sumo valor y completamente defendible.

Reglas, Procedimientos y Leyes (Cont.)

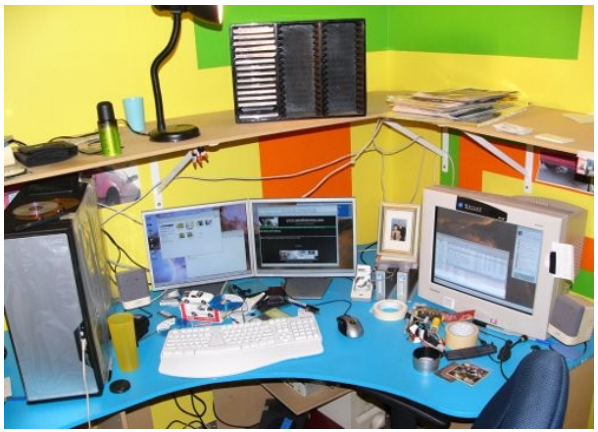
Evaluar el Caso: Detectar/Identificar el evento/crimen

En cualquier tipo de investigación, el analista forense de computadoras debe seguir un proceso de investigación adecuado. Este proceso inicia con la fase correspondiente a la evaluación del caso, luego se procede a realizar preguntas a las personas involucradas, y finalmente documentar los resultados, en un esfuerzo por identificar el crimen y la ubicación de la evidencia digital.

Las investigaciones de computadoras se realizan con dos tipos de computadoras:

A. Las computadoras utilizadas para cometer un crimen.

B. Las computadoras que son el objetivo de un crimen.



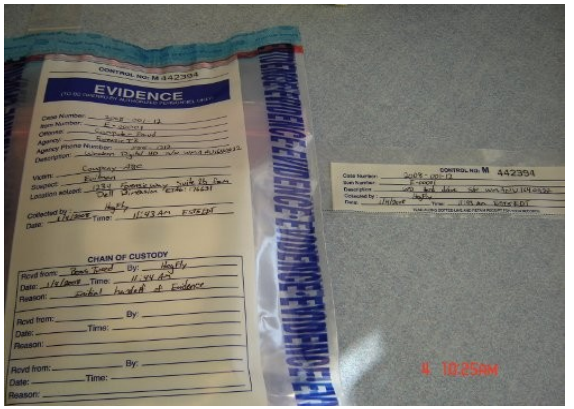
Reglas, Procedimientos y Leyes (Cont.)

Preservar la evidencia: Cadena de Custodia

La evidencia identificada debe ser preservada para mantener su integridad. Se debe preparar un Cadena de Custodia para conocer que persona manipuló la evidencia, y cada acción realizada por el investigador forense debe ser documentada para ser incluido en el reporte final.

Algunas veces una computadora y su evidencia relacionada puede determinar la cadena de eventos que dirijan al investigador con un crimen, como también puede proporcionar la evidencia con la cual se puede llegar a dar una condena.

Una Cadena de Custodia es una documentación exacta del movimiento y posesión de una pieza de evidencia, desde el momento en que fue tomada en custodia hasta que es entregada a un juzgado.



Reglas, Procedimientos y Leyes (Cont.)

Recolectar: Recuperar datos, Recolectar evidencia

Encontrar la evidencia, descubrir datos relevantes, preparar un Orden de Volatilidad, erradicar vectores externos de alteración, y preparar una Cadena de Custodia, es el proceso adecuado para la recolección de datos.

Después de recolectar los datos se debe crear un hash MD5 y SHA-1 de la evidencia. Antes de la recolección, se debe realizar una evaluación preliminar para buscar evidencia. Luego de lo cual, se procede a recolectar y capturar el equipo utilizado para cometer el crimen, y documentar los artículos recolectados, como USB sticks, CDs, DVDs. Se debe tomar fotos de la escena del crimen antes de retirar la evidencia.

Después de recolectar toda la información, el investigador debe listar las acciones realizadas al inicio y durante la investigación. No es necesario tomar el sistema completo. Se puede identificar los datos relevantes y copiarlos, de otra manera puede conllevar a un sobre recolección.

Reglas, Procedimientos y Leyes (Cont.)

Examinar: Rastrear, Filtrar, Extraer datos ocultos

El Investigador Forense debe rastrear, filtrar, y extraer datos ocultos durante este proceso. Un parte de la evidencia puede desaparecer en corto tiempo. Tal evidencia se denomina evidencia volátil, debido a que necesita suministro eléctrico para que se mantenga. También existe evidencia que mantiene información cambiante, como registros, caché, tablas de rutas, caché ARP, tabla de procesos, estadísticas del kernel y módulos. Un ejemplo de orden de volatilidad es el siguiente:

1. Memoria Virtual: Espacio SWAP o Archivos de paginación.
2. Disco Físicos: Los discos duros de un sistema.
3. Copias de Seguridad: Medios de Backup tales como cintas magnéticas u otros medios.

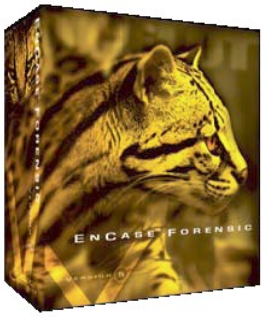
Es fundamental que se manipule lo menos posible la evidencia, debido a que esto puede alterar la copia exacta de la evidencia original.

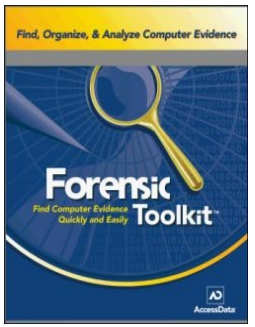
Reglas, Procedimientos y Leyes (Cont.)

Análizar

El análisis de los datos es muy diferente a obtener la evidencia y depende en gran medida a la manera en que se realizó la copia espejo (bit a bit). Existen varias técnicas para capturar la copia forense exacta de los discos o unidades de evidencia, en los cuales se analizarán los datos.

El análisis debe ser realizado sobre las copias duplicadas, así la evidencia original será protegida de alteración debido a que la primera regla forense es la preservación de la evidencia original. Una vez que se crea la copia, se debe utilizar la copia para los siguientes procesos. El análisis forense puede ser realizado utilizando varias herramientas forenses, tales como EnCASE, FTK (Forensics ToolKit), TSK (The Sleuth Kit), etc.



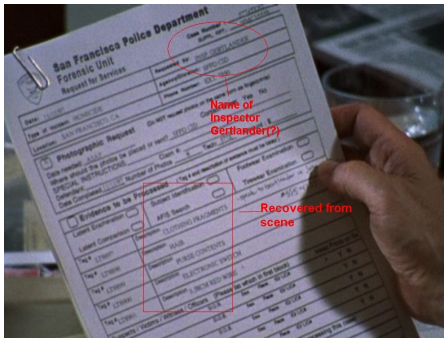


Reglas, Procedimientos y Leyes (Cont.)

Presentar: Reporte de la investigación y Testigo Experto

En el Reporte Final se incluye, todo lo realizado y los resultados. El Reporte básico incluye: ¿Quién?, ¿Qué?, ¿Cuándo?, ¿Dónde?, y ¿Cómo? de un crimen. En una buena investigación las acciones realizadas se pueden repetir y los resultados obtenidos serán siempre los mismos. Se dará una explicación de los diferentes procesos, sobre el funcionamiento del sistema y sus componentes. El Reporte incluirá los registros generados por las herramientas para mantener un rastro de todos los pasos realizados.

Un Testigo Experto es una persona que investiga, evalúa, educa, y testifica en un juzgado. Su rol es es apoyar a la corte a comprender evidencia compleja, expresar una opinión en la corte, asistir al juicio completo, apoyar a los abogados a obtener la verdad y no oscurecerla, y por último estar calificado para exhibir sus conocimientos.



Curso Online de Informática Forense

Días:

Sábados 17, 24, 31 de Agosto y 7, 14 de Setiembre del 2013

Horario:

De 9:00am a 12:00 (UTC -05:00)

Más Información:

http://www.reydes.com/d/?q=Curso_de_Informatica_Forense

Correo electrónico: caballero.alonso@gmail.com
Twitter: https://twitter.com/Alonso_ReYDeS
LinkedIn: http://pe.linkedin.com/in/alonsocaballeroquezada/
Skype: ReYDeS
Sitio Web: http://www.reydes.com

Webinar Gratuito
¡Muchas Gracias!

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Cómputo Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Jueves 15 de Agosto del 2013