www.eysglobal.com

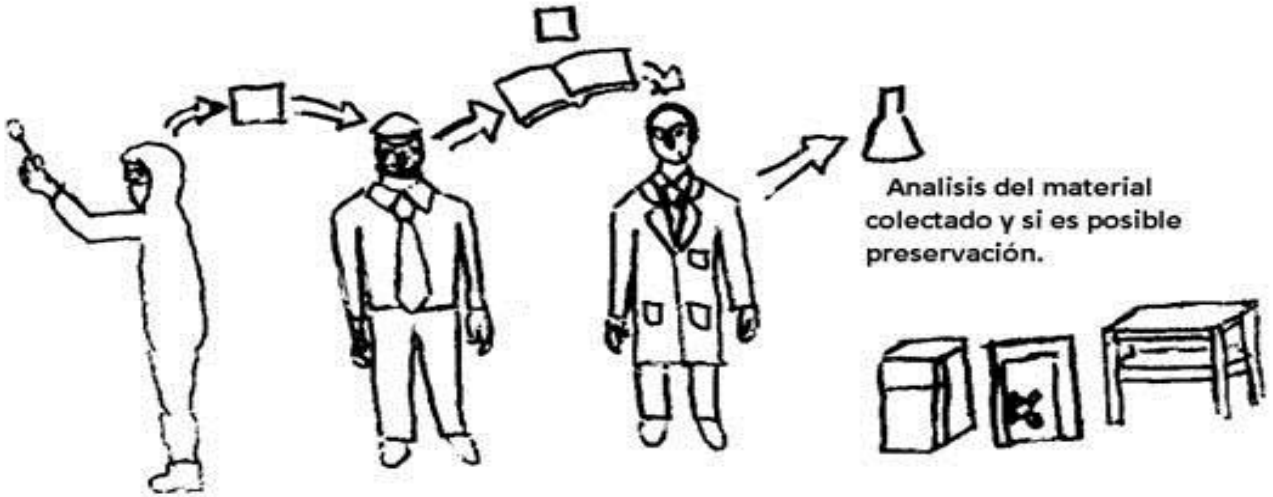
MÓDULO 1
TEMA 5: CADENA DE CUSTODIA

CADENA DE CUSTODIA

La cadena de custodia es un sistema documentado, formado por una serie de instrucciones y registros, que se aplica a los elementos probatorios y a la evidencia física por parte de las personas responsables de su manejo, desde el momento en el que se encuentran o aportan a la investigación hasta su disposición final.

DEFINICIÓN DE CADENA DE CUSTODIA DENTRO DE LA INFORMÁTICA

CADENA DE CUSTODIA



ESCENA DE LOS HECHOS
Inicia la recolección de material sensible significativo con las devidas precauciónes para evitar contaminación.

POLICIA
Traslada el material recibido y puesto bajo su custodia entregando el recibo correspondiente.

LABORATORIO
Recibe el material y lo analisa para confirmar el orígen así como identificación.
Emite un segundo recibo y anota en libro de entradas.

Analisis del material colectado y si es posible preservación.

Se almecena el material según su especie en refrigerador, bobeda anaqueles etc.

CADENA DE CUSTODIA

La CdC establece un mecanismo o procedimiento, que asegura a quienes deben juzgar que los elementos probatorios (indicios, evidencias o pruebas) no han sufrido alteración o contaminación alguna desde su recolección, examen y custodia, hasta el momento en el cual se presentan como prueba ante el Tribunal. Este procedimiento debe controlar dónde y cómo se ha obtenido la prueba, qué se ha hecho con ella (y cuándo), quién ha tenido acceso a la misma, dónde se encuentra ésta en todo momento y quién la tiene y, en caso de su destrucción (por la causa que sea), cómo se ha destruido, cuándo, quién, dónde y porqué se ha destruido. Este procedimiento de control debe ser absolutamente riguroso, de manera que no pueda dudarse ni por un instante de la validez de la prueba.

CADENA DE CUSTODIA

Para entender su importancia pongamos como ejemplo un caso que, desgraciadamente, está a la orden del día: un caso de corrupción.

Cuando la policía y los investigadores entran en la casa del sospechoso, resulta que encuentran un montón de documentación en papel referente a contratos inflados económicamente para estafar a la Administración Pública

CADENA DE CUSTODIA

CADENA DE CUSTODIA

Sin embargo, la evidencia digital tiene ciertas peculiaridades con respecto a otro tipo de evidencias, y es que la información que se puede presentar como medio de prueba la podemos encontrar en diferentes estados:

almacenada estáticamente. Información que se encuentra almacenada de manera persistente en un dispositivo a la espera de ser recuperada o utilizada.

Almacenada dinámicamente o en procesamiento. Información que se encuentra almacenada de manera temporal en un dispositivo volátil y que se perderá en el momento que el dispositivo deje de recibir corriente eléctrica.

En tránsito o desplazamiento. Información que se encuentra en movimiento por la red en forma de paquete de información que puede ser capturado y/o almacenado.

FASES DE LA CADENA DE CUSTODIA

El recurso sobre el cual trabaja la Informática Forense es muy distinto a cualquier otro en los casos de delitos, pues las evidencias por ser digitales son volátiles y cualquier manipulación indebida o inadecuada puede acarrear que la evidencia se estropee y pierda validez en un caso judicial.

FASE DE IDENTIFICACION

El primer paso que debe realizar el analista es identificar todos aquellos elementos que harán parte de la investigación. A la vez que se identifican deberán ser marcados o rotulados claramente para poder darles adecuado tratamiento a través de todo el proceso.

Un disquette, disco duro, memorias, portátil, todos podrán ser parte de la evidencia y así mismo serán marcados con un identificador único.

ETAPA 1: LEVANTAMIENTO DE INFORMACIÓN INICIAL

En esta etapa de la identificación es en la que el administrador del sistema solicita el análisis forense de la evidencia. Para esto debe suministrar al equipo de análisis información como fecha del incidente, duración y detalles del mismo. También información sobre datos de contacto del responsable del sistema afectado como teléfonos, correos, direcciones, etc. Es importante también suministrar información sobre el dispositivo o equipo afectado con el mayor detalle posible, como su dirección IP, marca, modelo, seriales, sistema operativo, etc.

ETAPA 2: ASEGURAR LA ESCENA

Los dispositivos que se toman como evidencia en el caso deberán ser correctamente identificados según el tipo de dispositivo, si es un sistema informático, dispositivo móvil, sistemas embebidos, etc., así como también según el medio de almacenamiento. En este punto la evidencia podrá ser volátil si se puede perder al apagar el sistema, por ejemplo se encuentra en ejecución en memoria, y no volátil como en el caso de información almacenada en un disco duro.

FASE DE VALIDACION Y PRESERVACION

Es muy importante preservar correctamente las evidencias recolectadas en la fase anterior. De poco o nada vale recopilar las evidencias si no se lleva un registro exacto de quienes han tenido acceso a ella, pues es el sustento ante un caso judicial de que las mismas no han sido alteradas durante el proceso.

ETAPA 1: COPIAS DE LA EVIDENCIA

El primer paso es sacar dos copias de las evidencias obtenidas. De esta manera nos aseguramos que mantenemos el original intacto y se trabajará solo con las copias y en todo momento habrá manera de comprobar que la evidencia no ha sido alterada.

Cada copia deberá tener una suma de comprobación de la integridad haciendo uso de funciones como MD5 o SHA1.

ETAPA 2: CADENA DE CUSTODIA

En todo momento se debe conocer quien ha tenido acceso a las evidencias recolectadas. Para esto existe la cadena de custodia. En cada etapa se preparará un documento donde se registran los datos de las personas que han accedido a la evidencia y en que fechas exactas. Toda la información que se pueda registrar será de apoyo en el proceso, como por ejemplo como se ha transportado la evidencia, a que sitios, etc. Es poder seguirle el rastro a la evidencia y garantizar su integridad.

FASE DE ANALISIS

Existen herramientas que se utilizan para analizar las evidencias digitales. En esta fase se debe identificar cuales de ellas son las más pertinentes para el análisis, y de esta manera conseguir elaborar la línea de tiempo donde se ubique cuando sucedieron los hechos del ataque.

ETAPA 1: PREPARACIÓN PARA EL ANÁLISIS

En esta etapa lo que se busca es montar todo lo necesario para el análisis de las evidencias. Se necesitará en algunos casos equipos donde se montarán las imágenes de las evidencias para su análisis, sistemas operativos, en fin, lo necesario para este análisis.

ETAPA 2: RECONSTRUCCIÓN DEL ATAQUE

Esta es la etapa que puede tomar mucho más tiempo. Lo que se busca es crear la línea de tiempo con la información recolectada sobre la evidencia, fechas en las que fueron manipulados archivos o borrados. Para esto el analista debe profundizar en el análisis mirando para cada archivo información sobre tamaños de archivo, marcas de tiempo MACD, rutas, permisos.

ETAPA 3: DETERMINACIÓN DEL ATAQUE

Una vez se haya determinado la línea de sucesos del ataque se pasará a determinar el punto por el cual el atacante ingresó al sistema. Esto pudo ocurrir por accesos no controlados al tener puertos abiertos en la red, sistemas operativos desactualizados, ataques de fuerza bruta, etc.

ETAPA 4: IDENTIFICACIÓN DEL ATACANTE

Habrá casos en lo que se solicite al analista la identificación del atacante. En este caso el analista hará uso de herramientas para detectar de donde pudo venir el ataque, desde que dirección IP y rastrear esta a quien pertenece.

ETAPA 5: PERFIL DEL ATACANTE

Hay distintos tipos de atacantes los cuales podrán ser identificado según el tipo de ataque que han realizado. Entre estos tenemos los hackers, SciptKiddies y profesionales de informática que usan sus conocimientos para realizar el ataque.

ETAPA 6: EVALUACIÓN DEL IMPACTO CAUSADO EN EL SISTEMA

No todos los ataques a un sistema tienen el mismo impacto. Algunas veces el atacante sólo ingresa al sistema pero no modifica o altera los archivos. En otras ocasiones si alcanzan a realizar cambios que afectan levemente o gravemente un sistema. En analista deberá medir el impacto causado, pues se podrán tomar medidas para corregir y mitigar el riesgo.

FASE DE DOCUMENTACION Y PRESENTACION DE LAS PRUEBAS

Consiste en documentar todos los pasos realizados sobre la evidencia, para posteriormente realizar los informes técnicos.

Etapa 1: Utilización de formularios de registro del incidente
Entre otros se deberán llenar los siguiente formularios

- Documento de custodia de la evidencia
- Formulario de identificación de equipos y componentes
- Formulario de incidencias tipificadas
- Formulario de publicación del incidente
- Formulario de recogida de evidencias
- Formulario de discos duros.

ETAPA 2: INFORME TÉCNICO

Es la elaboración de un reporte con todos aquellos aspectos técnicos del análisis efectuado. Tendrá un perfil para ser entregado como soporte técnico, dirigido a personal que conozca de los sistemas y pueda manejar este tipo de lenguaje.

ETAPA 3: INFORME EJECUTIVO

Este informe deberá ser mucho más sencillo en su presentación, empleando palabras mucho más entendibles, no dirigidas a personal técnico. En este documento se exponen los hechos ocurridos en el sistema atacado.