Computación Forense

Adquisición de Data y Duplicación

Clase 3a

Profesor: Ing. Alex Araya Rojas, MT

CISSP, CISM

Adquisición de Data y Duplicación

- **Definición**

  - Es uno de los procesos más críticos del proceso forense digital.
  - Un investigador forense deberá demostrar la exactitud de su trabajo para la extracción de la data.
  - Debe estar claramente establecido el o los métodos para la extracción de la información electrónicamente almacenada.

Adquisición de Data y Duplicación

- **¿Qué tipos de adquisiciones se pueden presentar?**
  - Cuando existe información que permanece sin alteración aunque el dispositivo se apague estamos hablando de adquisición estática.
  - Siempre es recomendable obtener 2 copias de la fuente original en discos sanitizados y verificar las copias con pruebas de integridad.
  - Copias bit a bit o respaldos?? Hay diferencia??
  - La experiencia, tipo de caso y requerimientos debe ir definiendo un paso a paso que debemos respetar en cada pericia forense que ejecutemos, siempre documente y aprenda de lo bueno y de lo malo!!

Adquisición de Data y Duplicación

- **¿Qué tipos de adquisiciones se pueden presentar?**

  - Cuando la información es volátil, por ejemplo la memoria RAM, hablamos de adquisiciones en vivo y deben tomarse con mucho respeto al procedimiento.

  - Esta información es especialmente importante para generar análisis de líneas de tiempo y solo hay una oportunidad para recolectarla.

  - Tenemos dos categorías, la información del sistema y la información de la red.

  - Si hacemos un listado de prioridades, esta es la primera información de normalmente debe recolectarse.

Adquisición de Data y Duplicación

- **Errores comunes**
  - Dentro de los errores comunes al tratar con adquisiciones en vivo están:
    - Utilizar los equipos de cualquier forma.
    - Apagar o reiniciar los equipos.
    - No generar una línea base de documentación del equipo ni su ambiente.
    - No documentar el proceso de adquisición de datos.

Adquisición de Data y Duplicación

- **Paso a Paso para adquisiciones en vivo**
  - Paso 1:
    - Prepárese para la respuesta a incidentes
    - Siempre disponga de discos y equipo en general para primera respuesta
    - Elabore y practique las políticas y metodologías de recolección

Adquisición de Data y Duplicación

- **Paso a Paso para adquisiciones en vivo**
  - Paso 2:
    - Documente el incidente
    - Organice los logs y cualquier otro tipo de información recolectada
    - Documente el proceso de recolección
    - Seleccione las herramientas adecuadas para cada situación, conozca sus herramientas antes del incidente y practique con ellas!!

Adquisición de Data y Duplicación

- **Paso a Paso para adquisiciones en vivo**
  - Paso 3:
    - Verifique las políticas aplicables según la organización o lugar.
    - Verifique que sus acciones hagan match con dichas políticas.
    - Respete siempre los derechos de los dueños y/o usuarios de los equipos.

Adquisición de Data y Duplicación

- **Paso a Paso para adquisiciones en vivo**
  - Paso 4:
    - Aplique al pie de la letra la estrategia de recolección de datos volátiles.
    - Siga la metodología religiosamente para no cometer errores.

Adquisición de Data y Duplicación

- **Paso a Paso para adquisiciones en vivo**
  - Paso 5:
    - Establezca los métodos de almacenamiento y transporte adecuados.
    - Asegure la integridad de la herramienta forense.

Adquisición de Data y Duplicación

- **Paso a Paso para adquisiciones en vivo**
  - Paso 6:
    - No apague o reinicie los equipos bajo investigación hasta que no haya extraído la inf. volatil.
    - Mantenga el log con todas las acciones.
    - Tome fotografías de la pantalla y documente estado.
    - Anote SO, hora del sistema, historial de comandos.
    - Revise si se aplican técnicas de cifrado de disco.
    - Haga un dump de la RAM.
    - Recolecte cualquier otra información volátil de interés.
    - Complete el informe y marque el inicio de la cadena de custodia.

Adquisición de Data y Duplicación

- **Puesta en Práctica**

  - El laboratorio de este tema le permitirá poner en práctica lo estudiado, tome nota de todo el proceso y utilice las horas de consulta para evacuar dudas sobre el procedimiento.

  - La ejecución de pruebas no en caliente, le permiten al perito estar mejor preparado para cuando lleguen los verdaderos casos, no desaproveche las oportunidades para poner a prueba los procedimientos, aplicar sesiones de lecciones aprendidas y seguir interiorizando los conocimientos.

Gracias