INSTITUTO NACIONAL DE CIBERSEGURIDAD

ANÁLISIS FORENSE DIGITAL

Unidad 2 – Adquisición de evidencias

universidad de león

MINISTERIO DE DEFENSA

SAPROMIL

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

INDICE

1. Volatilidad. Orden de adquisición.
2. El entorno. Información de interés, fotografías y croquis. Herramientas.
3. Forense tradicional, en frío. Imágenes y herramientas.
4. Forense en caliente. Adquisición de memoria RAM y otros datos volátiles.
5. Herramientas para Linux y Windows.

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

universidad de león

MINISTERIO DE DEFENSA

SAPROMIL

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

UNIDAD 2 – ADQUISICIÓN DE EVIDENCIAS

1. Volatilidad. Orden de adquisición.

❑Volatilidad

Es lo contrario a persistencia, siendo esta la capacidad de una evidencia de permanecer en un sistema informático.

Cuánto más tiempo una evidencia puede mantenerse disponible, menos volátil es.

La alteración o pérdida de la evidencia sucede por:

- ✓ Falta de suministro eléctrico, en apagados o reinicios en frío.
- ✓ Sobreescritura en durante la operación normal del sistema.
- ✓ Sobreescritura por acciones externas, como escritura de nuevos datos.

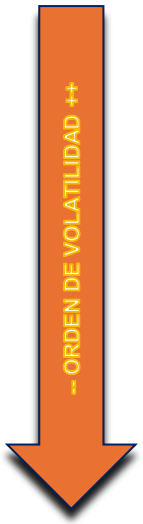
UNIDAD 2 – ADQUISICIÓN DE EVIDENCIAS

1. Volatilidad. Orden de adquisición.

❑Orden de adquisición de las evidencias

La volatilidad marca el orden de adquisición, que siempre tratará de preservar el mayor número de evidencias.

Priorizaremos en orden de mayor a menor volatilidad:



- ✓ Registros del procesador y cache. Se pierden en cuanto cargamos un programa nuevo.
- ✓ Memoria RAM total de la máquina o de uno o varios procesos.
- ✓ Ficheros temporales, fichero de paginación, conexiones de red, usuarios actuales, ficheros abiertos, hora del sistema.
- ✓ Archivos del sistema o sistemas de ficheros del disco.

UNIDAD 2 – ADQUISICIÓN DE EVIDENCIAS

1. Volatilidad. Orden de adquisición.

❑Adquisición de las evidencias

- ✓Registros del procesador y cache: Se pierden en cuanto cargamos un programa nuevo.
- ✓Memoria RAM: La adquirimos ejecutando en “live” herramientas lo mas livianas posibles, que modifiquen lo mínimo la memoria, aunque siempre modificaremos, como mínimo, las posiciones de memoria de las instrucciones del programa de adquisición.
- ✓Ficheros temporales, fichero de paginación, y resto de datos volátiles: Los obtenemos con herramientas del SSOO, normalmente integradas en scripts.
- ✓Sistemas de ficheros: será lo último y utilizaremos herramientas de copia bit a bit. Preferentemente en frío o bien a través de una instantánea que nos facilite una imagen coherente.

UNIDAD 2 – ADQUISICIÓN DE EVIDENCIAS

2. El entorno. Información de interés, fotografías y croquis. Herramientas.

❑Información necesaria del contexto

- ✓ Cada caso es un mundo, pero el análisis forense necesita de contexto como hilo conductor de la investigación.
- ✓ La información debe ser recolectada de la fuente primaria en la medida de lo posible, no de terceros, ya que se va degradando.
- ✓ Es importante contar con los testimonios de las personas que han detectado el incidente, con el objetivo de saber:
  - ❑ Instante exacto en el que se ha detectado por primera vez.
  - ❑ Hechos que han llamado la atención para detectarlo.
  - ❑ Cualquier otro dato relacionado con la detección y actividad del sistema en ese momento.
  - ❑ Personas implicadas y hechos ocurridos sobre el sistema hasta la intervención.

UNIDAD 2 – ADQUISICIÓN DE EVIDENCIAS

2. El entorno. Información de interés, fotografías y croquis. Herramientas.

❑Información física del entorno

- ✓ En algunos casos, puede ser interesante disponer de la información del entorno físico:
  - ❑ Dispositivos externos conectados.
  - ❑ Ubicación de ratón
  - ❑ Información en la pantalla, notas escritas, cuadernos.
  - ❑ Números de serie/modelo/datos identificativos.
  - ❑ Características de la sala, ventanas, puertas, accesos.
- ✓ Todo esto se consigue mediante fotografías y en algunos casos, levantando un croquis de la habitación y ubicación de los elementos.

Recuerda, en general, sólo hay una oportunidad para la adquisición. Si tenemos dudas sobre la necesidad de una información, lo prudente es recopilarla en esa única oportunidad.

UNIDAD 2 – ADQUISICIÓN DE EVIDENCIAS

2. El entorno. Información de interés, fotografías y croquis. Herramientas.

❑Herramientas

- ✓ Grabadora de voz, para las posibles entrevistas.
- ✓ Dispositivo móvil con cámara y app de fotografía que sobreimpresione marca de tiempo y geolocalización, como Smart GPS Camera o GPS Map Camera, disponible para Android e iOS.
- ✓ Dispositivos para almacenamiento y transporte de evidencias físicas cómo discos, dispositivos móviles, tablets, portátiles, etc…

  Visitar: *https://www.idstronghold.com/*
- ✓ Sistema de etiquetado de evidencias, bolsas de plástico, etiquetas y rotuladores indelebles.
- ✓ Aplicaciones instaladas u online para la realización de croquis, por ejemplo draw.io, https://app.diagrams.net/
- ✓ Y lo más importante y eficaz de todo: CUADERNO Y BOLÍGRAFO!!!

UNIDAD 2 – ADQUISICIÓN DE EVIDENCIAS

3. Forense tradicional, en frío. Imágenes y herramientas.

❑Adquisición en frío

- ✓En frío es con los dispositivos apagados.
- ✓La información volátil la damos por perdida.
- ✓Sólo adquirimos los sistemas de ficheros o discos completos.
- ✓ Es un proceso sencillo, que sólo necesita de los recursos de almacenamiento adecuados y las herramientas pertinentes.
- ✓En cuanto al medio destino de copia, tenemos dos posibilidades:
  - A. Copia de disco a disco, la más rápida en el caso del uso de clonadoras, pero poco versátil.
  - B. Copia de disco a imagen, más lenta pero muy versátil.

UNIDAD 2 – ADQUISICIÓN DE EVIDENCIAS

3. Forense tradicional, en frío. Imágenes y herramientas.

❑Adquisición en frío (ii)

✓En cuanto a los datos copiados, tenemos tres posibilidades:

A. Copia física, bit a bit o copia forense, consistente en la copia a nivel de bloque del contenido del disco, independientemente del significado de dicha información. Es la copia que usaremos por defecto.

B. Copia lógica, o a nivel de fichero, dónde copiamos solamente aquellos bloques que, según el sistema de ficheros, contienen información. Sólo la usaremos en caso de imposibilidad de obtener una copia bit a bit, normalmente por permisos en el sistema, como en caso de móviles o dificultades técnicas, como en el caso de almacenamientos RAID.

C. Copia selectiva, dónde, a nivel de fichero, seleccionamos aquellos ficheros que nos resulten más interesantes.

UNIDAD 2 – ADQUISICIÓN DE EVIDENCIAS

3. Forense tradicional, en frío. Imágenes y herramientas.

❑Herramientas

- ✓Software para el clonado: Hay multitud aplicaciones para la copia bit a bit, tanto comerciales, como opensource y/o gratuitas como integradas en algunas distribuciones Linux. Algunas de ellas son:
  - ❑ La más básica, en formato raw, dd, o su versión mejorada para forense dcfldd.
  - ❑ FTK Imager, que nos permite adquirir en un formato propietario.
  - ❑ Guymager, la más versátil del mundo opensource.

- ✓Hardware para el clonado, clonadoras que nos permiten copiar de un disco a múltiples disco destino de forma simultánea. Los discos tienen que ofrecer una "geometría" idéntica y las clonadoras nos facilitan esta configuración.

Ver https://www.forensiccomputers.com/tableau-tx1-forensic-imager

UNIDAD 2 – ADQUISICIÓN DE EVIDENCIAS

4. Forense en caliente. Adquisición de memoria RAM y otros datos volátiles.

❑Adquisición en caliente

- ✓Se lleva a cabo con el Sistema operativo arrancado, y hay dos posibles motivos:
  - Puede haber datos en memoria que nos interesan en el análisis del caso.
  - Estamos haciendo Incident Response, y nos encontramos en un proceso de evaluación temprana, dónde nos interesa adquirir ciertas evidencias para un triage y evaluación de alcance y otros aspectos del caso.
- ✓Toda adquisición en caliente requiere de la ejecución de un programa, externo o interno al SO, o bien el establecimiento de una conexión.
- ✓Cualquier acción puede provocar alteración de la evidencia, por lo que tenemos que tener en cuenta que es lo prioritario para el caso.
- ✓Con una adecuada selección de los artefactos adquiridos, podemos responder muchas de las preguntas encargas al analista.

UNIDAD 2 – ADQUISICIÓN DE EVIDENCIAS

4. Forense en caliente. Adquisición de memoria RAM y otros datos volátiles.

❑Memoria RAM

- ✓ En la memoria volátil o RAM se encuentran todos los datos de ejecución del sistema:
  - Artefactos del sistema de ficheros.
  - Ficheros abiertos
  - Memoria gráfica
  - Formularios y páginas web
  - Credenciales
  - Listado de procesos, conexiones, sesiones de red y so, etc…
- ✓ Los fabricantes toman medidas para aleatorizar el uso de la memoria, lo que dificulta el trabajo de análisis.
- ✓ Con el conocimiento adecuado se puede localizar cualquier dato de los programas que están en ejecución en la máquina víctima.

UNIDAD 2 – ADQUISICIÓN DE EVIDENCIAS

4. Forense en caliente. Adquisición de memoria RAM y otros datos volátiles.

❑Otros datos volátiles

- ✓ Un camino intermedio entre la adquisición y análisis de la RAM y la pérdida de los datos volátiles es la extracción de algunos datos mediante la ejecución de comandos.
- ✓ Podemos obtener datos como fecha del sistema, zona horaria, usuarios conectados, ficheros en uso, procesos, conexiones de red, datos de uso del sistema, versiones de programas, programas instalados, etc.…
- ✓ En este caso, el principal problema es la falta de confianza en las herramientas del sistema vulnerado, además de la extensa cantidad de comandos y opciones que podemos utilizar.
- ✓ Por ello es recomendable, en la medida de lo posible, usar comandos de fuentes seguras así como automatizar el proceso, para evitar dejarnos información esencial.

UNIDAD 2 – ADQUISICIÓN DE EVIDENCIAS

5. Herramientas para Linux y Windows.

❑Herramientas de Triage

Ya hemos indicado algunas herramientas para la adquisición en frío.

Para la adquisición en caliente es recomendable usar scripts o automatizaciones personalizdas o al menos personalizables.

En nuestro caso usaremos Wintriage y Lintriage, ambas aportaciones de la empresa Securizame a la comunidad.

FIN UNIDAD

Unidad 2
ADQUISICIÓN DE EVIDENCIAS

INSTITUTO NACIONAL DE CIBERSEGURIDAD

universidad de león

MINISTERIO DE DEFENSA

SAPROMIL

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES