Nombre del estudiante: Diego Castro - **Fecha de elaboración:** 23/05/2024

TRABAJO PRÁCTICO N° 4: METODOLOGÍAS DE ANÁLISIS FORENSE

1 - Metodologías para el análisis forense de IoT

1. Preparación:

- Identificación del caso
- Identificación de la infraestructura IoT

2. Extracción y Adquisición:

- Detección de la infraestructura
- Extracción y Adquisición de Objetos
- Validación y Resguardo
- Supervisión del Transporte

3. Análisis:

- Preparación del Ambiente
- Análisis de Datos y Relaciones

4. Presentación:

- Armado del Informe
- Preparación del Informe

Beneficios de GAFIoT:

- Se ajusta al proceso general forense.
- Ordena el proceso forense al identificar las actividades de cada fase según las capas del modelo IoT.
- Incluye actividades lo suficientemente genéricas como para ajustar la tarea forense a diferentes entornos IoT.

2 - Metodologías para la Forensia de Bases de Datos

Metodologías para el análisis forense de bases de datos:

1. AUDBForense: Esta metodología combina elementos de las metodologías AUDB (Auditoría Forense de Bases de Datos), ForenseUDE (Universal Forense Digital Evidence) y ForenseDB (Forense Digital en Bases de Datos). Se compone de 4 fases:

- **Preparación:** Identificación del caso y de la infraestructura IoT.
- **Extracción y Adquisición:** Detección de la infraestructura, extracción y adquisición de objetos, validación y resguardo, supervisión del transporte.
- **Análisis:** Preparación del ambiente y análisis de datos y relaciones.
- **Presentación:** Armado del informe y preparación del informe final.

2. ForenseUDE: Esta metodología se basa en el modelo PURI, la norma ISO/IEC 27037 y el modelo EDRM. Consta de 9 fases:

- **Gestión de la información:** Implementación de procesos de gestión de la información y riesgos asociados.
- **Identificación:** Desarrollo y ejecución de estrategias para identificar y validar fuentes de información.
- **Preservación:** Activación de la preservación de los datos potencialmente relevantes.
- **Recolección:** Recolección de la información potencialmente relevante.
- **Procesamiento:** Reducción del volumen de ESI y conversión a formatos más confortables.
- **Revisión:** Evaluación de la ESI para determinar la revelación del descubrimiento electrónico.
- **Análisis:** Obtención de una comprensión adecuada del contenido de la información recolectada.
- **Producción:** Preparación y producción de los resultados de la investigación.
- **Presentación:** Muestra de los resultados de la investigación.

3. ForenseDB:

Esta metodología se enfoca en los datos contenidos en la base de datos en sí y no en el servidor que la contiene o en las aplicaciones que corren sobre ella. Se distingue en esta propuesta:

- No aplica a una base de datos en particular, sino a bases de datos relacionales en general.
- Presta especial atención al tratamiento de los datos personales y la propiedad industrial.
- Clasifica la evidencia digital en diferentes tipos de datos.

La metodología propone 8 fases:

- **Preparación Inicial:** Análisis de alternativas para evitar desconectar el servidor.
- **Relevamiento e Identificación:** Relevamiento de la infraestructura tecnológica y obtención de información de configuración.
- **Recolección:** Aplicación de procedimientos adecuados de preservación.
- **Adquisición:** Consideración de las herramientas forenses más adecuadas.
- **Preparación y Procesamiento:** Recreación de un entorno similar al SGBD en el laboratorio.
- **Extracción y Análisis:** Extracción de datos y estructuras a nivel de base de datos.
- **Producción y Presentación:** Armado de un informe de resultados.
- **Evaluación Final:** Propuesta de mejoras en la seguridad, configuraciones y auditorías de datos.

3 - Metodologías para el Examen Manual de Dispositivos (EMD)

El Examen Manual de Dispositivos (EMD) es una técnica forense digital que implica el uso de la interfaz de usuario del dispositivo para buscar, examinar y recopilar manualmente contenido que reside en o es accesible por el propio dispositivo.

Ventajas del EMD

- Permite una evaluación rápida del valor potencial del dispositivo para la investigación.
- Puede identificar evidencia indiciaria de manera rápida y directa.
- Puede evitar el acceso a información privada o no pertinente al caso.
- Puede evitar el secuestro de dispositivos que no sean de interés para la investigación.

Limitaciones del EMD

- No siempre es lo más adecuado y pertinente para la investigación digital.
- Puede poner en duda la validez e integridad de la evidencia.
- No es un reemplazo para el análisis forense de dispositivos realizado en el laboratorio.
- Es un proceso "en vivo" que puede causar cambios irreversibles en el dispositivo.

- No es adecuado cuando se requieren datos que existen más allá de lo que es visible a través de la interfaz del dispositivo.

Metodología EMD

La metodología EMD propuesta por Horsman consiste en considerar 7 preguntas que ayudan al analista forense a evaluar la conveniencia (o no) de utilizar esta metodología:

1. ¿Qué datos son relevantes para la investigación?
2. ¿Pueden encontrarse todos los datos?
3. ¿Pueden reunirse sin comprometer la evidencia?
4. ¿Preocupa la autenticidad o fiabilidad de la evidencia?
5. ¿Pueden capturarse los datos relevantes suficientemente?
6. ¿Los datos capturados pueden registrarse en la cadena de custodia?
7. ¿El método de captura es fiable y justificable?

Actividades del EMD

Respondiendo una a una estas preguntas se pueden tomar acciones tendientes a una recolección eficiente de la evidencia, con actividades como:

- Pre-evaluación del dispositivo
- Conversación con el propietario
- Valoración de la evidencia a primera vista
- Considerar la presencia de metadatos
- Acceso a datos sin procesar
- Identificar el riesgo y su impacto
- Definir otra metodología a seguir para la extracción de los datos

4 - Metodología Triaje Forense Digital

El Triaje Forense Digital es una técnica utilizada para identificar y priorizar rápidamente la evidencia digital relevante en una investigación. Es similar al triaje médico, donde se clasifican a los pacientes en función de la gravedad de sus lesiones para garantizar que reciban la atención médica adecuada de forma prioritaria.

Ventajas del Triaje Forense Digital:

- Permite identificar pruebas relevantes de manera rápida y eficiente.
- Ayuda a descartar dispositivos o datos no relevantes de la investigación, ahorrando tiempo y recursos.
- Orienta al analista en la investigación si el cúmulo de datos es importante.

Desventajas del Triaje Forense Digital:

- La selección apresurada de evidencia puede llevar a la pérdida de pruebas cruciales.
- Los scripts de búsqueda mal formulados pueden descartar información útil.
- Requiere de herramientas y metodologías especializadas.

Metodologías de Triaje Forense Digital: Existen dos metodologías comunes de Triaje Forense Digital:

- **Cyber Forensic Field Triage Process Model (CFFTPM):** Se enfoca en encontrar evidencia utilizable de manera inmediata, identificar víctimas en riesgo urgente, guiar la investigación en curso, identificar posibles

cargos y evaluar el peligro del delincuente. Se desarrolla en 6 fases: Planificación, Triaje, Uso/Perfiles de usuario, Cronología, Internet y Evidencia específica del caso.
- **Case-Based Reasoning Forensic Triager (CBR-FT):** Limita la recopilación de datos no relevantes al apuntar solo a áreas probatorias conocidas de un sistema basado en experiencias pasadas de investigación. Se centra en dónde se ha localizado la evidencia en casos anteriores y dirige el análisis a estas áreas. Comprende dos etapas: Extracción de datos de ubicaciones de alta prioridad y Extracción de datos basada en las características del caso.

Elección de la Metodología: La elección de la metodología adecuada depende de las características del caso, la experiencia del analista y las herramientas disponibles. Es importante considerar los objetivos de la investigación, la cantidad de datos disponibles y el tiempo disponible para el análisis.

5 - Metodologías Propias de la Ciberseguridad: NIST SP 800

Se centra en el análisis de datos relacionados con incidentes y la determinación de la respuesta adecuada para cada caso. La guía puede aplicarse independientemente de la plataforma de hardware, el sistema operativo, los protocolos o las aplicaciones específicas que se utilicen.

Fases de la gestión de incidentes: La guía NIST describe cuatro fases principales para la gestión de incidentes:

1. Preparación:

- Establecer un equipo de respuesta a incidentes.
- Adquirir las herramientas y recursos necesarios.
- Desarrollar planes de respuesta a incidentes.

2. Detección y análisis:

- Identificar y analizar posibles incidentes de seguridad.
- Evaluar los precursores e indicadores disponibles.

3. Contención y erradicación:

- Tomar medidas para contener el incidente.
- Minimizar el impacto.
- Erradicar la causa raíz del problema.

4. Recuperación:

- Restaurar los sistemas afectados.
- Mejorar las defensas de seguridad.
- Aprender de la experiencia del incidente.

Aspectos clave de la guía:

- **Énfasis en el análisis de datos:** La guía destaca la importancia de analizar cuidadosamente los datos relacionados con incidentes para comprender la naturaleza del problema, identificar la causa raíz y determinar la respuesta adecuada.
- **Metodología flexible:** La guía proporciona un marco general para la gestión de incidentes, pero permite flexibilidad para adaptarlo a las necesidades específicas de cada organización.

- **Énfasis en la preparación:** La guía subraya la importancia de estar preparado para responder a incidentes de seguridad, estableciendo un equipo de respuesta a incidentes, desarrollando planes y adquiriendo las herramientas necesarias.

Aspectos adicionales para la priorización de incidentes: Incluye información sobre los factores que se deben considerar al priorizar la gestión de incidentes:

- **Impacto de la información del incidente:** Se debe considerar el impacto en la confidencialidad, integridad y disponibilidad de la información de la organización.
- **Recuperabilidad del incidente:** Se debe considerar el tiempo, los recursos y el esfuerzo necesarios para recuperarse del incidente.

Estrategias de contención:

- **Daño potencial y robo de recursos.**
- **Necesidad de preservación de la evidencia.**
- **Disponibilidad del servicio.**
- **Tiempo y recursos necesarios para implementar la estrategia.**
- **Eficacia de la estrategia.**
- **Duración de la solución.**

Estrategias de erradicación y recuperación: Incluye información sobre las estrategias de erradicación y recuperación que se deben considerar, incluyendo:

- **Restaurar sistemas a partir de copias de seguridad limpias.**
- **Reconstruir sistemas desde cero.**
- **Reemplazar archivos comprometidos con versiones limpias.**
- **Instalar parches.**
- **Cambiar contraseñas y reforzar la seguridad del perímetro de la red.**

	Fase/Evaluación	GAFIoT	AUDBForense	Examen Manual de Dispositivos (EMD)	Triaje Forense Digital	NIST SP 800-61
1	Planificación	Sí	Sí	No	Sí	Sí
2	Identificación de la evidencia	Sí	Sí	Sí	Sí	Sí
3	Extracción	Sí	Sí	Sí	Sí	Sí
4	Preservación	Sí	Sí	No	No	Sí
5	Análisis y correlación de los datos	Sí	Sí	Sí	Sí	Sí
6	Informe y presentación de la evidencia	Sí	Sí	No	No	No
7	Normas procesales y criminalísticas	Sí	Sí	No	Parcialmente	Sí
	Grado de Completitud (%)	**100%**	**100%**	**57%**	**71%**	**86%**