1. Busca en los apuntes de clase y/o en las referencias bibliográficas del tema información para contestar a las siguientes preguntas:

a) ¿Cuáles son las diferencias entre los datos de contenido y los metadatos? ¿Qué tipo de información revela cada tipo de datos?

Mientras que los datos de contenido son aquellos que transmiten el significado de una comunicación, como las personas que salen en una foto, los metadatos son los datos de los datos, como la resolución de la foto.

b) ¿Cuáles son los diferentes tipos de evidencia electrónica?

Una evidencia puede ser de tipo volátil (Memoria RAM, procesos en ejecución, etc.) o no volátil (Discos duros, pendrives, CD 's, etc.).

c) ¿Cuáles son las diferencias entre la evidencia electrónica y la evidencia tradicional?

Principalmente la electrónica se encuentra en medios electrónicos o digitales, mientras que la tradicional puede encontrarse en papel, objetos, testimonios, etc.

También por el formato. Si bien la evidencia electrónica puede encontrarse en un elemento físico como un disco duro, la información de la evidencia es intangible y replicable, ya que es digital.

Otra podría ser el método de adquisición de evidencias, pues en el caso de las evidencias electrónicas son necesarios procedimientos digitales, que en el caso de las tradicionales, son de otro tipo (Como identificación de huellas dactilares, recopilación de testimonios, etc.).

d) ¿Cómo se autentica la evidencia digital para que sea admisible en un juicio?

Mediante el hash que hemos creado para verificar que lo analizado es una copia exacta de la evidencia original, o que la integridad de dicha copia se mantiene a lo largo de todo el proceso de análisis. Ya sea que la hayamos obtenido en frío o en caliente. Aunque si es en caliente, el hash no se hace a la evidencia original, sino a lo que hemos obtenido.

e) ¿Qué son los modelos de procesos forenses digitales? Nombra y describe dos de ellos.

Los modelos de procesos forenses digitales son marcos metodológicos que guían la investigación de incidentes que involucran evidencia digital, como crímenes cibernéticos o fraudes. Estos modelos ofrecen pasos estandarizados para garantizar que la recolección, preservación, análisis y presentación de evidencia digital sea realizada de manera adecuada, legalmente aceptable y reproducible en tribunales.

- Modelo NIST:

  Se compone de cuatro fases principales:

  1. **Recolección (Collection)**: Se identifica y adquiere la evidencia digital, asegurando que los datos originales no sean alterados. Esto se realiza mediante la creación de copias exactas de los datos, como imágenes forenses, preservando la integridad de la información.

  2. **Examen (Examination)**: Se organiza y analiza la evidencia recopilada. Aquí se utilizan técnicas para filtrar información, buscar patrones relevantes y recuperar datos eliminados o cifrados.

  3. **Análisis (Analysis)**: Se interpreta la información obtenida en la fase de examen. Este análisis busca reconstruir cronologías y eventos relacionados con el caso, identificando patrones de actividad. Los hallazgos deben ser reproducibles.

  4. **Informe (Reporting)**: Los resultados del análisis se documentan de manera clara y estructurada. Este informe debe ser entendible y detallado, incluyendo los métodos y hallazgos clave, para ser utilizado como evidencia en un tribunal o ante las partes interesadas.

- Modelo de las "4 Fases":

  Consiste en un proceso de cuatro fases que abarcan desde la adquisición de la evidencia digital hasta su presentación en una corte:

  1. **Identificación**: En esta fase, se detectan los dispositivos y la evidencia digital que pueden estar relacionados con el incidente en investigación.

  2. **Preservación**: Una vez identificada, la evidencia se preserva de tal manera que no sea alterada o corrompida durante el proceso de investigación. Se suelen usar técnicas como la creación de imágenes forenses (clones exactos de discos duros) para trabajar sobre copias sin comprometer los datos originales.

  3. **Análisis**: Aquí, los investigadores examinan la evidencia utilizando herramientas y técnicas especializadas para descubrir información relevante (como recuperación de archivos eliminados, análisis de logs, etc.). El análisis debe ser objetivo y reproducible.

  4. **Presentación**: Los hallazgos de la investigación se documentan de manera comprensible para audiencias no técnicas, como jueces o jurados. Se presentan las conclusiones y las pruebas recolectadas, garantizando la claridad y exactitud.

f) ¿Qué buscan establecer los estándares y buenas prácticas para la evidencia digital y el análisis forense digital?

Buscan dar una serie de pautas para ayudar a una mejor adquisición de evidencias y protección de estas durante el análisis, para así realizar un análisis forense exitoso. Por ejemplo, señalando la importancia de preservar el entorno de pruebas, indicando cómo se guardan las pruebas, su transporte, su conservación, etc.

De esta forma, si seguimos sus pautas, podemos establecer una metodología a seguir.

2. Los dispositivos digitales no paran de proliferar. Como futuro investigador digital forense necesitarás procesar y analizar grandes cantidades de datos rápidamente. Busca en Internet los diversos dispositivos digitales a los que nos podemos enfrentar durante el desempeño de la función de perito forense informático. Para cada uno de ellos contesta a las siguientes preguntas:

a) Discos duros de almacenamiento en PCs / portátiles:

- Tipos de Datos: Datos del Sistema Operativo, Programas y Aplicaciones, Datos de Usuario, Datos Temporales, Copias de Seguridad.
- ¿Dónde se localizan?: En las particiones del disco duro, sectores del disco, y tablas de partición.
- Forma de recuperación: Desde el Sistema Operativo, Software de Recuperación (Recuva, EaseUS Data Recovery, etc.), Copia de Seguridad, Servicios de Recuperación Profesional.

b) Memoria RAM:

- Tipos de Datos: Datos de programa, Datos de usuario, Datos de sistema.
- ¿Dónde se localizan?: Los datos en la RAM se localizan en celdas de memoria organizadas en filas y columnas, y se accede a ellas a través de direcciones de memoria. Existen diferentes tipos de RAM, cada uno con una estructura y localización de datos específicas.
- Forma de recuperación: Volcados en caliente.

c) Libros electrónicos:

- Tipos de Datos: Texto, Imágenes, Formatos y Estructuras, Marcadores y Notas, Datos de Usuario.
- ¿Dónde se localizan?: Dispositivos de Almacenamiento Local, Nubes de Almacenamiento, Bases de Datos de Proveedores, Memorias Externas.
- Forma de recuperación: Conexiones USB, herramientas de análisis de dispositivos móviles, clonado de discos, etc.

d) Videoconsolas:

- Tipos de Datos: Juegos y aplicaciones, Multimedia, Metadatos.
- ¿Dónde se localizan?: Disco duro interno, Tarjetas de memoria, Nubes de almacenamiento.
- Forma de recuperación: Imágenes forenses del disco duro, Herramientas forenses, Recuperación de datos borrados.

e) GPS:

- Tipos de Datos: Rutas y trayectorias, Historial de ubicación, Configuraciones del dispositivo.
- ¿Dónde se localizan?: Memoria interna, Tarjetas SD.
- Forma de recuperación: Análisis de la memoria, Herramientas de análisis forense.

f) Televisores:

- Tipos de Datos: Contenido multimedia, Configuraciones.
- ¿Dónde se localizan?: Memoria interna, Dispositivos externos.
- Forma de recuperación: Imágenes forenses, Recuperación de registros de actividad.

g) Altavoces Inteligentes:

- Tipos de Datos: Comandos de voz, Preferencias de música, Configuraciones del dispositivo.
- ¿Dónde se localizan?: Memoria interna, Nubes de almacenamiento.
- Forma de recuperación: Acceso a registros de voz, Análisis de tráfico de red.

h) Localizadores de Artículos con Control Remoto:

- Tipos de Datos: Historial de ubicación, Configuraciones del dispositivo.
- ¿Dónde se localizan?: Memoria interna, Nubes de almacenamiento.
- Forma de recuperación: Análisis de datos de ubicación, Herramientas de recuperación.

i) Coches Inteligentes:

- Tipos de Datos: Datos de navegación, Registros del vehículo, Configuraciones del usuario.
- ¿Dónde se localizan?: Sistema de infoentretenimiento, Nubes de almacenamiento.
- Forma de recuperación: Acceso a la unidad de control, Análisis de registros de viaje.

j) Teléfonos Móviles:

- Tipos de Datos: Contactos, Mensajes, Aplicaciones.
- ¿Dónde se localizan?: Memoria interna, Tarjetas de memoria, Nubes de almacenamiento.
- Forma de recuperación: Extracción forense, Recuperación de datos borrados.

k) Tablets:

- Tipos de Datos: Aplicaciones, Multimedia, Documentos.
- ¿Dónde se localizan?: Memoria interna, Tarjetas SD, Nubes de almacenamiento.
- Forma de recuperación: Análisis de la memoria interna, Recuperación de datos borrados.

l) Cámaras de Fotos:

- Tipos de Datos: Imágenes, Metadatos.
- ¿Dónde se localizan?: Tarjetas de memoria, Memoria interna.
- Forma de recuperación: Extracción de imágenes, Análisis de metadatos.

m) CDs, DVDs, Blu-rays:

- Tipos de Datos: Contenido multimedia, Metadatos.
- ¿Dónde se localizan?: Soportes ópticos.
- Forma de recuperación: Lectura forense de discos, Recuperación de datos borrados.

n) Disquetes:

- Tipos de Datos: Documentos, Metadatos.
- ¿Dónde se localizan?: Soporte magnético.
- Forma de recuperación: Lectura de disquetes, Restauración de archivos.

o) Almacenamiento en la Nube:

- Tipos de Datos: Archivos, Configuraciones.
- ¿Dónde se localizan?: Servidores de la nube.
- Forma de recuperación: Acceso a cuentas de usuario, Investigación de registros de actividad.

3. Existen numerosas herramientas forenses digitales en el mercado. Busca información sobre las herramientas de análisis forense digital más utilizadas y contesta las siguientes preguntas:

a) Autopsy:

- Tipo de Análisis Forense: De Disco y Captura de Datos.
- ¿Es sólida desde el punto de vista forense?:

  Aparece en estos artículos: Enlace_1 y Enlace_2.

- Características:

  1. La herramienta Autopsy es una de las más utilizadas y recomendadas.
  2. Análisis de sistemas de archivos (NTFS, FAT, ext2/ext3, etc.).
  3. Recuperación de archivos eliminados.
  4. Soporte para la extracción de datos de imágenes de discos.
  5. Incluye herramientas para el análisis de metadatos y time stamps.

b) The Sleuth Kit:

- Tipo de Análisis Forense: Visor de archivos.
- ¿Es sólida desde el punto de vista forense?:

  Aparece en este artículo: Enlace_2.
- Características:

  1. Herramientas de análisis para sistemas de archivos NTFS, FAT, Ext2/3/4.
  2. Análisis de imágenes de disco (dd, E01, etc.).
  3. Permite examinar archivos ocultos y borrados.

c) Log2Timeline (Plaso):

- Tipo de Análisis Forense: De Análisis de Registro.
- ¿Es sólida desde el punto de vista forense?: Es una herramienta sólida y efectiva desde el punto de vista forense, gracias a su capacidad para recolectar y analizar datos de múltiples fuentes, su enfoque en la creación de líneas de tiempo y su integración con otras herramientas.
- Características:

  1. Extrae eventos de múltiples fuentes como logs del sistema, archivos de aplicaciones, etc.
  2. Genera una línea de tiempo detallada para ayudar a identificar actividades sospechosas.
  3. Formato de salida compatible con otras herramientas como ELK Stack o herramientas de visualización.

d) The Sleuth Kit (TSK):

- Tipo de Análisis Forense: De Análisis Electrónico.
- ¿Es sólida desde el punto de vista forense?:

  Aparece en este artículo: Enlace_2.
- Características:

  1. Análisis de particiones y sistemas de archivos.
  2. Soporte para FAT, NTFS, ext2/3, HFS +, entre otros.
  3. Recuperación de datos eliminados y análisis de metadatos.
  4. Funciones para detectar particiones ocultas o datos no asignados.

e) Wireshark:

- Tipo de Análisis Forense: Forense de red.
- ¿Es sólida desde el punto de vista forense?:

  Aparece en estos artículos: Enlace_1 y Enlace_2.
- Características:

  1. Captura de tráfico en tiempo real.
  2. Soporte para cientos de protocolos.
  3. Filtros avanzados de captura y visualización.

f) Autopsy (con módulos de móviles):

- Tipo de Análisis Forense: De Dispositivos móviles.
- ¿Es sólida desde el punto de vista forense?:

  Aparece en estos artículos: Enlace_1 y Enlace_2.
- Características:

  1. Soporte para análisis de imágenes de dispositivos móviles, como datos extraídos por otras herramientas (p.ej., archivos .zip o .tar de dispositivos Android).
  2. Análisis de mensajes de texto, registros de llamadas y ubicaciones GPS.
  3. Extensible a través de módulos.
  4. Interfaz gráfica fácil de usar.
  5. Compatible con Linux y Windows.

g) Volatility:

- Tipo de Análisis Forense: De Adquisición y Análisis de Memoria.
- ¿Es sólida desde el punto de vista forense?:

  Aparece en este artículo: Enlace_1.
- Características:

  1. Soporta múltiples sistemas operativos (Windows, Linux, macOS).
  2. Ofrece una amplia gama de plugins para diferentes tipos de análisis.
  3. Permite la extracción de datos de procesos, conexiones de red, y más.

h) John the Ripper:

- Tipo de Análisis Forense: De Adquisición y Análisis de Memoria.
- ¿Es sólida desde el punto de vista forense?: Es una herramienta sólida y eficaz para el cracking de contraseñas, siendo valiosa en el ámbito de la seguridad informática y en el contexto forense para auditar la seguridad de las contraseñas y recuperar accesos.
- Características:

    1. Soporta múltiples tipos de hash (DES, MD5, SHA-1, SHA-256, etc.).
    2. Métodos de ataque: fuerza bruta, ataques de diccionario, ataques híbridos.
    3. Extensible mediante módulos personalizados.
    4. Interfaz de línea de comandos.
    5. Sistema de detección automática de plataformas.

i) Cuckoo Sandbox:

- Tipo de Análisis Forense: De Análisis de Malware.
- ¿Es sólida desde el punto de vista forense?: Es una herramienta poderosa y flexible para el análisis de malware, proporcionando una plataforma robusta para entender el comportamiento de software malicioso en un entorno seguro. Su capacidad para generar informes detallados, su integración con otras herramientas y su enfoque en el análisis automatizado la convierten en una opción valiosa en el ámbito forense y de ciberseguridad.
- Características:

    1. Análisis de comportamiento de malware.
    2. Informes detallados sobre las acciones realizadas por el malware.
    3. Soporte para diferentes tipos de archivos, incluyendo archivos ejecutables, documentos y scripts.

j) CAINE:

- Tipo de Análisis Forense: Sistemas operativos orientados a informática forense.
- ¿Es sólida desde el punto de vista forense?:

  Aparece en estos artículos: Enlace_1 y Enlace_2.
- Características:

  1. Proporciona un entorno amigable que facilita el uso de herramientas forenses.
  2. Incluye herramientas para análisis de sistemas de archivos, análisis de memoria, recuperación de datos y análisis de tráfico de red.
  3. Permite trabajar con diversas imágenes forenses, facilitando el análisis.
  4. Puede ser ejecutado desde un USB o CD/DVD, ideal para sistemas que no pueden ser iniciados desde el disco duro.
  5. Cuenta con buena documentación y una comunidad activa que ofrece soporte y recursos.

k) Browser History Capturer:

- Tipo de Análisis Forense: De Análisis a navegadores web.
- ¿Es sólida desde el punto de vista forense?: Es una herramienta útil para la recolección y análisis del historial de navegación en investigaciones forenses. Su facilidad de uso, capacidad de capturar datos de múltiples navegadores y opciones de exportación la hacen valiosa en el contexto de análisis de comportamiento en línea.
- Características:

  1. Soporte para navegadores como Chrome, Firefox y Edge.
  2. Extracción de sitios visitados, descargas y búsquedas.
  3. Interfaz fácil de usar y exportación de datos en varios formatos.

l) Autopsy:

- Tipo de Análisis Forense: De funciones específicas: hash y comprobación de integridad.
- ¿Es sólida desde el punto de vista forense?:

  Aparece en estos artículos: Enlace_1 y Enlace_2.
- Características:

  1. La herramienta Autopsy es una de las más utilizadas y recomendadas.
  2. Análisis de sistemas de archivos (NTFS, FAT, ext2/ext3, etc.).
  3. Recuperación de archivos eliminados.
  4. Soporte para la extracción de datos de imágenes de discos.
  5. Incluye herramientas para el análisis de metadatos y time stamps.

m) FTK Imager:

- Tipo de Análisis Forense: Montaje de Discos.
- ¿Es sólida desde el punto de vista forense?:

  Aparece en este artículo: Enlace_2.
- Características:

  1. Creación de imágenes de disco en varios formatos (E01, RAW).
  2. Visualización de contenido de discos y archivos.
  3. Herramientas para análisis de archivos eliminados.

n) PhotoRec:

- Tipo de Análisis Forense: Recuperación de datos.
- ¿Es sólida desde el punto de vista forense?:

  Aparece en este artículo: Enlace_2.
- Características:

  1. Recuperación de más de 400 tipos de archivos.
  2. No requiere instalación; funciona desde una unidad USB.
  3. Capaz de recuperar archivos de sistemas de archivos dañados.

o) Autopsy:

- Tipo de Análisis Forense: Utilidades para el Sistema de Ficheros.
- ¿Es sólida desde el punto de vista forense?:

  Aparece en estos artículos: Enlace_1 y Enlace_2.
- Características:

  1. La herramienta Autopsy es una de las más utilizadas y recomendadas.
  2. Análisis de sistemas de archivos (NTFS, FAT, ext2/ext3, etc.).
  3. Recuperación de archivos eliminados.
  4. Soporte para la extracción de datos de imágenes de discos.
  5. Incluye herramientas para el análisis de metadatos y time stamps.

p) Digital Forensics Framework:

- Tipo de Análisis Forense: Framework Forense.
- ¿Es sólida desde el punto de vista forense?:

  Aparece en estos artículos: Enlace_1 y Enlace_2.
- Características:

  1. Interfaz gráfica de usuario intuitiva que simplifica el proceso de análisis.
  2. Soporte para la adquisición de imágenes forenses de discos y dispositivos móviles.
  3. Módulos para analizar una amplia variedad de formatos de archivo y sistemas de archivos.
  4. Capacidad para crear informes personalizables y detallados sobre los hallazgos de la investigación.