Practica 1
La evidencia digital

Ejercicio 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?

Los datos de contenido se refieren a la información real de que archivo, documento, imagen, video o cualquier otro tipo de dato contiene. Por ejemplo, en un documento de texto, los datos de contenido sería el texto del documento.

Los metadatos son datos que describen otros datos, proporcionan información sobre los datos de contenido. Por ejemplo, los metadatos de una imagen nos pueden indicar el título, el autor, la fecha, la ubicación geográfica.

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

- **Evidencia volátiles**: Son aquellas que cambian con facilidad como puede ser la memoria RAM, cache, tablas de enrutamiento, son las que primeramente tendremos que adquirir puesto que nuestras acciones pueden modificar su valor original y desaparecen al apagar el equipo.
- **Evidencia no volátiles:** No cambian con tanta facilidad, aunque por supuesto nuestras acciden pueden alterar su valor, entre ellas están los discos duros, pendrives, CDs

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

La principal diferencia entre ambas evidencias reside en su formato y medio de almacenamiento. Las diferencias incluyen la vulnerabilidad a la alteración, la cadena de custodia, la autenticación, la trazabilidad, el volumen y la accesibilidad, y la capacidad de búsqueda y recuperación.

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

Es importante que usemos las funciones hash, para verificar que no han sido modificados los datos de la evidencia digital, mantener un registro adecuado de la cadena de custodia, la documentación de metadatos es importante para demostrar la autenticidad de las evidencias y es común contar con testigos que puedan respaldar la autenticidad de las evidencias.

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

- Modelo de Proceso de Adquisición, Preservación, Análisis y Presentación de Evidencia (APAPE)
- Modelo de Proceso de Investigación de Delitos Cibernéticos (Cyber Crime Investigation Process, CCIP)

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

Buscan establecer normas y directrices que ayuden a garantizar la integridad, autenticidad, confiabilidad y legalidad de la evidencia digital recopilada y el proceso de análisis forense.

Ejercicio 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:

Dispositivo	Tipo de datos que almacena	Donde se localizan	Formas de recuperación
Discos duros de almacenamiento en PCs / portátiles	Almacenan una amplia gama de datos, que pueden incluir documentos, correos electrónicos, archivos multimedia, registros de navegación web, contraseñas y registros de actividad	Los datos se almacenan en discos duros, unidades de estado sólido (SSD) y otros dispositivos de almacenamiento	Los datos se recuperan utilizando software forense que permite la copia y el análisis de los contenidos de las unidades de almacenamiento

	del sistema		
Memorias RAM	almacenan datos temporales utilizados por el sistema operativo y los programas en ejecución	se encuentran físicamente en la placa base de una computadora o en la placa principal de otros dispositivos electrónicos, como smartphones y tabletas	se puede recuperar mediante herramientas de adquisición de memoria RAM física o mediante técnicas de volcado de memoria
Libros electrónicos	almacenan principalmente texto, imágenes y, en algunos casos, contenido multimedia como videos o audio	se almacenan en dispositivos electrónicos como eReaders, tabletas, computadoras, teléfonos inteligentes y servidores de libros electrónicos	la forma de recuperación es la extracción de libros electrónicos almacenados en la memoria interna o en tarjetas de memoria
Videoconsolas	almacenan una variedad de datos, que pueden incluir información sobre cuentas de usuario, registros de juego, datos de juego en línea, comunicaciones de chat o voz, y en algunos casos, contenido multimedia como imágenes o videos	se almacenan internamente en el hardware de la propia consola. Esto incluye la unidad de disco duro (en consolas como Xbox y PlayStation), la memoria interna y, en algunos casos, tarjetas de memoria o unidades USB conectadas a la consola	Extracción de datos de la unidad de disco duro, extracción de datos de cuentas en línea, análisis de contenido de juegos y comunicaciones
GPS	almacenan información sobre la ubicación geográfica, la velocidad, la altitud y la dirección en un momento específico	se pueden encontrarse en una variedad de objetos y vehículos, como automóviles, teléfonos móviles, relojes, cámaras, drones y dispositivos de seguimiento personal	extracción de datos del dispositivo, análisis de registros y datos de geolocalización, acceso a registros de ubicación en línea

Televisión	pueden almacenar datos relacionados con el historial de navegación web, aplicaciones descargadas y utilizadas, configuraciones de red, datos de registro de visualización y, en algunos casos, información de cuentas de usuario	se almacenan en su memoria interna, discos duros, tarjetas de memoria o unidades de almacenamiento externas	extracción de datos de la memoria interna o el disco duro, análisis de registros y datos de visualización, acceso a cuentas en línea y servicios de transmisión
Altavoces inteligentes	almacenan comandos de voz y transcripciones de conversaciones, así como registros de actividad que pueden incluir eventos de encendido y apagado, configuraciones de dispositivos domésticos inteligentes y datos sobre aplicaciones y servicios conectados	se almacenan en la nube, en servidores de los fabricantes, y algunos registros de actividad también pueden residir en la memoria interna del propio altavoz	acceso a la cuenta en línea del usuario, acceso a la interfaz de administración del dispositivo, solicitudes legales al fabricante
Localizadores de artículos con control remoto	pueden almacenar información sobre la ubicación de los objetos a los que están unidos	almacenan datos de ubicación y envían señales a través de tecnologías inalámbricas, como Bluetooth o GPS	acceso a la aplicación móvil asociada, seguimiento de señales inalámbricas, datos de ubicación y registros de actividad
Coches inteligentes	almacenan una amplia variedad de datos, como registros de velocidad, frenado, aceleración, datos de navegación, ubicaciones GPS, información del sistema, datos de	pueden residir en diferentes sistemas del vehículo, como el sistema de infoentretenimiento, unidades de control electrónico (ECUs), módulos de control, tarjetas SIM	acceso a las ECUs del vehículo, extracción de datos de la unidad de infoentretenimiento, análisis de cámaras y sistemas de asistencia al conductor

	entretenimiento, historial de mantenimiento, entre otros	integradas o sistemas conectados a la nube que almacenan información de telemetría	
Teléfonos móviles	Almacenan una amplia variedad de datos, como mensajes de texto, llamadas, fotos, videos, contactos, ubicaciones GPS, aplicaciones y registros de navegación	Los datos se encuentran en la memoria interna del dispositivo, así como en tarjetas de memoria externa o en servicios en la nube vinculados	La recuperación de datos se realiza mediante herramientas forenses que extraen datos de dispositivos móviles, como Cellebrite y XRY
Tablets	Almacenan una amplia variedad de datos, como mensajes de texto, llamadas, fotos, videos, contactos, ubicaciones GPS, aplicaciones y registros de navegación	Los datos se encuentran en la memoria interna del dispositivo, así como en tarjetas de memoria externa o en servicios en la nube vinculados	La recuperación de datos se realiza mediante herramientas forenses que extraen datos de dispositivos móviles, como Cellebrite y XRY
Cámara de fotos	almacenan principalmente imágenes y videos	se almacenan en la memoria interna de la cámara o en tarjetas de memoria extraíbles, como tarjetas SD	extracción de datos de la tarjeta de memoria, análisis de metadatos, análisis de las configuraciones de la cámara
CDs, DVDs	Estos dispositivos pueden contener una variedad de archivos, desde documentos hasta medios multimedia	Los datos se almacenan en el propio dispositivo de almacenamiento	e pueden recuperar datos de estos dispositivos utilizando herramientas de software forense o clonando el dispositivo para su análisis posterior
Blurays	almacenan principalmente	se almacenan en el propio disco Blu-ray,	análisis de contenido, extracción y copia

	contenido multimedia, como películas, series de televisión, juegos o archivos de datos de alta definición	que consiste en una capa de grabación óptica	forense, análisis de protección de copia y DRM:
Disquetes	almacenan datos en un formato magnético y generalmente contienen archivos de texto, documentos, imágenes, y en algunos casos, archivos ejecutables de programas o sistemas operativos más antiguos	se almacenan en el disco magnético, que se inserta en la unidad de disquete de un ordenador	unidades de disquete especializadas, transferencia de datos a medios modernos, preservación de datos históricos
Almacenamiento de la nube	pueden contener una amplia gama de datos, incluyendo archivos personales, empresariales, correos electrónicos, documentos, imágenes, videos, bases de datos, registros de actividad, entre otros	se almacenan en servidores remotos, generalmente en centros de datos, que pueden estar ubicados en diferentes regiones o países, dependiendo del proveedor de servicios de almacenamiento en la nube	solicitudes legales y judiciales, acceso a cuentas de usuario, análisis de registros y metadatos

Ejercicio 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:

Tipo de herramienta	Nombre de la herramienta
De Disco y Captura de Datos	EnCase Forensic es una herramienta reconocida y sólida en el campo forense. Ofrece una amplia gama de capacidades, desde la adquisición forense de datos de

	disco hasta el análisis, la indexación, la generación de informes y la presentación de evidencia
Visores de archivos	X-Ways Viewer es una herramienta gratuita proporcionada por X-Ways, el mismo desarrollador del software forense X-Ways Forensics. Este visor permite a los investigadores visualizar y examinar imágenes de disco, archivos y metadatos recopilados con la versión completa del software. Ofrece una visualización detallada de la evidencia, lo que puede ser útil para revisar datos previamente adquiridos
De Análisis de Registro	Splunk es una plataforma que no solo se limita al análisis de registros, sino que es ampliamente utilizada para esta función. Proporciona la capacidad de recopilar, indexar y analizar grandes volúmenes de datos de registros generados por sistemas, aplicaciones y dispositivos
De Análisis electrónico	Nuix es una plataforma avanzada para el procesamiento y análisis de datos electrónicos. Ofrece capacidades para el descubrimiento de hechos, revisión de documentos, análisis de metadatos, búsquedas avanzadas y generación de informes
Forense de Red	Wireshark es una herramienta de código abierto y ampliamente utilizada para el análisis de tráfico de red. Permite la captura y análisis detallado de paquetes de red, lo que es esencial para identificar patrones, detectar actividades maliciosas o analizar la comunicación entre dispositivos
De Dispositivos móviles	Cellebrite UFED es una herramienta líder en el análisis forense de dispositivos móviles. Ofrece capacidades para la adquisición de datos de una amplia gama de dispositivos, incluyendo modelos antiguos y nuevos. Permite la extracción física y lógica de datos, incluyendo mensajes, imágenes, videos, registros de llamadas, información de

	aplicaciones y más
De Adquisición y Análisis de Memoria	Magnet RAM Capture es una herramienta que permite la adquisición de la memoria volátil (RAM) de un sistema. Esta memoria puede contener información crucial, como procesos en ejecución, conexiones de red, claves de cifrado, contraseñas y más
De Recuperación de Contraseñas	Ophcrack es una herramienta de código abierto que se utiliza para recuperar contraseñas de cuentas de usuario en sistemas Windows. Utiliza tablas precalculadas para realizar ataques de fuerza bruta o de tablas arcoíris, lo que le permite recuperar contraseñas basadas en hashes almacenados en el sistema
De Análisis de Malware	Cuckoo Sandbox es una herramienta de análisis automatizado de malware. Permite ejecutar, analizar y monitorear muestras de malware en un entorno controlado. Registra el comportamiento del malware, los cambios realizados en el sistema y las interacciones de red, generando reportes detallados sobre la actividad del malware
Sistemas operativos orientados a informática forense	Kali Linux es una distribución basada en Debian y está diseñada para la seguridad informática y pruebas de penetración. Contiene una amplia gama de herramientas para la informática forense, análisis de seguridad, auditorías y pruebas de penetración. Kali Linux es altamente valorado por su conjunto integral de aplicaciones forenses, lo que lo convierte en una opción popular para profesionales forenses y expertos en seguridad
De Análisis a navegadores web	Forensic Browser es una herramienta especializada que permite la extracción y análisis forense de datos de navegadores web. Ofrece la capacidad de recuperar datos de historiales de navegación, cookies, contraseñas guardadas, datos de formularios y otros detalles relevantes

De funciones específicas: hash y comprobación de integridad	Son funciones hash criptográficas comunes utilizadas para calcular valores hash de archivos o cadenas de datos. MD5, SHA-1 y SHA-256 son algoritmos ampliamente utilizados para calcular hash. Las herramientas como OpenSSL en la línea de comandos o aplicaciones como HashCalc permiten calcular hashes utilizando estos algoritmos
Montaje de Discos	FTK Imager, además de su capacidad para adquirir datos forenses, puede montar imágenes de disco para permitir el acceso a su contenido sin alterar la integridad de la evidencia original. Esto facilita la revisión del contenido y la extracción de datos específicos de la imagen sin modificarla
Recuperación de datos	Recuva es una herramienta popular para la recuperación de datos en entornos forenses. Permite recuperar archivos borrados de discos duros, tarjetas de memoria, unidades USB y otros dispositivos de almacenamiento. Esta aplicación busca archivos eliminados y restaurar aquellos que aún no han sido sobrescritos en el disco
Utilidades para el Sistema de Ficheros	Sleuth Kit es una colección de herramientas de código abierto para el análisis forense. Incluye utilidades como fls (para listar ficheros), icat (para extraer ficheros por su número de i-nodo) y otros programas que permiten examinar sistemas de archivos en busca de evidencia digital. Sleuth Kit es especialmente útil para analizar sistemas de archivos Unix y Windows
Framework Forense	SIFT es un conjunto de herramientas de código abierto y un entorno forense creado por SANS Institute. Proporciona un conjunto completo de herramientas forenses para el análisis de evidencia digital. Incluye herramientas para adquisición de datos, análisis forense de memoria, análisis de malware, visualización de datos, entre otras funcionalidades