Pregunta 1

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

¿Por qué es importante la investigación forense de correo electrónico y redes sociales?

Resolver delitos identificando a los autores y recopilando pruebas. Verdadero

Proteger a los actores con las evidencias que necesitan para buscar injusticia. Falso

Resolver delitos identificando a los criminales y recopilando evidencias. Falso

Proteger a las víctimas de delitos proporcionándoles las pruebas que necesitan para buscar justicia. Verdadero

Prevenir delitos identificando y neutralizando a los delincuentes potenciales. Verdadero

Prevenir crimenes identificando y neutralizando a los autores. Falso

Respuesta correcta

Pregunta 2

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

¿Qué es la extracción manual de los datos en el análisis forense de los dispositivos móviles?

a. El más sencillo de todos los métodos que se usa el teclado o la pantalla táctil para navegar a si no está bloqueado .

b. El más sencillo de todos los métodos, se usa el teclado o la pantalla táctil navegar a través del dispositivo y buscar la información relacionada con el caso.

c. Son métodos no faciles que se usa el teclado o la pantalla táctil navegar a través del dispositivo (si no está bloqueado) y buscar la información relacionada con el caso.

Respuesta correcta

Pregunta 3

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

Fases del análisis forense:

Adquisición: Se obtienen copias de la información sospechosa que puede estar vinculada con algún incidente.

Preservación: Se garantiza que la información recopilada este completamente salvaguarda con la finalidad de que dicha información no sea alterada.

Análisis: Es la parte más compleja, debido a que se necesita software, hardware y técnicas específicas para la investigación forense

Documentación: Se debe anexar toda la información recolectada con una lógica establecida entre las pruebas que se han obtenido.

Presentación: Es la forma en cómo se presenta la documentación que debe soportar el escrutinio legal y guiarse por el método procedimental.

Respuesta correcta

Pregunta 4

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

ISO 27035-3 – Fase de recuperación y aprendizaje

- Restaurar los sistemas y datos afectados: Esto implica restaurar los sistemas y datos a su estado anterior al incidente.
- Revisar el proceso de respuesta a incidentes: Es importante revisar el proceso de respuesta a incidentes para identificar áreas de mejora.
- Aprender del incidente y actualizar los planes de respuesta: Las lecciones aprendidas del incidente deben usarse para actualizar los planes de respuesta a incidentes.

Respuesta correcta

Pregunta 5

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

Componentes del estándar ISO 27035

- ISO/IEC 27035-1: Principios de gestión de incidentes
- ISO/IEC 27035-2: Pautas para planificar y preparar la respuesta ante incidentes
- ISO/IEC 27035-3: Directrices para las operaciones de respuesta a incidentes

Respuesta correcta

Pregunta 6

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

Un bloqueador contra escritura es una herramienta (hardware o software) que impide la escritura sobre un dispositivo de almacenamiento.

- Verdadero
- Falso

Pregunta 7

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

¿El comando es correcto para realizar una copia exacta del contenido para adquirir la evidencia digital forense?

dd if=origen of=destino bs=1k conv=noerror,sync status=progress

- Verdadero
- Falso

Pregunta 8

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

¿Qué permite el sistema de archivos de altas prestaciones?

- a. Nombres largos, Metadatos, Información de seguridad, Comprobación, Información estructural
- b. Nombres largos, Metadatos, Información de seguridad, Autocomprobación, Información estructural
- c. Nombres pequeño, Metadatos, Información de inseguridad, Autocomprobación, Información estructural
- d. Nombres largos, Metadatos, Información de inseguridad, Autocomprobación, Información desestructural

Respuesta correcta

Pregunta 9

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

Ventajas y desventajas del sistema de archivos FAT

Tiende a dejar fragmentos de los archivos borrados (ralentiza las operaciones)	Desventaja
File Allocation Table (Tabla de asignación de archivos)	Ventaja
No es redundante a fallos (puede dejar al sistema en un estado incongruente)	Desventaja
Aceptado en la mayoría de SO	Ventaja
Es muy popular en la gestión de discos y memorias externas	Ventaja
Usa una tabla de asignación de archivos	Ventaja
Sistema sencillo de archivos	Ventaja
Diseñado para archivos de tamaño reducido	Desventaja
No soporta permisos de seguridad	Desventaja

Respuesta correcta

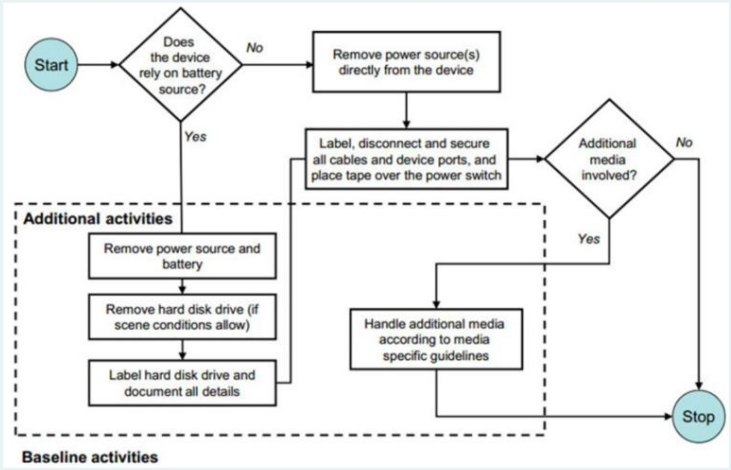
Pregunta 10

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

Explique con sus palabras que hace la recolección de evidencias digitales forense en Frío con esta imagen.



La recoleción de evidencial digitales forenses en frio segun la informatica forense es fundamental cuando nos enfrentamos a dispositivos apagados,tiene como objetivo principal preservar la integridad de la información evitando cualquier modificación que pueda ocurrir si esque el dispositivo se encendiera, con base en la imagen esta demuestra que este proceso inicia evaluando una condicion para determinar si el dispositivo depende de una batería caso contrario se procede a retirar directamente las fuentes de alimentación de energia, si uaa batería, se realizan pasos adicionales como remover la batería y de ser posiblese retira el disco duro.

En los 2 casos se etiquetan, se desconectan y aseguran todos los cables y puertos del equipo ademas se coloca cinta aislante sobre el interruptor de encendido para evitar activarlo accidentalemente, si esque hay medios de almacenamiento adicionales involucrados como discos externos o tarjetas de

Pregunta 11

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

La evidencia digitale es toda información digitalizada no suceptible de ser analizada por un método tradicional y de conclusiones refutables en la parte legal

- Verdadero
- Falso

Pregunta 12

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

¿Cuál es el sistema operativo que viene preinstalado los paquetes para el análisis forense de los dispositivos móviles?

Respuesta: Santoku Linux

Pregunta 13

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

Un sistema de archivos proporciona una forma de separar los datos de la unidad en piezas individuales, conocidos como archivos.

- Verdadero
- Falso

Pregunta 14

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

¿Qué sistema de archivos es optimizado para las memorias flash?

Respuesta: exFAT

Pregunta 15

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

Para que se establece un enfoque estructurado y planificado en el ISO 27035:

a.
- Informar y evaluar los incidentes de seguridad de información;
- Responder a incidentes de seguridad de la información;
- Detectar y gestionar las vulnerabilidades de seguridad de la información,
- Mejorar continuamente la seguridad de la información y la gestión de incidentes.

b.
- Detección y evaluación los incidentes de seguridad de información.
- Gestión incidentes de seguridad de la información.
- Detectar, evaluar y gestionar las vulnerabilidades de seguridad de la información,
- La seguridad de la información y la gestión de incidentes no son mejorados, como resultado de la gestión de seguridad de la información y las vulnerabilidades.

c.
- Detectar, informar y evaluar los incidentes de seguridad de información;
- Responder a incidentes y gestionar incidentes de seguridad de la información;
- Detectar, evaluar y gestionar las vulnerabilidades de seguridad de la información,
- Mejorar continuamente la seguridad de la información y la gestión de incidentes, como resultado de la gestión de seguridad de la información y las vulnerabilidades.

Respuesta correcta

Pregunta 16

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

Parámetros en la fase de documentación

- Propósito: Definir su propósito a que publico va dirigido y su objetivo
- Autores: Con su responsabilidad y contacto
- Resumen de Incidentes: Explicación de forma sencilla
- Pruebas: Incluir una descripción de las pruebas adquiridas.
- Detalles: Detallar cada uno de los pasos realizados
- Justificar: Justificando cada conclusión extraída del análisis
- Conclusión: Ser claros y resumidos
- Glosario: Para un mayor entendimiento para el público.

Respuesta correcta

Pregunta 17

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

Propiedades de las funciones hash

Bajo coste computacional:

No consume muchos recursos y se puede realizar en cualquier equipo y en un tiempo reducido.

Compresión:

Se tiene pocos caracteres hexadecimales, y es más manejable que la entrada.

Inyectividad:

Para cada entrada se genera un hash diferente. Lo ideal es que además sea único, pero está limitada la salida, por lo que habrá repeticiones.

Unidireccionalidad:

Es de un solo sentido, esto es, con una entrada A tenemos un resultado B, pero con B no podemos inferir A de nuevo.

Determinista:

Con una entrada A la salida siempre va a ser el mismo conjunto de caracteres B.

Resistente a colisiones:

Resistente a colisiones quiere decir que podemos encontrar dos entradas diferentes con la misma salida.

Respuesta correcta

Pregunta 18

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

El método de borrado seguro es consiste en la sobreescritura de la información original con ceros, aunque también es posible sobrescribirla con cualquier otro valor o valores aleatorios.

- (●) Verdadero
- ( ) Falso

Pregunta 19

Finalizado

Se puntúa 0,00 sobre 2,00

Marcar pregunta

¿En qué se enfoca el delito informático?

Ocultamiento de información

Destruir, dañar ordenadores o medios electrónicos

Infectar con malware un equipo

==========

Uso de evidencias forenses

Robar datos no sensibles

Esquivar la detección de algún evento

Respuesta incorrecta.

Pregunta 20

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

¿Por qué motivo se necesita el sistema de archivos swap?

- ( ) a. Cargar los programas y no saturar la memoria ROM
- ( ) b. Cargar el sistema operativo y no saturar la memoria Flash
- ( ) c. Cargar los librerías y saturar la memoria RAM
- (●) d. Cargar los programas y no saturar la memoria RAM

Respuesta correcta

Pregunta 21

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

Define los 5 puntos como principios para el manejo y recolección de evidencia computacional.

- ( ) a.
  - Recolectar evidencia digital, las acciones tomadas deben cambiar por ningún motivo esta evidencia.
  - El único que tiene acceso a la evidencia el juez
  - Todo debe ser documentado completamente, preservada y disponible para la revisión.
  - Un individuo no es responsable de todas las acciones tomadas con respecto a la evidencia digital
  - Cualquier agencia es responsable de cumplir estos principios.
- ( ) b.
  - Recolectar evidencia digital, las acciones tomadas no deben cambiar por ningún motivo esta evidencia.
  - El único que tiene acceso a la evidencia el profesional forense
  - Los documentado preservados y disponible para la revisión.
  - Un individuo es irresponsable de todas las acciones tomadas con respecto a la evidencia digital
  - Cualquier agencia es responsable de cumplir estos términos.
- (●) c.
  - Recolectar evidencia digital, las acciones tomadas no deben cambiar por ningún motivo esta evidencia.
  - El único que tiene acceso a la evidencia el profesional forense
  - Todo debe ser documentado completamente, preservada y disponible para la revisión.
  - Un individuo es responsable de todas las acciones tomadas con respecto a la evidencia digital
  - Cualquier agencia es responsable de cumplir estos principios.

Respuesta correcta

Pregunta 22

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

¿Cómo puedo implementar la ISO 27035-3?

a.
- Establecer un procedimiento de respuesta a incidentes
- Identificar los roles y responsabilidades de los miembros del equipo de respuesta a incidentes
- Capacitar al juez en la gestión de incidentes
- Implementar herramientas y tecnologías de respuesta a incidentes
- Probar regularmente el plan de respuesta a incidentes

b.
- Establecer una política y un procedimiento de respuesta a incidentes
- Identificar las responsabilidades de los miembros del equipo de respuesta a incidentes
- Capacitar al usuario en la gestión de incidentes
- Implementar herramientas y tecnologías de respuesta a incidentes
- Probar el plan de respuesta a incidentes dos veces

c.
- Establecer una política y un procedimiento de respuesta a incidentes
- Identificar los roles y responsabilidades de los miembros del equipo de respuesta a incidentes
- Capacitar al personal en la gestión de incidentes
- Implementar herramientas y tecnologías de respuesta a incidentes
- Probar y revisar regularmente el plan de respuesta a incidentes

Respuesta correcta

Pregunta 23

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

Qué actividades cubre la ISO 27035-3?

a.
- Identación y análisis de incidentes
- Contención y erradicación de incidentes
- Recuperación y enseñanza posterior al incidente
- Comunicación y gestión de partes interesadas
- Mejora del proceso de respuesta a incidentes

b.
- Identificación y gestión de incidentes
- Contención y aprendizaje de incidentes
- Recuperación y erradicación posterior al incidente
- Comunicación y análisis de partes interesadas
- Mejora continua del proceso a incidentes

c.
- Identificación y análisis de incidentes
- Contención y erradicación de incidentes
- Recuperación y aprendizaje posterior al incidente
- Comunicación y gestión de partes interesadas
- Mejora continua del proceso de respuesta a incidentes

Respuesta correcta

Pregunta 24

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

Una función hash es una metodología matemática computable mediante un algoritmo que tiene como entrada la información contenida en la evidencia y que genera como salida un conjunto de elementos de evidencia finita

- Verdadero
- Falso

Pregunta 25

Finalizado

Se puntúa 2,00 sobre 2,00

Marcar pregunta

Computación forense es una rama de las ciencias forenses que analiza, preserva y presenta los datos procesados electrónicamente y almacenados en un medio digital forense.

- Verdadero
- Falso