| DATOS PERSONALES | FIRMA |
| --- | --- |
| |  |  | | --- | --- | | Nombre: Edwin Mauricio | DNI: 0801199522118 | | Edwin |
| Apellidos: Gonzalez Sierra |

| ESTUDIO | ASIGNATURA | CONVOCATORIA |
| --- | --- | --- |
| MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD (PLAN 2022) | 14132.- INFORMÁTICA FORENSE Y RESPUESTA ANTE INCIDENTES | Ordinaria Número periodo 9197 |

| FECHA | MODELO | CIUDAD DEL EXAMEN |
| --- | --- | --- |
| 12-17/07/2024 | Modelo - E | Tegucigalpa |

| Etiqueta identificativa |
| --- |
|  |

**INSTRUCCIONES GENERALES**

1. **Lee atentamente** todas las preguntas antes de empezar.
2. La duración del examen es de **2 horas**.
3. Escribe únicamente con **bolígrafo azul o negro**.
4. No está permitido utilizar más hojas de las que te facilita la UNIR (puedes utilizar folios para hacerte esquemas u organizarte pero **no se adjuntarán al examen**).
5. **El examen**PRESENCIAL **supone el 60%** de la calificación final de la asignatura. Es necesario aprobar el examen, para tener en cuenta la evaluación continua, aunque esta última sí se guardará para la siguiente convocatoria en caso de no aprobar.
6. No olvides **rellenar EN TODAS LAS HOJAS los datos del cuadro** que hay en la parte superior con tus datos personales.
7. El **DNI/NIE/PASAPORTE debe estar sobre la mesa**y disponible para su posible verificación.
8. **Apaga el teléfono móvil**.
9. Las preguntas se contestarán en **CASTELLANO**.
10. Si en alguna de las respuestas se **detecta**un caso de **copia** de los materiales de la asignatura, de cualquier otra fuente (por ejemplo, Internet) o de otros compañeros, se va a calificar el **examen**con **0** puntos.

**Puntuación**

**Preguntas tipo test**

* Puntuación máxima 2.50 puntos
* Cada pregunta vale 0.25 puntos

**Supuestos prácticos**

* Puntuación máxima 7.50 puntos
* Cada pregunta vale 2.50 puntos

Preguntas tipo test

* Las respuestas erróneas NO restan
* Sólamente hay una opción válida en cada pregunta

**1.** Las principales características de un informe pericial deben ser:

1. Claridad, Concisión, Fundamentación y Justificación
2. Claridad, Fundamentación y Justificación
3. Claridad, Concisión y Justificación
4. Claridad, Concisión y Fundamentación

**2.** ¿Que debemos detallar en un informe pericial?

1. El procedimiento realizado por los peritos y sus resultados
2. El procedimiento realizado por los peritos, el resultado se detalla únicamente en sede judicial
3. El equipo utilizado por los peritos, el procedimiento y resultados, únicamente en sede judicial
4. Ninguna de las anteriores es correcta

**3.** Los métodos avanzados de adquisición más comúnmente utilizados son:

1. Jtag, Direct Chip y eMMC Off
2. Jtag Off, Direct Chip y eMMC
3. Jtag, Direct eMMC y Chip Off
4. Jtag y Direct eMMC

**4.** La adquisición de evidencias NO volátiles

1. Una evidencia no volátil no puede ser adquirida pues se degradaría
2. Se realiza en "frío" o en "caliente" en función de diversos factores
3. Se realiza siempre en "caliente"
4. Ninguna de las anteriores es correcta

**5.** ¿Cuales son las etapas de un análisis forense?

1. Recolectar, reservar y presentar
2. Recolectar, preservar y presentar
3. Recolectar, reservar, preservar, analizar y presentar
4. Recolectar, preservar, analizar y presentar

**6.** ¿A qué fase del análisis pertenece la identificación de volúmenes cifrados?

1. La identificación de volúmenes cifrados no pertenece a ninguna de las fases presentes en un análisis forense.
2. A la fase del Post-Análisis
3. A la fase de Pre-Análisis
4. A la fase de análisis

**7.** Atendiendo a la definición dada en los apuntes, ¿Qué es un sistema de ficheros?

1. Es la forma en que se organiza y mantiene la jerarquía de ficheros.
2. Es la forma en que se organiza y gestiona la jerarquía de ficheros.
3. Es la forma en que se organiza, gestiona y mantiene la jerarquía de ficheros.
4. Ninguna de las anteriores es correcta

**8.** ¿Cuál de las siguientes no es una particularidad de las tarjetas SIM?

1. Poca capacidad de almacenamiento de información
2. Puede contener contactos
3. Contiene datos multimedia
4. Podemos obtener los códigos ICCID

**9.** Con respecto a las evidencias no volátiles...

1. Son aquellas que cambian con facilidad
2. Deben ser las primeras en ser adquiridas
3. Desaparecen al apagar el equipo
4. Ninguna de las anteriores es correcta

**10.** Cuál de los siguientes no es un apartado de los indicados por la normativa UNE 197010 que deben aparecer en todos los informes periciales:

1. Identificación
2. Declaración de imparcialidad
3. Reverso
4. Conclusiones

## PLANTILLA DE RESPUESTAS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Preguntas / Opciones | 1 | 2 | 3 | 4 |
| 1 | X |  |  |  |
| 2 |  | X |  |  |
| 3 |  |  | X |  |
| 4 |  |  | X |  |
| 5 |  |  |  | X |
| 6 |  |  |  | X |
| 7 |  |  | X |  |
| 8 |  |  | X |  |
| 9 |  |  | X |  |
| 10 |  |  | X |  |

Supuestos prácticos

**1. ¿Cómo analizarías un terminal Android en Autopsy? ¿Qué pasos seguirías y qué podrías analizar con el plugin "Android Analyzer"? (Responder en 1 caras)**   
**R//** Primero realizaria una imagen al dispositivo con herramientas como magnet acquire y guardaria los hashes para garantizar la integridad del archivo, luego analizaria esta imagen con autopsy y determinaria datos importantes de la investigacion, con el plugin android analyzer, colocaria el dispositivo en modo de recuperacion y accederia a el obteniendo datos importantes como aplicativos de interes, acciones realizadas.  
  
**2. Explica las diferencias entre la adquisición JTAG y Direct eMMC (Responder en 1 caras)**

**R// JTAG es el metodo de adquisicion avanzado menos intrusivo, que consiste en realizar** microsoldaduras en el microchip y de este modo acceder a los datos, este proceso puede llegar a tardar hasta 24 horas en recolectar toda la informacion, a diferencia del metodo Direct eMMC, ya que se accede directamente a la memoria del dispositivo sin acceder al CPU, lo que puede agilizar mas el proceso de adquisicion, sin embargo, es mas intrusivo que el metodo JTAG por lo que se corre aun mas el riesgo de dejar inutilizado el dispositivo si no se realizado con los debidos cuidados.  
  
  
**3. En los apuntes se describen una serie de factores importantes a la hora de decantarnos por una adquisición "en caliente" o "en frío". Atendiendo a los mismos, así como también a la manera descrita para proceder durante una adquisición, responda a las siguientes cuestiones para el escenario planteado: ¿Qué tipo de adquisición realizaría?, ¿Por qué? y ¿Qué pasos seguiría para realizar dicha adquisición?  
  
ESCENARIO:Nos personamos en el domicilio de un hacker que se sospecha ha realizado un robo de criptomoneda. En dicho domicilio encontramos un ordenador encendido y nos percatamos que está ejecutando una distro de Linux en formato live sin que el ordenador posea disco duro alguno. Además, encontramos otro equipo apagado y diversos pendrives. (Responder en 1 caras)**

**¿Qué tipo de adquisición realizaría?**

R// Realizaria una adquisicion en caliente.

**¿Por qué?**

R// Para tomar la decisión del tipo de adquisicion, hay que poner atencion en los siguientes detalles:

* + - 1. Version live de linux
      2. No hay disco duro en el computador

Al ejecutar un sistema operativo en version live no hay escritura en un dispositivo de almaceramiento, solo contamos con la informacion volatil, por esta razon al apagar el equipo perderiamos toda la informacion del incidente.

**¿Qué pasos seguiría para realizar dicha adquisición?**

R// Primero acordonaria el area para garantizar que la evidencia fisica no ha sido manipulada, procederia a realizar una imagen en caliente del dispositivo encendedido y posterior realizaria imágenes del equipo apagado y del pendrive, asi mismo, resguardaria los 3 hashes de cada imagen obtenida para garantizar la integridad las mismas, una vez resguardado y procederia a realizar el analis de las imágenes y obtener programas, direcciones IP, direcciones de correo para poder realizar el analis de manera efectiva.