Prepara tu examen de AFI

Introducción

Cada centro, cada año y cada docente, puede plantear al alumnado un modelo de examen concreto que, a su criterio, pueda servir como una correcta evaluación del módulo.

Para ayudar a preparar las evaluaciones, he pensado que podría ser de ayuda crear un archivo único para cada módulo, que pueda crecer cada año con el feedback y apoyo de la comunidad, con cuestionarios de todo tipo, con solucionario o solo los enunciados, pues la intención primera es poder ofrecer una idea de lo que podemos encontrarnos a la hora de una evaluación, poder aprender con ello, y no algo que una persona acabe memorizando, y esperando, sin comprender ni ahondar en la materia, que aparezca mágicamente en el examen.

Este documento, por tanto, no pretende ser una guía única y veraz de exámenes pasados o futuros, pero si una fuente de información sobre la que basar vuestros estudios.

Posibles modelos.

Modelo 1.

1. ¿Cuál de las siguientes no es una fase del análisis forense?

a. Presentación
b. Identificación
c. Construcción
d. Adquisición
e. Preservación

2. El objetivo fundamental del análisis forense es poder responder varias preguntas "When, Where, What, Why y _____"

3. A nivel general nuestro proceso forense debe cumplir las siguientes características: Reproducible, Independiente, Verificable y _____

4. Señala el elemento con mayor volatilidad

a. Tabla conexiones TCP
b. Tabla conexiones UDP
c. Registros BBDD
d. Fichero /var/logs/syslog .
e. Memoria RAM
f. Tabla ARP
g. Fichero c:/profile.sys

5. ¿Cuáles de las siguientes afirmaciones son falsas respecto a la cadena de custodia de una evidencia?

a. El objetivo de la cadena de custodia es garantizar la exacta identidad de lo incautado y de lo analizado
b. Cada persona que tiene contacto con la evidencia se convierte en un eslabón garante de su resguardo
c. El debate sobre la cadena de custodia se centra en su validez
d. Marcado de tiempo (timestamp) de cuándo se recoge y quién recoge la evidencia
e. En una ruptura de la cadena custodia es suficiente con el planteamiento de dudas de carácter genérico

6. A nivel forense la cronología de sucesos se denomina _____

7. A efectos de Análisis Forense de un dispositivo móvil apagado, ¿cuáles de las siguientes memorias serían de mayor utilidad?

a. Registros microprocesador
b. Memoria Secure Digital (SD)
c. Memoria RAM
d. Memoria NAND
e. Memoria ROM

8. ¿Cuáles de las siguientes herramientas utilizarías para realizar una extracción chip-off de un dispositivo móvil?

a. Cellebrite
b. iSeasamo Phone Opening Tool
c. EDEC Eclipse
d. Autopsy
e. Project-A-Phone

9. El método de extracción de datos de un dispositivo móvil que consiste en la extracción física del Chipset de memoria para transformarlo en una imagen binaria para ser analizada se denomina

a. STAC
b. HexDump
c. ChipDump
d. HexOff
e. Extracción Micro
f. Ninguna de las anteriores

10. ¿Cuáles de las siguientes son un tipo de servicios en la nube?

a. NaaS
b. SaaS
c. IaaS
d. CaaS
e. PaaS

11. Dentro de la UE se ha promulgado una ley relacionada con la protección y la privacidad de los datos denominada:
a. Cloud
b. LOPD
c. GDPR
d. Patriot
e. Ninguna de las anteriores

12. La fase de análisis forense en la nube que más dificultades plantea a nivel legal y logístico es la fase de _____

13. ¿Cómo se denomina el servicio cloud que cuando como contratados podemos pedir en todo momento, dónde, cuándo y quién ha almacenado, accedido y procesado los datos que alojo en el cloud? _____

14. Señala cuales de las siguientes afirmaciones son falsas sobre el análisis forense en el IoT

a. No hay definido una metodología y un marco para el análisis forense de IoT
b. Una amplia gama de dispositivos diferentes dificulta tener una estandarización para la recopilación de las evidencias
c. Los sistemas de ficheros pueden no estar estandarizados
d. Los dispositivos pueden tener sistemas operativos cerrados
e. Todas las anteriores son verdaderas

15. Señala los riesgos que tenemos al realizar un Análisis Forense de un dispositivo IoT
a. Sistema operativo no documentado
b. Conectores estándar
c. Falta de mecanismos de seguridad que permitan el borrado de eventos
d. Mecanismo de prevención de acceso a información sensible de usuarios no investigados
e. Bases legales establecidas para admitir las evidencias en proceso judicial
f. Todas las anteriores son falsas

16. Para poder garantizar la validez de la evidencia de un dispositivo IoT en un proceso judicial debemos asegurarnos de que no hay fallos en el seguimiento fiable de la fuente y en _____

17. Una herramienta que nos permite realizar ingeniería inversa y extraer imágenes de firmware de dispositivos IoT es _____

18. Las características que tiene que tener un informe forense son: Reproducible, Correcto, Completo, Verdadero y _____

19. ¿Qué punto faltaría incluir en un informe forense que ya tiene estos puntos? Resumen ejecutivo, Alcance, Antecedentes, Investigación, Conclusiones, Anexos

20. Señala las afirmaciones falsas sobre las recomendaciones generales al realizar un informe forense
a. En el informe no hace falta economizar el uso de palabras
b. Podemos hacer referencias a aspectos fuera del alcance definido
c. El informe ejecutivo se hace al final, partiendo de las conclusiones finales
d. Debemos tener en cuenta siempre la Ley de Enjuiciamiento Civil