Examen para AFI01.

Intento 1.

Pregunta 1

El análisis inicial de la situación, incluido el análisis minucioso del escenario tiene lugar en la fase de:

a. Procesado de evidencias.
b. Investigación.
c. Identificación.
d. Adquisición.

Pregunta 2

La cadena de custodia de las evidencias no tiene en cuenta las personas que han analizado la evidencia, pero no la han modificado. ¿Verdadero o falso?

Seleccione una:

Verdadero
Falso

Pregunta 3

¿Cuáles son las principales fuentes de información?:

a. Dispositivos físicos y fuentes lógicas.
b. Discos duros.
c. Dispositivos móviles.
d. Discos duros y dispositivos móviles.

Pregunta 4

¿Qué se considera vital para hilar todos los hechos y evidencias de una investigación?:

a. Cadena de custodia.
b. Metodología exhaustiva.
c. Detalles de la fase de identificación.
d. Timeline.

Pregunta 5

Los analistas forenses suelen llevar sus herramientas lógicas en portátiles o discos externos. ¿Verdadero o Falso?

Seleccione una:

Verdadero
Falso

Pregunta 6

¿Qué pasa si no se preserva la cadena de custodia?:

a. Que sería ilegal.
b. Que nos estaremos saltando varias fases y procesos.
c. Que no podremos responder las preguntas de manera correcta.
d. La evidencia podría ser impugnada.

Pregunta 7

¿Cuál es la información que se considera más volátil?:

a. Registros de CPU.
b. Memoria RAM.
c. Registros de accesos.
d. tabla ARP.

Pregunta 8

En una investigación forense deberemos de responder las siguientes preguntas:

a. ¿Qué motivación había?.
b. Todas las anteriores.
c. ¿Qué ha sucedido?.
d. ¿Dónde ha sucedido?.

Pregunta 9

Necesitaremos de herramientas especificas tanto físicas como lógicas en el análisis forense. ¿Verdadero o Falso?

Seleccione una:

Verdadero
Falso

Pregunta 10

¿Qué debemos de hacer cuando encontramos algo que nos llama la atención en un escenario forense?:

a. Avisar a las autoridades.
b. Comentarlo con el compañero.
c. Anotarlo.
d. Discernir en ese momento si es relevante o no.

Intento 2.

Pregunta 1

Existen 4 principales fases dentro del análisis forense. ¿Verdadero o falso?

Seleccione una:

Verdadero
Falso

Pregunta 2

Las fuentes de información no tienen que estar relacionada con las preguntas que debemos responder. ¿Verdadero o falso?

Seleccione una:

Verdadero
Falso

Pregunta 3

¿Cuál ha sido uno de los factores del crecimiento de la necesidad de forenses informáticos?:

a. Auge de los dispositivos móviles.
b. Transformación digital.
c. Aumento de aplicaciones y servicios.
d. Todas las anteriores.

Pregunta 4

A nivel de herramientas físicas necesitaremos:

a. Cables y conectores.
b. Baterías externas.
c. Palancas.
d. Cajas.

Pregunta 5

¿Qué elementos mínimos debe de tener el documento de cadena de custodia?:

a. Identificación unívoca.
b. Registro de control.
c. Código fuente.
d. Línea de tiempo.

Pregunta 6

Un forense a nivel informático tiene mucha de la base de los forenses tradicionales (metodología, preguntas a responder, etc.). ¿Verdadero o Falso?

Seleccione una:

Verdadero
Falso

Pregunta 7

¿Qué punto es necesario en nuestro informe?:

a. Resumen ejecutivo.
b. Nuestra opinión.
c. Informes de cadena de custodia.
d. Detalle de las evidencias analizadas.

Pregunta 8

¿Qué deberemos hacer como prioridad de la fase de Identificación?:

a. Saber que miembros del equipo trabajarán con nosotros.
b. Anotar las fuentes de información que pudiéramos considerar interesantes.
c. Eliminar cualquier elemento que pudiera distraernos.
d. Someter a una verificación exhaustiva todas las evidencias.

Pregunta 9

No es necesario conocer o investigar cuanto tiempo ha estado el atacante dentro de la organización. ¿Verdadero o falso?

Seleccione una:

Verdadero
Falso

Pregunta 10

Cuando investigamos un incidente a nivel forense deberemos:

a. Comprar las herramientas necesarias.
b. Tener clara la metodología y las fases necesarias.
c. Comentar los detalles del caso con amigos y familiares.
d. Avisar a nuestros compañeros de nuestra nueva asignación de tarea.