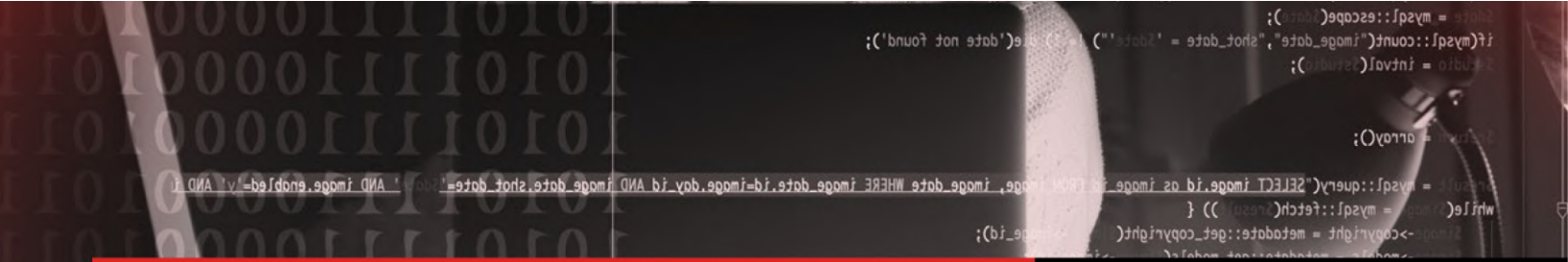

EC-COUNCIL | ASSOCIATE

pue

OBJETIVOS DEL EXAMEN CYBER FORENSICS ASSOCIATE

1 Análisis

- **1.1** Analizar imágenes forenses
- **1.2** Aplicar los conceptos necesarios para utilizar herramientas forenses
- **1.3** Aplicar análisis básicos de malware utilizando técnicas y herramientas forenses aceptadas por el NIST
- **1.4** Identificar técnicas anti forenses
- **1.5** Determinar el contenido importante de los registros de evento durante el análisis forense

2 Descrubrimiento

- **2.1** Aplicar los conceptos necesarios para detectar un mensaje oculto dentro de una imagen
- **2.2** Analizar una conversación entre dos dispositivos finales mediante un archivo PCAP
- **2.3** Verificar que los dispositivos están en el mismo estado en que se encontraron
- **2.4** Determinar cómo reunir evidencias mediante técnicas forenses
- **2.5** Aplicar los conceptos necesarios para descubrir evidencias en distintos sistemas de ficheros
- **2.6** Aplicar los conceptos necesarios para reunir evidencias en diferentes sistemas operativos
- **2.7** Identificar información relevante en una captura de red
- **2.8** Dado un escenario, recopilar evidencias de un delito cometido mediante correo electrónico

3 Evidencia

- **3.1** Determinar y recopilar los tiempos de inicio y cierre de sesión de un determinado usuario
- **3.2** Verificar la autenticidad de las evidencias
- **3.3** Resumir el manejo adecuado de la evidencia
- **3.4** Resumir el proceso de creación de una imagen de audio mediante técnicas de análisis forense
- **3.5** Aplicar la recopilación de evidencias a la cadena de custodia
- **3.6** Discriminar entre una adquisición en tiempo real y una adquisición estática

4 Documentación y reportes

- **4.1** Aplicar metodologías de investigación forense
- **4.2** Identificar y validar una lista de contactos de emergencia para la respuesta a incidentes
- **4.3** Analizar una escena y determinar qué se debe documentar de manera visual
- **4.4** Notificar hallazgos en un análisis de malware
- **4.5** Identificar los elementos de un informe forense completo
- **4.6** Comunicar los resultados de una investigación a un equipo interno

5 Fundamentos de la ciberseguridad forense

- **5.1** Identificar distintos tipos de delitos cibernéticos
- **5.2** Comunicar los incidentes y los procesos de respuesta
- **5.3** Diferenciar entre esteganografía y criptografía

CFA™

CYBER FORENSICS ASSOCIATE