



OXYGEN FORENSICS



Distribuidor certificado:

TAMCE

www.tamce.net

oxygen@tamce.net

 [Tamce.contramedidas](https://www.facebook.com/Tamce.contramedidas)

Certificación Examinador Oxygen Forensic® (OFCE)

Los estudiantes obtendrán los conocimientos sobre el uso de Oxygen Forensic® Detective. El curso suma el curso Básico y Experto al introducir métodos avanzados de recolección de dispositivos inteligentes y análisis de datos. Los estudiantes examinarán y recopilarán datos de dispositivos inteligentes iOS, Android y Windows Phone. Los estudiantes trabajarán para obtener imágenes físicas, comprender los formatos del sistema de archivos, los métodos de almacenamiento y las ubicaciones de las pruebas. Los estudiantes reciben capacitación e instrucción sobre almacenamiento en la nube y técnicas de extracción utilizando Oxygen Forensic® Detective. Los datos de la base de datos SQLite son extremadamente importantes para los análisis actuales de dispositivos inteligentes. Los estudiantes no solo recibirán capacitación sobre el formato de la base de datos SQLite y la creación de consultas SQL, sino que también se cubrirán las Listas de propiedades, la recuperación de datos eliminados, los registros de escritura anticipada, los archivos de memoria compartida y la interpretación de los artefactos de la base de datos utilizando el Visor SQLite y las herramientas secundarias.

Objetivos del curso

- Obtener un amplio conocimiento sobre los dispositivos inteligentes actuales, incluidos iOS, Android y Windows Phone.
- Comprender los formatos del sistema de archivos y los tipos de datos que se encuentran en los principales dispositivos inteligentes.
- Proporcionar información a los estudiantes para ayudarlos a localizar, procesar y recuperar artefactos del sistema de archivos del dispositivo inteligente.
- Obtenga los conocimientos necesarios para crear consultas SQL avanzadas para recuperar datos de aplicaciones no compatibles y archivos de caché dentro del sistema de archivos del dispositivo inteligente.
- Los estudiantes obtendrán valiosos conocimientos durante la capacitación que les ayudará a aprobar un examen de certificación.



Tema

Desarrollo

Historia e introducción rápida	CDMA/GSM Legal Técnicas de aislamiento Seguridad del Dispositivo
Diferentes formas de conectarse a un dispositivo móvil	Cable Bluetooth JTAG
Solución de problemas	Drivers Conexiones ADB
Passwords	iOS Android Blackberry
Extracciones lógicas / físicas de dispositivos inteligentes	Diferencias Representación de datos
Respaldo e Importación de Imágenes de Dispositivos Móviles	iTunes Android JTAG Other Forensic Solutions
Informes básicos	Crear informes básicos de en diferentes formatos
Extracción de Múltiples Dispositivos	iOS Android
Casos	Crear Casos, Eliminar Casos, Guardar Casos Extracción Importar imágenes
Análisis de Aplicaciones	Análisis de información de las apps
Key Evidence	Marcadores
Datos y grupos agregados	Contactos Fusionar / No Fusionar
Analítica	Análisis social Análisis de enlaces Línea de tiempo

Busqueda	Texto Expresiones Comunes Numeros
Reportes Avanzados	HTML PDF Imágenes asociadas Evidencia clave
Obtención de datos del sistema de archivos	iOS Android Windows Phone
Tipos de Archivos de Sistema	iOS Android Windows Phone
Recuperando artefactos del dispositivo inteligente	Áreas de evidencia Tipos de archivos Métodos de recuperación
Extraccion de la Nube	Tipos de autorización Principios de extracción de datos Soporte 2FA
Extraccion de Drones	Importar Extraccion Fisica de Drones Análisis de registro de Drones
Lista de propiedades	Tipos de almacenamiento Tipos de datos Datos PLIST
Base de Datos SQLite	Almacenamiento de datos Tipos de datos Desglose de SQLite FreePages Consultas SQL Crear / Ejecutar

Procedimientos de evaluación y criterios de calificación

La evaluación se calificara mediante un examen general al final del curso. Los participantes de este curso recibirán un certificado como Examinador Forense Certificado de Oxygen (OFCE) después de aprobar el examen. Los participantes que aprueben el curso de capacitación recibirán el certificado.