

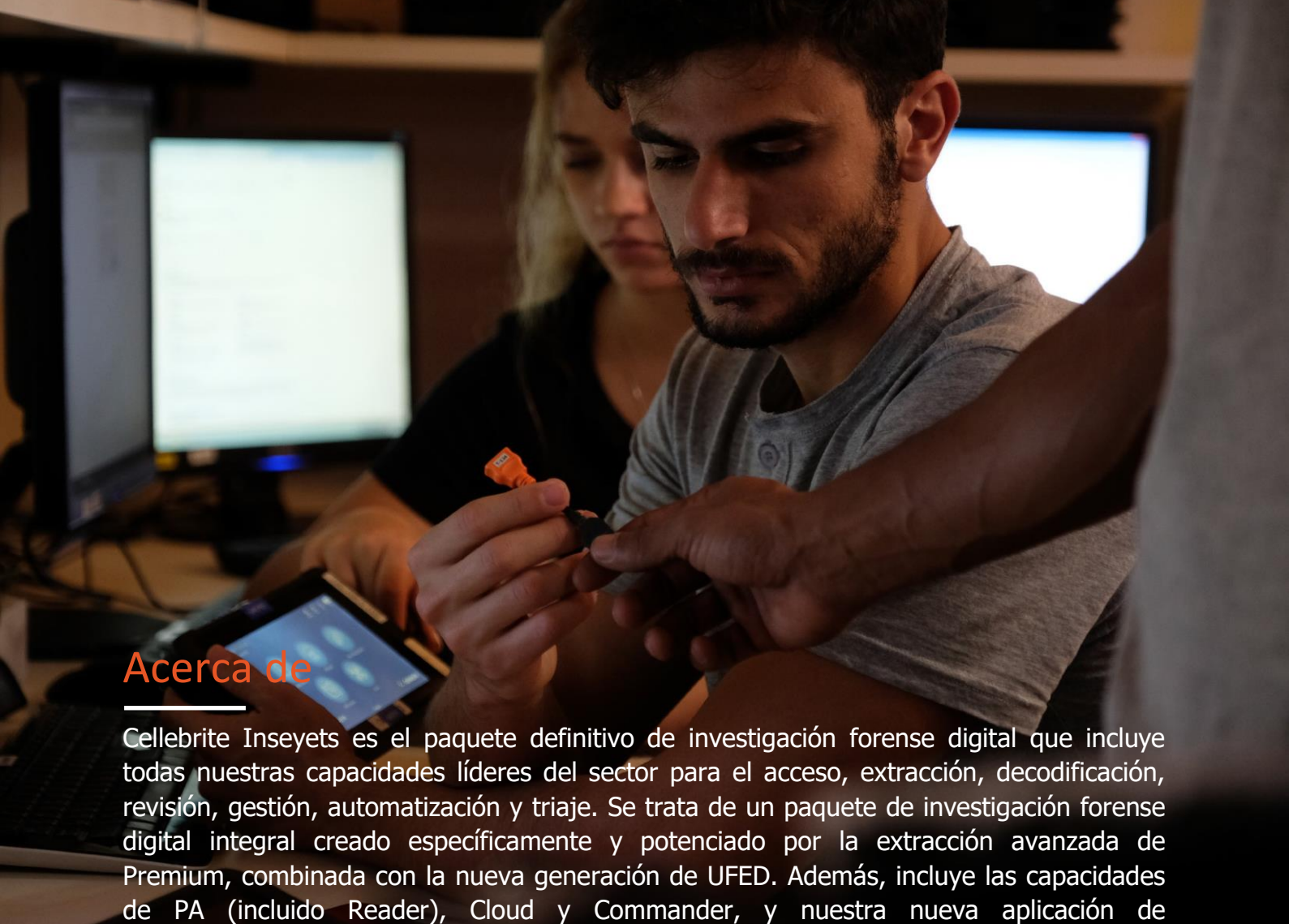
Cellebrite TRAINING

Formación básica en Cellebrite Inseyets (CIET)

2 días



Cellebrite



Acerca de

Cellebrite Inseyets es el paquete definitivo de investigación forense digital que incluye todas nuestras capacidades líderes del sector para el acceso, extracción, decodificación, revisión, gestión, automatización y triaje. Se trata de un paquete de investigación forense digital integral creado específicamente y potenciado por la extracción avanzada de Premium, combinada con la nueva generación de UFED. Además, incluye las capacidades de PA (incluido Reader), Cloud y Commander, y nuestra nueva aplicación de automatización de laboratorios, Cellebrite Autonomy.

Con una duración de dos días, el curso de incorporación a Inseyets de Cellebrite Training se ha diseñado para formar a los usuarios de forma rápida y eficaz para que obtengan una utilidad práctica inmediata de la herramienta.

- El día 1 se centra en la extracción de dispositivos Android e iOS a través de Cellebrite Inseyets y la implementación de las funciones tradicionales de UFED, como la extracción de SIM y tarjetas de memoria.
- El día 2 se centra en el análisis de datos mediante Physical Analyzer 10, con el objetivo de destacar ante los usuarios las nuevas y potentes funciones integradas desde las versiones anteriores.

Cellebrite recomienda encarecidamente tanto a los clientes antiguos como a los nuevos que realicen el curso de incorporación a Inseyets de Cellebrite Training y que continúen su trayecto formativo con nuestros cursos actualizados Cellebrite Certified Operator (CCO) para Inseyets y Cellebrite Certified Physical Analyzer (CCPA) para Inseyets para adquirir un conocimiento completo e integral de las herramientas.

Página web de Cellebrite Training: <https://cellebrite.com/es/cellebritetraining/>

Calendario de Cellebrite Training: www.cellebrite.com/en/training/schedule

Inseyets UFED de Cellebrite Training

Sesión de trabajo del módulo de incorporación

Prefacio

- Marcas comerciales
- Acerca de Cellebrite
- Acerca de Inseyets
- Centro de asistencia técnica de Cellebrite
- Centro de aprendizaje de Cellebrite
- Ayuda con el plan de estudios de Cellebrite
- Certificación de Cellebrite
- Acerca de su instructor
- Objetivos del curso

MÓDULO 1

Introducción a Inseyets UFED

- Introducción y objetivos del módulo

Lección 1.1

INTERFAZ DE INSEYETS

- Visión general de la interfaz de Inseyets
- Kits de Inseyets

Lección 1.2

OPTIMIZAR LOS AJUSTES DE EXTRACCIÓN DE INSEYETS

- Ajustes de Inseyets
- Ajustes de Inseyets.UFED
- Adquisición del dispositivo
- Pantalla principal de Inseyets.UFED
- Servicios de cámara de Inseyets.UFED
- Copia rápida
- Dron
- Herramientas del dispositivo
- Prácticas recomendadas para las extracciones
- Utilizar Streamline en Inseyets

Lección 1.3

HACER TRIAJE EN UN DISPOSITIVO

- Triaje de Cellebrite

Conclusión

Extracciones con Inseyets UFED

- Introducción y objetivos del módulo

Lección 2.1

REALIZAR LA EXTRACCIÓN/CLONACIÓN DE TARJETAS SIM

- Módulo de identificación de abonado (SIM)
- Tecnología eSIM
- Indicios de eSIM
- Extracciones de SIM
- SIM frente a USIM
- Procesamiento de pruebas de Tarjeta SIM
- Informe de la extracción de la SIM
- Actividad 2.1: Extracción de tarjeta SIM

Lección 2.2

EXTRACCIONES DE ALMACENAMIENTO EXTRAÍBLE

- Tipos de tarjeta Secure Data (SD)
- Actividad 2.2: Extracciones de tarjetas SD

Lección 2.3

FLUJOS DE TRABAJO DE EXTRACCIÓN EN ANDROID

- Actividad 2.3: Android Extracción física
- Actividad 2.4: Extracción del sistema de archivos de Android
- Actividad 2.5: Extracción lógica avanzada en Android
- Resolución de problemas de la extracción

Lección 2.4

MÉTODOS DE EXTRACCIÓN DE IOS

- Modo de aislamiento
- Modo de recuperación
- Guía de DFU
- Tipos de jailbreaking para checkra1n frente a checkm8

MÓDULO 2

Lección 2.5

FLUJOS DE TRABAJO DE EXTRACCIÓN DESBLOQUEADA EN IOS

- Actividad 2.6: Extracción lógica avanzada de dispositivos iOS
- Solución de problemas básicos de iOS

Conclusión



Extracciones avanzadas con el adaptador Turbo Link

- Introducción y objetivos del módulo

Lección 3.1

VISIÓN GENERAL DE LA FUERZA BRUTA

- Procesamiento después del primer desbloqueo (AFU)
- Bloqueado vs. desbloqueado
- Fuerza bruta (FB)
- Fuerza bruta autónoma
- Agente de Cellebrite
- Diccionarios

Lección 3.2

EXTRACCIONES AVANZADAS EN ANDROID

- Opciones de extracción de Android en Inseyets
- Flujo de trabajo para Android desbloqueado
- Actividad 3.1: Extracción avanzada de dispositivos Android desbloqueados
- Extracciones de Android por fuerza bruta
- Flujo de trabajo para Android bloqueado
- Actividad 3.2: Extracción de dispositivos Android bloqueado
- Extracciones de la Carpeta segura de Android

Lección 3.3

EXTRACCIÓN AVANZADA EN IOS

- Opciones de iOS en Inseyets UFED
- Estados de dispositivos iOS
- Flujo de trabajo para iOS desbloqueado
- Descripción general de fuerza bruta para iOS
- Secure Element de Apple
- Flujo de trabajo para iOS bloqueado
- Fuerza bruta supersónica
- Recuperación instantánea del código de acceso (IPR) para iOS
- Actividad 3.3: Extracción del sistema de archivos completo de iOS con Turbo Link
- Solución de problemas de las extracciones avanzadas

Conclusión

Después de la extracción

- Introducción y objetivos del módulo

Lección 4.1

SE HA COMPLETADO LA EXTRACCIÓN. ¿Y AHORA QUÉ?

- Actividades posteriores a la extracción
- Cómo documentar los valores hash

Lección 4.2

USAR CELLEBRITE READER

- Software Reader
- Usos del Reader
- Actividades posteriores a la elaboración de informes: Qué hacer tras la distribución del Reader

Lección 4.3

MANEJO DE PRUEBAS TRAS LA EXTRACCIÓN

- Visión general de asistencia
- Informes generales de triaje
- Desafíos del análisis con triaje

Conclusión

Sesión de trabajo del módulo de Integración de Inseyets Physical Analyzer de Cellebrite Training

Prefacio

- Marcas comerciales
- Acerca de Cellebrite
- Acerca de Inseyets
- Centro de asistencia técnica de Cellebrite
- Centro de aprendizaje de Cellebrite
- Ayuda con el plan de estudios de Cellebrite
- Certificación de Cellebrite
- Acerca de su instructor
- Objetivos del curso

MÓDULO 1

Visión general de Inseyets Physical Analyzer

Lección 1.1

- Introducción y objetivos del módulo

CONFIGURACIÓN Y AJUSTES DE INSEYETS PA

- ¿Para qué se utiliza Inseyets.PA?
- Actividad 1.1: Configurar Inseyets Physical Analyzer
- Datos, archivos y ajustes Configuración
- Otros campos de informes
- Actividad 1.2: Abrir extracciones en Inseyets.PA

Lección 1.2

GESTIONAR CASOS Y PRUEBAS

- Vistas de casos
- Identificadores de casos
- Tipos de pruebas
- Asistente del caso
- Modificar o eliminar un caso de la base de datos
- Motores de enriquecimiento
- Importar casos
- Exportar casos
- Abrir una extracción De otras herramientas
- Ajustar la zona horaria
- Cambiar el identificador del caso



MÓDULO 1

Lección 1.3

VISIÓN GENERAL DE LA INTERFAZ DE EXTRACCIÓN

- Resumen de extracción
- Análisis de múltiples extracciones
- Control de aprendizaje: Interfaz de datos del dispositivo
- Espacio de trabajo de Inseyets.PA
- Widgets
- Pestañas y panel de navegación

Lección 1.4

ANÁLISIS EN INSEYETS PA

- Abrir, visualizar y filtrar datos
- Explorador del sistema de archivos
- Datos analizados
- Análisis de cronograma
- Opciones de búsqueda
- Etiquetas
- Lista de observación
- Crear una lista de diccionario
- Análisis de malware
- Actividad 1.3: Ver datos en Inseyets.PA
- Verificación de hash
- Actividad 1.5: Validación de hash



Técnicas de análisis de datos

Lección 2.1

- Introducción y objetivos del módulo

DATOS DIGITALES

- Esquemas de codificación de datos
- ¿Qué es un binario?
- ¿Qué es ASCII?
- Esquemas de codificación de ASCII
- ¿Qué es Unicode?
- Información basada en la ubicación
- Instalar mapas sin conexión
- Actividad 2.1: Datos de ubicación
- Extracción de datos de imágenes
- Extracción automatizada de datos
- Actividad 2.2: Extracción de datos
- Clasificación de medios
- Actividad 2.3: Clasificación de medios
- AppGenie
- Actividad 2.4: AppGenie
- Gestionar etiquetas
- Actividad 2.5: Gestionar etiquetas
- Gestor de conjunto hash

Verificación y validación

Lección 3.1

- Introducción y objetivos del módulo

DESCRIPCIÓN GENERAL DE LA VERIFICACIÓN Y VALIDACIÓN

- Documentar el proceso de extracción
- ¿Qué es la verificación y validación?
- Cuándo validar
- Formas de validar y verificar
- Prácticas recomendadas de validación de datos

Lección 3.2

TÉCNICAS DE VERIFICACIÓN Y VALIDACIÓN

- Usar bases de datos SQLite para la validación
- Herramientas de terceros
- Técnica de desplazamiento manual

MÓDULO 4

Elaboración de informes con Inseyets Physical Analyzer

Lección 4.1

- Introducción y objetivos del módulo

ELABORACIÓN DE INFORMES EN INSEYETS.PA

- Fines de los informes de Inseyets.PA
- Formatos de informes de Inseyets.PA
- Seguridad del informe
- Personalización de informes en Inseyets PA
- Campos adicionales
- Informe de Inseyets PA: Informe de dispositivo preliminar

Lección 4.2

GENERAR INFORMES

- Prácticas recomendadas de elaboración de informes
- Proceso de investigación forense
- Elementos del informe: Establecer credibilidad y certificación
- Elementos del informe: Identificación de los dispositivos móviles
- Datos del informe: Inclusión o exclusión
- Elementos del informe: Adquisición de pruebas digitales
- Elementos del informe; análisis de pruebas digitales
- Prácticas recomendadas de almacenamiento
- Control de aprendizaje
- Actividad 4.1: Inseyets.PA – Generar un informe

Conclusión

Anexo A: Actividades adicionales

- Actividad 0.1: Instalación, licencias y paquetes de traducción de Inseyets PA
- Actividad 0.2: Analizar datos de Android
- Actividad 0.3: Analizar datos de iOS
- Tabla de codificación ASCII
- Acerca de Project VIC, CAID y el NCMEC
- Centro de aprendizaje
- Glosario



Acerca de Cellebrite

La misión de Cellebrite (Nasdaq: CLBT) es ayudar a sus clientes proteger y salvar vidas, acelerar la justicia y preservar la privacidad en comunidades de todo el mundo. Somos líderes mundiales en soluciones de investigación digital para los sectores público y privado y empoderamos a las organizaciones para dominar las complejidades de las investigaciones digitales sujetas al control judicial mediante la agilización de los procesos de inteligencia. La plataforma y las soluciones de investigación digital de Cellebrite, en las que confían miles de agencias y empresas líderes de todo el mundo, transforman la forma en que los clientes recogen, revisan, analizan y gestionan los datos en investigaciones sujetas al control judicial. Para más información, visítenos en www.cellebrite.com, <https://investors.cellebrite.com>, o síguenos en Twitter en @Cellebrite.

- Para más información, visítenos en www.cellebrite.com
- Póngase en contacto con Cellebrite de forma global en www.cellebrite.com/contact

11 1011

1000 11 1*

1110111000 111*

11011111100011111*
001000000111000001

0 0 1 1 11 1 10 01
1 10 0 1 01 1
1 1 111 *
0 1 0 01 0 0
1 0 1 11 1011 1000 11 1*

1 111
1 0 0 *
0 1 1 01 0 1 0

1 1 111 *
0 1 0 01 0 0
1 0 1

1 111
1 0 0 *
0 1 1 01 0 1 0

11 1011 1000 11 1*
0 0 1 1 11 1 10 01
1 10 0 1 01 1
1 1 111 *
0 1 0 01 0 0
1 0 1

1 1 111 *
0 1 0 01 0 0
1 0 1

11 1011 1000 11 1*

1 1 111 *
0 1 0 01 0 0
1 0 1

11011111100011111*
001000000111000001

11 1011 1000 11 1*