
MOBILE FORENSIC

Analizar el teléfono de un delincuente puede proporcionar una gran cantidad de información. Como resultado, la ciencia forense móvil y la ciencia forense digital en general se están convirtiendo en activos esenciales para las agencias policiales y de inteligencia de todo el mundo.
Los investigadores pueden deducir los motivos del ataque y sus consecuencias estudiando los procesos maliciosos. Investiguemos más.

Los investigadores pueden deducir los motivos del ataque y sus consecuencias estudiando los procesos maliciosos. Investiguemos

¿Qué es la ciencia forense móvil?

El proceso de recuperación de evidencia digital de dispositivos móviles utilizando metodologías establecidas se conoce como análisis forense móvil. La ciencia forense móvil, a diferencia de las técnicas forenses digitales tradicionales, se ocupa principalmente de extraer información de dispositivos móviles como teléfonos inteligentes, Android y tabletas.

Los dispositivos móviles incluyen una gran cantidad de información, que va desde mensajes de texto e historial de búsqueda web hasta datos de ubicación, lo que los hace increíblemente útiles para las investigaciones policiales.

¿Por qué es importante la ciencia forense móvil?

● Investigaciones criminales: debido a que los dispositivos móviles se utilizan cada vez más en actividades ilegales, la ciencia forense móvil puede ayudar a las organizaciones encargadas de hacer cumplir la ley a recuperar evidencia digital de los dispositivos sospechosos.

● Investigaciones de mala conducta de los empleados: los empleadores pueden necesitar investigar la mala conducta de los empleados, como el incumplimiento de las políticas de la empresa, el acoso o el robo de datos de la empresa.

● Litigios civiles: asuntos de litigios civiles como procesos de divorcio, cuestiones de propiedad intelectual o reclamaciones por lesiones personales or dispositivos móviles. puede usarse como evidencia.

¿Cuál es un ejemplo de análisis forense móvil?

En una investigación criminal, la medicina forense móvil podría incluir el análisis del teléfono inteligente de un sospechoso. Un investigador forense recuperaría datos del dispositivo

memoria, sistema de archivos y otras regiones de almacenamiento utilizando software y técnicas especializados. Es posible que se incluyan registros de llamadas, mensajes de texto, actividad en las redes sociales, historial de Internet y datos de ubicación GPS.

¿Cuáles son los pasos del proceso de análisis forense móvil?

1. Adquisición de pruebas: El primer paso es adquirir el dispositivo móvil y crear una imagen forense de sus medios de almacenamiento. Esto implica el uso de herramientas especializadas para hacer una copia bit a bit del almacenamiento del dispositivo, incluido el sistema operativo, los archivos y los datos del usuario.
2. Preservación de la evidencia: Una vez adquiridos los datos, se deben preservar para garantizar que permanezcan inalterados y admisibles en corte. Esto implica almacenar los datos en un entorno seguro y a prueba de manipulaciones y crear un registro de cadena de custodia.
3. Análisis de evidencia: luego, el investigador forense analiza los datos para identificar información y artefactos relevantes que puedan proporcionar información. en el caso. Esto puede implicar búsqueda de palabras clave, creación de datos y análisis de línea de tiempo, entre otras técnicas.
4. Interpretación e informe: El investigador interpreta los datos y presenta sus hallazgos en un informe escrito o testimonio. El informe debe ser claro, conciso y objetivo, y debe proporcionar una representación completa y precisa de los datos.
5. Presentación ante el tribunal: Finalmente, la evidencia digital se presenta ante el tribunal, pudiendo llamarse al investigador a declarar sobre sus hallazgos. El investigador debe estar preparado para explicar sus métodos y la precisión de sus hallazgos, y debería poder responder cualquier pregunta que surja.

Las 10 mejores herramientas para análisis forense móvil

1. CellebriteUFED:
2. Oxygen Forensic Detective:
3. Magnet AXIOM
4. Paraben E3:
5. XRY
6. MOBILedit Forensic Express:

7. Elcomsoft Phone Breaker:
8. FonePaw:
9. Andriller
10. BlackBag:

Herramientas más populares para análisis forense móvil

Cellebrite UFED es ampliamente considerada la herramienta forense móvil más popular. Lo utilizan organismos encargados de hacer cumplir la ley, organizaciones gubernamentales e investigaciones corporativas en todo el mundo. Cellebrite UFED puede extraer datos de un amplia gama de dispositivos móviles y sistemas operativos, incluidos iOS, Android, y Windows Phone, así como dispositivos GPS y otros dispositivos portátiles. Él admite métodos de extracción físicos y lógicos y puede recuperar datos eliminados, así como analizar y decodificar varios tipos de datos, como registros de llamadas, mensajes de texto, correos electrónicos y actividad en las redes sociales. Cellebrite UFED también proporciona capacidades integrales de generación de informes, lo que la convierte en una opción popular para los investigadores forenses digitales.

¿Cómo instalar Cellebrite UFED?

Cellebrite UFED es un producto de software propietario al que solo pueden acceder personas autorizadas que hayan adquirido una licencia. El programa suele instalarse en una estación de trabajo forense dedicada que cumple con los requisitos mínimos de hardware y software de Cellebrite

1. Obtenga una licencia: comuníquese con Cellebrite o uno de sus revendedores autorizados para comprar una licencia para el software Cellebrite UFED. Deberá proporcionar pruebas de sus calificaciones y experiencia en análisis forense digital.
2. Acceda al portal de atención al cliente de Cellebrite: una vez que haya obtuvo una licencia, se le proporcionarán las credenciales de inicio de sesión para acceder al portal de atención al cliente de Cellebrite.
3. Seleccione la versión de software adecuada: En el portal, seleccione la versión adecuada del software Cellebrite UFED para su sistema operativo de la estación de trabajo.
4. Descargue el software: haga clic en el enlace de descarga y espere a que el software se descargue en su computadora.
5. Instale el software: siga las instrucciones proporcionadas en el manual de instalación. asistente para instalar el software en su estación de trabajo forense.
6. Active la licencia: inicie el software Cellebrite UFED e ingrese su clave de licencia para activar la licencia.
7. Configure el software: configure los ajustes del software, como configuración de idioma, zona horaria y red.
8. Comience a usar el software: ahora puede comenzar a usar Cellebrite UFED
Software para extraer y analizar datos de dispositivos móviles.