

Especificaciones Técnicas

Software Forense para Dispositivos Móviles

El presente documento tiene como finalidad establecer las especificaciones técnicas mínimas requeridas para la contratación de un software forense destinado a la apertura, extracción, análisis, visualización e investigación de datos provenientes de dispositivos móviles.

- Funcionalidad de desbloqueo y apertura de dispositivos móviles, que permita bypass, fuerza bruta o acceso lógico a dispositivos protegidos por patrón, PIN, contraseña o sistemas biométricos, para todos los sistemas operativos del mercado de manera ilimitada.
- Compatibilidad Multiplataforma: Soporte para dispositivos con sistemas operativos Android, iOS y otros sistemas móviles relevantes.
- Extracción Avanzada de Datos: Capacidad para realizar extracciones físicas, lógicas, basadas en archivos de respaldo y mediante métodos avanzados, incluyendo extracción mediante exploits autorizados y acceso por vulnerabilidades conocidas.
- Análisis Automatizado: Motor de análisis capaz de identificar patrones relevantes, comunicaciones frecuentes, ubicación de eventos y relaciones entre usuarios.
- Visualización de Datos con Contexto Investigativo: Herramientas visuales que permitan la reconstrucción de hechos mediante líneas de tiempo, gráficos de conexiones, mapas y análisis contextual de la actividad del usuario.
- Reconocimiento de Contenidos Sensibles: Detección automática de contenidos sensibles como violencia, armas, drogas, material de abuso infantil o material explícito, utilizando inteligencia artificial o algoritmos preentrenados.
- Análisis de Aplicaciones de Mensajería: Soporte para el análisis de contenido de aplicaciones como WhatsApp, Telegram, Signal, Facebook Messenger, Instagram, TikTok, entre otras, incluso si los datos están encriptados o eliminados.
- Identificación de Contenidos Eliminados: Capacidad para detectar y recuperar contenido eliminado parcial o totalmente, incluyendo mensajes, imágenes y archivos.
- Geolocalización y Análisis de Movimiento: Detección y representación de datos de localización del dispositivo, incluyendo ubicación de imágenes, eventos y recorridos.

- Capacidad de Etiquetado: Permitir el etiquetado, clasificación y anotación de la evidencia manteniendo la integridad y trazabilidad.
- Integración con Otros Sistemas Forenses: Posibilidad de exportar y vincular la información con otros softwares o plataformas de análisis forense y judicial (ej Cellebrite Reader, Magnet AXIOM, i2 Analyst's Notebook).
- Conservación de la Cadena de Custodia: Garantías técnicas de inalterabilidad de la evidencia digital, con generación de hashes criptográficos y documentación automática de la cadena de custodia.
- Exportación Personalizada de Informes: Generación de reportes en formatos legibles (PDF, HTML, Excel), con capacidad de personalización según el tipo de caso.
- Licenciamiento y Soporte Técnico: El software deberá contar con actualizaciones periódicas y soporte técnico especializado.