

# Introducción a pruebas forenses digitales

## PRUEBAS FORENSES DIGITALES

El uso de dispositivos digitales en la vida cotidiana sigue creciendo, a medida que las personas incorporan la tecnología a sus vidas. Se calcula que, desde 2010, el número de usuarios de teléfonos celulares llegó a más de 5.000 millones en todo el mundo. Además, siguen presentándose nuevos dispositivos, entre ellos, tabletas, lectores y reproductores con Wi-Fi, y automóviles y aparatos domésticos con conexión a Internet.

Este predominio de los dispositivos electrónicos en la sociedad se combina con una creciente presencia de evidencia recolectada desde dispositivos digitales en causas penales. Las investigaciones actuales sugieren que los teléfonos celulares y sus posibles evidencias pueden encontrarse en más del 50% de los delitos violentos y un porcentaje aún más alto en delitos relacionados con drogas en algunas jurisdicciones. La investigación y conservación adecuadas de la evidencia y el mantenimiento de su integridad es fundamental para los casos que se llevan a juicio.

Al igual que otras evidencias, debe haber un protocolo para establecer la forma en que se documentan, recopilan y conservan los datos. Deben utilizarse herramientas especiales para extraer información de los dispositivos en los que se almacenan, sin poner en peligro su integridad. Además, la evidencia electrónica, al igual que cualquier otra evidencia encontrada en la escena del crimen, por lo general, deberá ser revisada por un experto, por lo que debe tenerse cuidado al capturar la información y empaquetar el dispositivo adecuadamente, a fin de que el examinador de pruebas digitales tenga mayores probabilidades de recopilar toda la evidencia posible que haya.

Es responsabilidad del equipo de intervención inmediata revisar la escena del crimen en busca de dispositivos electrónicos y de determinar de qué manera debe manejarse cada dispositivo.

**SIRCHIE®** se enorgullece de ofrecer soluciones para trabajo forense de alta calidad, que ayudarán en las investigaciones, desde la escena del crimen hasta los tribunales, incluidos los métodos para extraer información de distintos dispositivos electrónicos, así como paquetes para garantizar el traslado seguro del dispositivo al examinador de pruebas digitales.



## Pruebas forenses digitales

*Dado que los dispositivos digitales pueden contener impresiones latentes, trazas o evidencia biológica, el investigador debe documentar y preservar por completo esta posible evidencia para su procesamiento por imágenes digital de evidencias. Consulte nuestras secciones de recolección de evidencia e impresiones latentes de este catálogo para encontrar las herramientas adecuadas.*

## ¡SOLUCIONES DE VEHÍCULOS!

Sirchie ha desarrollado un vehículo para investigación de delitos cibernéticos/informáticos.



*Para obtener más información, consulte la Sección de Vehículos de este catálogo o visite nuestra página en Internet en [www.sirchie.com](http://www.sirchie.com)*

## CARACTERÍSTICAS DE LAS BOLSAS STRONGHOLD REUTILIZABLES:

- Diseño único que evita que los cables de datos actúen como conductos de señales.
- Cada bolsa StrongHold cuenta con una bolsa para evidencia, para permitir el manejo adecuado de la evidencia.
- Las bolsas vienen en dos tamaños: 25,4 cm x 17,8 cm (10" x 7") para teléfonos celulares y 33 cm x 22,9 cm (13" x 9") para tabletas, netbooks y notebooks.

## BOLSAS PARA ALMACENAMIENTO DE EVIDENCIA ELECTRÓNICA STRONGHOLD (REUTILIZABLE)

La bolsa StrongHold (patentada\*) es la bolsa para evidencia perfecta para cualquier tipo de dispositivo electrónico. Los equipos de intervención inmediata pueden utilizar esta bolsa para asegurarse de que se sigan los procedimientos adecuados para dispositivos inalámbricos y que la evidencia quede protegida de aquellos que puedan interponerse en el caso, después de haberse capturado las comunicaciones inalámbricas.

Estas bolsas ofrecen el mayor nivel de protección Faraday disponible. El material especial de triple trama usado en la bolsa StrongHold está realizado con una tela de níquel, cobre y nailon bañado en plata. La tela es fundamental para evitar signos indeseados de daños o eliminación de la evidencia de vital importancia.



NÚM. DE CATÁLOGO	DESCRIPCIÓN	PRECIO
FBAGR10	Bolsas Stronghold reutilizables para almacenamiento de evidencia 25,4 cm x 17,8 cm (10" x 7"), 1 unidad	
FBAGR13	Bolsas Stronghold reutilizables para almacenamiento de evidencia 33 cm x 22,9 cm (13" x 9"), 1 unidad	

## BOLSAS DE DISIPACIÓN ELECTROSTÁTICA Y ENVOLTURA DE ESPUMA

Los aparatos electrónicos como los teléfonos, las tabletas, los discos de almacenamiento de datos y las tarjetas SD pueden contener gran cantidad de información. Proteja la información que contienen sin exponerlos a electricidad estática o a impulsos electrostáticos con las bolsas de disipación electrostática de **SIRCHIE®**. El nuevo tamaño de 45,7 cm x 61 cm (18" x 24") es lo suficientemente grande como para guardar computadoras portátiles.



Las bolsas electrostáticas vienen en cinco tamaños para guardar diversos tipos de aparatos electrónicos, desde teléfonos celulares hasta discos duros. Para los dispositivos de mayor tamaño, como computadoras de escritorio o servidores, utilice la envoltura de espuma de disipación electrostática.

NÚM. DE CATÁLOGO	DESCRIPCIÓN	PRECIO
ESD0406	Bolsas de disipación electrostática, 10,2 cm x 15,2 cm (4" x 6"), 100 unidades	
ESD0608	Bolsas de disipación electrostática, 15,2 cm x 20,3 cm (6" x 8"), 100 unidades	
ESD0810	Bolsas de disipación electrostática, 20,3 cm x 25,4 cm (8" x 10"), 100 unidades	
ESD1012	Bolsas de disipación electrostática, 25,4 cm x 30,5 cm (10" x 12"), 50 unidades	
ESD1824	Bolsas de disipación electrostática, 45,7 cm x 61 cm (18" x 24"), 50 unidades	
ESDF24	Envoltura de espuma para disipación electrostática, 61 cm (ancho) x 7,6 m (24" x 25'), 1 rollo	

# Protección Faraday

# Pruebas forenses digitales

## BOLSAS "AGUJERO NEGRO" PARA PROTECCIÓN FARADAY (CON VENTANA)

Las bolsas Agujero Negro para protección Faraday están fabricadas con un sistema de protección ISOTech y materiales con ventanas para ofrecer vistas previas claras de la evidencia, al tiempo que se mantiene un alto nivel de protección. Estas bolsas incluyen capas externas protectoras para evitar que el material de protección quede expuesto; vienen en tres tamaños.



NÚM. DE CATÁLOGO	DESCRIPCIÓN	PRECIO
FBW10	Bolsa Agujero Negro para protección Faraday con ventana, estándar, 19 cm x 10,8 cm (7,5" x 4,25")	
FBW20	Bolsa Agujero Negro para protección Faraday con ventana, grande, 27,9 cm x 19,8 cm (11" x 7,8")	
FBW30	Bolsa Agujero Negro para protección Faraday con ventana, extra grande, 43,8 cm x 34,9 cm (17,25" x 13,75")	
FBW40	Equipo de bolsa Agujero Negro para protección Faraday, (1 unidad de c/u: estándar, grande, extra grande)	

## EQUIPO DE BOLSAS "AGUJERO NEGRO" PARA DATOS

Los equipos de bolsas "Agujero Negro" para datos tienen una conexión USB 2.0 filtrada electrónicamente y con protección que permite la carga, la transferencia de datos y el análisis de los dispositivos sin poner en peligro la protección. El equipo incluye la bolsa para datos, una bolsa de protección Faraday independiente para el traslado y un soporte para dispositivos que permite el uso de dispositivos con pantalla capacitiva táctil dentro de la bolsa para datos.



NÚM. DE CATÁLOGO	DESCRIPCIÓN	PRECIO
FDBK	Equipo de bolsas "Agujero Negro" para datos	

## TIENDA STRONGHOLD DE MESA

Esta solución liviana y portátil usa la misma tecnología y material StrongHold que las bolsas StrongHold reutilizables, y es perfecta para realizar evaluaciones forenses en dispositivos inalámbricos activos. La tienda trae una bolsa StrongHold inalámbrica para mantener las evidencias de dispositivos digitales seguras, hasta que puedan ser examinadas. Coloque su computadora portátil de investigación y la evidencia dentro de la tienda, coloque los brazos en forma segura a través de las mangas de protección Faraday, retire la evidencia de la bolsa que se incluye y conéctela a la computadora portátil de investigación para realizar un examen seguro.



NÚM. DE CATÁLOGO	DESCRIPCIÓN	PRECIO
FTENT20	Tienda Stronghold de mesa	
FTENT22	Tienda de mesa StrongHold con USB 2.0 protegido	

## CARACTERÍSTICAS DE LAS BOLSAS AGUJERO NEGRO PARA PROTECCIÓN FARADAY (CON VENTANA):

- Las instrucciones de uso que se encuentran en las bolsas garantizan que se usen de manera correcta.
- Bolsillos para tarjetas de evidencia en la parte posterior. Incluye diez tarjetas.
- La ventana permite la visualización previa de la evidencia, el control de energía del dispositivo y el estado del teléfono, y la revisión del adaptador correcto.

## CARACTERÍSTICAS DE LAS BOLSAS PARA DATOS:

- Dimensiones externas: bolsa de 43 cm x 29,85 cm (17" x 11,75") y cable de 50,8 cm (20")
- Área de uso: 34,9 cm x 27,9 cm (13,75" x 11")
- Conectividad: USB 2.0 filtrado, conexión interna hembra, conexión externa macho

## CARACTERÍSTICAS DE LAS BOLSAS PARA TRASLADO:

- Dimensiones externas: 54,61 cm x 34,9 cm (21,5" x 13,75")
- Área de uso: 47 cm x 33 cm (18,5" x 13")

## CARACTERÍSTICAS DEL SOPORTE PARA DISPOSITIVOS DE PANTALLA TÁCTIL:

- Dimensiones externas: 54,61 cm x 34,9 cm (21,5" x 13,75")
- Dimensiones externas: 10,2 cm x 12,7 cm (4" x 5")

## CARACTERÍSTICAS DE LAS TIENDAS DE MESA STRONGHOLD:

- Dimensiones: 50,8 cm x 35,6 cm x 35,6 cm (20" x 14" x 14")
- Doble revestimiento.
- Ventana de malla en la parte superior.
- Las mangas sin guantes permiten trabajar con total destreza en dispositivos pequeños.
- Diseñada para contener una computadora portátil junto con el dispositivo que se analiza.
- La solapa protectora permite almacenar varios dispositivos en la tienda al mismo tiempo.

## LA TIENDA DE MESA STRONGHOLD INCLUYE:

- 1- Tienda
- 1- Bolsa StrongHold (reutilizable)
- 1- Luz de LED

## CONTENIDO DEL EQUIPO DMSK:

- 5- FBAGR10 Bolsa para almacenamiento de evidencias StrongHold® reutilizable de 25,4 cm x 17,8 cm (10" x 7") para dispositivos portátiles
- 1- FBAGR13 Bolsa para almacenamiento de evidencias StrongHold® reutilizable de 33 cm x 22,9 cm (13" x 9") para PC
- 1- de cada una de las tarjetas del equipo de intervención inmediata (tarjetas tamaño bolsillo que establecen los pasos para conservar la evidencia forense en equipos portátiles tales como teléfonos inteligentes/agendas electrónicas, teléfonos celulares y unidades GPS).
- 1- Cargador remoto (cargador a batería, con consejos para los distintos dispositivos, a fin de que los dispositivos portátiles permanezcan cargados hasta la captura de datos).
- 10- ESD1012 Bolsas de disipación electrostática de 25,4 cm x 30,5 cm (10" x 12")
- 10- ESD0406 Bolsas de disipación electrostática de 10,2 cm x 15,2 cm (4" x 6")
- 10- IEB1200 Bolsas para integridad de evidencia de 30,5 cm x 39,4 cm (12" x 15½")
- 10- IEB9120 Bolsas para integridad de evidencia de 22,9 cm x 30,5 cm (9" x 12")
- 1- DMSKC Bolso de traslado de nailon negro

## REQUISITOS DE LOS SISTEMAS DE CAPTURA DE DISPOSITIVOS Y CAPTURA DE DISPOSITIVOS PORTÁTILES

- Procesador: 1.4Ghz+
- RAM: 1 GB
- Espacio de disco rígido: 200 MB
- Windows 2000, XP, 2003, Vista, Windows 7

**Obtenga más información de más dispositivos. Según el modelo, los sistemas de captura de dispositivos y captura de dispositivos portátiles pueden obtener los siguientes datos:**

- Historial de SMS (mensajes de texto)
- Contactos (ambos cargados en la memoria del teléfono o en la tarjeta SIM)
- Historial de llamadas
  - Llamadas recibidas
  - Números marcados
  - Llamadas perdidas
  - Fecha y duración de las llamadas
- Agenda
- Planificador
- Calendario
- Lista de tareas
- Sistema de archivos
  - Archivos del sistema
  - Archivos multimedia (imágenes, videos, etc.)
  - Archivos Java
  - Notas rápidas
  - Más...
- Bases de datos de agendas electrónicas
- Correo electrónico

## CONTENIDO DE LOS EQUIPOS DDRK Y DDRK1:

- 1- Tableta (DDRK1 únicamente)
- 3- FBAGR10 Bolsa para almacenamiento de evidencias StrongHold® reutilizable para dispositivos portátiles
- 1- Aplicación de software de captura de dispositivos portátiles (integrada en tabletas)
- 1- Aplicación de software de captura de dispositivos (integrada en tabletas) **DDRK1 únicamente**
- 1- Equipo de cables para dispositivos móviles con bolso de traslado
- 1- Suscripción por un año para licencias de software de captura de dispositivos y captura de dispositivos portátiles
- 10- ESD0406 Bolsas de disipación electrostática de 10,2 cm x 15,2 cm (4" x 6")
- 10- IEB9120 Bolsas para integridad de evidencia de 22,9 cm x 30,5 cm (9" x 12")
- 1- DDRKC Bolso de traslado de nailon negro

## EQUIPO DE CAPTURA DE DISPOSITIVOS MÓVILES DIGITALES

El equipo de captura de dispositivos móviles es un sistema de recopilación integral para dispositivos móviles, que permite el manejo adecuado de las evidencias con una protección Faraday completa para cualquier dispositivo de transmisión inalámbrica. Diseñado para un uso sencillo y para proteger la integridad de la evidencia, este equipo es fundamental para los investigadores en el campo.



NÚM. DE CATÁLOGO	DESCRIPCIÓN	PRECIO
DMSK	Equipo de captura de dispositivos móviles digitales	

## EQUIPO DE REVISIÓN DE DISPOSITIVOS DIGITALES

El equipo de revisión de dispositivos digitales le permite establecer un orden de prioridades en cuanto a los dispositivos digitales y contiene todo lo que necesita para procesar según criterios forenses más de 4.000 dispositivos móviles en la escena del crimen y extraer de forma válida a efectos de tratamiento forense los datos asociados a dichos dispositivos.



Equipo Núm. DDRK1 con tableta incluida en la imagen.

**Captura de dispositivos:** recopile y almacene los datos de más de 4.000 teléfonos celulares, agendas electrónicas y unidades de sistemas de posicionamiento global (GPS), incluidos los iPhone. Se entrega en formato MS Windows.

**Captura de dispositivos portátiles:** es una versión del sistema de captura de dispositivos para usar en campo. Se integra en una tableta y se entrega con pantalla táctil. También puede proporcionarse para ser instalado en cualquier computadora portátil o tableta con Windows.

Ambos paquetes de software son herramientas forenses avanzadas de recopilación y análisis. No se conforme con tener la mitad de los datos. La mayor parte de los productos de software forense para teléfonos celulares comerciales solo recupera archivos de datos lógicos. Eso es como hacer una investigación a medias en la escena del crimen. Si una herramienta no tiene funciones de análisis de avanzada, probablemente sea porque no obtienen datos suficientes para analizar. Por lo general, los datos e información del usuario eliminados, como mensajes de texto e imágenes, pueden encontrarse en el lugar en el que se eliminan los datos físicos en el teléfono. El sistema de captura de dispositivos está diseñado desde el inicio como una herramienta forense que ha sido respaldada en innumerables juicios.

En el sistema de captura de dispositivos se integró la tecnología punto a punto. Esta tecnología convierte los puntos de datos del sistema de posicionamiento global para que sean leídos directamente en Google Earth, a fin de que los investigadores puedan visualizar de manera sencilla y rápida dónde se encuentran las ubicaciones indicadas por el sistema.

## FABRICANTES DE DISPOSITIVOS Y SISTEMAS OPERATIVOS ADMITIDOS POR LOS SISTEMAS DE CAPTURA DE DISPOSITIVOS Y CAPTURA DE DISPOSITIVOS PORTÁTILES:

Alcatel, Android, BlackBerry, Garmin, Apple iOS, Kyocera, LG, Motorola, Nokia, Palm, Web OS, Samsung, Sanyo, Siemens, Ericsson, Symbian, TomTom, Windows Mobile, ZTE, tarjetas de memoria

NÚM. DE CATÁLOGO	DESCRIPCIÓN	PRECIO
DDRK1	Equipo de revisión de dispositivos digitales con tableta	
DDRK	Equipo de revisión de dispositivos digitales sin tableta	

# Equipos de exámenes forenses en dispositivos móviles

## Pruebas forenses digitales

### EQUIPO DE DISPOSITIVOS MÓVILES DIGITALES

Este versátil equipo de llaves de memoria para trabajos forenses incluye herramientas sencillas para la revisión de dispositivos digitales móviles, entre ellos, dispositivos iPhone, iPad e iTouch, dispositivos Android y teléfonos celulares.



NÚM. DE CATÁLOGO	DESCRIPCIÓN	PRECIO
DSRK100	Equipo de dispositivos móviles digitales	

### CAPTURA DE TARJETAS SIM

Este lector de tarjetas SIM está diseñado para recuperar los mensajes de texto (SMS) eliminados y cualquier otra información que pudiera almacenarse en la tarjeta SIM del dispositivo confiscado. El sistema de captura de tarjetas SIM incluye el software y un lector de tarjetas SIM para trabajos forenses.



NÚM. DE CATÁLOGO	DESCRIPCIÓN	PRECIO
SIM100	Captura de tarjetas SIM	

### EQUIPO DE CAPTURA DE PANTALLAS ECLIPSE

El equipo de captura de pantalla Eclipse está diseñado como un sistema integral y fácil de usar para la captura de información del usuario desde las pantallas de los teléfonos celulares, unidades GPS, tabletas y cualquier otro dispositivo portátil que pueda fotografiarse. El equipo Eclipse permite que el usuario capture las pantallas de dispositivos móviles, agregue notas y organice las imágenes. Eclipse guarda imágenes y video dentro del programa y puede exportar informes a la mayoría de los navegadores web.



NÚM. DE CATÁLOGO	DESCRIPCIÓN	PRECIO
ECL1000	Equipo de captura de pantallas Eclipse	

### CONTENIDO DEL EQUIPO DSRK100:

- 1- Llave iRecovery: diseñada para extraer información activa y eliminada de dispositivos iPhone, iPad e iTouch.
- 1- Llaves de memoria para recuperación de teléfonos: diseñadas para recuperar datos activos y eliminados de cientos de teléfonos inteligentes y tabletas, entre ellos, dispositivos Android, teléfonos Blackberry, Symbian y Windows 7, o de cualquier teléfono que tenga una tarjeta de almacenamiento extraíble, como las tarjetas MicroSD.
- 1- Captura de Tarjetas SIM: este lector de tarjetas SIM está diseñado para recuperar los mensajes de texto (SMS) eliminados y cualquier otra información que pudiera almacenarse en la tarjeta SIM del dispositivo confiscado.
- 1- Cable de datos Micro-USB
- 1- Cable de datos USB para iPhone
- 1- Cable de datos USB para iPhone 5
- 1- Maletín de plástico DSRKC

### EL SISTEMA DE CAPTURA DE TARJETAS SIM INCLUYE:

- 1- Software captura de tarjetas SIM
- 1- Lector forense para tarjetas SIM

### CARACTERÍSTICAS DEL EQUIPO DE CAPTURA DE PANTALLAS ECLIPSE:

- Cámara y base de alta calidad
- Proceso de captura rápida
- Hash de imagen y video
- Vista preliminar y organización de las capturas
- Video e imágenes en un único informe
- Control total para el usuario

### EL EQUIPO DE CAPTURA DE PANTALLAS ECLIPSE INCLUYE:

- 1- Cámara y base de hardware de Eclipse
- 1- Software Eclipse
- 1- Estuche duro para almacenamiento y traslado
- 1- Protección contra reflejos y brazo flexible
- 1- Bolsa Agujero Negro para protección Faraday de tamaño estándar

## CONTENIDO DEL EQUIPO DCRK:

- 1- DP2C P2 Commander Portátil, con disco duro externo
- 1- Windows Breaker
- 1- DCRKC Bolso de traslado de nailon negro

## EQUIPO DE REVISIÓN PARA COMPUTADORAS

El equipo de revisión para computadoras contiene herramientas fáciles de usar que permiten la captura de datos forenses en la escena del crimen desde cualquier sistema de computadoras. El equipo de arranque mantiene la integridad forense a través de un proceso de solo lectura de la computadora. DP2C P2 Commander es una llave de memoria de arranque que le permite buscar rápidamente evidencias en una computadora personal sin hacer cambios en la computadora. También le permite extraer los archivos que necesita. La llave de Windows Breaker es una llave de memoria que sirve para recuperar contraseñas de Windows.



NÚM. DE CATÁLOGO	DESCRIPCIÓN	PRECIO
DCRK	Equipo de revisión para computadoras	
WBS10	Llave de Windows Breaker de repuesto, 10 usos	

## EQUIPO DE ANÁLISIS DE COMPUTADORAS PARA EXÁMENES FORENSES DE DISPOSITIVOS DIGITALES

Este versátil equipo de llaves para trabajos forenses contiene herramientas fáciles de usar para la detección y la recuperación de datos de computadoras de escritorio, computadoras portátiles y notebooks.

## CONTENIDO DEL EQUIPO DSRK200:

- 1- Llave para recuperación de datos: USB de arranque que permite la recuperación de documentos, fotos, música y otros archivos eliminados, mediante un algoritmo de recuperación de datos de grado forense por grupos.
- 1- Llave de Windows Breaker: USB de arranque que permite omitir contraseñas de cuentas de Windows. Límite de 10 usos para la llave de Windows Breaker.
- 1- Llave de detección de material pornográfico: USB de arranque que busca en todas las imágenes y videos en una computadora, los analiza para ver si hay contenido pornográfico y crea un informe de imágenes y videos sospechosos.
- 1- Llave para chat: USB de arranque que detecta y analiza los registros de chat de los programas de chat en línea más populares.
- 1- Maletín de plástico DSRKC



NÚM. DE CATÁLOGO	DESCRIPCIÓN	PRECIO
DSRK200	Equipo de análisis de computadoras para exámenes forenses de dispositivos digitales	
WBS10	Llave de Windows Breaker de repuesto, 10 usos	