Introduction to Digital Forensics

DIGITAL FORENSICS

The use of digital devices in everyday life continues to increase as people integrate technology into their lives. It is estimated that as of 2010, there were over 5 billion cellular phone subscribers worldwide. In addition, new consumer devices continue to be introduced, including tablet computers, wi-fi readers and media players, as well as internet capable automobiles and appliances.

This prevalence of electronic devices in society is matched by a growing presence of evidence gathered from digital devices in criminal cases. Current research suggests cell phones and their potential evidence may be found in over 50% of all violent crimes and an even larger percentage in drug crimes in some jurisdictions. The proper investigation and preservation of this evidence and the maintenance of its integrity is vital to making cases that stand up to judicial challenges.

Like other evidence, there must be a protocol to establish how digital data is documented, collected, and preserved. Special tools must be utilized to extract information from the device on which it is stored without compromising its integrity. In addition, electronic evidence, like other evidence found at the scene, will usually require review by an expert, so care must be taken to capture the information and package the device properly so the digital examiner has the highest probability of gathering all of the potential evidence present.

It is the job of the first responder to review the crime scene for electronic devices and determine how each device should be processed. SIRCHIE® is proud to offer high quality digital forensics solutions that will aid investigations from the crime scene to the courtroom, including methods to extract information from various electronic devices, as well as packaging to insure the safe transport of the device to the digital examiner.

Noting that digital devices may contain latent, trace, or biological evidence, the investigator should thoroughly document and preserve this potential evidence for processing before the digital evidence imaging has been done. Please see our evidence collection and latent print sections of this catalog for the right tools.

VEHICLE SOLUTIONS!

Sirchie has developed a specially designed Mobile Computer/ Cyber Crimes Investigation Vehicle.

For more information see the Vehicle Section of this catalog or visit our website at www.sirchie.com

Faraday Protection & Electronic Storage

STRONGHOLD REUSABLE BAG FEATURES:

- Unique design that prevents data cables from acting as signal conduits
- Each StrongHold Bag comes with a clear evidence bag to allow for proper evidence handling.
- The bags come in 2 sizes: 10" x 7" for cell phones and 13" x 9" for tablets/netbooks/ notebooks.

STRONGHOLD ELECTRONIC INTEGRITY EVIDENCE STORAGE BAGS (REUSABLE)

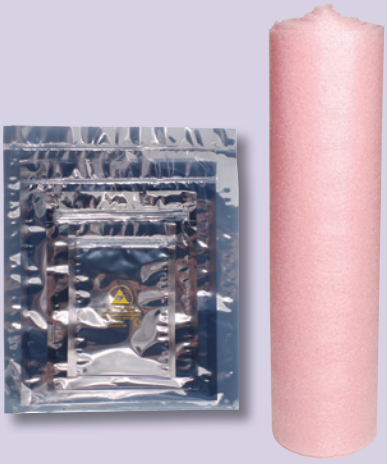
The StrongHold Bag (Patented*) is the perfect evidence bag for any type of wireless device. First responders can use this bag to ensure proper wireless procedures are kept and that the evidence is protected from potential case killers - after seizure wireless communications.

These bags provide the highest level of faraday protection available. The special tri-weave material used in the StrongHold Bag is made of a Nickel, Copper, and Silver Plated Nylon, plain woven fabric. This fabric is key in preventing unwanted signals from corrupting or erasing vital evidence.

CATALOG NO.	DESCRIPTION	PRICE
FBAGR10	10" x 7" Reusable Stronghold Evidence Storage Bags, 1 ea.	
FBAGR13	13" x 9" Reusable Stronghold Evidence Storage Bags, 1 ea.	

ELECTROSTATIC DISSIPATION (ESD) BAGS AND FOAM WRAP

Electronic devices such as phones and tablets, storage media like discs and SD cards, and PC's may contain a wealth of information. Protect the information they contain from exposure to damaging static electricity and electrostatic impulses with ESD bags from **SIRCHIE®**. *The new 18" x 24" size is large enough for laptop computers.*



Electrostatic bags come in five sizes for various types of electronics, from cell phones to hard drives. For larger devices, such as a desktop computer or server, use ESD Foam Wrap.

CATALOG NO.	DESCRIPTION	PRICE
ESD0406	Electrostatic Dissipation Bags, 4" x 6" (10.2cm x 15.2cm), 100 each	
ESD0608	Electrostatic Dissipation Bags, 6" x 8" (15.2cm x 20.3cm), 100 each	
ESD0810	Electrostatic Dissipation Bags, 8" x 10" (20.3cm x 25.4cm), 100 each	
ESD1012	Electrostatic Dissipation Bags, 10" x 12" (25.4cm x 30.5cm), 50 each	
ESD1824	Electrostatic Dissipation Bags, 18" x 24" (45.7cm x 61cm), 50 each	
ESDF24	Electrostatic Dissipation Foam Wrap, 24" wide x 25' (61cm x 7.6m), 1 roll	

BLACK HOLE FARADAY BAGS (WITH WINDOW)

Black Hole Faraday bags are manufactured with the ISOTech shielding system and materials with windows to offer clear previews of evidence while maintaining a high level of shielding. These bags include protective outer layers to keep shielding material from being exposed and come in three sizes.

CATALOG NO.	DESCRIPTION	PRICE
FBW10	Black Hole Faraday Bag w/Window, Standard, 7.5" x 4.25"	
FBW20	Black Hole Faraday Bag w/Window, Large, 11" x 7.8"	
FBW30	Black Hole Faraday Bag w/Window, XL, 17.25" x 13.75"	
FBW40	Black Hole Faraday Bag Kit, (1 each: Standard, Large, XL)	

BLACK HOLE FARADAY BAGS (WITH WINDOW) FEATURES:

- Usage instructions on bags themselves ensuring they are used correctly
- Pockets for evidence cards on back with 10 cards included
- Windows allow for preview of evidence, monitoring of power of device and phone condition, review for correct adapter

BLACK HOLE DATA BAG KIT

The Black Hole Data Bag Kit has an integral shielded, electronically filtered USB 2.0 connection that allows for charging, data transfer, and analysis of devices without compromising shielding. The kit includes the Data Bag, a separate faraday bag for transport, and a device cradle that allows use of capacitive touch screen devices inside the data bag.

CATALOG NO.	DESCRIPTION	PRICE
FDBK	Black Hole Data Bag Kit	

DATA BAG FEATURES:

- External Dimensions: 17" x 11.75" bag & 20" Cable
- Usage Area: 13.75" x 11"
- Connectivity: Filtered USB 2.0, female internal, male external

TRANSPORT BAG FEATURES:

- External Dimensions: 21.5" x 13.75"
- Usage Area: 18.5" x 13"

TOUCH SCREEN DEVICE CRADLE FEATURES:

- External Dimensions: 21.5" x 13.75"
- External Dimensions: 4" x 5"

TABLETOP STRONGHOLD TENT

This lightweight, portable solution uses the same Stronghold technology and material as the Reusable StrongHold bags and is perfect for performing forensic examinations on active wireless devices. The tent comes with a wireless StrongHold bag to keep your digital evidence secure until you're ready to examine it. Place your investigation laptop and the evidence inside the tent, insert your arms securely into the faraday sleeves, remove your evidence from the included bag and connect it to your investigation laptop for secure examination.

CATALOG NO.	DESCRIPTION	PRICE
FTENT20	Tabletop StrongHold Tent	
FTENT22	Tabletop StrongHold Tent w/shielded USB 2.0	

TABLETOP STRONGHOLD TENT FEATURES:

- Dimensions: 20" x 14" x 14"
- Double Lined
- Mesh Viewing Window on Top
- Gloveless Sleeves give full dexterity for working with small devices
- Designed to have a laptop in tent with device being examined
- Protective flap allows you to store multiple devices in tent at a time

TABLETOP STRONGHOLD TENT INCLUDES:

1- Tent
1- StrongHold Bag (Reusable)
1- LED Light

Mobile Device Forensics

DMSK CONTENTS:

5- FBAGR10 10" x 7" Reusable StrongHold® Evidence Storage Bag for handheld devices
1- FBAGR13 13" x 9" Reusable StrongHold® Evidence Storage Bag for PC
1- of each First Responder Cards (Pocket size cards that provide the steps to maintain your forensic evidence on handheld devices such as smartphones/pda, cellphone and GPS)
1- Remote Charger (Battery operated charger with tips for different devices to allow handheld devices to remain charged until acquisition)
10- ESD1012 10 "x1 2" Electrostatic Dissipation Bags
10- ESD0406 4" x 6" Electrostatic Dissipation Bags
10- IEB1200 12" x 1 5½" Integrity Evidence Bags
10- IEB9120 9" x 12" Integrity Evidence Bags
1- DMSKC Black Nylon Carry Bag

DS & DDS System Requirements

- Processor: 1.4Ghz+
- RAM: 1 GB
- Hard Drive Space: 200 MB
- Windows 2000, XP, 2003, Vista, Windows 7

Get more information from more devices. Depending on the model, DS or DDS can acquire the following data:

- SMS History (Text Messages)
- Phonebook (both stored in the memory of the phone and on the SIM card)
- Call History
  - Received Calls
  - Dialed Numbers
  - Missed Calls
  - Call Dates & Durations
- Datebook
- Scheduler
- Calendar
- To-Do List
- Filesystem
  - System Files
  - Multimedia Files (Images, Videos, etc.)
  - Java Files
  - Quicknotes
  - More...
- PDA Databases
- E-mail

DDRK AND DDRK1 CONTENTS:

1- Tablet PC (DDRK1 only)
3- FBAGR10 Reusable StrongHold® Evidence Storage Bag for handheld devices
1- DDS Deployable Device Seizure software application (integrated on tablet PC)
1- DS-Device Seizure software application (integrated on tablet PC) ***DDRK1 only***
1- Mobile Cable Kit with carry bag
1- One year subscription for both DS and DDS software licenses
10- ESD0406 4" x 6" Electrostatic Dissipation Bags
10- IEB9120 9" x 12" Integrity Evidence Bags
1- DDRKC Black Nylon Carry Bag

DIGITAL MOBILE SEIZURE KIT

The Mobile Seizure Kit is a comprehensive collection system for wireless devices that allows for proper evidence handling with full Faraday protection for any wireless transmitting device. Designed for ease of use and to protect the integrity of your evidence, this kit is essential for investigators in the field.

CATALOG NO.	DESCRIPTION	PRICE
DMSK	Digital Mobile Seizure Kit	

DIGITAL DEVICE REVIEW KIT

The Digital Device Review Kit allows you to conduct mobile triage and contains everything you need to be able to forensically process over 4,000 mobile devices on scene and extract in a forensically sound manner any data associated with those devices.

No. DDRK1 with Tablet PC pictured

Device Seizure (DS) - acquire and analyze data from over 4,000 mobile phones, PDAs and GPS devices including iPhones. It is delivered in a MS Windows format.

Deployable Device Seizure (DDS) is a version of Device Seizure designed for use in the field. It is integrated into a tablet PC and delivered in a touch screen format. It can also be provided for installation on any Windows laptop, or tablet.

Both software packages are advanced forensic acquisition and analysis tools. Don't settle for half the data. Most commercial cell phone forensic software only retrieves logical data files. That's like doing an investigation on half a crime scene. If a tool doesn't have advanced analysis features, it's probably because they don't get enough data to analyze. Deleted data and user data such as text messages and images can often be found in a physical data dump of a phone. Device Seizure was designed from the ground up as a forensic grade tool that has been upheld in countless court cases.

Point 2 Point has been integrated into Device Seizure. The Point 2 Point feature converts GPS data points to be read directly into Google Earth so investigators can quickly and easily visualize where these GPS locations are.

DDS and DS Device Manufacturers and Operating Systems Supported:

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

CATALOG NO.	DESCRIPTION	PRICE
DDRK1	Digital Device Review Kit with Tablet PC	
DDRK	Digital Device Review Kit without Tablet PC	

DIGITAL MOBILE DEVICE KIT

This versatile forensic stick kit contains easy to use tools for the review of mobile digital devices including iPhones, iPads, iTouch devices, Android devices, and cell phones.

CATALOG NO.	DESCRIPTION	PRICE
DSRK100	Digital Mobile Device Kit	

DSRK100 CONTENTS:

- 1- iRecovery Stick – designed to extract active and deleted information from iPhone, iPad, and iTouch devices
- 1- Phone Recovery Stick – designed to recover active and deleted data from hundreds of smart phones and tablets including Android devices, Blackberry phones, Symbian phones, Windows 7 phones, or any phone with removable storage such as MicroSD cards
- 1- Sim Card Seizure – This SIM reader is designed to recover deleted text messages (SMS) from and other information that may be stored on the seized device's SIM card
- 1- Micro-USB Data Cable
- 1- iPhone USB Data Cable
- 1- iPhone 5 USB Data Cable
- 1- DSRKC Plastic Carrying Case

SIM CARD SEIZURE

This SIM reader is designed to recover deleted text messages (SMS) and other information that may be stored on the seized device's SIM card. SIM Card Seizure includes software and a Forensic SIM Card Reader.

CATALOG NO.	DESCRIPTION	PRICE
SIM100	SIM Card Seizure	

SIM CARD SEIZURE INCLUDES:

- 1- SIM Card Seizure software
- 1- Forensic SIM Card Reader

ECLIPSE SCREEN CAPTURE KIT

The Eclipse Screen Capture Kit is designed as an easy to use yet comprehensive system for the capture of user information from screens of cell phones, GPS units, tablets, and any other portable device that can be photographed. The Eclipse kit allows the user to capture screen shots from mobile devices, add notes to them, and organize the images. Eclipse saves images and video within the program and is capable of exporting reports to most web browsers.

CATALOG NO.	DESCRIPTION	PRICE
ECL1000	Eclipse Screen Capture Kit	

ECLIPSE SCREEN CAPTURE KIT FEATURES:

- High quality camera and base
- Quick capture process
- Video and image hashing
- Preview and organization of captures
- Video and images in one report
- Total control for the user

ECLIPSE SCREEN CAPTURE KIT INCLUDES:

- 1- Eclipse Camera and Hardware base
- 1- Eclipse Software
- 1- Hard case for Storage and Transport
- 1- Glare Shield and Flexible Arm
- 1- Standard size Black Hole Faraday Bag

Computer Forensics

DIGITAL COMPUTER REVIEW KIT

The Computer Review Kit contains easy to use tools that allow for on-scene forensic acquisition of data from any computer system. The bootable kit maintains forensic integrity by read-only processing of the computer. The DP2C P2 Commander is a bootable thumb drive that allows you to quickly look for evidence on a PC without making any changes to the computer. It also allows you to extract files you need. Windows Breaker is a thumb drive password breaker for Windows.

DCRK CONTENTS:

1- DP2C-Deployable P2 Commander with external hard drive
1- Windows Breaker
1- DCRKC Black Nylon Carry Bag

CATALOG NO.	DESCRIPTION	PRICE
DCRK	Digital Computer Review Kit	
WBS10	Replacement Windows Breaker Stick, 10 uses	

DIGITAL FORENSIC COMPUTER ANALYSIS KIT

This versatile forensic stick kit contains easy to use tools for the detection and recovery of data from computers, laptops, notebooks, and netbooks.

DSRK200 CONTENTS:

1- Data Recovery Stick – Bootable USB that allows for recovery of deleted documents, photos, music, and more using a cluster-by-cluster forensic grade data recovery algorithm
1- Windows Breaker Stick – Bootable USB that allows for bypassing of Windows accounts – Limit of 10 uses per Windows Breaker Stick
1- Porn Detection Stick – Bootable USB that searches through all images and videos on a computer, scans them for pornographic content, and creates a report of suspected pornographic images and videos
1- Chat Stick – Bootable USB that detects and analyzes chat logs from the most popular online chat programs
1- DSRKC Plastic Carrying Case

CATALOG NO.	DESCRIPTION	PRICE
DSRK200	Digital Forensic Computer Analysis Kit	
WBS10	Replacement Windows Breaker Stick, 10 uses	