Digital Forensics

According to the United Nations, in 2014, there were almost as many cell-phone subscriptions (6.8 billion) as there were people on the earth (seven billion). Digital devices are fully integrated into all facets of our lives and can contain a wealth of information about the owners, their habits, their whereabouts, and their connections.

Along with this integration into our lives comes the growing presence of enormous amounts of evidence gathered from digital devices in criminal cases, such as emails, texts, and video. Currently, these types of evidence appear regularly in court and it is up to law enforcement to properly investigate, preserve, maintain, and analyze this evidence.

Like any other evidence, we offer the tools to package and transport digital devices appropriately so an examiner can effectively gather all the potential evidence.   In addition, we offer tools that empower any investigator to analyze digital evidence and advance your investigations.

Digital Device Forensics

With over 9 Billion wireless subscriptions worldwide as of 2016, every criminal investigation involves information that can be captured from a digital device, including phones and tablets. Understanding what information can be obtained from these devices, as well as how to collect and preserve the information legally is critical. This course will cover various digital devices, how wireless and cellular networks operate, and review data and information that can be obtained from carriers, devices, and the web. Attendees will receive training in tools that they will be able to take away from the class and apply in investigations.

For more information about this and all other training courses, visit www.sirchie.com or call us at (800) 356-7311.

TIPS Digital devices may contain latent, trace, or biological evidence and you should thoroughly document and preserve this evidence before extracting digital evidence from the item. We offer tools for collection and preservation in our Evidence Collection Section and our Latent Print Development Section.

Faraday Protection

Reusable Stronghold Electronic Integrity Evidence Storage Bags

HOT

With the highest level of faraday protection available, these bags, created from a tri-weave material, are essential for all investigators to have with them when entering crime scenes. It prevents unwanted signals from corrupting and erasing vital evidence. It's reusable and available in three sizes: 10" x 7" (ideal for cell phones), 12 ½" x 10" (ideal for tablets), and 14" x 19" (ideal for laptops).

10" x 7" (for phones)

14" x 19" (for laptops)

12 ½" x 10" (for tablets)

No. FBAGR10	Stronghold Faraday Bag, 7" x 10"
No. FBAGR13	Stronghold Faraday Bag, 12 ½" x 10"
No. FBAGR19	Stronghold Faraday Bag, 14" x 19"

Reusable Stronghold Electronic Integrity Evidence Storage Bag Kit

NEW

Get all three sizes in one kit: 10" x 7" (ideal for cell phones), 12 ½" x 10" (ideal for tablets) and 14" x 19" (ideal for laptops) in one convenient package.

No. FBAGR300	Stronghold Bag Kit

Electrostatic Dissipation (ESD) Bags and Foam Wrap

Protect the information on phones, tablets, SD cards, and other devices from static electricity and electrostatic impulses by placing them in these bags or foam wrap.

No. ESD0406	Electrostatic Dissipation Bags, 4" x 6", 100 ea.
No. ESD0608	Electrostatic Dissipation Bags, 6" x 8", 100 ea.
No. ESD0810	Electrostatic Dissipation Bags, 8" x 10", 100 ea.
No. ESD1012	Electrostatic Dissipation Bags, 10" x 12", 50 ea.
No. ESD1824	Electrostatic Dissipation Bags, 18" x 24", 50 ea.
No. ESDF24	Electrostatic Dissipation Foam Wrap, 24" x 25 ft, 1 roll

Black Hole Faraday Bags

Available in a range of sizes (including a duffel bag!), these bags feature four layers of shielding protection for preserving and transporting potential digital evidence. Their effective electromagnetic shielding is created with the ISOTech system, which protects devices from cellular, wifi, Bluetooth, radio signals that could corrupt potential evidence. Available in Standard (ideal for cell phones), Large (ideal for tablets or multiple devices), Extra-large (ideal for laptops), and a Duffel Bag (ideal for transport of many devices).

No. FBH10	Standard Black Hole Faraday Bag, 1 ea.
No. FBH20	Large Black Hole Faraday Bag, 1 ea.
No. FBH30	XL Black Hole Faraday Bag, 1 ea.
No. FBHD	Black Hole Faraday Duffel Bag, 1 ea.

Black Hole Faraday Bag Kit

Have all sizes with you when you're in a crime scene with the Faraday Bag Kit. It includes one of each size: Standard, Large, Extra Large.

No. FBH40	Black Hole Faraday Bag Kit

Black Hole Window Faraday Bags

Protect wireless devices, such as cell phones, GPS, Bluetooth devices, laptops, etc., from cellular, wifi, Bluetooth and radio signals with Black Hole Faraday Bag's ISOTech Shielding System. For your convenience, they have a window so you can see what device is in the bag.

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

Black Hole Data Bag Kit

Protect, charge, transfer data, or analyze data all with the protection of the ISOTech Shielding System. This kit features a USB 2.0 connection, a bag for transport, and a device cradle that lets you use touch screens from inside the data bag.

No. FDBK	Black Hole Data Bag Kit

Tabletop Stronghold Tent

Using Stronghold technology, this portable solution lets you access information on seized devices while keeping the device secure. Place your investigation laptop and the digital evidence inside the tent, insert your arms into the faraday sleeves, remove the suspected device from its stronghold bag and connect the device to your laptop.

No. FTENT20	Tabletop Stronghold Tent

Mobile Device Forensics

Our software tools for mobile device forensics are easy to use and give anyone the power to perform digital forensics investigations. This is especially important as backlogs for digital device labs can be as long as 12-18 months.

E3 Universal Digital Evidence Examination Software

Developed by Paraben, this powerful digital evidence software offers the ability to process any kind of digital data: computer file system/hard drive data; smartphone/mobile data; and emerging Internet of Things (IoT) data. One unified interface gives any lab or organization control over their processing for efficiency and consistency. Each package comes with 3 licenses of E3 Viewer

No. PBE3UNI	E3 Universal Digital Evidence Exam Software

E3 DS Mobile Evidence Examination Software

Developed by Paraben, this digital forensics software offers a simple, well-thought out and executed mobile device forensics tool. This software offers a comprehensive approach for mobile device forensics in a single tool that is capable of logical and physical imaging, data carving, app data parsing, password bypass, unique content analysis and more

No. PBE3MDS	E3 DS Mobile Evidence Exam Software

E3 Viewer for E3 Electronic Evidence Examination Software

E3 viewer is a case review tool that allows other investigators to review the resulting evidence from an investigation. A useful tool for attorneys, detectives, and collaborating investigators.

No. PBE3VIEW	E3 Viewer for E3 Electronic Evidence Exam Software

Digital Analyst Reporting Tool Software

This powerful digital forensics tool allows you to take reports generated by all the most popular extraction software on the market today, load the reports into DART, and instantly perform analysis and investigation across all the reports in one convenient, insightful place. The analytics are what drive DARTPRO to be a powerful tool for today's digital investigator.

No. DARTPRO   **Digital Analyst Reporting Tool Software**

MAPLINK Mobile Phone Mapping Software

MAPLINK provides an effective tool for utilizing Call Detail Records provided by cellular phone providers to develop reports and insights that support investigations. Reports can be created to show behavior patterns, location and travel of possible suspects or victims, and time lines of key communications in an efficient manner.

No. MAPLINK   **MAPLINK Mobile Phone Mapping Software**

Digital Mobile Device Kit

We've put together all the tools in the form of convenient USB sticks to review popular devices including Apple (iPhone, iPad, iPod Touch, iTunes backup) and Android (up to Android 5.1 (if

rooted)) devices.

No. DSRK100   **Digital Mobile Device Kit**

Digital Mobile Device Seizure Kit

This revised kit contains everything you need to collect, transport, and store multiple digital devices from a scene in a convenient package. Contains Faraday bags, electrostatic bags, and Integrity Evidence bags all in a nylon carrying bag.


No. DMSK100   **Digital Mobile Device Seizure Kit**

SIM Card Tools

Mobile phones on the GSM network will use SIM (Subscriber Identity Module) Cards that can contain valuable information in addition to what is on the phone.

DART SIM Card Adapter

Often, you'll find seized SIM cards are damaged. Don't let it hinder your investigation. With the HTCI SIM Adapter, you'll be able to read a damaged SIM card and access that information.
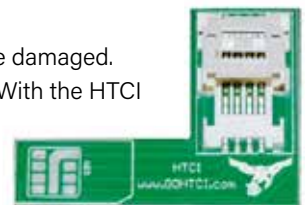
No. SIM300   **DART SIM Card Adapter**

HTCI SIM Toolkit

Use this toolkit to read GSM SIM cards and copy data from a suspect card to an HTCI Labs Slug card. A slug card will copy the original SIM card data, including the phone book and SMS entries from the suspect card. This toolkit can be reused once you remove all previous data.

No. SIM200   **HTCI SIM Toolkit**

SIM Card Seizure

Recover deleted SMS (text messages) and perform a comprehensive analysis of SIM card data. Software, card reader, and adapters for micro and nano SIMs are included.

No. SIM100   **SIM Card Seizure**