

Where is my Forensic Replicator (Lessons Learned in Developing an Information Technology Lab

Victor Williams
Dean
American Intercontinental University
6600 Peachtree Dunwoody Rd
Atlanta, GA 30328
770-722-2603

During the past 3 years, there has been a growing career in computer forensics. There are many reasons why the field is growing so fast. One of the reasons is that there are many shows on television that glorify the field of forensics. Another reason is that there is also a need because of the growing problem of Identity thief and child predators on the Internet.

With the growing need for individuals with a degree in Computer Forensics, American InterContinental University decided to add a Computer Forensics concentration to its Bachelor of Science in Information Technology degree. Since adding the Computer Forensics concentration, the School of Information Technology enrollment has grown by 20 percent. This in only the beginning, it is expected that this growth will last for the next 3 years.

As a result of the growth, it was very important that the School of Information Technology built a lab with the state of the art equipment in the Forensics' field. The Dean of the program researched many different companies and organizations to determine what was the best equipment for the program. Below is some of equipment that is being used in the School of Information Technology Forensics Lab.

PARABEN'S P3 POWER PACK

Forensic Replicator

Electronic media can be the key to a case and nothing is more important than acquiring that data. Paraben's Forensic Replicator duplicates exact copies of drives and media.

Paraben's Lockdown

Paraben's Lockdown is an advanced Firewire or USB to IDE **write-blocker** that combines speed and portability to allow IDE media to be acquired quickly and safely in Windows. Write-blockers prevent changes from being made to the suspect media.

P2 eXplorer

Paraben's P2 eXplorer allows you to mount your forensic image and explore it as though it were a drive on your machine while preserving the forensic nature of your evidence. This means that an image isn't just mounted to view logical files, it is mounted as the actual bitstream image, preserving unallocated, slack, and deleted data. P2X is easy to use.

Forensic Sorter

Sorting through data is an effective way to find exactly what you are looking for. Forensic Sorter classifies data into over 14 different categories, recovers deleted files, and filters out common

hashes, making your examination easier to manage, faster to process, and easier to find what you're looking for. Paraben's Forensic Sorter saves hours of examination time through this efficient classification and sorting process.

E-mail Examiner

E-mail Examiner doesn't just recover e-mail in the deleted folders; it recovers e-mail deleted from deleted items. With the ability to examine AOL 9.0, PST files (Microsoft Outlook), and ability to examine over 14 other mail types, you'll have the right tool for e-mail examination in your toolbox.

Network E-mail Examiner

With Network E-mail Examiner, you can now thoroughly examine Microsoft Exchange (EDB), Lotus Notes (NFS), and GroupWise e-mail stores. Network E-mail Examiner is designed to work hand-in-hand with E-mail Examiner and all output is compatible and can easily be loaded for more complex tasks.

Text Searcher

Text Searcher is a fast, comprehensive, and feature-rich text searching tool that will make any examiner more effective and more efficient. Text Searcher includes an indexing wizard, file libraries, supports multiple languages, and supports over 200 different file types.

Case Agent Companion

Paraben's Case Agent Companion is designed to optimize both the time of the examiner and the agent working the case. Built in viewers for over 225 file formats, searching, and reporting make Case Agent Companion the most comprehensive tool of its kind.

Decryption Collection Enterprise

Paraben's Decryption Collection is an advanced password recovery suite. Recover more passwords in a shorter amount of time. Everyone needs as many tools as possible in their toolbox. It loads a password cache for quick recovery of repeat passwords. English password recovery of 90% and higher.

PDA Seizure

The most advanced forensic tool for Palm, Windows CE, & BlackBerry devices. As an examiner you know better than anyone that the difference between making a case and losing a case is hard evidence. And with more bad guys going high tech, obtaining that evidence is becoming more difficult than ever. Paraben's PDA Seizure is a comprehensive tool that allows PDA data to be acquired, viewed, and reported on, all within a WindowsTM environment. You can also analyze Palm data that is stored on a PC.

PDA Seizure Toolbox

The PDA Seizure Toolbox was designed as a collection of the items that would be needed in different scenarios for PDA Seizure. The items in this toolbox in combination with the appropriate software allow for acquisitions of over 42 different PDAs.

Cell Seizure

Cell phone forensics is not to be compared with traditional bit stream forensics. Cell phone data storage is proprietary, based on the manufacturer, model, and system. Paraben's Cell Seizure was designed to allow forensic acquisition of user entered data and portions of unallocated storage on some devices. It also performs a forensic acquisition on all data stored on GSM Sim Cards including deleted data. Each device is unique and should be dealt with caution as each phone has unique considerations. Continual advances will be made to Paraben's Cell Seizure in reference to acquiring of proprietary data.

Paraben's Cell Seizure currently supports certain phone models from the following manufacturers: Nokia, Sony-Ericsson, Motorola, Siemens, Samsung, GSM SIM Cards

- Supports GSM as well as TDMA/CDMA phones
- Acquires text messages, address books, call logs, and more
- Acquires complete GSM SIM card information including deleted data
- Recovers deleted data
- Multi-language (Unicode) support for languages such as Arabic, Russian, Chinese, etc.

Cell Seizure Toolbox

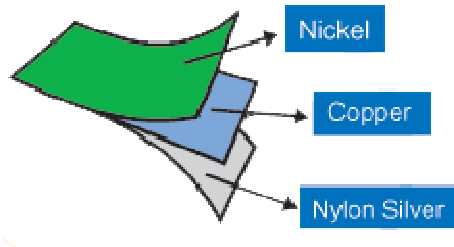
The cell seizure toolbox contains connections and cables for GSM SIM Cards, Nokia, Ericsson, Siemens, Motorola, Samsung phones, and a Remote Charger for all types of Nokia, Motorola, Ericsson, Siemens, and Samsung phones.

StrongHold Bag

Build a fortress around your wireless evidence and keep unwanted wireless signals out.

Paraben's Wireless StrongHold Bag (Patent Pending) 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.

The special tri-weave material used in the Wireless StrongHold Bag is made of a Nickel, Copper, Silver Plated Nylon plain woven fabric. This fabric is key in preventing unwanted signals from your evidence. Each StrongHold Bag comes with a clear evidence bag to allow for proper evidence handling.



Chat Examiner

Chatting online is not just a passing phase. More and more people are communicating through chat. And that means loads of digital evidence. As an examiner, you need a specialized tool to perform a thorough analysis of chat logs. Paraben's Chat Examiner is another specialized component of Paraben's P2 Forensic Collection that adds one more powerful program to your toolkit. Whether your case has ICQ, Yahoo, MSN, Trillian, or Miranda you'll be able to handle whatever comes your way. Please note that AOL Instant Messenger (AIM) does not have traditional data stores or logs and therefore will not be supported by Chat Examiner.

NetAnalysis

Forensic examinations can consist of gigabytes of data that can make or break a case. However, one of the most pivotal pieces of evidence is sometimes overlooked, internet cache and history. NetAnalysis is the ideal tool for dealing with this data. The powerful searching, filtering and evidence identification make this tool not only feature rich, but the perfect tool to add to your arsenal for dealing with internet related data.

Supports Internet Explorer 3, 4, 5 & 6, Netscape Communicator / Navigator up to 4.79 & Apple Mac Netscape Bookmark, Netscape up to 6.2 and the new Netscape 7, Mozilla Browser, Opera
Support for AOL ARL History Files
Recover Deleted Internet History from Unallocated Space
Cookie and URL Viewer/Decoder
Filter to identify Google Desktop searches

ImageMASter Solo III Forensic

Use:

- Forensically duplicate a suspect's data – identical bit by bit copy.
- Wipe data from a drive – removing all traces of the data. Meets U.S. Department of Defense specification DOD 5220-22M for sanitization of hard drives.

Benefits:

- Can make two evidence drives – identical copies for examining.
- Fast – data can be seized at speeds exceeding three gigabytes per minute.
- Built in hashing capabilities – makes sure that the new evidence drive matches the suspect's drive exactly.
- Built in Write Protection – so the suspect's data will not be overwritten by accident.

- Provide an Audit Trail and report Log for tracking what was done.

REMEMBER: Delete does not mean gone!

AccessData's Ultimate Toolkit™

Includes:

- **Forensic Toolkit® (FTK™)**
 - Find, Organize, & Analyze Computer Evidence
 - Generate audit logs and case reports.
 - Automatically recover deleted files and partitions.
 - Target key files quickly by creating custom file filters.
 - Identify and flag known child pornography and other potential evidence files
- **Password Recovery Toolkit™ (PRTK™)**
 - Recover Lost or Forgotten Passwords
 - Recovers all types of passwords regardless of password length.
 - Analyzes multiple files at one time.
 - Recovers multilingual passwords.
- **Registry Viewer™**
 - Analyze & Decrypt Registry Data from AutoComplete “form” data from Google, Yahoo, and more; Internet Explorer account login names and passwords; Outlook and Outlook Express account information including servers, users, and passwords
 - View files individually without reconstructing the full Registry
- **100 Client Distributed Network Attack® (DNA®)**
 - Uses the power of machines across the network or across the world to decrypt passwords.
 - Easy to read Statistics and Graphs
 - Optimization for password attacks for specific languages
- **WipeDrive™ Home & Small Office Solution**
 - Completely Eliminate Hard Drive Data
 - Securely overwrite and remove ALL of your data. DoD 5220.22-M Approved.
 - Verifies your data has been erased.

REMEMBER: Formatting your hard drive DOES NOT erase your data!

Because of the success of the Computer Forensics concentration in the School of Technology, other schools have started looking into adding a concentration in Forensics. The School of Business is in the process of adding a concentration in Accounting Forensics. The School of Criminal Justice is also in the process of adding a concentration in Field Forensics.