Paraben Forensic Toolkit

Digital Forensics

Rodrigo Lopes

October 31, 2006

Introduction

Paraben is a software company founded in 1999, headquartered in Pleasant Grove, Utah. The company first made itself noticeable by releasing the PDA Seizure application, being later complemented by the Cell Seizure and ultimately merged into the Device Seizure application.
Paraben also develops solutions for hard drive and media analysis, having a wide range of application that aim at specific steps of the forensic analysis process. Paraben claims to have created a shift in the way Forensics analysis is done, moving from monolithic applications that do all the tasks to an approach where different applications are used in specific stages of the process, which allows the investigator to focus on some particular aspect of the analysis with the right tool for it without the need for a whole toolkit.
Lately, Paraben has been focusing on enterprise forensics, developing solutions to monitor and secure enterprise networks, being proactive in the way it monitors what happens so that in an event of an incident, the forensically sound evidence will already be available, provided by the system. But the enterprise solution from Paraben isn't only a forensic tool, it aim at being a complete security solution, providing intrusion detection, and user behavior monitoring, so that any sudden changes in behavior pattern can be detected.

Handheld Forensics

Handheld forensics is the area where Paraben fisrt started to work on. It has one of the most complete solutions for analyzing handheld devices such as PDAs and Mobile Phones.
The first application to be developed was "PDA Seizure", in early 2002, and it became a success, supporting different vendors and software. Late, "Cell Seizure" was implemented and became the first commercial tool that allowed forensic analysis on cell phones.
The two tools ended up being combined in a single solution for handheld devices called "Device Seizure", currently on version 1.0.
Device seizure supports hundreds of cell phone models and includes the PDD (Palm DD Command Line Acquisition) as well as support for the Palm OS up to version 6, Windows CE/Pocket PC/Mobile up to version 4.x, Blackberry 4.x and earlier and finally Symbian OS up to version 6.0. Together with the toolbox, a Parabens solution is one of the best available.
The line of products is divided in three different products, one being the already referred "Device Seizure", the second software solution is the "SIM card seizure"

and finally, the last solution is the hardware that allows data to be extracted form handheld devices, the “Device Seizure Toolbox”.

Device Seizure

Device Seizure presents itself as a true forensic tool that, unlike many other available products, derives from forensic tools and not from data management software.
It can perform deleted data recovery and full device dump from some cell phone models, logical and physical acquisitions of PDAs and provides advanced reporting abilities. It can also connect on cell phone via Bluetooth or IrDA and perform live analysis on the device.
Device Seizure isn’t able to write any kind of information onto the devices, which allows a true secure forensic analysis, assuring the preservation of evidence.
The addition of support for new models can easily be done with log files, which makes the process easy and little time consuming on the investigating environment.
Paraben commits itself to continually improve the list of supported devices as well as extending what it can do on the devices already supported.
Focusing not only on the logical level but also at the physical level, Device Seizure may allow the extraction of more data than the allowed by the operating system. This physical acquisition is done by model type and implemented through plug-in extensions.
Viewers and data carvesrs are also included, to help the analysis of the retrieved data, as well as a useful reporting utility. All of this makes Paraben’s Device Seizure on the best solutions available for device forensics.

SIM Card Seizure

This tools allows the dump of the data included in SIM cards. It may included as a plug in for Device Seizure, but it is also offered as a stand alone Product. The tool also includes a write blocking SIM card reader to assure a truly forensic approach to the analysis of such storage devices. This tool is aimed at the investigator who only wants to perform analysis on the SIM card and not on a cell phone. It can retrieve a large set of different data from the card, like contact lists, sms, last dialed numbers and it can also recover some deleted data from unallocated space.

Device Seizure Toolbox

This is a hardware toolbox, designed to help the investigator acquiring and preserving handheld devices. It includes cables and adaptors that together with the appropriate software allow preservation and data acquisition from a wide range of devices. The contents include not only adaptors to retrieve data, but also power adaptors to feed energy onto devices, in case this is necessary.

Paraben also has solutions for preventing cell phones or other devices to communicate. Resuming, Paraben handheld solutions provide the tools for the forensic investigator to deal with a wide variety of situations and incipient scenarios, from the collection of physical devices to the analysis of the data they contain, all of this assuring good forensic practices.

Pricing

The cost for the Paraben's solutions for handheld devices is stated in the following table:

Product	**Price**
Device Seizure	$895,00
SIM Card Seizure	$129,00
Device Seizure Toolbox	$749,00
Device Seizure + Toolbox	$1.595,00

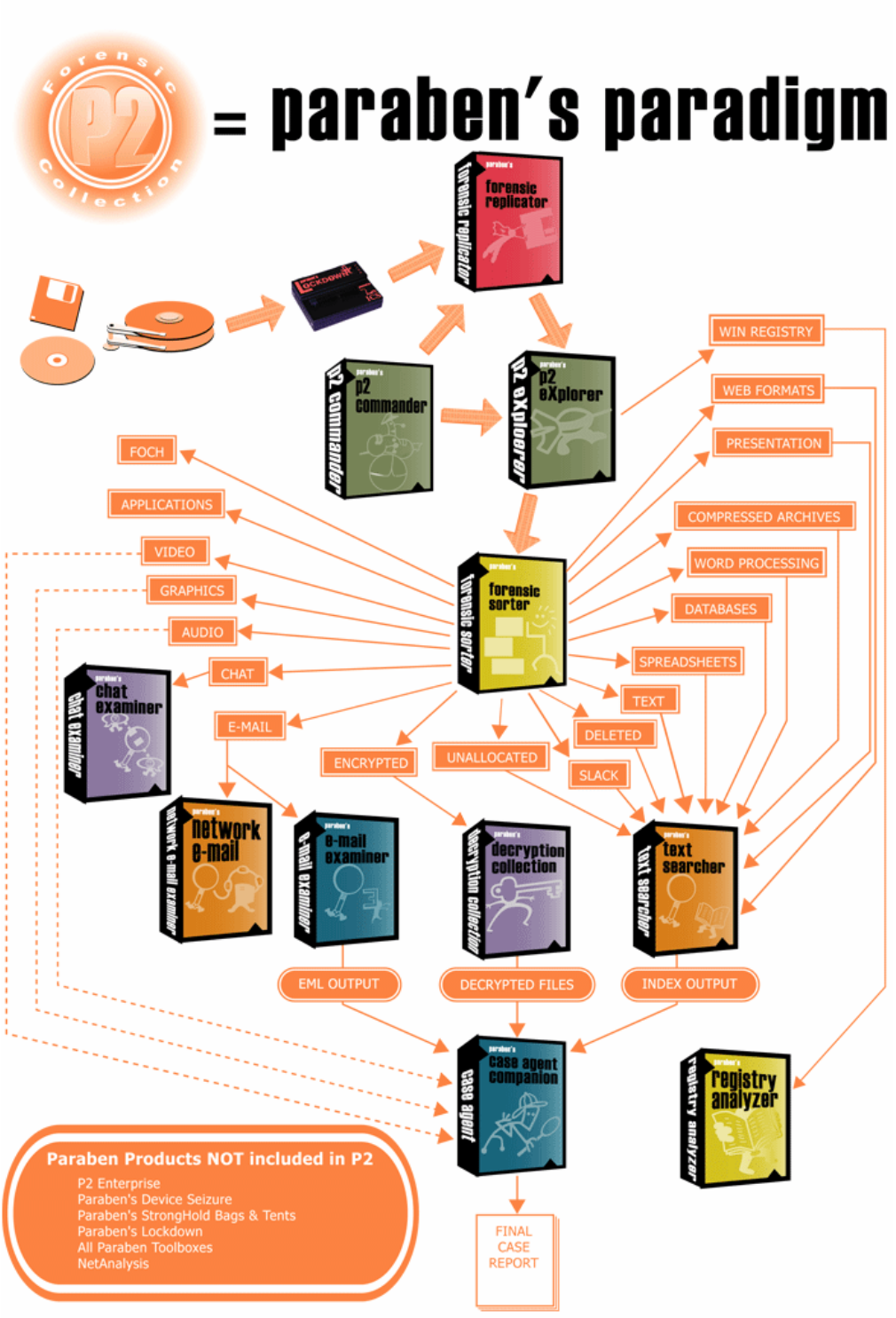
Hard Drive / Media Forensics

"Paraben's P2 Examination Process for hard drives is more than just a collection of software tools; it is a paradigm shift in computer forensics. "

"using more than one tool to complete the examination "

The two excerpts from Paraben's website describe what the company believes to have been an innovation introduced by them. The separation of the forensic analysis process into different steps, each one of them helped by a specific tool designed with specific goals in mind. Paraben offers a long list of tools which can

be applied in an investigation as the following diagram proposes. From the forensically sound replication of hard drives, to extracting, sorting and analyzing the data included in it. As in the handheld devices case, Paraben also offers a hardware device that allows reading hard drives without writing any data to them. This hardware device is a write blocker caller “Lockdown”.



From the diagram it can easily be seen what is the Paraben approach. After replicating the hard drive and sorting it, there are different tools to analyze different kinds of data, and even a Windows registry analyzer culminating with the report elaboration.
Those tools are sold separately or as a bundle in the Paraben's P2 Power Pack or P3 Power Pack. While the first includes the most commonly used tools, the second includes all the tools, even the handheld solutions. A brief description of each of the tools is provided below.

Tools

- Case Agent Companion

Tool to aid the investigator in his process of analyzing the evidence. Includes viewers for over 225 file types as well as searching and reporting functionality.

- Chat Examiner

As more and more people are using chat clients, this tool helps the investigator in the task of analyzing logs from chat clients. The tool supports MSN, Yahoo, Trillian and Miranda chat logs, allowing browsing and searching, also helping with the reporting.

- Decryption Collection

This tool helps recovering passwords for a large set of common applications such as Zip, Word, Powerpoint, Excel, Rar, PDF and so on. It as an easy to use interface and it allows up to 16 computers to process in parallel when trying brute force or dictionary attacks.

- E-mail Examiner

Just like Chat examiner, this tool helps the forensic investigator when it comes to dealing in data from a specific kind of application. As email exchange is becoming more and more usual, the amounts of data to analyze can be immense. This tool is provides forensically sound analysis of data from a wide variety of mail clients and also recovers deleted messages, helping with browsing and searching the results.

- Forensic Replicator

This tool is used to make forensically sound copies of media devices, form floppy disks, to usb drives and

hard drives. It can create compressed or fragmented images on the fly.

- Forensic Sorter

This tool is aimed at sorting the recovered data into different categories, saving time on the hard task of looking at the data and classifying it. It divides the data into 14 categories, included encrypted files.

- Network E-mail Examiner

This tool allows recovery of email from email storage such as Microsoft Exchange, Lotus Notes or Group Wise. It was designed to work in close connection with the email examiner and all results are compatible.

- P2 Explorer

Allows mounting images of media drives, preserving its actual bit structure and not only the file structure. This means that the unallocated and slack space is preserved. This tool allows the drive to be forensically explored without changing its contents and verifies the hashes. The tool also allows mounting images from other toolkits such as EnCase and SafeBack.

- Registry Analyzer

This is a specific tool to help in the potentially tedious task of analyzing what may be thousands of windows registry entries. This tool was purchased from MiTeC in 2005 and has been released under the new name by Paraben, who keeps updating the tool.

- Text Searcher

Easy to use tool to efficiently run specific text searches over the recovered data.

Pricing

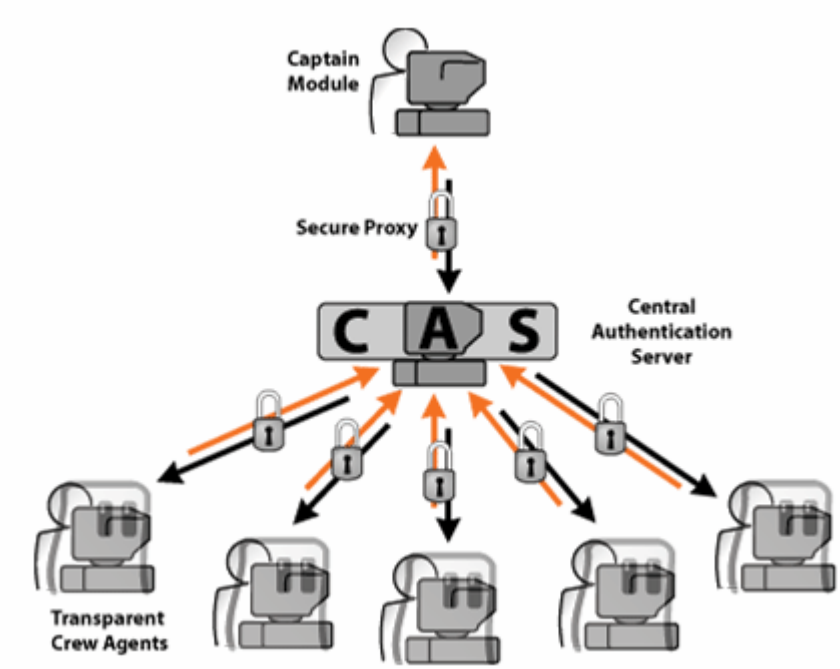
On the table below are the prices for the power packs offered by Paraben:

Pack	**Price**
P2 Power Pack	$1.495,00
P3 Power Pack	$3.495,00

Enterprise Forensics

Enterprise Forensics is a new product from Paraben, still in beta version.

Paraben states that this tool will be a complete forensics and security solution for enterprises. It is supposed to be proactive, monitoring the enterprise network and registering forensically sound evidence while the potential incidents are occurring. The tool works using different kinds of server and client modules. The diagram below illustrates what is the concept and main software modules involved.



As it can be seen from the diagram there are 4 different modules, three servers and one client. The central authentication server provides the authentication mechanism for the solution; it contains the rules for the interconnection of all other modules and also acts as repository for all collected data. The Secure Proxy serves one main purpose as it is the main communication pass through for the system. The captain module is the GUI for all the Paraben Enterprise solution allowing the customization and control of all the other modules. The client module is the crew agent, which is installed on every machine on the network. This module runs at the lowest possible level and is controlled by the captain module, recording and monitoring all the activity on the machines. The crew agent can also be remotely deployed by the captain module and supports both a forensic and non-forensic mode, with the forensic mode sending all the collected data to a central store.

The price for the solution is only available upon request and the announced functionality includes for the P2 Enterprise Edition includes:

- Drive Acquisition
- Network Monitoring
- Volatile Data Acquisition

- Telnet
- Network Searching
- Client Snapshot
- P2 Navigator
- Reporting

Shuttle version

The shuttle version of the Paraben Enterprise Edition is aimed at the field investigator, so it allows an easy deployment on the network and its forensic analysis. It also requires for the Crew Agent to be installed, but this time, the investigator can simply connect using the shuttle version and perform the analysis.

References

General:
http://www.paraben-forensics.com

Enterprise:
http://www.paraben-forensics.com/enterprise_forensics.html
http://www.paraben-enterprise.com/

P2:
http://www.paraben-forensics.com/catalog/product_info.php?cPath=25&products_id=187

Individual Poducts:
http://www.paraben-forensics.com/catalog/index.php?cPath=25