EDEC Digital Forensics
1805 E Cabrillo Blvd. Suite F
Santa Barbara, Ca 93108
http://www.edecdigitalforensics.com
http://www.faraday-bags.com

Tarantula Chinese Cell Phone Analysis Tool General Overview

Tarantula Specializes in Analysis of White-Box Phones

Currently, 30% of cell phones worldwide are based on chipsets designed and manufactured in China. This trend is expected to increase to over 50% going forward into 2012 and beyond, as Chinese mobile device production tops 800 million. While there are a myriad of legitimate mobile devices made by registered Chinese manufacturers and sold the world over, **white-box phones or "Clone Phones"** are devices that imitate big brand phones, known in China as "Shanzhai".

White-box mobile devices often contain unusual but desirable features like dual, triple or quadruple SIM card slots. These phones have traditionally been made by small Independent design houses imitating international handset manufacturer's designs, but now a number of these companies have become recognized brands throughout the world. For many years these ultra low cost devices remained as feature phones, but recently a shift has occurred with some Chinese-chipset hardware manufacturers beginning to support smartphone operating systems like Android. White-box phones on the market today support GSM, CDMA, 2g and 3g networks with 4g capability expected soon. Different levels of quality exist in the white-box world, with un-subsidized price points as low as $25, for feature phones, and as low as $90 for Android OS phones.

The lack of adherence to industry standards from manufacturers of white-box mobile devices has made them very difficult for digital forensic investigators to analyze with standard tools and techniques.

Forget Phone Support Based on Make and Model

There are literally tens of thousands of different models of white-box cell phones available on the market, many of which are knock-offs of popular models like the iPhone 4. Even two handsets that look identical may be very different internally, so it would be virtually impossible to develop methods for analyzing each and every handset. Luckily for forensic investigators, just a few major chipset manufacturers power most of these devices.

How is Tarantula Different?

EDEC Digital Forensic **Tarantula** is the first and only tool on the market capable of acquiring and decoding data from phones with chipsets manufactured by all four major Chinese chip companies, Mediatek, Spreadtrum, Infineon and Mstar.

To compare, Cellebrite's Chinex is a connectivity kit for its UFED Physical Analyzer. Chinex is capable of physical extraction of critical data from a subset of phones based on MediaTek chips only, not including Mediatek smart phones or international brand phones based on Mediatek chips. Micro Systemation's XRY system is capable of logical data extraction from a subset of several hundred Chinese phones, and was recently updated to support physical extraction from a small group of Chinese phones based on

Mediatek chips, using Micro USB or Mini USB connections. Oxygen Forensics recently updated their Oxygen Forensic Suite 2012 to support MediaTek phones for logical extraction.

The main difference with Tarantula is more support for Chinese phone extraction and analysis. We support more chipsets and more phones within those chipsets.

White-box Phones are Just One Piece of the Puzzle

Legitimate (well-known) cell phone manufacturers using Chinese chipsets include:

- Motorola – EX112, EX115, EX122, EX126, EX128, EX211, EX212, etc..
- Alcatel – OT606, OT213, OT665, OT710, OT710D, OT799, etc…
- Lenovo – A60, P70, etc…
- Doro – 410, 310, 326, etc..
- CSL – Blueberry line, DS line, etc…
- Other manufacturers – Vodafone, Spice Mobile India, Micromax India, Blu phones, etc…

Barriers to Analysis

Unique Operating Systems:

- Not open source
- Different operating system
- Different file system structure

Non-Standard Cables:

Another hindrance to forensic analysis is the absence of standards for hardware such as data cables. Even though the cables that come with these phones may look the same as the cables that come with Android or iPhone handsets, the wiring is often different. This is sometimes a deliberate strategy by manufacturers to maximize accessory sales. Unfortunately it also impedes the task of the digital forensics investigator, as it can be difficult to establish compatibility between these phones and forensic analysis tools.

Fortunately, there is a Solution

EDEC Digital Forensics Tarantula gives investigators the ability to physically and logically analyze data from a vast majority of Chinese mobile devices. For physical analysis, Tarantula supports all major Chinese chipsets and chip types, accounting for over 90% of the market for these devices. Physical extraction and analysis results in recovery of deleted data as well as undeleted data that is simply not previewable on these types of devices. The logical extraction process provides complementary information to our physical process as well. If time is an issue, logical extraction is a quick way to get some basic info from MediaTek chip devices, including pin codes and IMEI numbers.

Supported Chinese chipsets:

- MediaTek
- Spreadtrum
- Infineon
- MStar

Accessible Data:

- SMS
- Contacts
- Call Log
- Active Pin-Code
- Historical Pin-Codes
- Phone Id Info

- Multiple IMEI
- Deleted Data

Tarantula Hardware:

- Defines the pin configuration of the phone
- Adjusts the speed of extraction
- Facilitates bootloader injection and binary extraction
- Designed to not electrically short/harm/brick the phone

Tarantula Cable Set:

- Includes 31 data cables made for Chinese phones
- Support approximately 90% of Chinese phone connections
- Serial connectors
- Allows investigator to define the pin

Staying ahead of the curve

EDEC Digital Forensics is dedicated to helping law enforcement officials remain at the cutting edge of the industry. To meet this goal, we continually:

- Maintain the best solution for Chinese cell phone analysis with our team on the ground in China
- Develop new methods of extracting data from constantly changing devices.
- Increase decoding support for more user information (some things coming) - MMS, browser history, media files, chat programs, etc.

From the lab to the field

EDEC Digital Forensics continuously analyzes the end-use of our tools and upgrades them to support lab and field use.