Quarterly Magazine for Digital Forensics Practitioners

DIGITAL FORENSICS

/ MAGAZINE

Jim Grier explains how to carry out an investigation, when no artefacts exist, using his stochastic forensics approach

9 772042 061127
Issue 11 / £14.99
TR Media

/ REGULARS
ROBSERVATIONS, 360, NEWS, IRQ & MORE...

/ FROM THE LAB
IMAGE METADATA FOR EFFECTIVE DATA MINING

/ INTRODUCING
CYBER WARFARE & COVERT CHANNELS

/ BOOK REVIEWS
INCLUDING THE BASICS OF DIGITAL FORENSICS

CHINESE CELL PHONES & DIGITAL FORENSICS

In this article, we explain why investigators need to understand the macro trends in the cell phone industry driving the incorporation of more Chinese chipsets in phones and the challenges that they present to examiners. We also lift the lid on Tarantula, a new analysis system developed to analyze problematic Chinese "white box" cell phones and, increasingly, the legitimate branded phones based on Chinese chipsets.

by Kevin J North

/ INTERMEDIATE

Hercules had to defeat a hydra as one of his 12 labours. It was a monster with 9 heads, and if Hercules smashed one head, two more would take its place. For mobile forensic investigators, Hercules' hydra takes the form of Chinese cell phones. More specifically, knock-off phones, known internationally as "white-box" or "clone-phones" and "Shanzhai" (pirated goods) in China, have taken world markets by storm. In 2011, over 800 million cellular mobile devices in close to 40,000 models were manufactured in China. Approximately half of those were exported to world markets, comprising of more than 30% of the global cell phone market.

/ SIMPLE BEGINNINGS

Chinese cell phones came into existence as a result of China's unparalleled manufacturing base fuelled by abundant, low-cost labour, a flood of international investment, a robust supply chain, and the world's largest market. In southern China, manufacturing plants dominate the landscape and the city of Shenzhen is the epicentre of the cell phone industry. More specifically, Shenzhen's North Huangqiang Street is China's major hub for mobile phone commerce.

In the early 2000s, a Taiwanese integrated circuit (IC) manufacturer, MediaTek launched an innovative business

strategy in China, offering hardware packages called “systems on a chip” (SoC) for wireless communication devices. This development opened the door for small, entrepreneurial teams with as few as 4 people to design and contract manufacture, cell phones.

Entrepreneurs, both legitimate and illegitimate, leveraged these hardware packages and the manufacturing environment to rapidly produce even relatively small runs of phone designs. Hundreds of small companies known as independent design houses (IDH) in Shenzhen alone churn out white box phones with a dazzling array of features; many useful, some highly creative, and others entirely fake. The fastest producers can get from idea to market in less than 30 days compared to months or years for larger international cell phone companies. With near unlimited demand domestically and a foreign market hungry to participate in the digital revolution but often unable to buy expensive branded phones; China has become a world leader in mobile phone production, rivalling even their more established western counterparts.

While not produced with quality in mind, white box technology is attaining a level of complexity that is nearly state of the art. Knock off makers follow industry trends to take advantage of the accomplishments of legitimate technology developers. White-box devices have advanced rapidly from simple feature phones to include the same high end features on popular international brands, and now smart phones.

High-end clones can be visually nearly indistinguishable from the legitimate phones that they mimic, including popular iPhone and Blackberry handset models. In many cases the knock-offs use components from the same sub-suppliers as the legitimate manufacturer. White box phones often adopt famous brands that have nothing to do with the cell phone industry like Adidas or Marlboro and manufacturers are opportunistic, building a phone around available parts until they run out; then moving on to the next opportunity. The transient and shadowy nature of the industry frustrates any standardization for hardware or software found in these phones.

While IDH’s customize the phones they develop, the core features such as screen resolution, Bluetooth, media capability or network support are determined by the specifications of the SoC (chipset) they decide to use. For roughly ten years, the hardware packages from the top Chinese chipset manufactures were closed platform, offering only feature phone capability. In mid 2011, however, a major shift occurred with the introduction of Chinese chipsets supporting Android. The driving force of white box innovation is really at the hands of the SoC manufacturers, and they are meeting market demands with cutting-edge chip sets able to run smart phone operating systems, albeit at a higher price than the ultra low cost feature phones that still flood the market.

CHINA HAS BECOME A WORLD LEADER IN MOBILE PHONE PRODUCTION, RIVALLING EVEN THEIR MORE ESTABLISHED WESTERN COUNTERPARTS

In some cases, white box phone manufacturers like Tianyu or Oppo have become so sophisticated and so well established as producers that they eventually "go legit" with their own brands. More mainstream brands like HuaWei, ZTE, TCL and Lenovo are some of the largest brands using the Chinese chipsets in their phones, selling their phones through China's three largest carriers.

/ BARRIERS TO ANALYSIS

The non-standard nature of Chinese phones makes them vexing to mobile forensics examiners. They are often built on unique or modified operating systems with modifications that may only exist in a certain production run of a handset model. Until recently all white box phones were embedded platforms, not open source, and many contain distinct file system structures.

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.

While standard logical cell phone tools use synchronization to extract data, white box manufacturers typically block synchronization features. Even when the hardware is compatible, phone manufacturers may disallow synchronization through the software as a means of simplifying the devices. (The transfer of media files is typically supported however).

The barriers to analysis of white box phones come down to one core issue, the absence of industry standards. Unfortunately, hundreds of millions of cell phones are circulating in worldwide markets that are so cheap they are nearly disposable, that accommodate multiple SIM chips, function across national borders, and are inherently difficult to analyze, making them perfect for criminal activity and a huge challenge for investigators.

/ A GLOBAL ISSUE

Further compounding the threat, these phones are quickly internationalized, moving from China to Southeast Asia, the Middle East, Africa and beyond. They may be flashed and re-flashed with new software, exacerbating the problem of tracking the devices with issues like non-unique IMEI numbers and IMEI numbers that do not relate to manufacturing origin or phone model. Certain countries like the United Kingdom prohibit by law the changing of IMEI numbers, a practice that is commonplace with white box phones.

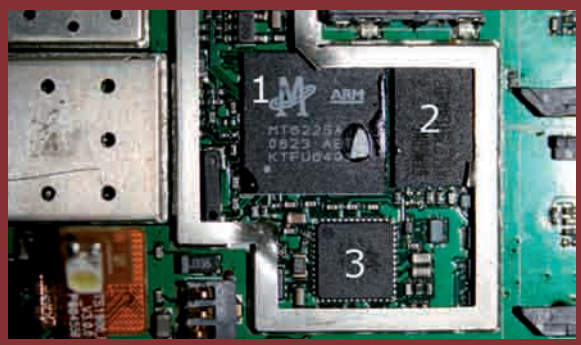
If you think the adoption of smart phones will make the Chinese phone problem go away, think again. Market research firm, Strategy Analytics, reports that while the US is still the largest smartphone market overall, China overtook the US as the largest market for smartphones retailing below $ 170 (the fastest growing segment of the market). Major Chinese chipset manufacturers; MediaTek, Infineon, Spreadtrum, and

/ INSIDE THE CHINESE CHIP MARKET

Approximately 800 million Chinese chipped cell phones entered the global market in 2011, making up nearly 35% of devices worldwide. Given the rapid increase in prevalence, popularity and sophistication of these devices, it is important to know who makes the chipsets that allow them to operate. As the industry leaders, the companies below will shape the future of white-box mobile devices.

Top White-box Chip Makers:

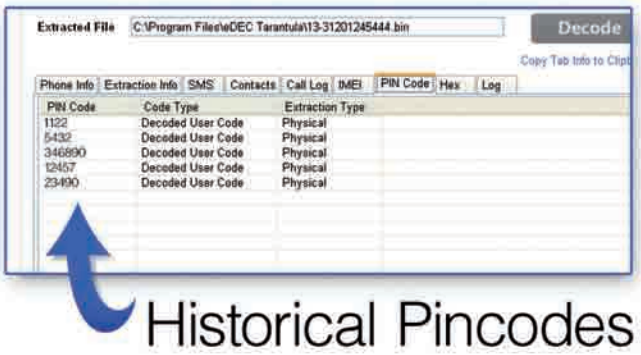
- **MediaTek (MTK): (Approximate Market Share 60%) MediaTek develops chips for everything from GPS systems to HDTVs. MediaTek is the world's second largest producer of semiconductors to the cell phone industry, after Qualcomm.**
- **Spreadtrum: (Approximate Market Share 30%) As the second largest white-box chipset manufacturer, Spreadtrum has its sights set on MediaTek and has doubled its market share over the past decade.**
- **Infineon Technologies: (Approximate Market Share 5%) A spin-off of Siemens AG in 1999, Infineon made its name by providing semiconductors to the automotive, industrial and multimarket sectors before entering the cell phone industry.**
- **M-star Semi Conductor: (Approximate Market Share 5%) Split from System General Technology in 2002, MStar specializes in mixed-mode integrated circuit technologies. MStar is known in China as "Little-M", contrasting the firm with "Big-M" – MediaTek.**



Mstar are racing to develop chipsets to serve this market and Chinese phone manufacturers like Huawei, ZTE, TCL, and Lenovo are designing smart phones. Even non-Chinese brands like Motorola and Alcatel are incorporating Chinese chipsets in some of their less expensive smartphones and in India, Spice Mobile and Micromax are designing smart phones around low-cost Chinese chipsets. Strategy Analytics predicts that the sales of lower cost smart phones will triple from 191 million phones in 2012 to 551 million phones in 2016, with 75% being exported to emerging markets. So whether they are in feature phones or smart phones, Chinese chip based phones are here to stay.

/ IT'S NOT ABOUT PHONES; ITS ABOUT CHIPSETS

Fortunately, even in the face of all these hindrances to analysis, there is a light at the end of the tunnel for mobile forensic professionals. Even with tens of thousands of handset models on the market, over 90% of the chipsets at the heart of these devices are designed and built primarily by four firms: Spreadtrum, Infineon, MStar and MediaTek (MTK). The concentration of manufacturers enables forensics technology



developers to focus their efforts on tools that can physically analyze the chipsets on which the phones are designed.

International mobile forensic companies are working on technologies to address the growing problem of phones based on Chinese chipsets. At the forefront of this effort is EDEC Digital Forensics with Tarantula, currently the only forensic tool that can extract and decode data from all 4 major Chinese chipset manufacturers (comprising about 90% of all phones that include Chinese chipsets), In addition to decoding data such as phone book contacts, call logs, and SMS messages, Tarantula acquires deleted data, PIN lock codes and IMEIs (both current and historical, if present) from most chipsets.

In demonstrations to the state police forces in Australia, Jason Hanel, Owner of Task Intelligence, a security and investigation firm located near Canberra, Australia, invited them to bring their own Chinese phones. In all cases, Tarantula has succeeded in getting data. Phones purchased whilst in Singapore and Indonesia were also tested with good results.

In addition, Cellebrite's UFED 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. Micro Systemation's XRY system is capable of logical data extraction from a subset of several hundred Chinese phones. Oxygen Forensics recently updated their proprietary Oxygen Forensic Suite 2012 to support MediaTek phones and Logicube has announced that it has a licensing agreement with EDEC allowing it to integrate Tarantula into its own CellXtract product allowing it to do physical analysis on Chinese phones.

/ INDUSTRY COOPERATION

While there may be competition between the leading developers of digital forensics tools, there is also a good deal of cooperation and collaboration. As much as executives want their products to outsell the competition, they recognize the need to provide effective tools to as many law enforcement as possible. This was evidenced in March of this year, eDEC and Logicube announced that they were partnering to combine Tarantula software with CellXtract hardware. The finished product is slated to debut at this year's Techno Security & Digital Investigations and Mobile Forensics Conferences in Myrtle Beach, South Carolina, USA.

In a release regarding the partnership, Logicube Executive Vice President and COO Farid Emrani stated, "Our digital forensics customers are encountering large quantities of these types of phones, creating an urgent requirement to extract and analyze data and evidence from them. Integrating Tarantula with Logicube's data extraction device, CellXtract, provides added functionality that will give law enforcement, military and government agencies an unparalleled solution to address the thousands and thousands of phones, including legitimate brands and white box, manufactured with Chinese chipsets."

/ LOOKING FORWARD

There is no doubt that cell phones based on Chinese chipsets will continue to present a challenge to investigators for the foreseeable future. MediaTek, Spreadtrum and other IC manufacturers are not only vying for position in the Chinese market, they are also making headway in the global market by signing deals with the world's top cell phone manufacturers. Feature phone chipsets that have been utilized by Chinese IDHs for years, such as Mediatek's MT6226 or MT6253 are showing up in low cost handsets from international firms like Motorola and Alcatel.

With the core strength of cell phone hardware manufacturing achieved, Chinese chipset manufacturers are now expanding their reach to include a wider range of mobile device types. MediaTek's smartphone chipset, MT6573, and Spreadtrum's SC8810 are capable of supporting Android tablets, a device category previously dominated by Western IC firms. Both companies are working to create chipsets that support Japanese and Korean networks, another category previously served by international players. The landscape of mobile devices is shifting as Chinese chipsets manufacturers evolve at unprecedented speed.

To be prepared for all potential scenarios, forensics investigators need to ensure that they are trained in the latest acquisition methods for the latest devices. By the same token, forensics tool developers will need to remain vigilant and cooperate with one another to remain at the forefront of Chinese chip technology.

While there are many factors that make analysis of Chinese built devices exceedingly difficult, the silver lining is that there is a whole industry rising to these challenges. The best way forensic investigators can prepare for the future is to pay careful attention to industry trends and seek out the appropriate educational programs to ensure that they are as well versed in this emerging field. The bottom line is that Chinese technology is here to stay, so we might as well adapt to it. /

/ AUTHOR BIO

Kevin J. North is an American freelance journalist who specializes in the fields of finance and technology. He is a graduate of Monmouth University in West Long Branch, New Jersey, with a Bachelors Degree in Public Relations and Journalism. Currently, Mr. North resides in Santa Barbara, California, where he writes and edits articles related to digital forensics, automotive safety technology and financial advice for investors. In addition to his work as a journalist, Mr. North serves as a consultant to the health and wellness, web design, entertainment, and data acquisition industries.

COMPETITION

/ THIS ISSUE WE HAVE A TARANTULA CHINESE CELL PHONE ANALYSIS KIT TO GIVE AWAY, COURTESY OF EDEC

/ QUESTION

In his article, "Visualising Photographic Image Metadata for Effective Data Mining", Ollie Whitehouse explains that image metadata can be stored in three formats, EXIF, IIM and XMP. What does the acronym XMP stand for?

A. EXTENSIBLE METADATA PLATFORM
B. EXTENDABLE METADATA PLATFORM
C. EXTENDABLE METADATA PROCESSES

/ TO ENTER

To enter the competition all you need to do is send an email to: competition@digitalforensicsmagazine.com, writing ISSUE11COMP in the subject line, include your name address and phone number with your entry.

TERMS AND CONDITIONS

This competition is open to anyone aged 18 or over, except for employees of TR Media Ltd and their immediate families. Only one entry is permitted per person. Entries can be submitted by email only to competition@digitalforensicsmagazine.com. TR Media shall not be responsible for technical errors in telecommunication networks, Internet access or otherwise, preventing entry to this competition. Closing date for all entries is on 1 June 2012 at 9.30am GMT. Any entries received after that time will not be included. The correct winning entry, chosen at random by the DFM team, will be notified by email on 01/07/2012. The winners may also be announced in Issue 11 of the magazine and on the Digital Forensics Magazine website. Submitting your entry constitutes your consent for us to use your name for editorial or publicity purposes, should you be one of the winners. TR Media Ltd reserves the right to change or withdraw the competition and/or prize at any time. By entering the competition, entrants are deemed to have accepted these terms and conditions.

DIGITAL FORENSICS / MAGAZINE

EDEC™

MOBILE FORENSICS PRODUCTS

MILITARY / LAW ENFORCEMENT / INVESTIGATION

Learn about our products at
www.edecdigitalforensics.com