JTAG-CHIPOFF-ISP FORENSICS- TOOLS & CHALLENGES

In the field of mobile-device forensics, the practices of “chip-off” and “JTAG” analysis have become topics of growing interest among the community. As mobile devices continue to bring new challenges to the examiner, these two disciplines warrant close attention, as they both offer examiners avenues for deeper data access, the ability to bypass lock codes, and a way to recover data from damaged devices.

While today’s commercial tools continue to provide innovations at an impressive rate and offer extensive and expanding phone support with increasing data-recovery abilities, the unfortunate reality is that there is a seemingly infinite number of devices that continue to challenge examiners, creating the requirement for alternative means of data recovery.

Ultimately, the goal for the mobile-device forensic examiner is to obtain a physical image of the memory chip from mobile devices. And while today such bit-by-bit acquisition support from the commercial tools is increasing, in many instances such a physical dump cannot be accomplished without direct access to the memory chip.

Additionally, for devices that are damaged or locked with an encryption scheme that is beyond today’s tools’ abilities to bypass or crack, the chip-off and JTAG methods are among the alternative solutions for examiners looking to gain access to the memory.

In a perfect world, the commercial tools would do it all, and the examiner could process easily and comprehensively the mounting piles of mobile devices in their lab. As anyone who has spent any time trying to acquire data from mobile devices knows, the general rule remains: you just never know what you will be confronted with next, and just how much data can be obtained. Further, considering that commercial tools most often connect to the device through a USB connection, some device manufacturers employ memory management schemes that inhibit the data transfer through the communication port via controllers that make it impossible to acquire a complete image of the memory. Simply put, chip-off or JTAG techniques are the only way to obtain a complete image on some devices.

INTRODUCTION TO CHIPP-OFF & JTAG

The chip-off technique describes the practice of removing a memory chip, or any chip, from a circuit board and reading it. The chips are often tested and programmed with the “JTAG” method. The term JTAG is the original acronym and name of an IEEE group that set the standards for what would become the 1149.1 Standard Test Access Port and Boundary-Scan Architecture. In plain English, the group established a universally accepted means for testing wire-line interconnects on printed circuit boards. Today, the ports are used for testing

integrated circuits, and they are the common test and debug interface for mobile devices and digital products.

These are not new concepts by themselves, and have in fact been in practice for several years in the integrated circuit programming and testing fields. However, a byproduct of both of these low-level access techniques is the ability to acquire raw data from the memory chip. For the mobile-device examiner, these practices offer another way to access and acquire the raw data from the memory chip.

Prior to engaging in the practice of chip-off or JTAG efforts for mobile-device forensics, a solid understanding of key characteristics of the mobile device's structure is necessary to properly and successfully pursue these techniques. Particularly, the examiner must have a familiarity with modern mobile-devices' configurations, the memory types, how they manage data internally, where memory chips are located, and how to identify JTAG connectors on the motherboard of a mobile device. Building this solid foundation of knowledge of where and how data is stored (and erased) is essential for the examiner heading down the chip-off or JTAG roads.

Additionally, a solid command of the skills for repair, dismantling, and chip removal is crucial to properly pursue these techniques.

Chip-off and JTAG are as far from push-button forensics as one can get, and examiners intent on pursuing these practices have to be educated, prepared, and very patient.

- **NAND Memory (TSOP and BGA)**
- **NOR Memory**
- **Volatile RAM**
- **Flash Translation Layer—Controller Chips**
- **Wear Leveling—Garbage Collection**

SIMILARITIES & DIFFERENCES BETWEEN CHIP-OFF & JTAG FORENSICS

Initially, the major difference between chip-off and JTAG is that the chip-off technique is a more destructive method; once a memory chip is removed from a mobile device, it cannot be returned to the original mobile device. It follows, of course, that once a memory chip is removed from a mobile device, the device cannot be returned to normal operation or examined using a commercial tool. When a device is damaged beyond repair, but the memory chip is intact, the chip-off technique is likely the only opportunity to obtain data from the device.

JTAG is often a preferred method with devices that are operational but inaccessible using standard tools.

While both techniques offer the ability to obtain a complete image of the device, both are not without their risks and difficulties not to mention that both techniques take time and care to perform properly.

Chip removal from a device is the practice of desoldering the chip from the circuit board, and requires a set of tools and precise techniques to ensure the memory chip is removed from the device properly. The risk of damaging the chip and therefore losing the data is very real without proper care and handling.

JTAG, the less risky of the two solutions in terms of jeopardizing the data, still requires precision disassembly of the device, probing the JTAG Test Access Ports for the proper connection for data, and soldering connectors to the JTAG ports. Ideally, an examiner will have the schematics of the device to identify the proper connections for data. But such schematics are not easily obtained so extra time and tools are required to identify and then solder connectors to the proper contacts.

THE CHIP-OFF PRACTICE

Once a chip is removed, the next step is to ensure it can be read with a chip-reading apparatus. For some chip types, preparation is relatively easy. For example, the TSOP-style NAND chip that is commonly found in thumb drives, SD cards, digital voice recorders, digital answering machines, and the iPhone 2 and 3G, is typically an easier type of memory chip to remove and read with chip-reading equipment. It certainly requires precision handling, but compared to its BGA-brethren, TSOP is an easier chip to read and acquire data from.

This is largely due to the relative standardization of the TSOP memory architecture and pin configuration, and therefore the actual chip-reading equipment requirements are limited. The TSOP-style chip has connectors around the outer edge of the chip, and these are connected by soldering onto the motherboard. Removal from the board, as well as attachment to a chip-reading adapter, is relatively easy, and no rebuilding of the connectors is typically necessary.

A BGA chip, on the other hand, has multiple connectors on the underside of the chip, and these are soldered to the motherboard of the device. Additionally, they are often secured with epoxy, which makes the task more challenging. The BGA-style chip construction does not follow a common standard, but rather is developed by the chip manufacturers to their own discretion and demands of their handset customers.

So, whereas the access to and connectivity with the pins on a TSOP NAND chip are relatively manageable, the connectors on a BGA NAND chip require, in many cases, rework through a process known as “re-balling”—or effectively rebuilding the connectors on the chip to be connected to the chip-reading equipment.

As luck would have it, the BGA-style chip is the most commonly used in mobile devices these days, and will likely remain so, due in part to its ability to store and manage high volumes of user data. But, as advances in BGA connection to motherboards improves at the manufacturer level, the requirement to solder and epoxy the chips to the boards is diminishing. More precise and versatile connection techniques are being employed, ultimately saving chipset manufacturers time and money as yields are improving. Fortunately for the examiner, the reballing effort has become less burdensome on newer devices.

DATA ACQUIRED FROM CHIP-OFF & JTAG: WHAT TO EXPECT

The data from a chip is acquired using their lasers and robotic precision machines with lots of blinking diodes, the data will inevitably be showcased on flat-panel screens the size of billboards. The neatly and completely decoded data will showcase just where the suspect had traveled throughout the time of interest, and reveal every last deleted picture and text message in its original format.

Unfortunately, such a pretty outcome is not quite ready for primetime in the real world, although absent the blinking diodes we are getting there. The advancements in decoding using the commercial mobile-device tools, computer forensics software, and the chip-reading tools themselves are being used regularly and seeing continual improvement.

But, in many instances, the results of such deep access and recovery of the physical memory data from mobile devices is a large pile of zeroes and ones or hex data that the examiner needs to manually carve through and decode with other tools and skills, utilizing the range of solutions in the toolbox from traditional computer forensic solutions to custom scripts to carve for data. A few of the forensic mobile-device tools are accommodating for the data acquired outside their own support, thus making it easier for the examiner to work with and implement custom scripts.

IN CONCLUSION: BE PREPARED & RESPONSIBLE WITH THE APPROACH

While the use of chip-off and JTAG can be very useful for data recovery, it is imperative that examiners understand the risks involved and gain a proper understanding before making attempts on devices certainly when it comes to evidence. We cannot stress enough the

importance of proper training, plenty of practice and when you are ready to perform the activity on a real case—to perform a first run-through with similar devices.

Chip-off and JTAG techniques are indeed opening up new avenues for the mobile-device examiner to recover data, and we have heard of more than a few instances where old phones in evidence archives that were believed to be inaccessible are now being looked at again, this time successfully. For this purpose and to tackle broken, destroyed, or otherwise inaccessible devices the two techniques are worthy of pursuit.