JTAG - ChipOff - ISP Forensics - Tools and Challenges

JTAG

In order to delve as deeply as possible into a mobile device for your forensic investigation, you may need to access the device's contents on a physical level—creating and sorting through a raw data dump of the smartphone's NAND or NOR flash memory chips. There are many tools and techniques which allow forensic investigators to obtain this level of access, even if the smartphone is locked.

Joint Test Action Group (JTAG) is an industry standard devised for testing printed circuit boards (PCBs) using boundary scan and was designed to quickly and easily test PCBs coming off a manufacturing assembly line. JTAG Forensics is a process that uses that same process and involves connecting the the Test Access Ports (TAPs) on a PCB via solder, molex or jig and then uses a supported JTAG Box (Riff, Z3X, ATF, etc.) to instruct the processor to acquire the raw data stored on the connected memory chip to get a full physical image from the device. This process is non-destructive to the phone.

A typical digital board with JTAG devices includes the following main components:

- Various JTAG components such as CPLDs, FPGAs, Processors, etc., chained together via the boundary-scan path.
- Non-JTAG components (clusters).
- Various types of memory devices.
- Flash Memory components.
- Transparent components such as series resistors or buffers.

A typical boundary-scan test system consists of two basic elements: Test Program Generation and Test Execution. Generally the Test Program Generator (TPG) requires the netlist of the Unit Under Test (UUT) and the BSDL files of the JTAG components. The TPG automatically generates test patterns that allow fault detection and isolation for all JTAG testable nets of the printed circuit board (PCB). The TPG also creates test vectors to detect faults on the pins of non-scannable components such as clusters and memories that are surrounded by scannable devices. The test execution tool provides means for executing

JTAG tests and perform in-circuit-programming in a pre-planned specific order called a test plan. Essentially all embedded systems platforms have a JTAG port to support in-circuit debugging and firmware programming. ARM architecture processors, Modern 8-bit and 16-bit microcontroller chips, FPGAs & CPLDs, MIPS & PowerPC processors, Intel core, Quark processors, PCI bus connector, etc comes with JTAG support.

The JTAG forensic method is a difficult procedure, and could be risky if attempted by an individual without the proper training and expertise due to the delicacy of the operation. JTAG method can only be successful as long as the device can still turn on. If the phone you need to pull data from has been damaged to the point where it no longer functions at all (whether by water damage, fire damage, or excessive physical trauma), chip-off methods are required for physical acquisition (and due to the damage to the phone, a full physical acquisition may not be possible). JTAG is one of many methods of forensic physical acquisition, and like the other methods, it doesn't have a 100% success rate. JTAG forensics has a few risks, despite being a non-invasive acquisition method, due to the delicate work and electrical skills needed to apply the leads to the phone's proper access points. While the smartphone is powered on, the forensic examiner must partially disassemble the phone to expose its motherboard, then carefully solder the leads to the correct access ports.

Chip-off

Chip-off Forensics is the process in which a BGA memory chip is removed from a device and prepared so that a chip reader can acquire the raw data to obtain a physical data dump. A chip reader, like the UP 828P Programmer or a SIREDA test socket, is required to perform the read and in the case of the UP 828P, a specific adapter will be required depending on the specific chip. Unlike JTAG, chip-off is a destructive process, and the device will no longer function. Many examiners start with a non-destructive technique like JTAG or ISP before submitting to a Chip-off.

When all other forensic extraction options – including JTAG – have been exhausted; however, there are certain situations in which a chip-off may be the initial preferred method. These include situations in which it is important to preserve the state of memory exactly as it exists on the evidence device. Most of the chip-off projects involve extracting data from cellular phones; however, the

chip-off method can be used to extract data from nearly any device that utilizes flash memory (NAND, NOR, OneNAND or eMMC). In addition to cell phones we have extracted data from digital voice recorders, GPS units, tablets, USB drives, gaming systems, network devices and vehicle components.

Method of doing Chip-Off

1. The memory chip is physically removed. This is accomplished using appropriate heat (desoldering) and chemicals (adhesive removal).
2. The chip is cleaned and repaired (or re-balled) as necessary.
3. The raw data is acquired or "imaged" from the chip using specialized chip programmers and adapters.
4. The raw forensic image is then analyzed using industry standard forensic tools and custom utilities

Success rates of chip-off forensics remain high, approximately 95%, but there is always some risk to the chip during the removal and cleaning process. Chip-Off is a destructive process and will make the mobile device inoperable.

Chip-off is the most difficult way of data extraction from mobile devices. This method forces examiner to work with encryption and encoding, unknown or hardly known file systems, new formats of databases

Some Examples

1. **Distracted Driving** – in a wrongful death case involving a smashed cell phone, data acquired via chip-off demonstrated that the driver was interacting with a social media website at the time of impact.
2. **Sexual Exploitation** – incriminating audio recordings were deleted from a voice recorder that did not possess a data port. The device memory chip was removed, read and found to utilize the common FAT file-system. Deleted recordings were recoverable using common forensic software.
3. **Domestic/Cheating Spouse** – in one case a wife attempted to destroy her "secret" phone with a hammer and, in another, a husband threw his phone into a pond. In both cases relevant SMS text messages and pictures were recovered via a chip-off exam.
4. **Questionable Death** – a password locked Blackberry smartphone was found with the victim. A chip-off extraction was performed to directly access the memory and circumvent the device password. Recovered SMS text messages indicated that the death was a result of suicide.

ISP

In-System Programming (ISP) applied to forensics, is the practice of connecting to an eMMC or eMCP flash memory chip for the purpose of downloading a device's complete memory contents. eMMC and eMCP memory are the standard in today's smartphones, and the ISP practice enables examiners to directly recover a complete data dump without removing the chip or destroying the device. Identifying the taps that connect to the memory chip using a multimeter is required in ISP technique. Thus, for each evidence phone, a second identical phone that can be destroyed will be needed.

It benefits the examiner who faces the challenges of tightening budgets, yet wants to expand their expertise in retrieving evidence from locked smartphones. A cost-effective technique, ISP provides examiners with the same results of a chip-off at a lower price-point.

Similar to JTAG extractions, the forensic examiner has to solder wires to places on the board. This technique is useful for a few reasons, one is that some phones don't have accessible TAPs, or two, the manufacturer has disabled data access through the TAPs. So to get around this, we solder wires to resistors and capacitors. The hard part is finding pinouts of the device you're looking for, which tells you what pins you need to solder to. This method is usually a bit more tough due to the fact that the pins are usually much smaller than JTAG TAPs, which in turn usually needs a microscope and a much finer solder tip, as well as a steady hand. This process also works on passcode enabled devices, but again, not encrypted devices. The usual pins that are needed to be soldered: Data 0, Vcc, Vccq, CLK (clock), CMD (command), Ground. The pins that are needed to be connected to a box that knows how to access and interpret the data. Devices such as the Riff Box 2, Medusa Pro, and Easy JTAG

<u>Need of ISP</u>

- ISP enables examiners to bypass lock codes, and recover a complete data collection from phones not supported by JTAG or commercial tools.
- It's a non-destructive practice that achieves the same results as a chip-off, while leaving the original evidence intact.
- Acquires data much faster than JTAG, enabling examiners to process more phones faster.

- Less resources and tools are required to perform an ISP download compared to Chip-Off.