CHIP-OFF FORENSICS

Extracting a full bit-stream image from devices containing embedded flash memory
by Jim Swauger

As digital forensic investigators we are accustomed to challenges. We are challenged by malfunctioning hard drives, data encryption, new or uncommon application artifacts and many other stumbling blocks on a regular basis. In most cases we are able to adapt and overcome; however, one hurdle that often thwarts even the most resourceful forensic investigator is extracting ALL data from devices which contain embedded flash memory technology. Typically, in order to complete a thorough examination and recover “deleted” content, we must have access to every bit of raw data contained on the target storage devices. When dealing with traditional hard drives this is often referred to as a forensic bit-stream image and includes a copy of every sector of the target drive. There are a plethora of software and hardware tools on the market that make this type of collection relatively easy. Unfortunately, the options to obtain access to this type of low-level data from embedded flash-memory devices (like cellular phones) are limited at best. And these limited options are directly inverse to the popularity and evidentiary value of embedded flash-memory devices. For example, nearly half of the US and UK population owns a Smartphone, which are essentially fully-functional handheld computers carried by their owner nearly every waking minute. Just think of all the probative evidence they might hold!

While forensic tool vendors are regularly introducing and refining utilities to help examiners extract and analyze more evidence from cell phones and other mobile devices, extraction possibilities are dependent on the make and model of the target device. Due to the proprietary nature of these devices, forensic tool vendors must research and develop solutions for each particular phone model or device family. With literally thousands of models on the market today, this results in limited support with preference given to the more popular devices. When a particular device is submitted to a lab for analysis, examiners must go through their toolkit hoping some tool can recover the data important to their case. In some cases, it is possible to obtain a full image of the flash memory using a commercial tool or advanced technique, but too often the extraction possibilities are limited to only logical-level data such as active test messages, pictures, call logs, etc. This limited data extraction does not allow for a full examination or recovery of deleted data and other potentially critical system or application artifacts – possibly leaving tons of critically relevant forensic evidence out of reach.

So, how do we obtain a full forensic image from embedded flash memory chips if physical extraction is not supported by commercial utilities? What if there is support for the device but the phone itself is physically broken? In these cases, chip-off forensics, “defined as the extraction and analysis of data stored on flash memory chips” may allow for the complete collection of all data stored on the subject evidence device. At a very high level, this process is similar to imaging a hard drive with a handheld imaging unit. We are essentially disconnecting the storage component from the device, connecting it via an appropriate adapter, and reading the raw data using a specialized programming unit.

/ COMMON CHIP-OFF SCENARIOS

A chip-off extraction allows examiners to get access to data stored on some popular devices which are currently a source of frustration for many investigators. For example, deleted content stored on Blackberry and “throw down” phones with crippled data ports (such as Treo/680 models) can be recovered. Devices secured with a passcode, pattern, or other lock can be extracted. Also, the chip-off process makes it possible for badly damaged devices (including water damage), and items lacking connection ports to be acquired and analyzed. A few example successes include:

- We were able to acquire data stored on a pattern locked device at issue in a questionable death investigation. The recovered contents confirmed that the deceased had committed suicide.
- Even though the evidence phone was broken in half, a chip-off was successfully performed to recover deleted text messages at issue in a child sexual exploitation case.
- In a vehicular wrongful death case involving potential cell phone distraction, low-level Internet history artifacts recovered from a flash extraction were able to show the driver was interacting with a social media website at the time of impact.

/ SPECIALIST TOOLS AND SKILLS

A chip-off project does require access to some specialized tools and electronic rework skills. In addition to standard forensic utilities used to assist with examinations and reporting, the chip-off process requires electrical rework equipment and chip programmers. The rework equipment is used to remove, clean, and prepare memory chips prior to data acquisition. The chip programmers are used to actually interface with the memory chip and download the stored data to a raw image file.

Common rework equipment includes hot-air or infrared rework stations, soldering stations, preheaters, digital convection ovens and various probes, tweezers, brushes and BGA stencils. Common laboratory consumables include solder balls or paste, desoldering braid, flux and cleaning solvents. A stereo-microscope is also recommended for chip and PCB inspection.
Chip programmers are needed to read the data from the removed chips and anyone doing regular chip-off extractions will quickly find that there is no magic bullet when it comes to programmers. There are several manufacturers that produce universal programmers which can read the flash memory chips we are targeting; however, no one programmer has out-of-box support for the thousands of chip models that an examiner may encounter. Therefore, it is essential for examiners to have access to multiple programmer device models; some of which can be quite expensive.

The other component required for each chip-off job is an appropriate adapter compatible with the target chip package. These adapters allow the programming unit to make the electrical connections with the different chip models. Some programmers utilize universal adapters that work for several chip models whereas other programmers require a specific adapter for each chip.

It is worth mentioning that the skills required to remove, clean, and re-ball these memory chips are also very specialized. It can take many hours of practice and on-the-job experience to become a proficient rework technician. It may make sense to take a team-based approach to chip-off by partnering, at minimum, a rework technician with a digital forensic investigator.

/HOUSTON/\n
The ultimate goal of a chip-off project is to capture and analyze the raw data saved on a target device’s flash memory chip on the printed circuit board (PCB). In order to accomplish this, the typical chip-off project progresses through three distinct phases: Assessment, Acquisition and Analysis. The assessment phase involves researching the target device to make sure it is a good chip-off candidate and preparing it for the extraction. The acquisition phase involves the actual chip removal and capture of data. The analysis phase involves the recovery and interpretation of the acquired data.
traditional methods. In most cases, a pre-collection should be performed before disassembling the device. This is essentially the collection of whatever data can be captured using standard forensic tools, usually a logical, file-system level, or manual “camera” collection. We do this because there is no going back, once the chip is removed most standard vendor extraction and reporting tools cannot be utilized.

CHIP-OFF FORENSICS – WHICH IS DEFINED AS THE EXTRACTION AND ANALYSIS OF DATA STORED ON FLASH MEMORY CHIPS – MAY ALLOW FOR THE COMPLETE COLLECTION OF ALL DATA STORED ON THE SUBJECT EVIDENCE DEVICE

WARNING: CHIP-OFFS INVOLVE SOME RISK

If the target data is important, it is highly recommended that a control device of the same model be obtained for testing. For example, if you are attempting to collect data from Blackberry 9650 then purchase a 9650 from eBay so the chip-off process can be tested on an expendable device. Keep in mind that even very similar devices and like models of different product revisions can use different flash chips, PCB layouts and thicknesses, and various means to secure the chip to the board. These all affect the chip removal process and care should be taken to ensure you are not “practicing” on your original evidence.

Device teardown is where we physically take apart the device and identify key components. Specifically, we are looking for the flash memory chips that may be used to store user data. Experienced chip-off investigators can often quickly locate these chips but novice examiners will need to look for candidates by finding chips with common memory manufacture logos or markings (ST, Samsung, Toshiba, Spansion, etc.) and then researching the model number printed on the component. With a specific target chip model number in hand, the investigator can check to make sure they have access to a chip programmer and compatible adapter.

THE ACQUISITION PHASE

This is when the rubber meets the road and actual chip-off happens. Once confident that you have identified the target chip and have access to a programmer and adapter capable of reading the chip, it is time to proceed with chip removal.

The first step is to strip and prepare the PCB. This involves removing detachable components such as cameras, displays and keypads and stripping away metal shielding, tape, and stickers from the target chips. Next is the actual removal of the chip. This can be accomplished using an infrared or hot-air rework station. Often the choice comes down to the technician’s personal preference and the type of chip involved. TSOP chips can be easily removed and cleaned using a hot air rework station and desoldering braid. On the other hand, BGA chips are more difficult – the evidence chip must be heated to the target temperature, using flux as necessary, until the solder connections have melted and adhesive bonds have been separated. Then the chip can be carefully lifted from the PCB. Once separated, chips will then need to be thoroughly cleaned; or “dressed”, prior to re-ballin. The cleaning process may vary depending on the chip condition but, generally, this
is accomplished by using desoldering braid and light pressure with a soldering iron. Care must be taken because too much pressure or excessive temperatures can damage the pads or cause them to completely separate from the chip.

After a final light rub with cleaning solvent, the chip is ready to be re-balled. Re-balling is the process of affixing tiny spheres of solder to each lead pad on the chip. Common flash BGA chips usually have anywhere from 40 to 225 of these tiny pads spaced by less than 0.8mm – a solder ball must be attached to each one. Again, different technicians may employ different techniques during the re-balling process. One method involves coating the pads with a sticky flux. The tiny solder spheres are then applied to the pad with the help of a stencil or, in some cases, manually placed one by one. The flux holds the balls in place and facilitates bonding between the solder and pads. The balls are then melted; or “reflowed”, to permanently affix each solder ball to a pad. Once a solder ball is attached to each pad and the chip has cooled, the flux residue is removed with a cleaning solvent.

The chip is now ready for reading. The appropriate chip package adapter is attached to the programmer and the re-balled chip is placed into the adapter. The target chip manufacturer and model number is selected from the programmer user interface – this instructs the programmer which algorithm and other parameters to use during the data extraction. The chip data is then read, verified, and then saved as a raw image file. This is subsequently hashed with your algorithm of choice, such as MD5 or SHA1s, for future data integrity validation.

/ FLASH MEMORY CHARACTERISTICS

Flash memory is a solid-state (meaning there are no moving parts) and non-volatile (meaning power is not needed to retain data) data storage technology that can be repeatedly erased and reprogrammed. While this article focuses on mobile phones, flash memory is embedded in all kinds of consumer devices available on the market today. Forensic examiners will typically encounter flash memory in a BGA (Ball Grid Array) or TSOP (Thin Small-Outline Package) microchip package. These are surface mounted components which can be found on the device PCB (Printed Circuit Board). BGA chips are by far the most common type of chip likely to be found in cellular devices; unfortunately, they are much more difficult to work with than their TSOP counterparts. TSOP chips are a low profile chip with pins extending from opposite sides of the chip. BGA chips have the bottom face covered with pads arranged in a grid pattern. These pads align with a pattern on the host PCB and are connected with tiny balls of solder.

/ THE ANALYSIS PHASE

Once the raw data has been extracted, analysis can begin. The data examination is often the most challenging aspect of a chip-off project. In addition to vast differences in device operating systems, file systems, and data storage structures, the examiner must understand and account for the low-level characteristics of flash memory. Data stored in flash memory is saved in pages; these pages contain a certain number of bytes, like 512 or 2048 and are analogous to sectors on a hard drive. Multiple pages are grouped into larger blocks, similar to clusters in a FAT file system. However, in flash memory spare data is interspersed between the pages or blocks. This spare data contains information related to the pages or blocks such as active versus bad, error correction data, and most importantly to the examiner, addressing information which will allow the data blocks to be reassembled in the correct order. This is important because due to wear leveling algorithms, the high-level data saved to flash memory is not contiguous, meaning the pages are not in logical order. When raw data is extracted from a flash chip, the data which makes up the file-system is also not in order. Think of this as a book with all of the pages ripped out and randomly shuffled. With a book, the physical pages can be correctly reordered by referencing the page numbers. In our case, the logical file-system can be reordered by referencing the addressing information contained in the spare area. The process can be daunting and may require development of custom programs or scripts for a particular device.

WHILE MANY LABS MAY NOT HAVE THE RESOURCES, PERSONNEL, OR DESIRE TO PERFORM CHIP-OFFS THEMSELVES, THERE ARE OPTIONS TO PARTNER WITH A LAB THAT DOES TO ASSIST WITH SOME OR ALL OF THE CHIP-OFF PROCESS
Depending on the situation, it is not always necessary to logically rebuild the file system after a chip-off dump. If the investigator is only interested in smaller artifacts such as SMS, web-history, contacts or call logs, these can often be searched or carved directly from the raw extraction. However, larger files such as pictures and video cannot be directly read because the chunks of interspersed spare data will corrupt the data stream.

Despite analysis challenges due to flash data storage characteristics, we have the potential to recover anything stored on the device – assuming the data is not irreversibly encrypted. When dealing with standard cell phones, we are commonly looking for deleted SMS messages, address books, call logs, pictures, etc. For smartphones, once the file system has been reconstructed, these can be analyzed like a computer by using popular forensic software utilities. Any number of operating system and application artifacts may be recovered. This includes geo-location data, Internet history, instant messaging or any other data associated with the thousands of smartphone apps available on the market. Fortunately, some cellular forensic tool vendors are beginning to develop programs that assist with the rebuilding of the higher-level files systems and even process the data to interpret common artifacts like SMS messages, call logs, emails and pictures.

DESPITE PRECAUTIONS, THE CHIP-OFF FORENSIC EXTRACTION PROCESS DOES CARRY SOME RISK OF DAMAGE TO THE MEMORY CHIP AND LOSS OF DATA

COMMON ISSUES & PROBLEMS

In some cases, the examiner will identify the target memory chip and find the particular chip model is not supported by any available programming devices. In these cases, the examiner will need to communicate with the various manufacturer and request support be added for the new chip model. Sometimes support for new chips can be added relatively quickly but in other cases the manufacturer will require additional information, such as a datasheet for the target chip. This is similar to a chip blueprint and contains technical information needed to engineer and implement support for the chip. In limited cases, a new adapter will need to be designed and manufactured. Depending upon availability of components this can take several months.

Also, despite precautions, the chip-off forensic extraction process does carry some risk of damage to the memory chip and loss of data. During the removal process, the chips are exposed to high-temperature profiles which are required to melt lead-free solder. These temperatures, which can exceed 220°C (428°F), may cause inadvertent damage; especially when chips have been previously been exposed to moisture. In addition to the solder points, chips are sometimes fixed to the PCB using epoxies or other glues. These adhesives can make it more difficult to remove and clean the chip. This is particularly true in the case of BGA chips. A glued chip may require treatment with chemical glue softening compounds, longer exposure to high temperatures during removal or, in the case of chips under-filled with adhesive, require more aggressive cleaning which increases the chance of damage to the surface land pads. In order to limit risk associated with moisture, PCBs and chips can be slowly “baked” at a low temperature to eliminate moisture from the components.

CONCLUSION

The chip-off process is definitely an advanced technique that, unfortunately, carries some significant barriers to entry. In addition to high costs associated with equipment, the ability to reliably remove and prepare the chips is a skill that is not easily mastered. While many labs may not have the resources, personnel, or desire to perform chip-offs themselves, there are options to partner with a lab that does to assist with some or all of the chip-off process. Currently, there are only a few larger agencies and specialized forensic firms offering chip-off services; however, we expect this number to increase as forensic investigators require more physical-level access to data stored on devices utilizing flash memory. Given the ever-increasing prevalence of embedded memory and the population’s reliance on consumer electronic devices that use it, it is important to know that there is the last resort chip-off option that just may make recovery of seemingly out of reach “smoking gun” evidence possible.

AUTHOR BIO

Jim Swauger is a partner with Binary Intelligence, a private firm specializing in digital forensics and high-tech investigations. He has over 15 years of experience in digital forensics field, starting as a computer forensic specialist with the Ohio Bureau of Criminal Investigation’s computer crime unit, then as technical security investigator for a top financial institution and now as an expert witness and consultant. Jim is a licensed private investigator and holds several industry certifications including CFE, OFP, EnCE and GIAPP. He can be contacted directly at jsauger@binaryintel.com.