12-2008

iPhone Forensics Methodology and Tools

Haitham AL-Hajri
Edith Cowan University

Krishnun Sansurooah
Edith Cowan University, k.sansurooah@ecu.edu.au

DOI: 10.4225/75/57b3d559fb871
6th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2008.

iPhone Forensics Methodology and Tools

Haitham AL-Hajri
Krishnun Sansurooah
School of Computer and Information Science
Edith Cowan University
iPhone@e4nzx.com
ksansuro@student.ecu.edu.au

Abstract

iPhone mobile devices are rapidly overtaking the new generation of mobile phones market, especially among the young generation. It is also gaining a lot of popularity among security specialists and fancy gadgets for collectors. The device is considered as a "special" mobile phone due to its ability to perform multi-operations if not multitasking. It can therefore be used as a entertainment media device, a camera, a GPS, Internet surfing via Wi-Fi technology, Internet Mobile Edge Services, personal organizer, and finally performing as a cell phone with all the usual services including sms, and so forth. However, the difference between the iPhone and the other conventional phones vendors is its ability to store and process huge volume of data which is supported by decent computing capabilities of the iPhone processor. As part of every technology, such a device can be used for legal and illegal activities. Therefore the potential risks from such "special" technology are not limited to the possibility of containing illegal materials, such as audios and visuals, including explicit materials, images, documents and the possibility of propagating malicious activities rapidly. Such modification can breach or tamper with the telecommunications network authorities and regulations. The goal of this paper is to focus on both the logical and the physical extraction of the iPhone generation one through the extraction of the iPhone flash drive NAND memory chip and also the logical extraction of data onto the second generation of iPhone using various techniques and methods at our disposal.

Keywords

Forensics methodologies, iPhone forensics, forensics tools, digital forensics evidence handling,

INTRODUCTION

iPhone mobile phone is becoming the most popular devices among the youth age. As iPod has changed the way of listening to music, as well the iPhone is revolutionizing the world of cell phone. iPhone is a result of combining the iPod capability with the functionality of cell phone, which has result in a powerful multimedia mobile phone. Adding the ability to store large volume of data has opened the gates for great potential misuse. Such a large storage device that can transfer stored data on the go can jeopardize serious risk of loss or theft if it contains sensitive cooperate data. In addition it can cause a threat to organization data when the iPhone can be synced to their system and can either download malicious tools or upload some sensitive executable files or documents. The iPhone device can be modified to be powerful hacking devices given its functionalities have been tailored to suit the malicious intention. Therefore the importance of having a sound forensic methodology or approach to acquire and analyze extracted data is essential. The aim of this paper is to have an overview of the tools scripts and forensics approaches that can be applied to the iPhone in case it has been found at a crime scene or been reported as an abuse of technology.

General Forensics Guidelines

Before arriving on any crime scene with any digital devices are involved be either an iPhone or any mobile devices, the following are general guidelines that could be put in practice prior and upon arrival.

Steps Taken Upon Arrival to the Scene

1. Obtaining appropriate approval and authorization letter.
2. Arriving to the scene.
3. Securing the scene.
4. Establish documentation and seizure form.
5. Locating the mobile device.
6. Photograph the crime scene and document everything
7. Use digital cameras or video recorders.
8. Record the names or ID of the examiners on the tape or the photos.
9. Cite the time, day and date, the venue, and also always get a witness to certify the collection of evidence.
10. Check the state of the mobile is it on or off. (iPhone has two buttons the home button, which turns the of sleeping mode and the power button which if it has been hold for more than 5 seconds will display a message if the user wants to turn the iPhone off).
11. Check if the device has password lock enabled, and if it is enabled, it should be obtained before disconnecting the phone.
12. Check the mobile connection. If it is connected to anything. In this case to any computer system that have iTunes (iTunes is a software used for syncing the iPhone to the computer).
13. If the mobile phone is connected to a computer, take photos of connection and the computer screen. Including the syncing process and documenting the software version used.
14. Tagging and bagging. In cases of ordinary mobile devices, it is recommended that the device to be placed in a Radio Frequencies Control bag. So device will need to be isolated from the network coverage and prevent it from receiving any calls or messages therefore it will not tamper with evidences on the devices.

A seizure form is attached in the Appendix 1 to have a better idea about how to fill in a seizure form when an iPhone is part of a crime scene.

FORENSIC METHODS

This section will demonstrate the forensic approaches and the tools required for each steps keeping in mind that these tools are subject to upgrades and might not matching set some phones with different firmware.

Logical Approach

The logical approach will illustrates the software tools that can be used for recovery of data. This section will list some tools and scripts associated with the forensics scene. The iPhone is a very useful tool, but one should be aware of some very important things due to its characteristics. It is considered as a fully-fledged computer, which is running a slimmed version of UNIX operating system and Apple's Leopard. Therefore, like most operating systems, deleting a file is simply just deleting the pointers that point to the physical location of the

storage block hence allowing the initial injection of data on the storage disk initial to remain in the block. This method of data extraction will therefore explore all the possibilities while using a logical approach to extract all the data from the iPhone 3G. Obviously, it I very important that everything that has be extracted from the iPhone 3G follow the rules of evidence which are cited below:

(i) Evidence is admissible
(ii) Evidence is authentic
(iii) Evidence is complete
(iv) Evidence is reliable
(v) Evidence be understandable and believable

The free tool that was used is known as '***ibrickr 0.91***' which can be downloaded from www.ibrickr.com. Normally iPhone 3G will grant access to only "genuine" built-in mechanism signed by Apple to be installed. However, the ***ibrickr 0.91*** will use the loop-hole in the firmware and bypass, thus forcing an unsigned application to be installed even though it does not come from apple. Once that the software has been downloaded, one should run the application which is install itself in *C:\ProgramFiles\ibrickr* once this has been performed, connect the iPhone 3G need to be connected to its dock connector and the other end to the USB port allowing the iPhone to maintain its charge while performing the recovery process. This will then allow a connection to be established between the iPhone and the toolkit.

Having already connected the iPhone 3G to the machine and detected by iTunes, we can start downloading the forensics recovery payload within the 'ibrickr'. The forensics recovery toolkit will comprise of OpenSSH, netcat, just to cite a few of them at this stage.

Once confirmed that the forensics toolkit has been properly installed and activated, the iPhone is ready to be jail broken and to start installing the payload, it could happen that the iPhone get jammed – i.e. the phone appear to be not functioning, then one should manually force it to go into recovery mode by holding the Power and the Home buttons until the iPhone hard powers itself off, powers itself back on, and finally will display the recovery screen. However, with the iPhone 3G with the new firmware version, it seems that the way that the iPhone communicates is different from the previous versions. With the 2.x version of the iPhone, the same approach is used but the way that it is delivered has considerably changed. Therefore, as mentioned previously the aim is still the same – i.e. booting form the iPhone boot ROM to accept unsigned applications.

A tool known as "Pwnage" is use to exploit this weakness which was designed and written by a group of hackers known as iPhone Dev Team. This tool is use to crack the iPhone by modifying the boot loader which in turn will normally is likely to destroy the file system on the iPhone 3G and before restoring the device firmware, we'll use another tool "Xpwn" which is an open source tool designed by David Wang to organize proprietary *img3* formats in which the RAM disk are stored. Once that you have already completed this section, we will need to unpack and repack the RAM disk through 'xpwntool' which is the actual RAM disk management tool. To be able to mount the RAM disk, we will need to unpack it first which will need to acquire the encryption key and the initialization vector.

Now that we have already extracted the RAM disk, the new file will contain HFS file systems that will be mounted as a read-write mode. Having completed the unpacking of the RAM, we will have to repack the decrypted RAM disk back to it correct format to overwrite the old one. This will be done through Xpwn tool downloaded earlier. Now that we have successfully created a custom firmware bundles we need to get the iPhone 3G into Device Failsafe Utility (DFU) mode. Obviously the forensic toolkit and all the changes can be undone after having created the image by using the iTunes 'restore' option to bring your iPhone 3G back to its normal (original firmware) state.

Wi-Fi & SSH Connection

Since a link has been created in between them, we can open a communication through the wireless network onto the iPhone 3G (make sure that the Wi-Fi is turn on). When the iPhone has already joined the wireless network, make a note of the IP address and confirm that the computer can ping the iPhone. Obviously if you don't have any access point (AP) available then you will have to create an ad-hoc network so that the iPhone can be allowed to connect to. Note that when creating the ad-hoc network some iPhone appears to have difficulties in connecting onto encrypted network which can be bypassed by recreating the network but this time without the password. Make sure that the iPhone is joining the wireless network and then select the option that the iPhone be connected through a static address on the network. Once the iPhone is visible and active on the network, we need to open a connection via SSH from the desktop by typing '*ssh –l root x.x.x.x*' where the "x" denotes the IP address of the iPhone which was recorded earlier and when prompted, enter the password which is normally "alpine" which was set initially when installing the forensics recovery toolkit and once that completed this would mean that you have been successful in logging into the iPhone and we should proceed with the recovery of the media partition.

With the recovery toolkit that was installed earlier on the iPhone 3G and the Wi-Fi connection with the desktop machine, we can commence to recover the media partition of the iPhone and for this we will need ***"dd"*** and ***"nc"***. The ***"dd"*** tool is a disk copy tool that allow you to copy the raw disk image where as the ***"nc"*** mostly known as the *"netcat"* tool is use to send and receive data across a network. Note that both command line tools need to be installed on both the iPhone and the desktop to be able to send and retrieve the data.

MD5 Hash

As with any piece of evidence for forensics use, it is very important to be able to verify the integrity of the information and one way to do so with the iPhone is to make an MD5 digest of the iPhone as it will ensure that the partition data has not been tampered during the transit and enforce data integrity.

This shows that the ssh connection to the iPhone and then goes up to the root level where it is then *umount* command unmounts the */private/var* partition by force. Given that there are other application that are using the iPhone's disk, it cannot be unmounted without force hence the option "*–f*" and then the partition is remounted with a read-only option (*ro*) hence backing it with the md5 command to create a digest of the raw device which depending on the capacity of the iPhone, this might be very time consuming to achieve. It is also noted that during this period of time, the iPhone has to be kept alive else it might go into a sleeping mode, thus causing the Wi-Fi connection to drop and hence freezing the whole process. Therefore a good trick to keep the iPhone alive is to run a ping session from the phone while waiting for the entire process to finish. Once this operation is

finished, the md5 output will return the md5 Digest of the raw partition which just need to be copied and the stored in a safe location for further reference when you will need to compared the image.

However, the best and fastest way to recover the media partition is to send it over to the desktop PC without encryption. Unfortunately, using Wi-Fi will send encrypted data over the network due to the wireless WEP or WPA in place onto the wireless network that you are using. One way to achieve this is so setup up the command on both side (the iPhone and the desktop) to run the *"netcat"* command requesting in the first instance your desktop to listen to a network port while you the iPhone will be transmitting the data which is the disk image on that particular port. This means that on the desktop, request the *"netcat"* tool will to listen to a local port which when it receive the information, it is passed to the disk copy utility which will convert the data back into the image file. The following syntax used

$ nc –L -p 8888 | dd of=./rdisk0s2 bs=4096.

Once this is done, the desktop will be listening for incoming data sitting idle waiting to receive the data. Therefore, open an ssh connection to connect the iPhone using the following command

($ ssh –l root x.x.x.x

 # /bin/dd if=/dev/rdisk0s2 bs=4096 | nc z.z.z.z 8888)

Then the raw partition will begin to transfer the data over the network and this will normally be time consuming depending of the size of the iPhone used. Note that while this is being carried out, only the iPhone disk storage will be transferred which will result in the capacity being less than what the advertised capacity is. When this is completed compared the md5 hash that was recorded previously from the iPhone to see that they both match hence no alteration has been made to the images. Make sure that when analyzing the iPhone that it is carried out only on a copy of the original disk as some tools have slightly altered the disk image during the examination and analysis. If the operation fails untimely, make sure that the iPhone is sitting on the dock and is charging else it will shut down the wireless connection when the battery enters the sleep mode.

As soon as the raw disk has been transferred and recovered from the iPhone, it can be injected through the numerous commercial forensics toolkits available to be read. However, the forensic investigator has to be very careful as the disk image is saved with an HFS/X image extension – i.e. the fifth generation of HFS which most of the commercial forensics tools such as Encase, FTK, Paraben Seizure Box does not recognize. The only way to be able to read this format with the other forensic toolkits is to change the identifier from HX to H+ denoting an HFS/+ file system. Note that prior to effect any change, documenting all the steps is compulsory so that you may have a trace of what has been done and where has it reached so far.

DATA CARVING

Data carving is the method of removing or extracting a collection of data from a larger data set. These carving techniques often occur during a digital investigation where unallocated file system space is analyzed to extract files. The files are "carved" from the unallocated space using file type-specific header and footer values. File system structures are not used during the process. (Dickerman, 2006).

Therefore to recover deleted files, a data carving tool is needed. The recovered raw partition will show as one huge partition to the desktop machine and contains both live and deleted data. (Zdziarski, 2008). The data carving tool will scan the disk image for traces of desired files, e.g. images and other files which are carved out for further analysis thus funneling the search further down. Such examples of data carving tools are Encase, CarvFs, Foremost, Scalpel. In this report we used Foremost as it is a free forensics toll which was developed by US Air Force of Special Investigations. Scalpel is a tool based on Foremost and handle the challenge that allow most forensic investigators to specify the headers and sometimes the footers which are optional – meaning allow the examiners to specify the beginning and the end of the desired data on the raw image.

Since Foremost and Scalpel uses both a *conf* extension, it is therefore very helpful for the examiners as it can be bundled together and allow the investigator to uncomment certain types of files that need to be carved due to the sample configuration loaded in the those tools.

The following are just examples where the investigator should be looking at – i.e. places of interest on the iPhone are:

- Photos taken by the iPhone camera;
- Photos that have been syncing with a desktop;
- Photos from web browsing;
- Google Maps tile;
- Contacts and their details;
- YouTube last visited to associate with any particular crime;
- Web browser of the visited pages;

Potential location of evidence within iPhone.

(i) **Voicemail messages** – the AMR codec considered as the standard speech codec used by the iPhone to store the voicemail messages which normally sit in nicely in a 65 K but for larger or longer messages extending the file size will allow you to get the entire message. Using the following syntax
amr y 65535 #! AMR

(ii) **Property List** – this is the list where all the XML configurations are held. This means that the examiner can retrace the different websites that the owner of the phone has visited or also what is the different Google Maps direction that he was looking at. Use the following syntax
plist y 4096 <plist </plist

(iii) **Dynamic dictionaries** – this is associated with keyboard caches used by the iPhone. Searching this allow you to see what the user has been entering, such as chat message, email messages, any password, username/ID, Short Messaging Services. Use the following syntax
dat y 16834 DynamicDictionary

(iv) **SQLite databases** – this allows the user to store address books, calendars, Google Maps tile graphics. These databases are normally 'live' on the iPhone, but deleted databases can allow the investigator to trace back what the user was looking at. Use the following syntax
sqlitedb y 5000000 SQLite\x20format

(v) **Electronic mails** – scanning of email headers is a very good way of recovering both live and deleted email. Syntax use is
email y 40960 From:

(vi) **Web pages** – scan all the websites visited and hence uses the following syntax
htm y 50000 <html </html

(vii) **Images** – all the formats that the iPhone allows such as gif, jpeg, png can be scanned by removing the prefix preceding the corresponding lines in the configuration file as shown through the following syntax
png y 40960 \x89PNG

(viii) **PGP blocks** – PGP-encrypted messages are not very useful without the key but often there are unencrypted messages within the same line. The syntax that accompanies this is
txt y 100000 -------BEGIN

(ix) **Other files** – specially*.pdf &.doc/.docx* can be stored locally onto the iPhone when emailing or when browsing the web. The following syntax are recommended;
pdf y 5000000 %PDF- %EOF
doc y 12500000 \xd0\xcf\x11\xe0\xa1\xb1

To carry this task it would normally take in between half an hour if using Scalpel and a few hours compared to using Foremost where the potential data will be recovered to a directory named foremost-output or scalpel-output. The other good things about this tools is that it also generate and audit file known as *audit.txt* within the output file confirming that information been recovered or what seems to be recovered data. Obviously it is at the investigator's discretion to determine whether the data is valid or not.

Validating Images

Recovery tools can sometimes make mistake when generating too much of data meaning that they extract a lot of data that may partially be corrupted or unneeded. Therefore, finding valid images can be time consuming when it has to go through thousands of files. Thus, the introduction of ImageMagick which contains a set of image processing benefits, one being the ability to display information about the images and this could give the examiner an advantage. The identify tool is great when bundled with the ImageMagick for filtering and analysing through the thousands of files generated after the data carving process.

String Dumps

Another way of addressing this issue is to make a string dump, meaning that the strings that were extracted from the raw disk image and be saved and exported and therefore analysed at a later stage. However, the output file will be huge, but it will allow loose text searches for a particular conversation or message or any other data to be found.

Timestamp

Having already gone through the process of data carving which is very practical when it comes to recover files or data that have been intentionally deleted, the disk image can also be mounted as a live partition to allow the forensic investigator to work/access live data on the iPhone. As we all know that when you are to present evidential data in a court of law you need to be precise and very direct. One of the crucial aspects is timestamping to determine when did that action occurred. In the iPhone many of the timestamps are represented in a UNIX timestamp format that needs to be converted to actual time and date. This can be done by either using a UNIX time stamp converter or using a command written in Perl script.

Disk Analysis

Once that the disk image has been transmitted from the iPhone – i.e. – in the HFS/X file system or if you have converted it to HFS+ this can be mounted on a Windows machine for further analysis through some modifications. Since Windows does not like and understand the HFS/X disk image by default, we need to download the HFSExplorer which is an application that will allow the extraction of the HFS+ volume and the Sun Java Virtual Machine and hence upload raw image files as the one that we have dumped from the iPhone earlier. Please make sure that the disk image is the saved as a.*dmg* extension.

IMAGE GEOTAGS

Geotagging is the process of adding geographical identification metadata to various media such as videos, websites, photographs or RSS feeds and is a form of geospatial metadata. This normally consists of latitude and longitude coordinates, though it can also comprise of altitude, bearing, and place names. This process can help users locate a wide variety of location-specific information. Geotagging enabled image search engine, information services, news, websites, or other resources. (Wikipedia, 2008). When it comes to the iPhone, these are images. This can be either enable or disable and in many cases people forget to disable it which when extracted will reveal the exact location of where this photo was taken and that location can help the examiner to arrest a criminal or a pedophile. For that to happen, the forensic examiners need to use ***Exifprobe*** which a camera utility that has the ability to extract image metadata. Therefore if the image is tagged, there will be a GPS latitude and longitude as shown below:

JPEG.APP1.Ifdo.Gps.LatitudeRef = 'N'

JPEG.APP1.Ifdo.Gps.Latitude = 31,55.60,0

JPEG.APP1.Ifdo.Gps.LongitudeRef = 'E'

JPEG.APP1.Ifdo.Gps.LongitudeRef = 115,49.60,0

Added to these extracted details, the timestamps can also be retrieved to indicate at what time was the shot taken as described below:

JPEG.APP1.Ifdo.Exif.DateTimeOriginal = '2008:10:28 15:47:39'

JPEG.APP1.Ifdo.Exif.DateTimeDigitized = '2008:10:28 15:47:39'

PHYSICAL APPROACH

The physical method will include the possibility of opening the device and to look into extracting data from the memory chip. Therefore the forensic examiner should be familiar with the device memory technology that has been used. In addition the type of memory that might have the evidential data.

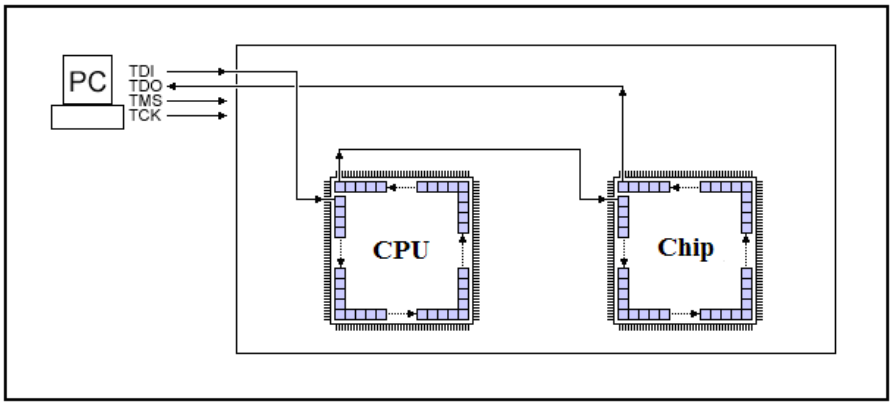
The iPhone has two main memory chips technology installed, NOR and NAND chip. The main differences between NAND and NOR chip is in the way of handling writing and reading of data. NOR has the ability of reading faster than writing which it is a good candidate to handle all the iPhone applications and process, for the reason that NOR has a function called execute in place (XIP) which allows programs that have been stored in NOR flash memory chip to be executed from the chip itself instead of loading the program to the RAM for it to run from there. By doing so NOR will help reduce the need of using RAM resources to execute programs allowing NOR to act as fast random access memory(RAM) with the luxury of having the programs in same location on the flash memory chip all the time. While NAND chip writing capability is faster than reading therefore it is a good candidate to be used for storing media and data. (Calligaro, 2005). The forensic examiner will look into the content of the devices which it's usually stored on the NAND chip. However it is important to know what sort of application could be stored or booted in the NOR chip, having the possibility of stored malicious code or encryption code could be resident in NOR.

JTAG METHOD

JTAG was initially created as a testing solution for issues with circuit boards also known by logic boards. JTAG is a project of a group of European Electronic Companies called Joint Test Action Group (JTAG. The development of printed circuit board has become more popular and complex in both size and functionality (Oshana, 2002). The joint test action group worked on performing a boundary – scan testing in the hardware from the IC level. That specification result in establishing the IEEE 1149.1 standard detailing the specification in how to access the embedded chip for testing purposes, the technique was named after the group initials JTAG. JTAG method can be used to produce a forensically sound image of an embedded memory chip within small digital devices such as cell phone. JTAG has the capability of allowing a direct access to the memory in order to create a memory dump using the debugging mode or the extest mode. The two techniques is being explained in detail on the small scale digital forensics article (Breeuwsma, 2007).

JTAG also referred to as a boundary scan control uses serial protocol for scanning the boards. The five pins are defined as follows:

JTAG Testing Pins



Example of JTAG Testing Pins. Figure 1

TCK/CLOCK: this pin is detected for clock testing. It synchronizes the internal state of machine (device) operation.

TMS/MODE: this pin stands for Test Mode Select Input. It determines the state/mode of the device controlling the test logic by receiving the incoming data. (Davis, 2008)

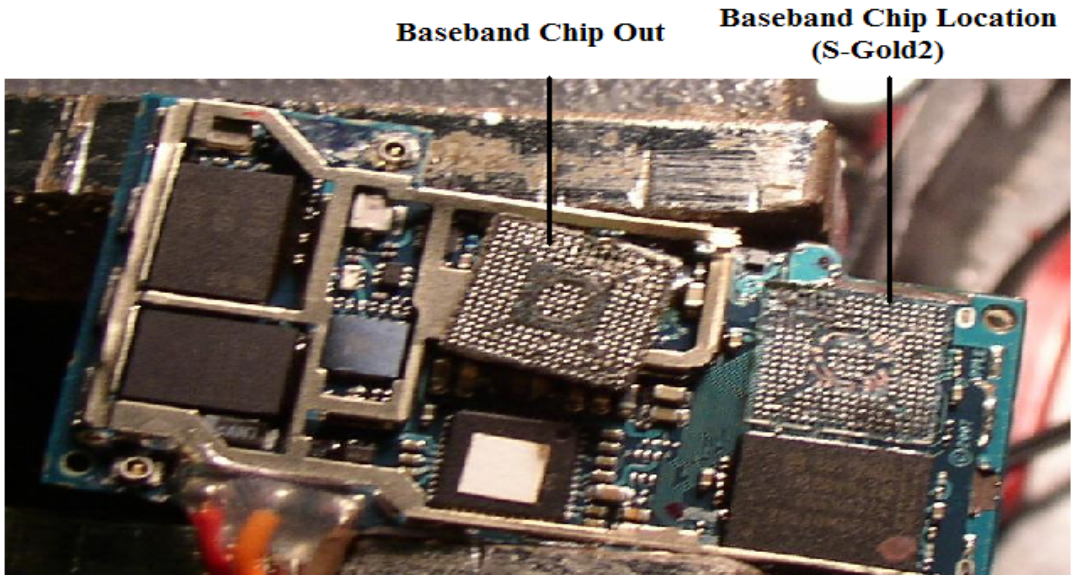
TDI/DATA INPUT: this pin stands for Test Data Input. It receives input of data depending on the state on the tap controller. (Davis, 2008)

TDO/DATA OUTPUT: this pin stands for Test Data Output, where the received signals on the data input will show in the data output depends on the TAP controller sometimes the TDO will be shifted a number of clock cycle depends on the internal length. (Davis, 2008)

Finally the fifth pin that may be used in some boards is the reset pin as follows:

TRST/RESET: this pin resets the JTAG test logic regardless of the state if TMS or TCLK

According to George Hotz also know by (geohot) JTAG pins can be found under the iPhone baseband chip known by (S-Gold2). Once the baseband is chip out of the logic board, its easy to connect the five JTAG pins TDI (Test Data In), TDO (Test Data Out), TCK (Test Clock), TMS (Test Mode Select) and TRST (Test ReSeT). but it requires a lot of soldering and modification to power up the baseband chip (S-Gold2) (Madigan, 2007).



IPHONE logic board with baseband chip detached (Madigan, 2007) figure 3

Such approach has its own advantages and disadvantage the following is a summary of main advantages and disadvantages of JTAG approach:

Physical Extraction Method (Memory Removal)

Physical extraction of the iPhone memory chip is not an easy task to operate on. As shown on figure(x1) the Samsung NAND chip is a 48 leg chip that seats on the edge of the iPhone logic board. it requires a lot of work around and de-soldering technique. However it is a method to be used in cases where other methods fail to obtain data. This method is ideal to be used on extreme cases where the mobile device is damaged severely, that have damaged the logic board; therefore it failed to communicate with its components, to the extent that it can't be turned on. in some cases the device will have destroyed connectors on board that won't allow cables to connect. This method is been used by criminals as an anti-forensics technique to avoid any possibility of extracting data from the seized device. (Keonwoo Kim, 2007).

Memory removal stages

The memory chip has to be extracted from the printed circuit board by de-soldering the chip from the board. However, there are three possible methods on extracting the embedded memory chip in general the following is the three stages in physical extraction approach:

A- De-Soldering of the memory chip.

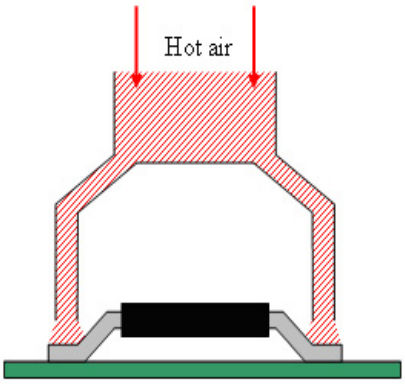
In this stage the chip will be de soldered from the board using special de-soldering equipment because the chips are usually packed in TSOP (Thin Small- Outline Package) or Micro BGA (Ball Grid Array) and this packages require handling with extra care to prevent it from getting damaged in the process of de –soldering. TSOP CHIP can be de-soldered using many ways but the best and most preferred method is using Hot Air. This method relate by applying hot air streams to the board that is hot enough to melt the soldering of the memory chip connection. Then using a vacuum to suck the chip out of the board figure 3 illustrates the method of extracting the chip. Extracting Micro BGA is a complex process using hot air and rework station, by using temperature profile to melt the connection but the issue here is that there are chances that the high temperature will burn the chip. Therefore sensitivity and care should be taken while handling this approach (Breeuwsma, 2007).

B – Preparing the chip for further process.

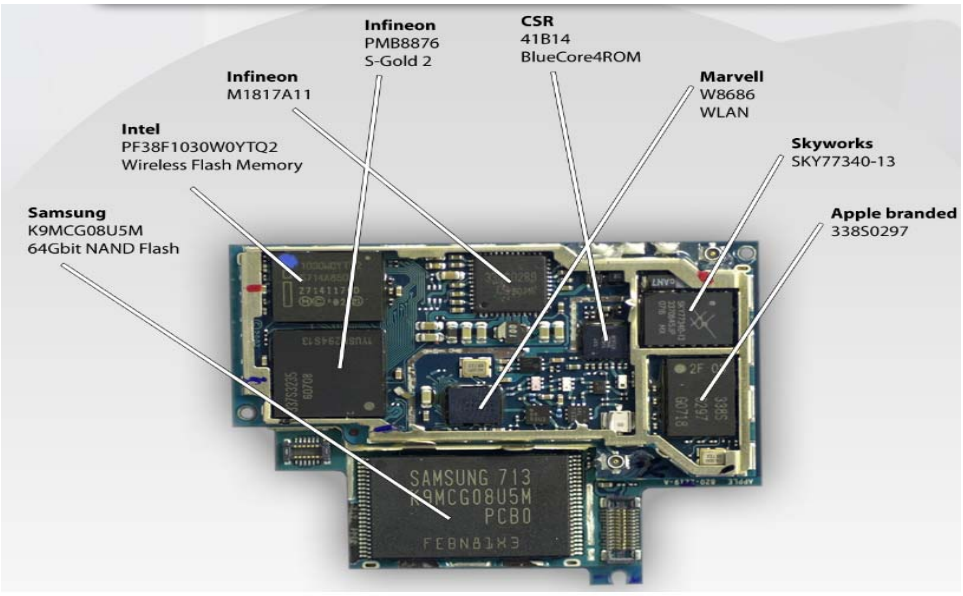
After the memory chip has been extracted from the printed circuit board, the chip needs to be cleaned from the leftover solder in the connection pin. Some pins might need to be aligned and straighten again in order to be plugged in the chip reader/programmer device for further investigation (Breeuwsma, 2007).

C – Flash memory reader/programmer

Few tools have been developed to read memory chip set, these tools are commercially available. One of the famous venders in this trend is the BPM Microsystems who will know by producing programmers/reader tools for different micro chips programs to suite a wide range of different type of memory chip set. Each chip requires a specific software driver to enable the device to communicate with the memory chip set. In case there is no any available driver for the specific chip, it might take longer to develop a suitable software solution in order to read the chip (Microsystems', 2008). There are other commercial tools, which can be used to read from the extracted memory chips and can be used for different memory chip set and they don't require any driver.



Extracting TSOP Using Hot Air Method Figure 3



The iPhone chip processors & internals figure (X1) (mydigitallife, 2008)

REFERENCES

CarvFs (n.d.). The Carve Path Zero-storage Library and file system. Retrieved October 19, 2008, from http://ocfa.sourceforge.net/libcarvpath/

Calligaro, M. (2005) RAM, ROM, NAND, NOR that's a lot of capital letters. Retrieved September 10, 2008 from http://blogs.msdn.com/windowsmobile/archive/2005/08/19/453784.aspx

Davis, L. (2008) JTAG Interface (JTAG Bus Description) Retrieved September 28, 2008, from http://www.interfacebus.com/Design_Connector_JTAG_Bus.html

Foremost (2008). Foremost – Latest version 1.5.4. Retrieved October 17, 2008 from http://foremost.sourceforge.net/

Keonwoo Kim, D. H., Kyoil Chung, and Jae-Cheol Ryou. (2007, December). *Data Acquisition from Cell Phone using Logical.*

Approach. Paper presented at the World Academy of Science, Engineering and Technology.

Madigan, J. (2007) iPhone JTAG Interface discovered. Retrieved September 17, 2008, from http://www.jasonmadigan.com/2007/08/02/iPhone-jtag-interface-discovered

Marcel Breeuwsma, M.D.J., Coert Klaver, Ronald van der Knijff and Mark Roeloffs. (2007) Forensic Data Recovery from Flash memory. Small Scale Digital Device Forensics Journal, Vol 1 (No.1).

Microsystems, B. (2008). Web site information related to services and products. Retrieved September 13, 2008 from http://www.bpmmicro.com/whoweare.htm

Mydigitallife. (2008). Apple iPhone Internal Hardware Components Close Look! My Digital Life. Retrieved August 19, 2008, from http://wwwmydigitallife.info/2007/07/03/ apple-iPhone-internal-hardware-components-close-look.

Oshana, R., (2002) Introduction to JTAG. Retrieved September 23, 2008, from http://www.embedded.com/columns/beginners corner/9900782

Siliconfarest,. (2005), Boundary-Scan Testing / JTAG Standard. Retrieved September 26, 2008, from http://www.siliconfareast.com/jtag.htm

Wikipedia (2008). Geotagging. Retrieve October 21, 2008, from http://en.wikipedia.org/wiki/Geotagging

Appendix 1

SEIZURE FORM

Case Number: (1-25042008) **Date**: (25/04/2008)

Time: 11:45 AM

Location: 145 central street

Suburb: Victoria park

Post Code: (6001) **State**: WA

Other Notes

Investigator Name	**Haitham AL-Hajri**
Investigator ID	**1000 60 20**
Investigator Name	**Krishnun Sansurooah**
Investigator ID	**1000 60 21**

IPhone Type	**[ ] First Generation (2G) [ ] Second Generation (3G)**
IPhone Module	**[ ] 4GB [ ] 8GB [ ] 16GB**
IMIE Serial Number **(located on bottom back of the iPhone)**	**(00002000204)**
password protected	**[ ] Yes [ ] No**
State of the Mobile	**[ ] ON [ ] OFF [ ] Syncing**
SIM CARD	**[ ] Yes [ ] No**
IS the iPhone attached/connected to	**[ ] Power Source** **[ ] Computer /Laptop**
Is the computer Running iTunes software	**[ ] Yes (Version Number : _ _ _ _ _ _ _ _ _ _ _ _)** **[ ] No**
Dose the Location support Wi-Fi facility	**[ ] Yes (Access Point name : _ _ _ _ _ _ _ _ _ _ _ _)** **[ ] No**

Notes:

Name: Haitham AL-Hajri **Signature: Haitham**

Witness: **Signatures: haithy**

Time: 13:25

COPYRIGHT