BEST PRACTICES FOR A COLLECTION OF AN IOS MOBILE DEVICE

by Richard A. Rodney

As the use of iOS devices continues to proliferate in the business space, they present some unique challenges when data must be collected from them. Bring Your Own Device (or BYOD) policies in many organizations have further altered the landscape that computer forensic professionals must navigate.

What you will learn:
• The procedure to follow for performing a forensic collection of an apple iOS device such as iPod, iPhone or iPad.
• What you should know prior to performing a collection of an iOS device.
• Some important items you can collect from an iOS device.
• Methods of blocking mobile wireless signals.

What you should know:
• Familiarity with mobile operating systems.
• Familiarity with Apple devices and iOS versions.
• Familiarity with the concept of encryption.

Of the many new challenges facing computer forensic and ediscovery professionals, the proliferation of mobile devices, specifically Apple iOS devices, presents professionals with new questions as to how they should manage collections for these devices. The explosion of permissive Bring-Your-Own-Device (“BYOD”) policies in businesses, coupled with the rapid acceptance of non-Windows based (i.e. Apple) products in the business space, has in short order changed the landscape for digital evidence detection, collection and use forever.

Businesses must adapt to new technologies while mastering (and regulating) their own use of them. Lawyers, computer/mobile forensic technicians and ediscovery practitioners must also adapt to new technologies, particularly to the increasingly accepted mobile/cloud/BYOD based business environment, and develop new strategies and methods for ensuring that digital evidence is thoroughly, efficiently and defensibly collected and preserved. Apple/iOS devices are now present in the network architecture (at least through BYOD) of most every major business in the country, and this article focuses on considerations and best practices for collecting data from these devices once they’ve been identified and access to them has been secured.

APPLE/iOS
Apple iOS devices in the form of the iPod, iPhone and iPad present some unique challenges for the early stages of managing, preserving and collecting...
electronic files. There are two primary questions to answer when collecting data from any of these devices: One, what is the precise model version of the device? Two, what is the precise operating system ("OS") running on the device, including the update history of the OS running on the device?

There are sometimes subtle and, often times, not so subtle differences between generations of iOS devices and the year they are released. Apple has had a semi-annual release schedule for many of its devices for a few years now. This means for example, that iPhone 3 and 3GS devices produced in the same year are different and may require different processes and software to reliably collect from them. Just as with the different model versions, different OS versions present their own different challenges and solutions. Each version of iOS was designed to update and improve the user experience, but not all users perform all updates. There are various reasons for this but regardless, you have to be aware of the current version of iOS on the device you are about to collect from.

Apple/iOS devices feature various Pass code/pass lock encryption elements that must be disabled to ensure an uninterrupted and successful collection. If devices are encrypted and users have not provided security access, there are a variety of processes that can be used to gain root user access (also known as jailbreaking) to achieve and maintain access to data on the device.

As mobile forensics and ediscovery are becoming more common place, it is a good idea to recognize the roots of the discipline. As with most computer forensics tactics, mobile forensics was born of law enforcement and the intelligence communities varied needs to access content on mobile devices. From there these disciplines have been adopted in the corporate and legal worlds for a variety of needs from human resources matters to theft of intellectual property. From there these disciplines have been adopted in the corporate and legal worlds for a variety of needs from human resources matters to theft of intellectual property. One of the tried and true methods is screen capture. Plug the mobile device into a projector, and do a print of the contents of each screen. This is an effective if somewhat painstaking and methodical process. This method was more useful for early semi smartphones and other cellular phones that had no access to the cloud and could store very little active data. With most smartphones such as the iPhone and tablets such as the iPad, being as or more powerful than computers from 5 to 10 years ago, it is not an understatement to refer to most mobile devices as mobile desktops. The project-a-phone method is not practical for most smartphones and absolutely not for any tablets. To that end there have been several tools to come on the market to address collecting and analyzing mobile devices. Without any implied preference, examples are: Cellebrite’s UFED device, Accessdata’s Mobile Phone Examiner plus (MPE +), BlackBag Technologies Blacklight and Paraben’s Device Seizure. There are many other tools but these are the ones I know through my own vetting process. They all can be utilized effectively for collection and analysis of iOS devices.

Before we get into a step by step of what to do, as any mobile forensic professional will acknowledge, seizure of a device is only as good as your ability to keep its contents unchanged. Mobile devices can
be updated wirelessly via mobile data service or WiFi, so turn the antenna off. In fact, disable all wireless services as soon as reasonable before collecting. Airplane mode is a good choice to stop all communications to the mobile device. Another method I have learned is wrapping the mobile device in aluminum foil. This method is one I like to refer to as a poor man’s faraday box. A faraday box, or faraday bag or room, utilizes material that effectively blocks all incoming and outgoing wireless signals for a device. Why would you want to do so? Simply put if the mobile carrier sends out an update to the operating system or an Information Technology technician pushes a firmware or software update to the device mid collection, this can effectively change the files on the mobile device up to and including wiping existing files. This would render the purpose of your collection fruitless.

COLLECTING FROM AN IOS DEVICE
Now we’ve wrapped our brains around a few procedures and tools, let’s discuss a standard workflow for collecting from an iOS device.

• First step, put the device airplane mode or find other means to block mobile data and WiFi signals from reaching the device. I also recommend disabling the pass code device locking feature as soon as you can.
• Second step, you will want to ensure the mobile device is charged. Collect the power cables, if you can or have one handy, then Charge it up!
• Third step, while the device is being acquired, perform some social engineering. Find out what the passwords are for the device, version of iOS, model of device (iPhone 4 or 4s, iPad 2 or 3, etc), year it was released for sale, did the user create an encrypted ITunes backup?
• Fourth step, choose the appropriate tool for the collection. Consider what will be done with the files after they are collected. Will analysis be performed for the purposes of establishing when and where the phone was used? Will eDiscovery and data normalization be performed along in order to add specific user create content for a legal review with documents from other sources?

The reality is that all the tools mentioned will work well. There may arise a scenario where more post-collection work is required to fit one scenario versus another. Always go in to the process with as much information as can be known or acquired.

While there are a few different approaches and variations to the process of collecting, what has been presented is basic, repeatable and adaptable. With any computer forensic collection remain agile. Since we are focusing on iOS here, let’s hone in on some core concepts mentioned earlier to make an effective collection. The simplest question that can hamper a collection by going unanswered is: “What is the passcode to unlock the device?” There are few devices that can confound access more so than an iOS device that is locked. Even to Jailbreak an iOS device, it must be unlocked first. One of the many exploits to collect from an iOS device is to jailbreak the device. If the device cannot be accessed, jailbreaking will not be impossible but certainly difficult. Next, consider the device itself and remember that different versions of iOS devices in specific generations and within years of production have different make-ups. Each can use different processors, have different iOS versions and the user may or may not have upgraded. Another thing to consider: Is physical or logical access to the device needed? Physical access is everything that has ever been stored or deleted on the device. Logical access is only to those items currently considered “live” on the device. For example, iPad 3 currently can only be acquired via logical access by the leading tools (including Blackbag’s Blacklight which is an apple centric collection and analysis tool). But all developers are working to solve this problem, which will allow them to get ready to start all over for iPad 4. Regardless, consider what is needed and what may need to be considered acceptable for access.
KEY COLLECTION CONSIDERATIONS

Another consideration that was mentioned earlier is whether or not the device is encrypted or has an encrypted iTunes backup. I can tell you from personal experience, this situation can drive you mad. I once performed a forensic collection of several mobile devices of which one subject had an iPhone and another device. The person from whom I needed to collect the esd on their iPhone was cooperative but had forget they had set an encrypted iTunes backup for their iPhone. A fact that they did not inform me of because they did not recall they had done it. After several failed attempts to collect the device it occurred to me ask if they had an encrypted iTunes back up. The user recalled that they did but could not remember their password and was reasonably certain they had set it up on their home computer which was a mac. The user agreed to try to access their device and unlock the encryption on their office computer which they had synched to. After several attempts he recalled the password and we were able to access the iPhone. The tool I used was able to collect the esd from has phone, where previously it sat in a state of collection for roughly 8 to 10 hours on four different attempts to collect. I can only imagine what these situations must be like for law enforcement or collections from less cooperative subjects; thankfully, so far I only have to imagine!

Something else to consider is the amount of storage the particular iOS device is capable of. Remember earlier, I referred to some mobile devices as mobile desktops? Well most people given the chance will save everything they can locally. So a 64GB iOS device is great for the end user, not so much for the collector.

Apple iOS devices are considered dense storage devices, or another way to view them is as a portable hard disk drive with a user interface. At their core, they are storage devices and as such many things can be saved to them like thousands of pictures, music files, movie files and documents. The storage capacity of the device will determine how long the collection will take. Under the best of circumstances the time to collect or harvest is nebulous. But having some idea up front if you are dealing with a large storage capable device or not is extremely useful in planning the collection.

So, you have collected: What’s next? This goes back to the question: What is your end-game? Basic and standard information will be available depending on the mobile carrier such as

- where the phone or tablet was last used.
- numbers called.
- WiFi networks connected to.
With this information known, you can get granular and look at important electronic evidence artifacts. Many are standard but some are apple/iOS only items like sqlite tables.

- Do you need to know what emails / text messages were sent and when?
- Do you need to know the location and time stamp of a stored picture or picture taken with camera?
- Is it important to know what applications were downloaded and used?

All that you need to know is there and available to varying degrees. If the user only set their email to store the last 100 emails then that is all that is available. The point is once you have harvested the files from the phone, you can lay out a very accurate map of the travels and activities of the phone user or disprove actions that they are assumed to have taken. Choose the right tool for your analysis and subsequent ediscovery processing and review. Keep in mind that while iOS is very organized, there are a lot of files that may be considered responsive to your analysis via standard keyword or live search. As most ediscovery and review platforms are Microsoft based, you want to consider this as well for your overall strategy.

One thing I would advise, when practical, is to analyze and export your responsive esi using a Mac computer. This is not always necessary and, in fact, it is a good idea to have multiple analysis tools, but there are some files that are just better viewed and more accessible in a Mac environment.

IN SUMMARY
Collecting from an iOS device is difficult but not impossible. There are specific facts you need to know about the device and its manufacture, and variations in the methods that must be used depending on those facts. The keys for successful collection of data from Apple/iOS devices is the same as it is for any collection: Know the device; know the user, know the purpose of the collection, know the data that is being targeted and know how to use (and have access to) the right tools to defensibly collect it.

ABOUT THE AUTHOR
Richard Rodney serves as the Chief Technology Officer for SiteLogic Technologies with its headquarters in New York City. Richard has over 20 years in Litigation Support, ESI technologies and Computer Forensics. Richard manages the Electronic Services and Project Management group for SiteLogic and serves as the chief architect of technology related services with a concentration on consulting, forensic collections and analysis, and processing. Richard is a certified forensic and mobile forensic examiner having achieved both the ACE and AME certifications from Accessdata’s training group. Richard received his initial computer forensics training from instructors with the International Society of Forensic Computer Examiners CCE bootcamp program. Richard has also been trained by instructors at Blackbag Technologies to perform collections and analysis of Apple devices using their tools.

Richard is a devoted father of a daughter, who also enjoys reading, fitness activities, and movies. Richard also enjoys learning about and using new technology. Richard is long time supporter of the New York "Football" Giants team in the NFL, the New York Yankees in MLB and the New York Knicks in the NBA. Richard is a graduate of Lincoln University and Brooklyn Technical High School.