“IT’S JUST A PHONE!” - People, Rumors, and Cellular Forensics

By Kevin J. Ripa, PI, CDRP, EnCE, CEH

FACT 1

With most anything that has to do with computers, we usually hear rumors before fact. These rumors start to take on a life of their own until they become more like fact than the real facts.

FACT 2

For anyone in any field for any length of time, it is known that there are those who are excellent at what they do, and those who are excellent at marketing. Unfortunately we also know that both excellent work AND excellent marketing are rarely found in the same package, and sadly it is those who are excellent at the marketing that usually are heard first and loudest.

FACT 3

How many times have we heard that someone can do something, and it turns out that they can’t? Or that their idea of the “something” wasn’t YOUR idea of the “something”? Or that what they were advertising as the best “something” on the market wasn’t even close to the best “something”? But sadly you don’t know enough about the “something” to know the difference.

Allow me to digress for a moment. In the world of data recovery, rumors abound. The biggest one is that if your hard drive is clicking, or is no longer accessible, you can just throw it in the freezer over night and it will work again long enough to get your data back. Although this has a very loose basis in fact from about 10 to 15 years ago, it is a myth nowadays, and yet people still try it, and some people will even tell you they have a

buddy or brother or friend of a friend who just did it yesterday. As with most urban legends, this does not stand up to scrutiny, and when pressed, the buddy, or brother, or friend of a friend either doesn't exist, or it turns out that it wasn't really them, but someone else they knew, and you can never get to that "someone else".

We have heard the rumor that anything that happened on a cellular device can be recovered using forensics. This is a myth that you shouldn't believe. And we have heard that cell phones can be infected with monitoring software by opening a malicious email attachment, or through a text message. Another myth.

Unfortunately, many people don't know the first thing about the technology, so when they hear someone talking about it, they assume the talker is actually correct in what they are saying. Sadly this is usually not true. A lot of people talk in generalities but the truth rarely survives such comments. So then here is the straight talk about cellular forensics, and malicious software for cell phones.

When we talk about cellular forensics, many people automatically think that if you do computer forensics, you must be able to do cellular forensics. In fairness, for both cases you are dealing with data and preserving and searching it. That is where the similarity ends. While it is true that someone already versed in computer forensics is better poised to enter the realm of cellular forensics, this does not automatically make them an expert.

With computers, accessing and imaging the data on the hard drive is the same for the largest majority of all storage devices. Then the analysis can be done using the appropriate software. With cellular devices, there is so much more to be taken into consideration. No two devices are the same. There are literally thousands of different cellular devices, and their data structure, not to mention method of accessing the data

forensically can change not just from brand to brand, but from model to model. Just because it is an LG phone, does not mean that we can do the same thing with one model that we can do with another. As well, a 3G iPhone is different from a 4G iPhone, and in fact, the forensics can differ between versions of 3G! Our lab has literally hundreds of cables just to be able to connect to any device that may come our way. (By the way, did you know that forensics on automobile GPS devices is also possible?)

One of the most frequent comments received from a perspective customer who wants a cellular device analyzed, is "Why does it cost so much? It's just a cell phone!" Well in that case, I can do the full blown extraction and analysis of JUST THE PHONE PORTION (call lists in and out) for a very small price. "What was that? You want the text messages, emails, internet activity, and data portions?" Hmmmm….seems like it's not just a phone anymore! In fact, when I started doing computer forensics a number of years ago, hard drives averaged around 2-4 GB in size. Now I have a 16 GB memory card in my Blackberry that will hold any kind of data I want to put on it. I can buy a 64 GB iPhone. What about the iPod, iPad or the iTouch? None of them is a phone, but none of them is really a computer either!!! Are you starting to see the complexities here?

Let's look at a normal, everyday flip phone. Just a phone, right? Well a phone will make and take calls. That is it. Nothing more. So what will the flip phone do? It keeps incoming and outgoing logs of sometimes hundreds of made and received calls. And missed calls. And messages. What about SMS? MMS? Does it take pictures? Just try finding a cellular device today that DOESN'T take pictures. Have you heard of geotagging? If I can extract pictures (even deleted ones), and then go one step further and tell you where exactly the photo was taken, do you think that might be important? (Did

he just say deleted ones?) The vast majority of phones today are GSM phones with SIM cards. What does this mean? Well what if the perp has a second SIM card that he uses for all the bad stuff. A good analyst will be able to tell you about other SIM cards, even if they are not present. Most phones (even normal flip phones) have the capability of receiving a media storage card like an SD card. You can get them in sizes up to 128 GB now.

So then what is the difference between a 128 GB storage card in a cell phone, and a 128 GB external hard drive connected to a computer? Do you still think it is “just a phone?”

In the case of cellular forensics, as indicated before, one size does not fit all. Virtually all cellular devices can be broken down into 5 categories:

Blackberry

iPhone/iPad/iTouch

Android

Win CE

Symbian (your run-of-the-mill cell phone)

Generally speaking, these categories follow the lines of the internal operating system, allowing that from one Blackberry to the next (for example), the data can reside differently and take different tools to extract. The next thing that needs to be understood is that there are roughly 2 different areas within the device. The logical data, and the physical data. On many phones, you can only access the logical data and not the physical data. In cases such as i-devices, getting the physical data from a 64 GB iPad can take as

much as 48 hours or more just to do the data dump. With some, you can break the user password, and with others you cannot.

Blackberry

With Blackberrys, only the logical data is extractable**. If data has been deleted, it is not recoverable** with current technology. Recovering the user password or bypassing it is not possible** with current technology, and repeated attempts will cause the device to wipe out all resident data. This can be triggered with as little as one wrong attempt, but the default number of attempts you have are 10. Anyone that tells you they have hardware or software that can recover deleted data from a Blackberry is simply lying to you as of the time of this writing.

i-Devices

These are much more forgiving. Forensically speaking, i-devices are just about the biggest tattle tales out there. For example, even when you delete your text message, it isn't deleted. I don't mean that a forensics guy can undelete it if it isn't overwritten. I mean it isn't really deleted. When you think you have deleted it, you have merely given an instruction to the device telling it not to show the message to you anymore, but it is still there and not going anywhere. Analysts have tried to see how many messages can be stored before they start getting really deleted, and the largest list (with no deletions so far) is 14,000 messages. How about geotagging? Every picture you take with an i-phone (unless disabled) can be tracked to exactly where and when you took it. Yes, WHERE. The camera captures the latitude and longitude of the location when you took the picture, and it is embedded in the image for examiners to extract. For i-devices, deleted information CAN be recovered if it has not been overwritten yet by new data. Both

logical and physical dumps are possible, but there is very little to salvage from the physical. The devices do such a great job of keeping it all in the logical, which is easier for us to analyze anyway.

Android

Very much like a computer hard drive, and the code to run these phones is all open source, so there is very little mystery to them. Having said that, the analyst must be conversant in forensics at the Hexadecimal level, because tools are still lacking for these devices. Get the wrong person doing your forensics on this device and you will never know what they didn't get. As with a computer hard drive, you can do logical and physical dumps, and extract deleted information if it hasn't yet been overwritten.

Win CE

Palm and other devices that run on Windows CE are the closest to a normal computer in their structure. Can be logically and physically analyzed, and deleted data can be recovered if not yet overwritten.

Symbian

This basically covers all other phones, generally speaking. That number is well over 3000 devices and growing. Physical dumps can be done from many of them, but that does not mean necessarily that deleted information can be had. In some cases, the devices are completely inaccessible and the only way to pull data off is to mount the device in a camera contraption that is available and videotape and photograph manually scrolling through every area of the device. With some you can recover the user password to access the phone and with others you can't.

It cannot be stressed enough how important it is to tell your examiner (or anyone you are asking a question of) what the model of the device is. If you ask a question like, “Can I recover all the deleted text messages off of a client’s phone?”, and you actually get a specific yes or no, do NOT hire that person. This question simply cannot be answered without first knowing the model of the phone. Is the device CDMA, TDMA, GSM, GSM hybrid, HSPA? The point isn’t to fill your head with mindless acronyms and silliness. It is to show you that these are not “just phones”, and doing forensic analysis is not a simple task.

Taking a 3 day course does not automatically qualify someone as an expert in this field. What equipment are they using? Do they have an out of date copy of Data Pilot, (sadly very common) or are they running with the big boys and girls, and using numerous tools? There is no single cellular forensics tool that will do every phone out there. You need a number of tools to be able to cover the widest array of devices. Just because someone plugs the phone into a 60 dollar tool and it says it can’t extract data, doesn’t mean it can’t be done. Any reputable shop will be running overlapping tools such as Cellebrite, MobilEdit, Oxygen, Lantern, MPE, Device Seizure, etc. Most people doing cellular forensics don’t have Cellebrite, for example. This tool is a tool that is almost a must have for the cellular forensics toolbox. It shouldn’t be the only tool, but it should be one of the first. Sadly it is not, because for the big boy version with Physical access at the time of this writing, it starts at about $8000.00. Add on the almost 2K licensing fee each and every year, and this is just one of the devices I mentioned! Getting into cellular forensics (or any data forensics) is not a cheap proposition. Taking a 1-3 day course from

someone who shows you how to find Malware on a phone is NOT learning cellular forensics!

You will recall the ** I had placed after some of the Blackberry entries. These could apply to many of the other devices as well. These are caveat asterisks. The reason I use them is because even though I say that certain things cannot be done, I mean using hardware and software being used by even the very skilled examiner. In some cases, you CAN get deleted data from a device that says it is not possible, such as a Blackberry. These are the same techniques used on any device that does not allow access to portions of its data, or in cases of dead batteries with no replacements, no cords, no SIM cards, smashed screens, fire/flood damage, etc. Ultra advanced techniques such as doing a flasher box dump can be used, and in extreme cases, the phone can be dismantled and the data chip actually delaminated or desoldered from the circuit board and accessed through what is known as a chip reader. Lest you think, “Yay!!!! So it is possible!”, you need to come to the table with very deep pockets. This is truly “last resort” stuff, and in many cases, will leave the phone a destroyed mess.

Let’s take a look at malware and hacking analysis of devices. This is usually more prevalent a question than forensics. You get a call from a client saying, “My husband/wife/boyfriend/girlfriend/ neighbor/boss hacked my phone and knows everything I am doing!” Sadly there are many fearmongers out in the world who will scare you into believing many things are possible, just to help you part with your money.

Here are some rules that apply to cellular devices. These are hard and fast as of the time of this writing, and are subject to change.

FACT: Symbian phones cannot get monitoring software installed on them. They simply have no interface for it. By this, I mean someone actually installing something on the phone to monitor its activities.

FACT: In order to be able to be monitored, it must be a mainstream, popular Personal Digital Assistant style device. (Smart Phone)

FACT: There is currently NO known monitoring software that can be installed on a smartphone remotely.

FACT: Monitoring software does exist, and can be very effective if installed and executed properly, but 90% of the time it isn't installed properly, and so either doesn't work properly, or is easily detected.

FACT: In order to install monitoring software on a smart phone as of the time of this writing, the perp MUST have physical access to the device for 5-15 minutes, depending on their skill level. By this, I mean unfettered access to hold the device in their hands and manipulate it. If you take your device to the bathroom with you, and it is never out of your care and control, then it is not hacked, and your information leak vector is something else.

FACT: You can NOT get monitoring software on your phone via email attachment, SMS, etc. The hype surrounding this is actually for things like viruses and adware and things. Not nearly the same as monitoring software.

In the case of an iPhone, even if you have let it out of your sight, and someone you suspect could very well have been alone with your phone for a while, if your iPhone isn't jailbroken, then nothing could have been installed. All of the hard core monitoring software available for iPhones can only run if the device is jailbroken. What is

jailbreaking? Jailbreaking is altering the iPhone operating system to allow the installation of NON Apple software. This is usually quite obvious, and the best sign is finding a program on your device named Cydia or Icy or Installer.

There is a lot of hype about monitoring software for phones, but the fact is that there are only 3 or 4 good programs that can do this monitoring. We have tested well over a dozen pieces of software, and most simply did not work as advertised, or required a degree in programming in order to install and run. Having said that, the ones that work are incredible in their capability. They have the capability to capture all incoming and outgoing calls, voice mails, SMS, MMS, BBM, emails, and internet activity. They then email the captured data to you, or store it on a website that you access to see the captured data. The best, most expensive ones will even make your phone ring when the monitored phone rings, so that you can listen in on the call like a third party. To scare you even more, they can allow you to call the device, and it will answer your call WITHOUT ringing or otherwise alerting the user. This allows you to listen to the surroundings of the phone completely undetected.

I must reiterate though, that this is NOT currently possible without first having the device in your hands to install the software. IT CANNOT BE INSTALLED REMOTELY.

In the case of malicious software, viruses, or other bugs that CAN get on your phone remotely, (but cannot monitor in the way people think), as well as in the case of the real monitoring software that does work and has been installed manually, there are thankfully telltale signs of this infection.

In the case of the best and most expensive monitoring software, you will need an expert to definitively detect and identify its existence. In the case of everything else, some of the common signs are as follows:

Look at the list of installed programs on the device. The vast majority will be authored/copyrighted to the manufacturer. For example, Research in Motion/Blackberry. Anything that is not should be identifiable by its name, such as the latest Urban Spoon app or Tetris.

The device will use up the battery exponentially faster than it ever did. If you have a device that used to last 3 days on a charge, and it is now lasting 6 hours, start finding out why.

The device will typically get very hot to the touch, even when not in use.

The best programs, of which there are about 3, (and one of them is specific to Blackberrys only) will NOT be detectable except through the battery life reduction, heat, and data usage, and even then, depending on your usage, you may not see a degradation in this service.

When it comes to protecting against the run-of-the-mill virus and adware garbage that is targeting more and more phones, there are some options. The following are only two of them, and they have free versions that are almost as powerful as the paid version. www.mylookout.com and smrtguard.com are the websites. They both do much more than just watch for viruses and malware. They can also be used to create online backups of your devices in case of loss of device, change to a new device, etc. One of the greatest features is that you can use the web interface to make the phone trigger a loud, audible alarm to find it in case you have misplaced it. You also have the option of going online

and locating the device via its GPS function. Ever left a phone in a cab? This sure would have been handy!

One last tidbit of information specific to iPhones. If they are locked, or in other words require a 4 digit code to unlock and use, there are currently only 2 methods of extracting the data unless you know that code. These two methods use VERY expensive hardware and software. Now there will be some people (the bargain basement sort) that will promise they can still access the data, but they are actually jailbreaking or hacking the phone in order to do it, and this will leave telltale signs. Instead of believing half truths and generalities, you are welcome to contact me at any time at kevin@computerpi.com. I am more than happy to answer any questions and give guidance where I can.