Volume 11, Issue 7

Penny Hill, Chapter Administrator Kathleen Watson CFE, Newsletter Editor acfe.toronto@sympatico.ca

"IT'S JUST A PHONE!" - People, Rumors, and Cellular Forensics

By Kevin J. Ripa, PI, GSEC, GCFE, GCFA, BAI, EnCE, CDRP, CEH .

Part II

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 Do they have an out of date copy of Data Pilot, (sadly very common) or are they running with the big boys and girls, and using numerous tools?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 $12,000.00 USD. Add on the $3300.00 USD 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.

Continued on page 2

Dinner Meetings Update

The ACFE Toronto Chapter hosted our January dinner meeting on January 24th at The Royal Canadian Military Institute.

This meeting, the first of the new year, was well attended. The chapter would like to thank Ryan Duquette MSc, CFE – Hexigent Consulting for his presentation "DEFENDING YOUR DIGITAL DATA"

We would like to congratulate Jeff Hayden, who was the winner in our draw for a certificate for free admission to an ACFE dinner meeting.

Community Partner Update

At the ACFE Toronto Chapter, we like to keep up-to-date on what our Community Partners are doing. If any of our members know of anything new taking place with any of our Community Partners please send email us acfe.toronto@sympatico.ca.

"IT'S JUST A PHONE!" - People, Rumors, and Cellular Forensics

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, or a technique called JTAG. 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 Smart Phone.

FACT: There is currently NO known monitoring software that can be installed on a smartphone remotely. (At least not for less than a few hundred thousand dollars).

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.

Continued on page 3...

"IT'S JUST A PHONE!" - People, Rumors, and Cellular Forensics

...continued from page 2

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. I am more than happy to answer any questions and give guidance where I can.

Career Corner

If you have a position you would like posted email us at acfe.toronto@sympatico.ca.

About the Author

Kevin J. Ripa is the President of Computer Evidence Recovery, Inc., and has been involved in numerous complex cyber-forensics investigations. He can be contacted via his website at www.computerpi.com. Information in article current as of time of writing.

CONFERENCE
FRAUD INVESTIGATION TECHNOLOGY – 2

JAMES D. RATLEY, CFE
President, Associaton of Certified Fraud Examiners, Austin TX

Interviewing Prospective Witnesses & Evaluating Deception

You cannot prepare enough for your interviews. The psychology of deception is very complex and often manifests itself through verbal and non-verbal cues. Learn why observation is critical during the entire investigation but more so during the interviewing process. You will see how the various environmental and psychological factors can enter into the simplest of interviews and also learn that developing the right questions in the right sequence can produce very beneficial results.

Association of Certified Fraud Examiners
Toronto Chapter (ACFE TORONTO)
&
Council of Professional Investigators of Ontario (CPIO)

WEDNESDAY APRIL 5, 2017 (One Day)
7:45 am (Registration) to 4:30pm
Location: BMO INSTITUTE FOR LEARNING
3550 Pharmacy Ave., Toronto, ON M1W 3Z3

For more information or to register, click here

The Blotter

That's the spirit: Brampton man charged in spiritual scam

A Brampton man faces charges for allegedly duping a woman out of cash and jewelry by claiming he could get rid of evil spirits because he was so “close to God.” Read More

Toronto teen who befriended women on Instagram charged in fraud scam

A Toronto teen who used Instagram to meet several women over the last four months, has been busted in an identity theft and fraud investigation. Read More

Ex-Visium fund manager convicted of fraud by Manhattan jury

A former portfolio manager at Visium Asset Management LP was convicted of securities fraud on Thursday, following a trial that stemmed from a federal investigation that led to the New York-based hedge fund's closure last year. Read More

City Employee Arrested; Charged With Fraud and Theft

The Estevan Police Service has arrested and charged a City of Estevan employee with fraud after a ongoing investigation. Read More

Former French president Nicolas Sarkozy faces jail after he is charged with fraud and running a corrupt election campaign.

The 62-year-old faces jail if he is found guilty of a range of crimes including fraud, false accounting and breach of trust. Read More

3 Toronto men charged in credit card fraud near Belleville

Charges have been laid against three Toronto men in connection with the attempted use of fraudulent credit cards east of Belleville. Read More

Connect on LinkedIn

Did you know the ACFE Toronto Chapter has a new LinkedIn group? Find lots of great connections, articles, discussions, postings. Just go to LinkedIn ACFE Toronto Chapter page by clicking here and ask to be connected to be a part of this lively site.

Your Board of Directors

President	William Vasiou, MBA, CPA, CGA, CFE, DAC
Vice President and Training Chair	Astra Williamson, CPA, CGA, CFE
President Emeritus, Secretary and Conference Chair	Tom Eby, MBA, CPA, CA
Treasurer	Erik Bettencourt, CPA, CMA, CFE
Director and Newsletter Chair	Kathleen Watson, CFE
Director and Membership Chair	Ryan Duquette, MsC, CFE, CFCE, CEECS, EnCE, ACE
Director and Social Media Chair	Ryan Watt
Director and Membership and Certification Chair	Linda Lister, CPA, CGA, CMA, CFE, DIFA
Director and Community Outreach Chair	Dorian Dwyer, CFE
Director and Chapter Administrator	Penny Hill

About the ACFE

The ACFE is the world's largest anti-fraud organization and premier provider of anti-fraud training and education. Together with more than 70,000 members, the ACFE is reducing business fraud world-wide and inspiring public confidence in the integrity and objectivity within the profession. Visit www.acfe.com for more details.

Upcoming Events:

February 15, 2017 IIA Toronto presents – FS Series Coordinating Assurance Across the 3 Lines of Defense
Speaker: Baskaran Rajamani, Partner, Deloitte
Venue: The Albany Club - 91 King Street East; Toronto, ON M5C 1G3
8:00 – 10:00 am
More Information and Registration

March 1, 2017 ISACA Toronto presents – Blockchain Security
Speaker: Mat Cybula, CEO & Founder of Cryptiv Inc.
Venue: Ivey Tangerine Leadership Centre - 130 King Street West; Toronto, ON M5X1A9
6:00 – 9:00pm
More Information and Registration