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

Volume 11, Issue 7

Happy New Year

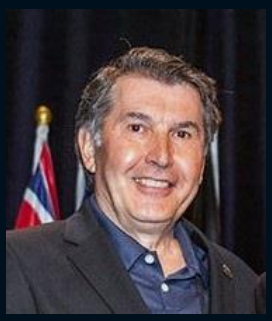
As president of the Toronto chapter of the ACFE and on behalf of the members of the Board, I would like to wish all our members and associates a happy and healthy New Year.

2017 is shaping up to be an interesting year with the incoming USA president, Wall Street insiders, and a bull market. Conflicts of interest, economic extortion, and the potential bribery are already raising red flags. When congress's first act is to try to eliminate the independent office of the ethics commissioner then we as ACFE's have the potential for continuous employment.

Of course that's south of the boarder, but we have no reason to be smug. We have pay for play at the federal and provincial levels and when one examines the tone at the top, one cannot get any higher than our political representatives.

As a reminder our first dinner meeting will be held on January 24, titled "Defending Your Digital Data" with Ryan Duquette. It promises to be an interest session. Check the ACFE Toronto website for additional details.

Have a successful and prosperous new year.



William Vasiliou, MBA, CPA, CGA, CFE, DAC
Chapter President

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

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

Part One

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.

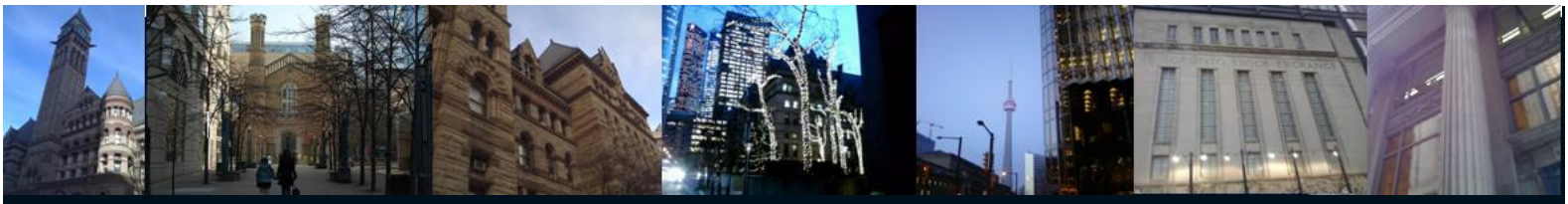
Continued page 3...

The Annual Canadian Fraud Conference Returns home to Toronto!!!

Once again the Association of Certified Fraud Examiners is bringing the Annual Canadian Fraud Conference home to Toronto. The 23rd edition of this premier conference is set to take place **in 2017.**

This conference, geared towards the needs of the Canadian CFE, is by far the most comprehensive and informative program available.

The conference will include two and a half days of workshops, presentations by distinguished fraud professionals and countless opportunities to network with other CFEs from across the country and around the world. We are so very proud to be part of this prestigious program returning home to the greatest city in Canada! Stay tuned for exact dates!!!



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; and
- 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.

Continued page 4….

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.

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.

Continued in February

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.

Career Corner

Experienced Operations Manager Required

INVESTIGATIVE RISK MANAGEMENT INC. "IRM" is a licensed niche firm operating in the Province of Ontario. IRM is headquartered in Barrie, Ontario, with a Sub Office in Toronto. We are seeking an experienced Operations Manager.

Duties and Responsibilities:

. recruitment; and training of field investigators;
. schedule assignments to investigators;
. oversee day to day operations;
. ensure contractual timelines are met;
. provide regular updates to clients:
. review, edit and assist in the production of detailed reports;
. conduct employee reviews;
. participate in, and assist with, tradeshows and various committee functions;.

Experience:

. 10 years investigation; insurance adjuster; or legal experience required;
. exceptional organizational skills;
. excellent managerial and interpersonal skills and communication;
. excellent written and verbal communication skills;
. Proven ability to deliver with high quality, on-time, and within budget;
. flexible approach to achieving goals; team-player; collaborative.
. strong follow up and customer focused approach;
. Excellent computer skills
. Financial management skills

Please forward a detailed resume and financial expectations in confidence to: brians@irmi.ca

All compensation will be discussed in person through the appropriate interview process.

"How people treat you is their karma; how you react is yours."

~ Wayne Dyer

The Blotter

Former MaRS employee facing 11 charges in fraud investigation

Thornhill resident Allen Gelberg, 61, allegedly used his position as director of the Collaboration Centre with MaRS to defraud his employer, as well as several service providers, of more than $970,000. Read More

York regional police charge 9 people in alleged $30M fraud

York regional police say they began investigating AC Simmonds Group in November 2014 following several complaints from people alleging they had been defrauded. Read More

2 Markham residents charged by Toronto police in mortgage fraud case

Sivakumar Kumaravelu, 57, and Naguleswary Sivakumar, 54, both of Markham were arrested and charged with fraud over $5,000 after surrendering to Toronto police Wednesday, Jan. 4. Read More

Cops' lawyer fights suspension amid fraud and money-laundering charges

A lawyer charged with fraud and money laundering related to dealings he had with top executives of a police union is appealing his suspension. Read More

18-month jail sentence for former UW employee convicted of fraud

A former manager at the University of Waterloo was sentenced to jail time Friday for defrauding the school of nearly $177,000. Read More

Business owners say fraud, theft by former bookkeeper had huge impact

When the owner of Double H Electric Ltd. in Mount Pearl found out a trusted employee had stolen tens of thousands of dollars from his company, he lost faith in humanity for a while. Read More

Canadian bank failed to report 1,200 suspicious transactions

For keeping the transactions secret, the bank, whose name has been removed from the documents, was fined $1.15 million — the first and only time a bank has been penalized for this kind of offence in Canada. 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 Vasiliou, 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:

January 17, 2017 IIA Toronto presents – Key Trends in Internal Audits
Speakers: Geoff Rodrigues, CPA, CA, CIA, CRMA, ORMP and
Peter Yien, CPA, CA, LPA, CISA, CRISC, CPA (Illinois)
Venue: The Albany Club - 91 King Street East; Toronto, ON M5C 1G3
8:00 – 10:00 am
More Information and Registration

January 24, 2017 ACFE Toronto presents – Defending Your Digital Data
Speaker: Ryan Duquette, Founder, Hexigent Consulting
Venue: RCMI 426 University Ave., Toronto, ON M5G 1S9
More information and Registration

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