News, Resources and Useful Information for the Online Investigative and OSINT Professional from Toddington International Inc.

Toddington International Inc.

Online Research and Intelligence Newsletter

MAY 2018 EDITION

In This Edition

Welcome to the Newsletter

Welcome to the May 2018 edition of TII's Online Intelligence Newsletter. A lot has been happening at TII these past two months, including the development of a brand new two-day training program:

"*Critical Thinking for Investigators*" is an intensive two-day classroom-based workshop designed to help investigators and intelligence professionals avoid making incorrect assumptions by using logic, reasoning, critical thinking, and scientific methodology in their investigations. Attendees will acquire skills required to turn online data into meaningful, actionable intelligence. All too often, mission critical investigations fail because those involved jump to conclusions and draw faulty inferences that leave the trail cold. Correct conclusions are not the result of guessing, but by applying efficient thought processes. Currently being offered on an in-house basis, this program will be publicly available in the Fall of 2018.

We are also pleased to announce that "*Hunted*", the hit UK-based reality TV series

which casts a number of TII personnel, was nominated for a prestigious BAFTA award in the "Reality and Constructed Factual" category. TII team members will again be traveling to the UK in the coming months to film the fourth season of *Hunted*, along with a new "Celebrity Edition", in support of "Stand Up to Cancer".

Growing to serve you better: we are also excited to announce that the TII team is expanding yet again – more to come on this in next month's newsletter.

In this edition of the newsletter, TII's Kathy Macdonald, shares insights on the importance of documenting digital evidence during investigations, and presents solutions to overcoming potential challenges in the article, "Capturing and Seizing Digital Evidence – Important Considerations for Today's Investigator".

Your feedback is important to us: contact us anytime at https://www.toddington.com/contact-us/.

E-Learning Graduates

Congratulations to the following students who are among those who successfully completed the 40-hour **Using the Internet as an Investigative Research Tool™** e-learning program with TII this month:

- Harrison Van Riper
- Slawomir Kiraga
- Kiran Hussain
- Rebeka King
- Kim Damiano
- Jeryes Khaleel
- Wilfred Barboza
- Martin Hansson
- Ena Popadic
- Jennifer Lamb
- Jason Nachum
- Giuliano Petti
- Karen Ettinger Narwal
- Kenneth Johansson
- Dan-Eddie Nielsen
- Gerrit Schippers
- Danielle Butler
- Camilla Hägglund
- Jennifer-Lee Heise
- Emily Wu
- Jason Manning

- Todd Mitchell
- Sarah Grant
- Elizabeth Blackwell
- Joseph Nastasi
- Galya Kabbani
- James Rhode Del Rosario
- Benadeth Beroin
- Susan Shaw
- Susan Wilson
- Chrissy Gardner
- Ayesha Pornea
- Jack Wallis

Capturing and Seizing Digital Evidence – Important Considerations for Today's Investigator

By Kathy Macdonald, M.O.M., MSc., CPP
Associate, Toddington International Inc.

Social media offers an exceptional source of intelligence for investigators. Learning how to search and gather intelligence online is an effective skill that helps investigators acquire relevant information. This article helps guide police, non-specialist investigators, and many kinds of responders, who may be called upon to collect and seize digital or electronic evidence for their investigations.

Digital evidence can be found in places like a person's cellphone, or online in places like social media. For the most part, digital evidence can be obtained through a search following informed consent, or it can be seized after a search warrant is obtained. Although seizing digital evidence can be complicated and challenging, an investigator can always start by simply asking questions about the data and about why they are looking at it.

Investigators should consider the type of data that might be contained within a device or on a particular social media platform. They also should consider whether there is an assumed reasonable expectation of privacy within it because people have both an objective and a subjective expectation of privacy with regard to information contained on their devices. This means that investigators should take both an unbiased and unemotional standpoint, along with an emotional personal viewpoint when they consider looking at data or viewing it in a device like a computer, a tablet, or any Internet-connected apparatus like a cellphone. Basically, investigators should ask, "What is it that I am looking at and why am I looking at it?" and "Who owns this data?" Regardless of where digital evidence can be found, an investigator must understand their grounds for looking at that data and understand their authority for seizing it.

To begin with and more importantly to be effective, an investigator always must prepare a search plan prior to conducting an investigation using social media. When an investigator gathers publicly available information, he or she should ensure that they are not leaving digital footprints on websites and apps that could reveal too much information about the investigator or the network used to conduct the search. Investigators also must ensure they are on proper legal footing in the event that they come across digital evidence or information that could substantiate a crime. If they do not collect information in a proper manner, any evidence that they acquire could be inadmissible in court. Furthermore, by developing a search plan, an investigator will save valuable time and resources, and assemble the best evidence possible in the event the case is challenged in court.

Investigators should document the source of digital evidence and seize this evidence through legal means if it is to be relied on in court. Even if the information is found in social media, investigators must follow proper procedures in extracting the evidence correctly from the platform. Some information may be directly related to an investigation or crime, or may even be used as collateral or circumstantial evidence. Accordingly, this information as digital evidence, should be carefully documented and preserved throughout the investigative process to ensure its continuity.

In this example from a child pornography investigation, police conducted a warrantless seizure of the accused’s cellphone under exigent circumstances. Police had received information that a person was uploading pornographic

images of young children to several accounts in social media. These accounts were subsequently closed. Police learned that the suspect had opened several accounts with basically the same information including, a name, a date of birth, a web address and phone number. All postings ended with the initials of the suspect and listed a public park as a residential address. Investigators found another profile linked to this person posting live video, a commercial pornographic website, containing explicit sexual content relating to very young looking males. Police confirmed that mugshots of the suspect matched his social media accounts. The EXIF data from pictures and videos led to a public WiFi address with an identified IP address for a local restaurant.

It appeared to police that this was a simple investigation with all details pointing to one suspect. Police, however, were very suspicious of someone who posted child pornography in such an open fashion--the suspect was using his own name without even trying to hide his identity.

Police followed the suspect and approached him at a local restaurant he was known to frequent. They did not immediately arrest the suspect, but quickly confiscated his cellphone and put it into "airplane mode." In doing so, they severed any contact between the device and the Internet.

Police believed they had grounds to arrest the accused, however, after taking his cellphone, they let the suspect leave the restaurant. Police then obtained a search warrant and had the cellphone forensically examined pursuant to this warrant. The cellphone held digital evidence pertaining to the charges of child pornography. The suspect was subsequently arrested and in court the officers testified that they seized the cellphone to preserve evidence in the event the suspect dropped the phone into his coffee or a hot liquid. The court accepted the officers' testimony that they seized the cellphone under exigent circumstances and the suspect was convicted.

Another example illustrates the importance of following proper procedures in the collection of digital evidence found in social media. In this investigation, numerous postings were reported related to terrorism and extremist viewpoints, and social media postings pertaining to vulnerabilities at facilities considered to be critical infrastructure. Police monitored numerous “key posts” that appeared on multiple website accounts. They believed these to be associated to one person and they took steps to capture the key posts and all of the comments and discussions. When interviewed, the suspect even admitted to being the administrator of the multiple social media accounts in question. Police subsequently charged this suspect with terrorism-related offences, but in court the accused was found not guilty on all counts. This was a complicated investigation and demonstrated some of the problems involved in capturing digital evidence using social media.

Several considerations were made with respect to the decisions when monitoring, collecting, and capturing digital evidence, including:

1. Collect all the source code and metadata for the Timelines and Key Posts. Without the source code, it was not possible to view videos or comments, to expand the posts, or to navigate through the screen using the links in the original pages.
2. When capturing the "Timelines," ensure that none of the timeline pages are hidden, which would have otherwise been visible to a reader, including expanding posts that read, “See More” or “Continue Reading,” etc.
3. Capture all artifacts of text that would be visible to a user but may appear hidden.
4. Use commercial grade software that properly captures a scrolling page and any of the banners superimposed over other parts of the image.
5. Capture “Comments” and any notations of posts made by friends or followers.
6. Collect "Screenshots" on an ongoing and daily basis of all portions of the discussions between the administrator, friends, or followers.
7. Ensure that any "key posts" are complete so the context for the key posts is not missing. This is important in court to help interpret content and context, and help to prove intent.

It is clear that information found in social media is unpredictable and changeable. Account holders can post, forward, like, share, comment, edit, delete, or change a photograph or information at any given time. Various agencies and organizations have published “best practices” guides for the investigation of computer-based electronic evidence, and individual police services may also have their own guidelines and policies relating to the collection and preservation of digital evidence from social media.

While conducting their searches investigators must focus on the significance of digital evidence. Investigators should identify any potential sources of evidence, judge the importance of it, and include the details in their report. Because there is a very high expectation of privacy in personal computers, police should in most cases obtain a prior judicial authorization to seize and search a personal computer. If police come across a computer in the course of a search and their warrant does not provide specific authorization to search computers, they still may seize the computer; however, if they wish to search the data, they will have to obtain a separate warrant. Furthermore, there are no fingerprints on the computer data so a responder must prove who "possessed" the data. Generally, this entails proving who committed the crime.

The following information from page 166 of the book, *Evidence and Investigation:*

From the Crime Scene to the Courtroom, offers some basic rules to help guide non-specialist investigators and responders who may be called on to collect and protect computer-based electronic evidence.

- If there is reason to believe that a computer is involved in a criminal offence, take immediate steps to preserve that evidence.
- Consider your legal grounds for seizing such evidence (do you require a search warrant?).
- Do not attempt to access the computer. If it is off, do not turn it on. If it is on, do not search through it.
- Allow any print jobs to finish.
- Do not touch the keyboard or click the mouse.
- If a computer forensic examiner is not available, ensure that the computer is turned off by removing the power cord from the socket on the back of the computer; do not pull the plug out of the wall, because this could result in data being written to the computer's hard drive if it is connected to an uninterruptible power supply.
- In the case of a laptop computer, if it continues to operate after the power cord has been disconnected, remove the battery and do not put it back into the computer; however, be aware that in certain circumstances battery removal could result in data loss.
- If you have the technology available (camera, smartphone), and the computer is on, photograph the screen. Also photograph the computer itself and anything that is attached to it. Otherwise, create a written record of the computer set-up before touching or disconnecting anything.
- Document, ideally on video or in a series of photographs, all the steps taken to collect the computer and its components.
- Seize all associated storage media, peripheral devices, manuals, notes, and documentation.
- Look for any potential passwords in the vicinity of the computer. Popular places to "secretly" store such passwords include pieces of paper, labels, or "stickies" attached to the underside of the computer keyboard, mouse pad, or desk.
- Allow all components to cool down before packaging them securely for transport to the facility where they will be examined.

A police officer, now retired after 25 years with the Calgary Police Service, Kathy brings almost three decades of investigative experience and security awareness to her position as Instructor with Toddington International. In 2009, the Governor General of Canada invested Kathy with the Order of Merit of the Police Forces (M.O.M.), in

recognition for her outstanding work in the area of cyber safety and cyber security.

Kathy has extensive experience developing and delivering cyber awareness and crime prevention programs to both public and private sector organizations worldwide. Her areas of expertise include online fraud, the application of social engineering techniques, child online risk, social media, targeted intrusion, and privacy.

Learn more about Kathy Macdonald and her work here.

Upcoming Select Worldwide Training Dates

"Advanced Internet Intelligence & Online Investigations"
2-Day Course

May 14 - 15, 2018, Hong Kong
May 23 - 24, 2018, Singapore

"Introduction to the Blockchain Revolution"

3-Day Course

September 24 - 26, 2018, Dubai
November 25 - 27, 2018, Dubai

"Advanced Internet Intelligence & Online Investigations"
Fall 2018 Series
3-Day Course

September 10 - 12, 2018, Cambridge, UK
September 18 - 20, 2018, Dubai
October 3 - 5, 2018, Vancouver, BC
November 5 - 7, 2018, Toronto, ON
December 11 - 13, 2018, Dubai

"Cyberpsychology & Threat Intelligence: Assessing Risk Online"
Fall 2018 Series
2-Day Course

November 15 - 16, 2018, Toronto, ON
November 29 - 30, 2018, Vancouver, BC

TII is pleased to offer a number of specialized and customizable in-house training programs for both the public and private sector in a variety of formats, in addition to having available a number of expert speakers.

To learn more about what we can do to empower your workforce, contact us.

Resources for the OSINT Professional

blindfold.madbit.co – New tool for turning off or "blind folding" retweets on Twitter

plusprivacy.com – App that can be used to "control the privacy settings in your social network accounts, hide your email identity, block ads, trackers and malware and prevent unwanted apps and browser extensions from tracking you and collecting your private data"

imageidentify.com – Interesting AI project from Wolfram Alpha that attempts to identify the content of an image (drag and drop input)

tweetdeck.twitter.com – Real-time Twitter tracking and discovery tool

openknowledgemaps.org – Visual interface that maps scientific findings on a particular topic, provides an overview, and assists in identifying relevant, open access content

archive.is – Searchable website/page archive that is a useful alternative to the Wayback Machine at archive.org

peoplefindthor.dk – A search interface for Facebook (requires a Facebook account)

haveibeenpwned.com/passwords – Check to see if your password has been compromised in a data breach

tunnelbear.com – VPN for private browsing that hides your IP address and location, blocks trackers, and secures your data from third-parties

glutenproject.com – A unique, searchable database of certified gluten free products

humantraffickingsearch.org – Human trafficking search site that provides information on human trafficking worldwide

stolencamerafinder.com – Uses the serial number of photos to search the web for

other photos taken with a stolen camera

phototracker.ru/lite - Track online use of images and more

addons.mozilla.org/en-US - A new Firefox add-on that helps you control your web activity around Facebook by isolating your identity into a separate container. This makes it harder for Facebook to track your activity on other websites via third-party cookies.

dataselfie.it - Data Selfie is a browser extension that tracks you on Facebook and shows you your own data traces, revealing what machine learning algorithms could predict about your personality.

Want more? Visit our continually updated, FREE online research resources page featuring hundreds of links, cheat sheets, investigative guidelines, and more!

Comprehensive E-Learning Program:

"Using the Internet as an Investigative Research Tool™"

Take your Online Research and Intelligence Skills to new levels for only $499.99

The most comprehensive and up-to-date Internet research and investigation e-learning program available anywhere, Using the Internet as an Investigative Research Tool™ is designed to enable investigators, researchers, and intelligence personnel to find better online information, in less time, at less cost, with less risk.

For a fraction of the cost of classroom-based training, our flexible and interactive virtual classroom environment allows candidates to progress at their own pace and competency level, with a qualified personal instructor on hand at all times to ensure success. Initially launched in 1998, this highly-acclaimed and continually updated online course has been successfully completed by well over eight thousand investigators and knowledge workers around the world.

Enrollment takes only a few moments; online credit card payments are accepted, group discounts and licensing options are available for five or more registrants. Visit the course page **to find out more and instantly register, or** contact us **directly with any questions**.

Bonus: Tuition fee includes a one-year subscription to TII's Premium Resource Knowledge Base, a premium resource of some 4,000 deep web resources and sites (an additional $299 value)!

As a federally certified educational institution in Canada, TII can provide Canadian students with a T2202A Tuition Tax Receipt.

More Online Training

Introduction to Intelligence Analysis
40-Hour E-Learning Program

This program provides a rich and interesting opportunity to explore the key concepts and intellectual foundations which inform intelligence analysis activity. Students will develop awareness of, and experience in, using common tools and methodologies to conduct analysis assignments, as well as learn how to fashion one's insights and ideas in a way that communicates effectively to clients and other intelligence consumers. **Sign up or learn more** here**.**

Criminal Intelligence Analysis
40-Hour E-Learning Program

This program is designed to equip aspiring and inexperienced analysts, as well as other interested law enforcement and investigative professionals, with the knowledge and skills required to undertake criminal intelligence analysis work, and to understand criminal intelligence analysis products when encountered. **Sign**

up or learn more here**.**

Strategic Intelligence Analysis

40-Hour E-Learning Program

This program is intended for professionals working in public sector enforcement, intelligence, national security, and regulatory compliance roles, or those aspiring to do so. Students will be equipped with the skills and knowledge required to effectively conceive, plan, and implement strategic analysis projects, and deliver impactful strategic advice to clients and other end users. **Sign up or learn more** here**.**

Open Source Intelligence for Financial Investigators

40-Hour E-Learning Program

Essential for all financial institutions and corporations required to comply with the *European Union Fourth Anti-Money Laundering (AML) Directive* and similar legislation, or otherwise engaging in enhanced due diligence activities, this comprehensive training provides financial and business professionals with the latest tools and techniques required to effectively gather online OSINT, with the aim of enhancing compliance activities and minimizing potentially detrimental risks to an organization — both quickly and accurately. **Sign up or learn more** here**.**

"How-Tos" and Articles of Interest for the OSINT Professional

"GRPD for Dummies": The General Protection Data Regulation takes effect on 25th May 2018 and affects anyone handling personal data of EU citizens, anywhere in the world (Britain will transfer these new laws to the UK despite Brexit); very heavy fines for failure to comply.

How to preview a shortened URL on your computer or smartphone without opening it.

It's not just the GPS and communications interfaces in your phone that can give away your location but the device's gyroscopes and accelerometers as well. "Side-channel attacks" using these sensors could compromise your privacy in ways you may not expect.

What does Facebook know about you? "Facebook scraped call, text message data for years from Android phones."

A great guide to understanding search engines: "How Search Engines Crawl & Index: Everything You Need to Know."

"How Facebook Groups Are Being Exploited To Spread Misinformation, Plan Harassment, And Radicalize People."

Facebook builds detailed, sophisticated profiles of its users' lifestyles, likes, dislikes, and political leanings in order to target advertising. It then sells these profiles to third parties. How can you regain control of your personal data?

"Are You Listening? The 20 Best Social Media Monitoring Tools."

"Twitter as Data" by UCLA's Zachary C. Steinert-Threlkeld: Available for free to download from the Cambridge University Press for a limited time.

Surprising (or not so surprising?) MIT study findings: "Can You Believe It? On Twitter, False Stories Are Shared More Widely Than True Ones."

Piecing together the final moments of a victim's life, and identifying possible suspects, with Google's knowledge of their respective devices. A controversial and sometimes effective approach.

A new AI algorithm developed by the Chinese tech firm Baidu can create a plausible fake voice, demonstrating why it's becoming harder to believe anything you see or hear on the internet.

Google Search Tips: "5 Search Features Google Removed (And How to Bring Them Back)."

"Social Media Use in 2018": Pew Research Center survey results.

"How life online influences young people."

How our digital footprint is used to gather information about our well-being, also known as "digital phenotyping."

Is your password secure? How to create a strong password for your online accounts.

How to archive open source content for online investigations, including Facebook and Twitter content, and tips on saving photos and videos from popular social media sites.

Spending too much time on social media platforms and want to cut back? A good way to figure out which apps you spend the most time on in iOS is hidden in Settings > Battery. It tells you which apps you've spent the most (and possibly too much) time on.

"It's a gold mine of stuff that shouldn't be public" - A search engine created by anonymous hackers has been launched that allows anyone to search for sensitive data stored in the Amazon cloud.