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





Toddington International Inc.

Online Research and Intelligence Newsletter

SEPTEMBER 2018 EDITION

In This Edition

- Welcome to the Newsletter
- "10 Tips for Successful Online Insurance Fraud Investigations"
- Upcoming Select Worldwide Training Dates
- Resources for the OSINT Professional
- E-Learning: "Using the Internet as an Investigative Research Tool"
- More Online Training
- "How-Tos" and Articles of Interest for the OSINT Professional

Welcome to the Newsletter

Welcome to the September 2018 edition of TII's Online Intelligence Newsletter. With the summer (almost) behind us and the fall just around the corner, our team has been busy prepping for another global training tour, and the launch of three brand new classroom courses, which we will be formally announcing here soon.

Yaniv Pereyaslavsky Appointed as TII Associate



Yaniv Pereyaslavsky is Toddington International's London, UK-based associate, and is responsible for the delivery and development of advanced training programs for global audiences, in addition to the provision of consulting services to select clientele.

Prior to joining Toddington International, Yaniv gained extensive experience in Intelligence, Surveillance, Target Acquisition, and Reconnaissance (ISTAR) roles in both the

Canadian federal government, working on reporting, intelligence, and security surrounding consular missions and soft-power diplomacy in Africa, South America, and the world at large.

Within the private sector, Yaniv has extensive experience in both corporate intelligence and strategic planning in advanced technology industries. With a strong background in surveillance technologies, machine learning, and cybersecurity, he was responsible for intelligence reporting contributing to multimillion dollar projects for key stakeholders. Yaniv's work in the high technology sector has included complex open source investigations, information operations, government relations, and the overseeing of comprehensive competitive intelligence products.

Yaniv studied Security and Strategy at the University of British Columbia and the University of Copenhagen. He is certified in Advanced Cybersecurity and Field Security by the United Nations, and is a certified Strategic and Competitive Intelligence Professional (SCIP).

"Open Source Intelligence for Financial Investigators" – Completely Revised and Updated E-Learning Program Now Available



Unable to attend one of our classroom based training programs?

The **completely revised and updated edition** of our **"Open Source Intelligence for Financial Investigators"** program has now been released. This course is 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, at all levels, with the latest tools and techniques required to effectively gather online open source intelligence, with the aim of enhancing compliance activities and

Subscribe	Past Issues	Translate
	a : = : : :	

Exploring real-life case studies, this course will enable financial investigators to gather often circumspect information about the online activities, reputations, and business profiles of individuals and corporations, and to effectively evaluate data and sources based on specific online indicators. This advanced practical knowledge of research techniques and methodologies, coupled with technical advances, will enable financial institutions and corporations to prevent potentially costly problems through the early recognition of warning signals.

To learn more, download a brochure, and sign up for fast access, <u>click here</u> or <u>contact us</u>.

E-Learning Graduates

Congratulations to the following students who are among those who have successfully completed the 40-hour <u>Using the Internet as an Investigative</u>

Research Tool™ e-learning program with TII this month:

- Anna Grön
- Susan Lucas
- Matthew Green
- Shela Febrero
- Samuel Weber
- Khemil Nagawa
- Steven Filer
- Jonas Östlund
- Johanna Burke
- Kelvin Briggs
- Cecilia Renntun
- Sarah Brooks
- Samantha Rubinic
- Phillip McCormick
- Martin Ingdotter Olsson
- Nico Ramirez
- Erika Wallace
- Rita Plantera
- Megan Hammond
- Cynthia Tran
- Chris Gentle
- Gwendolyn Williams

- · vicki nguyen
- Ismael Moran



10 Tips for Successful Online Insurance Fraud Investigations



By Norm Wilhelm Head of Investigations, Toddington International Inc.

It's difficult to talk (or write) about a subject such as insurance fraud as it's such a wide-ranging and inclusive topic that one could easily create a hundred subcategories of discussion covering insurance industries, types of fraud, logistics, metrics, statistics, historical examples, legal cases, tools, or techniques, and we would still just be scraping the surface of the subject as a whole. So, to help focus the reader on what this article is about, I'm going to make five declarations right at the start:

Subscribe	Past Issues		Translate
-----------	-------------	--	-----------

- Z. It focuses on now made is detected using cyper investigations,
- 3. It focuses on techniques more than tools;
- 4. The reference information is relevant to provinces in western Canada;
- 5. And, it presumes that the reader already has an understanding of the topic.

More specifically, I'm talking about the cyber investigation of persons who have been involved in motor vehicle accidents and later make fraudulent claims related to injuries, lifestyle, loss of income, amount of income, capability to work, and are receiving support benefits. According to industry reports and news articles over the last five years, this is becoming more and more of a problem for motor vehicle insurance companies. *Who's to blame?* Insurance companies blame the opportunistic claimants and the defense lawyers who work the system; defense lawyers say it's the insurance company's fault for finding any reason to deny a claim and treating claimants like a criminal; the general population sees the insurance company as not doing a good enough job of investigating, and see defense lawyers as 'working the clients' for their own profit. Those are just a few of the opinions being expressed, and who is at fault for the problem often depends on whose report or article you read.

Regardless of fault, many insurance companies across Canada have increased their spending on investigations and prosecution, whistle-blower hotlines, and their public awareness projects in a commitment to reduce fraud. As an example, the motor vehicle insurance company called ICBC (Insurance Corporation of British Columbia) states that they performed over 10,000 investigations in 2013 and the same number again in 2016, with past statistics identifying that they had over 550 convictions for fraud-related court cases they initiated between 2010 and 2015. More recently, the number of fraud tips from hotlines increased to 1,990 in 2016, and the number of ICBC investigations rising to over 16,000 in 2017. ICBC experts estimate that 54% of their cases investigated contained elements of fraud, with fraudulent or exaggerated claims estimated as causing 10-20% of all claim costs, about CA\$600 million per year. Even the general public believes 4 out of 10 claims have elements of fraud, according to insurance industry studies from 2017, with 17% of respondents personally knowing someone who intentionally filed a fraudulent claim. ICBC is supported in their efforts by other industry organizations such as the CCAIF (Canadian Coalition Against Insurance Fraud), the CANATICS (Canadian National Insurance Crime Services), and a service industry of private investigators licensed by the provincial government and regulated by the PIABC (Professional Investigators Association of British Columbia).

Over the past 11 years, as a licensed private investigator working civil court cases, most of my work has been (and still is) related to motor vehicle insurance

by the time a me has been assigned to me, it has already been tagged with several 'flags' of warning by the insurance company employees and the analysis program(s) they are using, usually based on irregularities in information, incongruent claimant behaviour, or hotline tips that indicate something unusual is going on. In addition, by the time it gets to me, it has already been looked at by (at the very least) an adjuster, a manager, a paralegal, and a lawyer; the file may have changed adjusters hands and lawyers over the last few years; the ICBC cyber unit might have completed a preliminary scope; an SIU investigator may have already looked at it; and sometimes, another PI firm has already taken a shot at the file. In other words, I don't get the easy cases, I get the toughest cases where there were no easy answers and everyone who has handled it ahead of me says "we know they are doing something, but we can't figure out what it is, or we can't prove it". These people are not dummies; the adjuster, the manager, the paralegal, the lawyer, the investigators, they are all skilled at what they do, but if you don't spend enough time doing cyber investigations, it's hard to build up the experience necessary to know what is unusual, how to deconstruct information, how to develop new lines of query, where to look for information, or how to make a user account reveal more information - and that's what I've been doing for over a decade.

Every claimant file I handle has a person with a different combination of lifestyle, family, education, occupations, activities, travel, hobbies, and widely varying levels of social networking and use of technology. As a result, there's no common style or scam method. If anything, these types of fraud cases would be divided into the following main categories:

- Persons who appear to be legitimately injured and are not acting fraudulently;
- Persons who have no injuries but claim to be injured;
- Persons who exaggerate the extent, duration, and impact of their injuries on themselves;
- Persons who exaggerate the extent, duration, and impact of their injuries on their income;
- Persons who falsify their income potential, business potential, or employment capabilities;
- Persons who claim to not be working or earning income but actually are.

The following are examples of how widely varied the fraud activity can be, and also one of the main problems with talking about civil court cases: the content has to be anonymized to protect the privacy of the person involved, and even the companies involved (i.e., these cases are not necessarily related to motor vehicle insurance).

Subscribe	Past Issues		Translate
	in the meantime	riuu joirieu ariu piayea jor a iocai roller aerby tearri.	

• Example 2: The rancher who claimed to be completely disabled but was

- Example 2: The rancher who claimed to be completely disabled but was working under a 'stage name' in another occupation.
 Example 3: The retail clerk who claimed to be still injured, spending the
- Example 3: The retail clerk who claimed to be still injured, spending the next three years unemployed. Instead, the clerk spent that time trying to become a professional online gamer. This included creating a website, posting scheduled broadcasting times for subscribers, trademark branding, sales of branded merchandise, acquisition of sponsors, hosting game tournaments, upgrading computer equipment, and operating over 75 social networking accounts. The clerk was still also weightlifting in their spare time.
- Example 4: The folk musician and disk jockey who claimed to be injured, but was actually still working as a DJ, and had recorded, produced, and posted over 20 digital songs for sale online; plus the musician claimed he had been intending to become an airplane pilot.
- Example 5: The bookkeeper who claimed to be injured while in the meantime running a 'ghost kitchen' that catered to a specific cultural food type, and was advertised on social networking websites.

In all of these cases, I used the same set of templates, tools, and techniques that I use for every file, and it's part of what I teach to others with Toddington International. Here are 10 points that every cyber investigator can do (or should be doing) to improve their chances for success when working on a file.

- 1. <u>Develop a Key Word List:</u> Before starting your online search, you should have a key word list containing all the information you will be searching. This should include all the information you have gained from whoever gave you the assignment, be it your supervisor, another department, or a client.
- 2. <u>Develop New Key Words:</u> Before starting your online search, you need to expand your list to include all reasonable search variables. For the name, you would include all the first name variations and combinations of first and last names; don't forget to include maiden names and former married names. Include alternate names for the claimant's occupation or employment title, and the alternate names and spellings for any sports, hobbies, or activities they participate in. Your list should also include not just where the person lives now, but where they used to live and where they were born. And don't forget alternate names for geographic areas; for example, if a person lives in Vancouver, you won't just search using the word Vancouver, you may also need to include other regional names such as Burnaby, Delta, Langley, New Westminster, Richmond, Surrey, or White Rock.
- 3. <u>Search Everything</u>: Check every key word you have that is possible to search

Subscribe	Past Issues	Translate

- **4.** It Takes Time: Back in 2009, we could do a full cyber search process and write a report in 2.5 hours, and we did almost all of it with just Google search results. This is no longer the case. Information is hidden more deeply (in the Deep Web), privacy settings are complex, and all leading social networking websites need to be searched individually. The depth of content has also increased significantly. Back in 2009, we were looking at up to 4 years of content; nowadays, we are looking at up to 14 years of content, and that's if the privacy settings on the account let us see it. When we find it, it takes time to look at it and time to capture it.
- 5. Review All Historical Content: I find that some cyber investigators will only look back to the date of loss or to the date of the motor vehicle date, usually because of organizational policy and guidelines. I believe this to be a serious mistake. I have found back-trails to current information many times by going back in time to view an individual's old activity, often identifying their sports, hobbies, interests, old friends, family members, telephone numbers, and former residences. All of this information helps to confirm identity on current accounts that have been 'privatized', and gives us ideas of which new websites to search or new key words to use.
- 6. <u>Analyze Every Image:</u> Again, this is an area I believe many cyber investigators do not exploit as well as they should. Any image you find related to the plaintiff should be checked for potential new information, including image content, accompanying text, or metadata. Many images can be located more accurately using 3D Google Maps or compared if the location they are at is the same as the address they provided. There are also geolocation tools that will aggregate social media data for a user or particular location. In one case earlier this year, I was able prove a specific person was operating an account and what their activity was because of the unique patterns on the shoes the person was wearing. Also, if you have checked all the historical photos, you will also be able to assess if the person is a 'true poster' (someone who posted unaltered images they have taken themselves and posted in a timely manner) and the content can be treated as facts; or they may be a 'necroposter' or 'third-party' poster (someone who posts older images or images from other people's accounts) whose image content and posting dates should be checked and verified before being treated as facts. This also includes watching the videos that we find; videos posted after the DOL (date of loss) can contain very useful information.
- 7. <u>Don't Stop The Search Process After Locating the First Account:</u> More frequently than I would like, I find that some cyber investigators will find that

the search process after finding that first account as far too many times I have found a second account; and then a third account; and then a group page, etc. In a file I completed just two weeks ago, the person had over 15 social networking accounts, six of them on Facebook alone. Check every possible match you find as every account you find increases your chances of finding new information.

- 8. <u>Cross-Reference Your Information:</u> When a person you are investigating has multiple accounts, they often don't use them all at the same time. They may use one all the time, then move on to the next one as preferences change and new websites evolve. Producing a chronological timeline of social account use can help identify what may be an undated image of interest from one account when placed beside a text comment about a specific location posted at the same time on another account. This can also help identify patterns of activity, or get an idea of how frequently a person is engaged in a specific activity. It can also be a very powerful tool in showing how frequently a person is online, and when the numbers are taken together, can indicate a much higher online presence than looking at single accounts by themselves.
- **9.** <u>Check Any Domain Names:</u> Any indication of a private website should be checked using 'whois' and domain registration search tools. This not only provides the opportunity for confirming addresses and telephone numbers, but can indicate what type of employment or business opportunity the claimant may be involved in. Make sure you search the domain using the Wayback Machine to confirm when the website was operational and if there are saved copies of old webpages (for websites that the claimant may have deleted).
- 10. <u>Check Their COA (Circle of Acquaintances)</u>: The first thing that a claimant usually does after getting a lawyer after an accident (if they haven't done it already nowadays) is that they 'privatize' their accounts. For many claimants, this means doing what they are legally allowed to do, which is change their privacy settings so people like us cant see their account content anymore. Others take a more drastic approach, some going so far as deleting all their content, but usually they limit themselves to changing their account names so that it breaks the link with Google search results. But they can't make their friends, family, and acquaintances do the same thing; and sometimes they don't want friends, family, and acquaintances to know why they want to either. This is the key to finding many of the accounts of claimants and information about the claimants; the acquaintances will usually lead to the account, and often to new information.

In closing, I would like everyone reading this to remember an important point: not every case is fraud. In many cases, we see unusual behaviour, high demands for

harder, but it's not suspicious to keep your content private, and in the end, the demand for privacy also benefits us and our families. Let the facts we find support the theory, rather than forcing the facts we find to fit theory.

Toddington International will be announcing 2019 dates for our brand new "Investigating Insurance Fraud Online" training series in the next issue of this newsletter. Contact us if you would like to be placed on our waitlist to receive more information.



Serving as Head of Investigations at TII, Norman Wilhelm is a licensed private investigator with over 20 years of experience in open source intelligence and online investigations.

He is a highly decorated and accomplished former member of Canadian military intelligence, who later worked in the human resource management industry and then at one of Canada's largest private investigation companies, specializing in online investigations and research. The majority of his work over the past

nine years has supported workplace investigations, threat assessments, insurance fraud, class action suits, and family law. In November 2013, he was recognized by the Supreme Court of British Columbia as an expert in open source intelligence and online investigations.

His current work at Toddington International includes research on internet resources, curriculum development and instruction on the topic of online investigations, delivering courses to investigators working at private companies, corporate security units, regulatory agencies, provincial government departments and federal agencies.

Upcoming Select Worldwide Training Dates



North America

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

Early-bird pricing available for a limited time only

October 3-5, 2018, Vancouver, BC (Registration closes soon)

November 5-7, 2018, Toronto, ON

"Cyberpsychology and Threat Intelligence: Assessing Risk Online" (2-Day Course)

Early-bird pricing available for a limited time only

With Forensic Psychiatrist
Dr. Cynthia Baxter MD FRCPC DABPN

November 29-30, 2018, Vancouver, BC

A ground-breaking program that will provide the skills to collect and analyze social media content in order to assess the threat and risk of violent behaviour in a wide range of scenarios.

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

October 22-23, 2018, Singapore

Contact us for more information.

"Cyberpsychology and Threat Intelligence: Assessing Risk Online" (2-Day Course)

November 19-20, 2018, Hong Kong

November 22-23, 2018, Singapore

Contact us for more information.

Oceania

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

November 5-6, 2018, New Zealand

November 8-9, 2018, Australia

Contact us for more information.

Africa

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

October 25-26, 2018, South Africa

Contact us for more information.

"Advanced Internet Intelligence & Online Investigations" (5-Day Course)

December 9-13, 2018, Dubai

Contact us for more information.

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 – we also have available a number of expert speakers available.

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

Resources for the OSINT Professional



whopostedwhat.com - A promising new Facebook search tool (in beta)

<u>blokada.org</u> - Android app for blocking ads, trackers, and malware that works beyond the browser across all apps on the device

<u>geocreepy.com</u> - Geolocation intelligence tool that gathers information from social networking programs using location data

<u>wireguard.com</u> - Free and open source VPN which aims to be simpler to set up and maintain than current VPNs, while offering a higher degree of security

<u>sarimhaq.github.io/block-facebook-website</u> - Chrome extension to block Facebook-related websites

archive.org - "Wayback Machine" for searching the Internet Archive

wire.com - Secure, encrypted app for messaging and file sharing

Subscribe Past Issues Transla

worldingo.com/en/products_services/worldingo_translator.ntmi - riee online translation

<u>ghostery.com</u> - Ghostery browser extension provides tracking protection and control over ads

<u>telegram.org</u> - Private messaging alternative to WhatsApp, with end-to-end encryption

adblockplus.org - Extension for blocking ads, compatible with multiple platforms

archive.is - Search engine for archived webpages

<u>lumendatabase.org</u> - Searchable database of all legal complaint notices and requests for content removal

<u>selfcontrolapp.com</u> – macOS application that allows you to block access to specific websites

corporationwiki.com - Wiki designed for corporation searches

<u>adamlynch.com/askblocker</u> - Browser extension that blocks notifications and location-sharing requests

<u>zetoc.jisc.ac.uk</u> - Comprehensive database of research publications, with alert and RSS options

<u>wickr.com</u> - Secure Android collaboration platform and messaging app used by journalists and others to keep information private

<u>addons.mozilla.org/en-US/firefox/addon/resurrect-pages/?src=featured</u> - App that lets users visit unavailable webpages or broken links

<u>rootabout.com</u> - Search-by-image (reverse image search) tool, searchable by file or URL

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

"Using the Internet as an Investigative Research Tool™"



Back-to-School Sale



Take Your Online Investigation and Intelligence Skills to New Levels for a Time-Limited Special Price of \$399

The most comprehensive and up-to-date internet research and investigation e-learning program available anywhere, <u>Using the Internet as an Investigative</u>

<u>Research Tool™</u> 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 and group discounts and licensing options are available for five or more registrants. Visit the <u>course page</u> to find out more and instantly register, or <u>contact us</u> directly with any questions.

ubscribe Past Issues Tra

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

Open Source Intelligence for Financial Investigators (Newly Updated)

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.

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

Subscribe Past Issues

and to understand criminal intemgence analysis products when encountered. 31911

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.

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

"Why Is Your Location Data No Longer Private?"

"You know that silly fear about Alexa recording everything and leaking it online? It just happened"

<u>The evolution of the "Deep Fake" - Are we are another step closer to wondering</u> whether we can really believe anything we hear and see?

<u>Time to leave WhatsApp? "WhatsApp Co-Founder Leaving Facebook Amid User</u>
<u>Data Disputes"</u>

"Franken-algorithms: the deadly consequences of unpredictable code"

"How social media took us from Tahrir Square to Donald Trump"

AP investigation finds that even with "location history" paused, some Google apps on both iOS and Android still automatically store time-stamped location data without asking

"Americans are now spending 11 hours each day consuming media"

The UK faces a "democratic crisis" due to the spread of "pernicious views" and the manipulation of personal data, a parliamentary committee is set to warn

"Instagram's New Security Tools are a Welcome Step, But Not Enough"

"What's the biggest influence on the way we think? (Googling it won't help)"

Terms and Conditions: A recent analysis of 757 apps found that nearly 60% of them collected more information than stated in their privacy policies

"Apple to close iPhone security loophole police use to crack devices"

"Haunted by a mugshot: how predatory websites exploit the shame of arrest. Sites are collecting people's mugshots, then charging huge sums to remove them.

Should Google be doing more to stop it?"

Apple iOS feature "Significant Locations" tracks your physical movements and stores your "favourite locations"

"How to Download Your Data With All the Fancy New GDPR Tools"

follow on Twitter | friend on Facebook | forward to a friend

Copyright © 2018 Toddington International Inc., All rights reserved.

unsubscribe from this list | update subscription preferences

Drag to outliner or Upload Close