"The success of every one of our customers is our priority and we work diligently to produce and maintain the very best training materials in a format that is effective, enjoyable, interesting and easily understood."

Julie Clegg, President
Toddington International Inc.

TII Logo

Toddington International Inc.

Online Open Source Intelligence Newsletter

NOVEMBER 2013 EDITION

IN THIS EDITION:

WELCOME TO THE NOVEMBER EDITION OF THE TII ONLINE RESEARCH AND INTELLIGENCE NEWSLETTER

This month we are pleased to bring you articles by guest authors Allan Rush and Mike Ryan as well as our regular listings of Research Resources and articles of interest to the Open Source Intelligence professional.

The last 6 weeks have been busy with open and bespoke courses being delivered to private and public sector clients in North America, Europe and Asia. We've been seeing an increase in enrollment on our Using the Internet as an Investigative Research Tool™ and the Introduction to Intelligence Analysis e-Learning programs, and interest in our new courses relating to Financial Crime, Online Security and OSINT Project Management has been high, with clients now booking in-house training courses in these subject areas.

We're pleased to be speaking at a number of conferences this next few weeks including the 7th Annual HTCIA Asia Pacific Training Conference running December 2nd - 4th in Hong Kong and the Breaking the Silence: A Violence Against Women Prevention and Response Symposium hosted by the Ending Violence Association of British Columbia, November 27th - 29th in Richmond, BC.

We are proud to be participating in the creation of **OSIRA** (the Open Source Intelligence and Research Association), a professional body mandated to recognize and support standards for Online Intelligence and Research practitioners. The Inaugural OSIRA Conference will be held May 7 – 8, 2014 in London, UK at the Royal United Services Institute, with qualified delegates attending on an invitation only basis. Sponsors interested in reaching influencers in the information collection and analysis marketplace are currently being

accepted. Visit the OSIRA website for more information and to request email updates on upcoming events.

We encourage our public sector clients to reserve dates now for training courses to be booked before the end of the Fiscal Year. Please feel free to contact us anytime for information on upcoming training programs, bespoke course outlines and booking information.

Just a few of the delegates at our recent International Chamber of Commerce Commercial Crime Services 3-day Internet Intelligence Workshop held at Cambridge University. The fourteenth time this course has been run over the past decade, this particular even saw public and private sector attendees arrive at Queens' College from Continental Europe, Scandinavia, the Middle East, Africa and Oceania. The next ICC course runs April 6th - 9th, 2014. An electronic brochure is available for download at the ICC-CCS website under "Training". You can also contact the ICC London office directly by email or by calling +44 20 7423 6960 (+0 hours GMT).

Upcoming Canadian Training Dates (Vancouver and Toronto)

We are pleased to be presenting our Advanced 3-Day Internet Intelligence Training Workshops in **Vancouver, January 13th - 15th, 2014** and in **Toronto, January 20th - 22nd, 2014**

With a diverse group of delegates already signed up, these conferences will again be great networking opportunities in addition to providing attendees with highly valuable skills. Registration fees include a one year subscription to the TII Premium Resource Knowledge Base and a one year membership with the Open Source Intelligence and Research Association (OSIRA)

For more information, to download a brochure and reserve your place, visit our website.

Upcoming Australian Training Dates (Sydney)

Returning to Australia **Feb 4th - 5th, 2014**, Toddington International will be delivering two separate courses in Sydney.

Led by TII President Julie Clegg, our new Advanced Internet Intelligence Project Management workshop will provide attendees a solid understanding of the principles and processes required to produce timely, actionable and relevant online open source intelligence products for all sectors, levels of authority, and operational requirements.

In a separate training track, TII Senior Associate Mike Ryan will be delivering our comprehensive Advanced Financial Crime Investigations program.

Again, registration fees include a one year subscription to the TII Premium Resource Knowledge Base and a one year membership with the Open Source Intelligence and Research Association (OSIRA).

For more information, please visit the Innoxcell website, email or call +852 3978 9999 (+8 hours GMT).

Avon and Somerset Constabulary

UK Police Training: Avon and Somerset Police 5-Day Internet Intelligence and Investigation ("3I") Training Programme

January 13th - 17th, 2014

Social Media and Internet technologies are playing an increasingly critical role in proactive and reactive police operations at all levels. In recognition of this, Avon and Somerset Police and Toddington International have joined forces to form a training partnership that will provide essential online operational skills to frontline police investigators across the United Kingdom.

At their purpose built computer classrooms near Bristol, the Avon and Somerset Police Investigative and ICT Training Unit will facilitate this highly acclaimed and comprehensive 5-day internet intelligence and investigations training programme.

Utilizing a dynamic and continually updated curriculum, combined with real-world case studies and challenging exercises, the course is open to all police and related personnel and runs regularly throughout the year. Hundreds of officers and police staff have already successfully completed this course over the past decade.

A course brochure is available on the Avon and Somerset Police website - For more information and to book your place on the course contact us.

Congratulations to our Latest eLearning Graduates!

Congratulations to those who have completed the "Using the Internet as an Investigative Research Tool" e-Learning program this month including: Julie Brady - Jersey Financial Services Commission, Diane Melo - RBC, Maria Correia - RBC, Serene Leung - RBC, Selina Amin - RBC, Andres Betancourt - RBC , Geoff Soguel - RBC, Samantha Hollamby, Steve Watson - Zurich Insurance.

TOR TAILS: ONLINE ANONYMITY AND SECURITY TAKEN TO THE NEXT LEVEL

By David Toddington, CEO, Toddington International

The Internet connection at our home had been running slowly for some weeks and after a final round of basic analysis of our WiFi network, it was time to contact my ISP's technical support department to get to the root of the problem. After an acceptable hold time and a quick chat with a

patient but somewhat bored sounding tech support representative, I was requested to visit a specific web site to check my upload and download speeds.

Feeling I knew a better site for the job than the one he suggested, I deviated and instead pointed my browser to a different speed test site. “No, that’s not the site I told you to visit” said the tech support rep only a second or two after I hit my keyboard’s Enter key, “but it’s still a good site, what does it say?”. I told him my connection speeds. “How about this site?” I said to the support rep as I pointed my browser to to www.speedof.me without telling him where I was going. “Oh cool” came the reply, “I’ve never seen that site before. I think I’ll start using it”.

And with that, I was reminded that certainly at my Internet Service Provider, even the lowliest front line support person could look at my Internet connection and see exactly what web sites I was visiting in real time.

Are You Being Watched?

In terms of network surveillance, my contact with the technical support representative at my ISP demonstrated just how easy it could be for even a low level network administrator to track the online movements of any users under their control. For those of us who care about privacy however, this issue goes far beyond the trust we give to the administrators who maintain the networks we use to connect to the Internet: keep in mind when using an insecure wireless network (such as those free connections available at coffee shops and in hotel lobbies) that there are a variety of freely available network protocol analysis tools available that if configured correctly, could enable anyone in the immediate area to be inspecting your WiFi traffic, and possibly seeing exactly what you are doing online.

Beyond the risk of having passwords and other forms of confidential information intercepted, search keywords, the specific websites you visit and the frequency of your visits could allow an adversary to build a detailed profile on your work and personal life that could be exploited in any number of ways.

Anonymity, Censorship Avoidance and “Snoop Proofing”

Originally developed by the US Naval Research Laboratory, TOR (“The Onion Router”) is a distributed, anonymous and decentralized network of thousands of proxy servers designed to obfuscate the pathways you use on the Internet. Creating private network pathways by building chains of encrypted TCP connections on volunteer run Tor proxy servers (or “relays”), Tor gives users the ability to progressively erase their online footprints as they make their way to and from their various online destinations.

As an essential part of every online investigative and research “tool kit” we recommend the Tor Browser Bundle to help maintain operational integrity and defend against network surveillance, censorship and the disclosure of a user’s online details including location and Internet connection information.

Tor is not infallible however. There are a number of highly sophisticated attacks that have been demonstrated that could possibly be employed by a very determined and well provisioned adversary under very specific circumstances.

While the Tor Browser bundle by itself may provide an adequate level of security for most situations,

there are times when operating in a high threat environment, it may be necessary to go further to preserve operational integrity.

Enter "Tor Tails"

When using a computer system it is important to consider the variety of digital "artifacts" that are continually created on that system during its use. When recovered and examined, these artifacts could provide information about a number of details including the times a computer was in use, email content, information about web sites visited, keywords used in search engines, social contacts, documents created and/or edited and much more.

Operatives in high threat environments should be aware that the same techniques applied by law enforcement personnel to recover digital evidence from a computer or device for evidential purposes can also be used by an adversary to recover the sensitive and confidential information they are responsible for protecting, from the devices they are using.

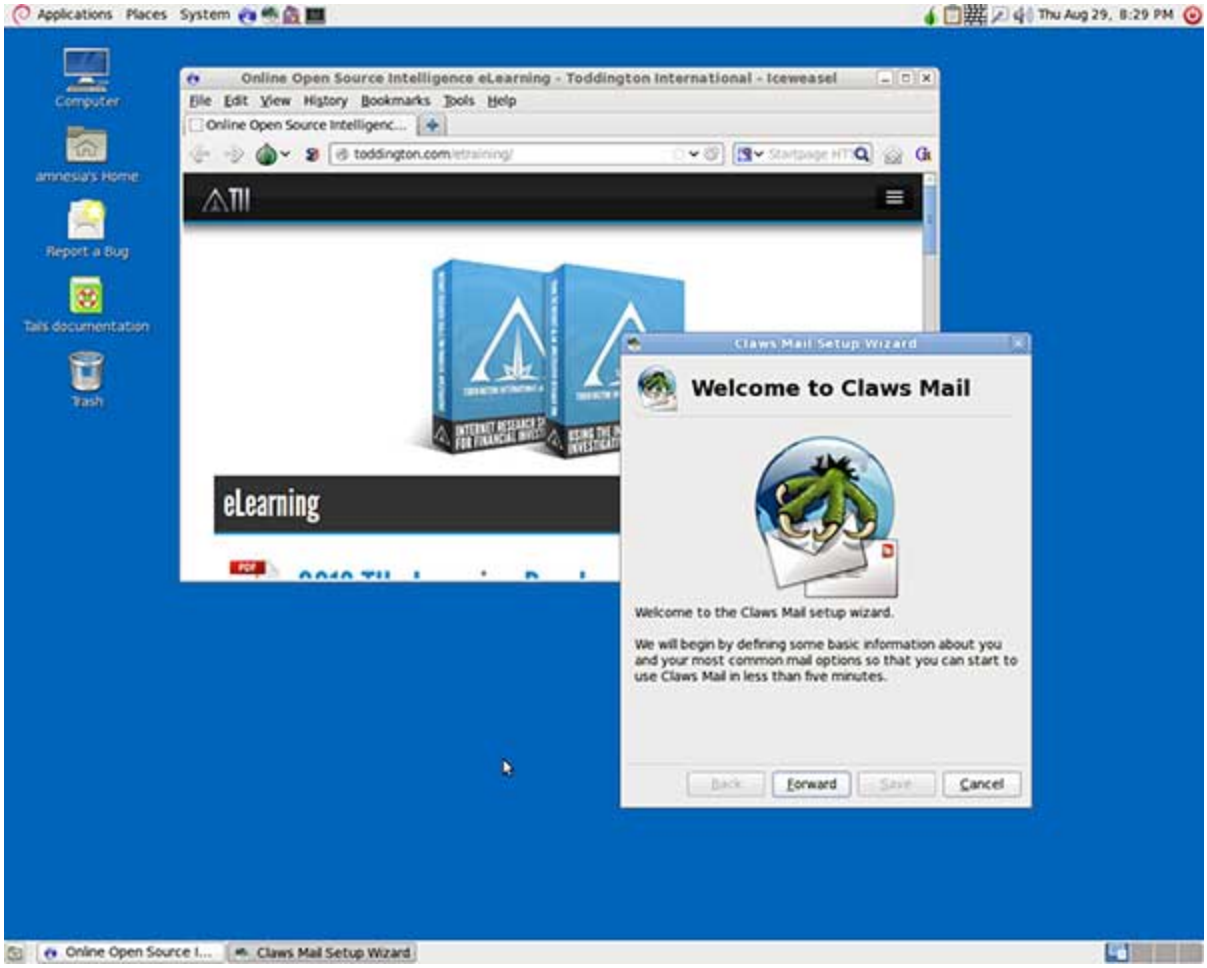
Securing yourself online in a hostile environment requires more than just a tool to obfuscate your online usage, it also requires a tool that will enable you to keep tell-tale information off the device you are using to access the Internet.

"Tor Tails" allows users to take advantage of the Tor Browser Bundle but with the added benefit of leaving no trace of their activities on the computer being used unless explicitly configured to do so. Tails is a complete operating system based on Debian GNU/Linux, designed to be run from a USB stick, SD card or DVD.

Installing Tails

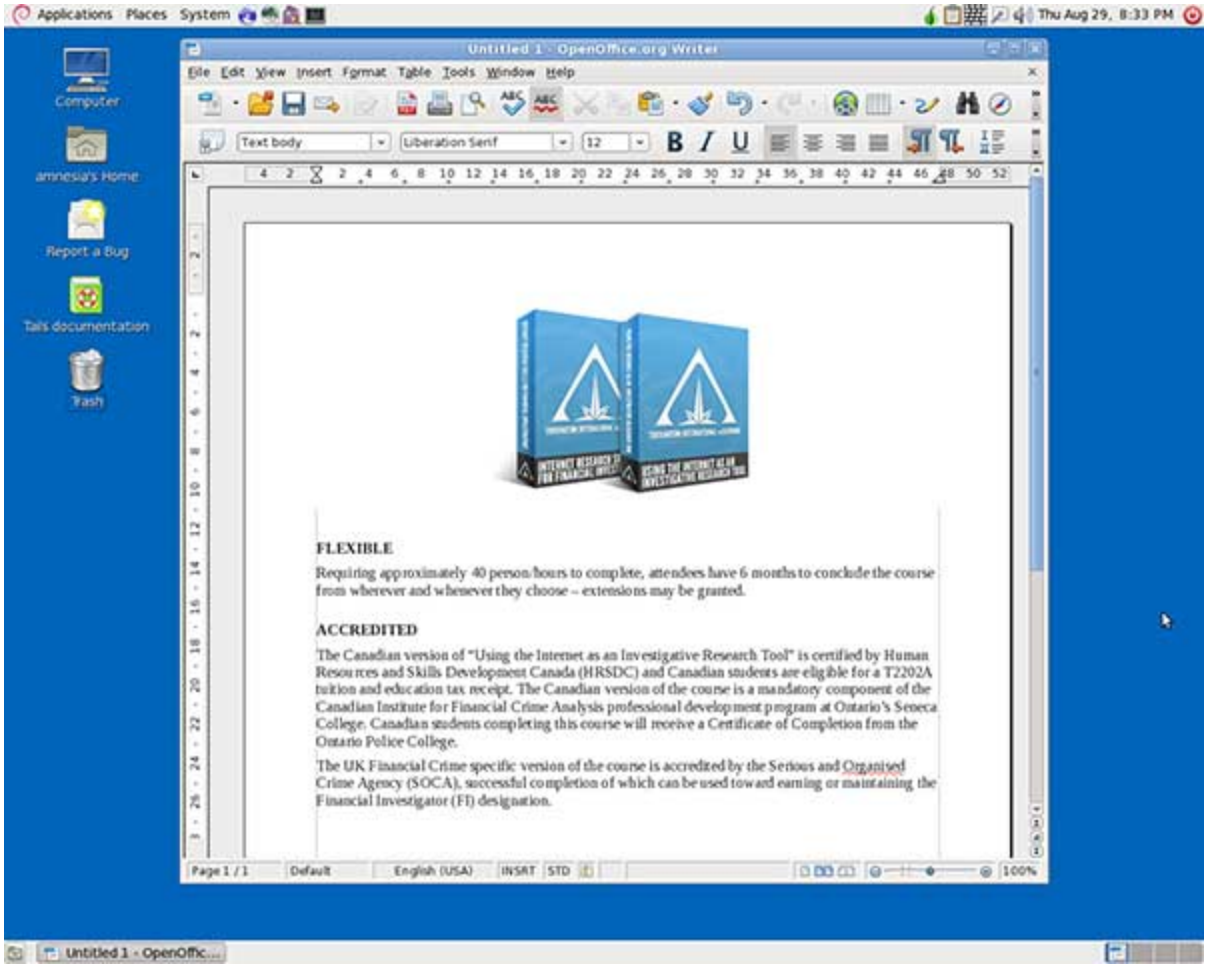
We found downloading Tails to be somewhat slow, so be sure to leave adequate time for this process. Once the Tails file was downloaded we used the Pen Drive Linux universal USB installer to load Tails on to a USB stick. For those who have not installed the Linux Operating System on to a USB stick before, we recommend following the step by step instructions on the Tor Tails site.

With Tails now installed on the USB stick, it was inserted in our shut down Windows laptop. When the machine was powered up the boot menu was selected (F10 on this particular ASUS device) and the stick was selected as the boot device. The Tails "Amnesic Incognito Live System" OS loaded without difficulty and appeared in form and function not unlike an earlier version of Windows. During the entire boot process, the laptops hard drive was not accessed at all and no artifacts were left on it that would indicate the computer had been used in any way while Tails was running.



The Amnesic's GNOME desktop with"Ice Weasel" and "Claws Mail" running in the foreground.

A competent OS, the Amnesic Incognito Live System comes bundled with a number of useful tools including Ice Weasel (a Linux based Firefox browser with Tor Browser patches), Pidgin (an encrypted Off-the Record IM client), Claws Mail client, Liferea feed aggregator, Aircrack-ng (WiFi network analysis tool) and a host of encryption and privacy clients.



The MS Office compatible Open Office Suite is also included with the Tor Tails bundle.

Beyond the obvious Tor Browser and encryption tools, the level of thought around security that has gone into the Amnesic system is demonstrated by the inclusion of a virtual keyboard to circumvent a hardware based keylogger attack on the machine being used. If using a machine that could be susceptible to compromise, a Tor Tails user enter characters using mouse clicks on the on screen's virtual keyboard rather than using the actual physical keyboard.

Users concerned about being observed while using Tails in a public environment can lower their profile by using the "Windows Camouflage" option when booting up the Amnesic Incognito Live System. While not identical to Windows it is a passable representation for to the casual observer.

On all of our training courses we spend varying degrees of time articulating the need for privacy and security, both on a personal and operational level. Discussing case studies in which the monitoring of online activity has caused sometimes irreparable damage to operational integrity, a key recommendation we make is the appropriate use of the Tor Browser in conjunction with the disciplined used of OPSEC protocols.

The Tor Bundle and Tor Tails by themselves will not make a user safer. But used properly, with the bigger security picture in mind, these freely available tools provide a formidable option for keeping users safe in potentially harmful environments.

Tor Tails is free, open source software and is available for download at https://tails.boum.org.

E-LEARNING: "USING THE INTERNET AS AN INVESTIGATIVE RESEARCH TOOL"

The most comprehensive and up-to-date Internet Research 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 a classroom based training course, 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 over six thousand investigators and knowledge workers around the world.

"This information packed course was comprehensive, well-constructed and presented in a format which takes the student through the steps of learning on-line skills at a pace which allows for good understanding of the materials presented. I would highly recommend (and have done) that anybody interested in this area take this course. I was particularly impressed at the balanced and easily understood way in which the various areas were covered. This is a course which someone with a reasonable level of computer skills can take and become proficient in without having to have years of IT expertise, and yet come away with a high level of knowledge of the principles of Online Investigative research. This approach gives the student the confidence to challenge themselves and improve, which is the best recommendation for any kind of course." ~ recent e-Learning attendee

Group discounts and licensing options for private and public sector organizations are available.

For more information and immediate sign up, visit: http://www.toddington.com/etraining

FINDING UNKNOWN FACEBOOK AND TWITTER ACCOUNTS USING KNOWN EMAIL ADDRESSES AND MOBILE PHONE NUMBERS

By Allan Rush, Network Investigator, Dyfed-Powys Police

I expect most investigators have searched for email addresses and mobile numbers within Facebook and Twitter in a hope to find an associated account. But what about the times when it returns a negative result?

Does it mean that there isn't an account linked with the email or mobile number, or that the user has made good use of their security settings to stop them from being traced in this manner?

In this situation I suggest it's time to forget your password… well at least navigate to that section on Facebook or Twitter anyway

If you navigate to the "forgotten your password" section (no need to sign in) of these two social media giants you can enter an email address or mobile phone number here to ascertain if it is linked with a profile.

When entering either a mobile number or email address here https://www.facebook.com/login/identify?ctx=recover on Facebook the result can tell you one of three things:

Nothing - It may return a negative so we assume that the number or email is not linked with any known Facebook profile / account.

Secondly it may return a positive result that includes the profile name (and often the profile picture) along with any other associated details. Additional associated details such as further email addresses or mobile numbers (depending on what was originally searched) will be displayed in partial form such as a*******h@hotmail.com or occasionally a*******h@h******.com or for a number like +**********09 (I'll get back to these in a little while).

Thirdly it may return a result where the profile name is not revealed but instead the email address or mobile number that was searched is repeated under a generic blue profile image. This may also include any other associated details displayed in partial form like +**********09. This is often how a result will be displayed if the email address or mobile number returned a negative result within Facebook itself.

Although this last response doesn't identify an actual account to research, it does at least positively confirm that the email address or mobile number you searched is positively linked with a Facebook profile. It may also provide further investigative opportunities (keep reading) and should ensure any

application to Facebook for subscriber details is going to reveal something worthwhile.

For your peace of mind, searching for email addresses and mobile numbers in the “forgotten your password box” on Facebook and clicking search does not notify the user of the account of your activity (just don’t click “continue” after the result is returned).

Staying with Facebook we can use the "**forgotten your password?"** section even more to our advantage.

How about searching here with the known username of your subject? Entering the vanity name or ID number for the Facebook profile will return a result where the profile is identified (often with the profile picture) along with any associated details (such as email addresses and mobile numbers) partially displayed as mentioned previously.

Back to those partial email addresses like a*******h@hotmail.com, testing has revealed that each asterisk displayed in the email addresses displayed indicates a missing character. This allows us to have a guess at the subjects email address.

Now some are easier than others but they give us a big clue with the beginning and end of the email username and since most people use very traditional formats i.e. allanrush@hotmail.com the address can sometimes be worked out (I have had quite a bit of success with this). Without teaching anyone to suck eggs, consider nicknames used by the subject, dates of birth etc… and bear in mind addresses often containing full stops and underscores.

If you think you might have worked out the email address try entering your concoction back into the “forgot your password” section to see if it returns a result. Clues here that you have the right email address include the result returning the user name you were looking for, or if the profile previously returned additional partial details (obscured with asterisks) then do these match the ones previously displayed?

Now to Twitter; this works slightly differently than Facebook and will only confirm if a mobile number or email address is positively linked to a Twitter account, but that can still be useful intelligence. Navigate to https://twitter.com/account/resend_password

However in the “forgot your password” section on Twitter there is one big difference than with the Facebook method. After entering an email address or mobile number do not press return or click submit! Instead just wait a few seconds after entering your search details and a message will be displayed either saying “looks good” or “email or phone is invalid”; hitting return will send a notification to the account holder!

SUGGESTING A NEW MONEY LAUNDERING MODEL

By Mike Ryan, BBA, LL.B, Senior Associate: Toddington International Inc.

Credit: Images_of_Money via Flickr

The traditional money laundering model (Placement – Layering – Integration) has been the standard method of analysis employed by international bodies, law enforcement, regulators and private sector practitioners. This description of proceeds of crime in motion, viewed as a flow that enters and passes through various forms to exit at a different place to then ostensibly appear as originating from an alternative source, has been the prevailing tool to describe the increasingly complex world of sophisticated profit motivated criminal activity. The major impediment to this traditional model has been that its application is for the most part retrospective, and it therefore offers few predictive indicators.

The traditional model engages only when the subject matter of a transaction is tainted by or is used in conjunction with some criminal or illicit act. Without that predicate association to criminality it is not possible to distinguish the first stage (Placement) from thousands of identical transactions. The model offers little proactive analysis into the subject matter of the transaction itself – the criminal activity that generates the proceeds of crime at the onset. Further, the model does not easily accord with fraudulent criminal activity where the proceeds of those crimes are already on deposit - the Placement stage appears to have been sidestepped. In the ever expanding world of Internet based crime and virtual payment mechanisms such as BitCoin, criminally derived proceeds will become increasingly oblivious to discernable Placement mechanisms. Historically the model has conformed best to cash based criminal activity, and therein lays its greatest weakness - without a mechanism to analyze for the origin of the proceeds of crime, law enforcement and to a greater degree due diligence efforts are limited to monitoring for suspicious deposit typologies, and regulated reporting based on quantity deposit frequency, assembly characteristics, and contaminants.

John Broome, former Chairman of the Australian National Crime Authority, in his book *(Anti-Money Laundering International Practice and Policies, 2005 Thomson Sweet & Maxwell Asia*) proposed an expanded money laundering model to *"…identify in the money laundering process the point at which the criminals are most vulnerable to detection."* Broome buttresses the traditional model with the concepts

of Generation and Consolidation prior to Placement, and follows Integration with a sixth stage described as Realization.

Broome's model broadens the analysis to consider the source of the proceeds of crime and the preparatory conduct which always occurs before the Placement event - not just an analysis of the activities undertaken during the interaction with the financial sector. The Generation stage seeks to identify the criminal source(s) and gives context to the Placement efforts by examining for indicators of the predicate criminal activity. Historical and current criminal activity indicators provide the opportunity to examine for the Generation of proceeds of crime.

The Consolidation stage recognizes the assembly process that has application to both cash and non-cash based financial crime environments, and it addresses the preparatory efforts required to enter the Placement stage. During the Consolidation stage there will be indicators of association with persons or entities that form nominee relationships - so necessary for the successful completion of a money laundering event. Criminally derived wealth coleuses at points of compromise where there is expertise and opportunity to enter the traditional money laundering cycle, and that cohesion is an event itself. Consolidation includes the formulation and perfection of nominee relationships that separate possessory and beneficial interest, and stymie efforts to truly "know your client". Combined, Generation and Consolidation serve to pull the analysis back to engage predictive indicators that are preparatory to Placement. The analysis now has a structure upon which to evaluate for vulnerability prior to Placement.

Following the traditional third stage of Integration, Realization recognizes the reconnection of the criminal with the laundered proceeds of crime on the basis of an expanding level of wealth. Realization presents a vulnerability risk based upon the inordinate quantity of that wealth and the timing of its acquisition. Also important is that as a stage, Realization recognizes the movement of laundered proceeds of crime beyond Integration. That allows Integration to be viewed as a process to be examined for similarity or differences across the range of assets that have flowed through the money laundering event.

Expanding the analysis to include these preparatory and terminating stages ensures that a broader range of meaningful inquiries can be made, and the expansion permits the development of predictive indicators that are associated with the predicate and ultimate criminal behavior. Law enforcement efforts in most jurisdictions will require confirmation of the predictive indicators at all six stages, but regulators and private sector practitioners will require fewer indicators to be confirmed depending upon the level of risk their respective industries mandate.

In at least one common-law jurisdiction, Broome's model has been applied and a working list of predictive indicators assembled. This expanded model and its associated predictive indicators operated so effectively that policing resources were more efficiently deployed and prosecution costs minimized. Due diligence requirements that do not carry the criminal burden of proof may find this method useful.

USEFUL SITES AND RESOURCES FOR ONLINE INVESTIGATORS

Click Here to visit TII's Free Internet Research Resources

- http://www.hashtags.org - Website for viewing hashtag analytics and recent hashtag-related tweets
- http://casesensitivesearch.com - Search engine for when you need your search to be case sensitive
- https://talky.io - New service that promises anonymous P2P based video chats and more
- http://us.searchboth.net - Search engine that lets you search for and compare both Google and Yahoo results
- http://fefoo.com - Multi-search utility that allows you to search multiple search engines from its interface
- https://archive.org - Internet Archive's Wayback Machine: Great site for viewing the progression of a website over time (366 billion saved pages)
- http://www.binsearch.info - Usenet search engine with advanced search features
- http://www.taggalaxy.com - Nifty visual image search tool, searchable by tags
- https://millionshort.com - Search engine that removes up to one million of the top results, and locates hidden, less popular results
- http://www.wiinkz.com: Meta search tool with cool interface - Search Google, Yahoo, Bing, Ask, Blekko, DuckDuckGo & Clusty
- http://www.qwant.com - Search engine that aggregates social media, web, and news content in separate result streams
- https://kbhpodhnfxl3clb4.onion.to - Search engine for crawling the deep web via Tor (The Onion Router)
- http://statistics.data.gov.uk - UK government linked data site launches http://goo.gl/4nXn7l
- http://www.entireweb.com - Meta search tool that lets you search trending, or real-time, topics
- http://flumes.com - Real-time social media search tool
- http://www.easybib.com - Free reference and citation generator for creating bibliographies
- http://linktally.com - Find out how many times a URL was shared on Google+, Facebook, LinkedIn, and Twitter
- http://goo.gl/ETLsBt - Worldwide Western Union Agent Locator, searchable by location or agent name
- http://here.com - Mapping interface with city and country maps, driving directions, satellite views and street level feature
- http://www.foia.cia.gov - The CIA's Freedom of Information Act Electronic Reading Room
- http://visualping.io - Website monitoring tool that notifies you of changes on a website
- http://govinfo.library.unt.edu - CyberCemetery: Archive of US government websites that have shut down
- http://www.corpsearch.net/watchlists.html - Corporate Intelligence Project: Watchlist, regulatory, negative media and global sanctions searches
- http://www.verbase.com - New crowdsourced, interactive semantic search engine that claims to be

the only search engine providing ad- and spam-free results (secure version available)
- https://privatelee.com - Search engine, claiming to be private and secure, with useful PowerSearch commands
- http://www.amtrak.com/train-routes - Real-time train tracking map powered by Google
- http://www.citizenaudit.org - Searchable full-text database of nonprofit documents (form 990 search)
- https://metrics.torproject.org/exonerator.html - ExoneraTor: "A website that tells you whether a given IP address was a Tor relay"
- https://www.blippex.org - Blippex: A novel new search engine that draws from an index generated by its users
- http://www.brbpub.com/free-public-records/ - Database providing links to free public record resources
- http://offshoreleaks.icij.org - Searchable database of company ownership information in 10 offshore jurisdictions
- https://www.vinelink.com/vinelink/initMap.do - Directory of incarcerated offender databases
- http://www.trendpaper.com - Aggregating trending Facebook news into a customizable news feed
- http://www.blogsearchengine.org - Search engine for blogs
- https://defcad.com - "DEFCAD": Search engine for 3D printable models

... ALSO OF INTEREST

- Paul Szoldra reports: “Burglary Suspects Get Arrested After Police Spot Their Photo On Instagram” http://goo.gl/boNn05
- Useful tips on “How to Opt Out of Data Tracking on Your Most-Used Sites” http://goo.gl/bdfQ7C
- "What Your Search History Says About You (And How to Shut It Up)” http://goo.gl/ibGp55
- What are Web Archives? - “Anatomy of a Web Archive” http://goo.gl/ax5F8s
- A guide for new Google Maps features http://goo.gl/ZjuAWk
- "5 Ways To Unlock The Benefits Of Semantic Search" http://goo.gl/N5aL7d
- Instagram becoming a marketplace for drugs with the help of hashtags http://goo.gl/UM2rPT
- Using the Tor network, “MafiaLeaks” puts tipsters in touch with anti-mafia journalists http://goo.gl/9FDk3T
- "The Role of #Hashtags in Social Media and Search" http://goo.gl/xGn2ai
- Big Data: A hacker hideout? http://goo.gl/i2c8XC
- Check if your Adobe account was one of the 150 million compromised in last month's hack http://goo.gl/TBy5JP
- "Facebook Hasn't Even Begun To Exploit Everything It Knows About You" http://goo.gl/WxYrjr
- "Cost-Effective Searching: Online strategies & practices to get the most for your search dollar and your time" by Marcy Phelps http://goo.gl/2MsDfn
- Canada: Police need judge’s specific permission to search computers, Supreme Court rules http://goo.gl/xeX4pZ
- Resurrected Black Market For The Dark Web as ‘Silk Road 2.0’ Relaunches http://goo.gl/xJ4Coh
- Comprehensive, unofficial Tor user's guide with necessary explanations, how-tos, and other useful tips http://goo.gl/jgFAA4
- "Meet Darknet, the hidden, anonymous underbelly of the searchable Web" http://goo.gl/b4jRPI
- Avoid being a victim of social media scams with these 11 tips http://goo.gl/NYJiZJ
- In a new partnership, Bing gets access to public content created by Twitter users http://goo.gl/I0RT1p
- Facebook rolling out Graph Search in UK http://goo.gl/3tWNQ0
- Virtual' Filipina girl identifies 1,000 webcam sex tourists http://goo.gl/WZaUdD
- Face recognition scanning being used by retailers to deliver personalized “Minority Report” style ads

http://goo.gl/e3g1kv

- "Where to Find and Access Big Data" http://goo.gl/drlqgw
- Good question - Could Bing ever become Google? http://goo.gl/DN6FvM
- "A Global Social Media Census" of the world's largest 24 social media sites http://goo.gl/yfHAAe
- Is the demise of net neutrality inevitable? http://goo.gl/6mXWqk
- Five Technology Trends to Watch http://goo.gl/MQnuem
- Secure email might be on the verge of a radical makeover if the “Dark Mail Alliance” has its way http://goo.gl/s3sNov
- Online tracking may be taken to new level as “Facebook Tests Software to Track Your Cursor on Screen” http://goo.gl/hwjuBB
- Mozilla launches geolocation lookup pilot project “Mozilla Location Service” http://goo.gl/02UsxX
- BlueLine: A social network for law enforcement agencies http://goo.gl/rK3zFs
- Overlooking smartphone security? - “Don’t Be Silly. Lock Down and Encrypt Your Smartphone” http://goo.gl/oFbKru
- 7 Very useful Google search operators http://goo.gl/yhXyqX
- "Super Searcher Secrets" (.PDF) by Mary Ellen Bates http://goo.gl/8Z0JwA
- See how third party sites are monitoring your web activity using Firefox's Lightbeam http://goo.gl/rXWGhB
- Instagram - An unregulated gun market? http://goo.gl/Qdu5G7
- Google launches Universal Analytics, and here's how you can upgrade http://goo.gl/bw3LNe
- Protecting your privacy with Facebook Graph Search http://goo.gl/Zxo9H7
- New map from Google and Arbor Networks lets you monitor global DDoS attacks in real-time http://goo.gl/lxYVZi
- AIS security vulnerability: “Ship Tracking Hack Makes Tankers Vanish from View” http://goo.gl/uiZ7Sb
- "Big Data FAQ: Separating Signal From Noise" http://goo.gl/6L8Z9U
- Clive Thompson reports: “The Darkest Place on the Internet Isn't Just for Criminals” http://goo.gl/vUF7rQ
- Interesting results - “The Secrets Online Searchers Keep [Study]” http://goo.gl/UqnbsS
- Google launches “Google Media Tools” for reporters and journalists http://goo.gl/J84GmB
- "9 Ways to Maintain (Some) Privacy on Social Media and the Web" http://goo.gl/rgqkYm
- Data analysis - “Finding the hidden patterns in big data” http://goo.gl/tRzXgV
- "Think you can live offline without being tracked? Here's what it takes" http://goo.gl/E7X51k
- "How To Tell If Others Can See Your Private Photos And Posts On Facebook" http://goo.gl/gl4eoJ
- "Big Data Opportunities [INFOGRAPHIC]" http://goo.gl/yQnrZB
- A beginners guide on how to use Twitter Analytics http://goo.gl/SuPYK9
- Time to rethink your privacy protocols? Study finds 145 of top 10,000 websites use “fingerprinting” to track users http://goo.gl/eGYZnF
- Five website monitoring tools that track and monitor changes on websites http://goo.gl/B8mk89
- What do your Tweets say about you? IBM researcher claims she can evaluate personality traits via tweets http://goo.gl/UIsPg4
- A self diagnosis cautionary tale: “Is the internet making you (think you're) ill? You're a cyberchondriac" http://goo.gl/LSfTor
- Guerrilla Marketing: Using OSINT for Target Identification http://goo.gl/HfN7m
- "What Big Data Knows About Us" http://goo.gl/frDPX6
- "How to See Which Browser Extensions Are Slowing Down Your Browser" http://goo.gl/sENcUo
- Tip of the day - Access blocked sites via Google Translate http://goo.gl/jSti1X
- The evolution of search and what the future holds http://goo.gl/Zg8irt

- How much does your search engine know about you? http://whyprivatesearch.com
- "Disconnect Search, Built By Ex-Google And Ex-NSA Engineers, Lets You Use Google, Bing And Yahoo Without Tracking" http://goo.gl/ID8ayo
- Educational analytics system could provide essential insight to teachers but privacy issues for students http://goo.gl/vMLe47
- Hyper-targeting consumers: “Selling Secrets of Phone Users to Advertisers” http://goo.gl/aNP2Ch
- On Tor & OPSEC: “The great machines can keep enemies at bay, as long as the gatekeeper remembers to close the door” http://goo.gl/K4vng1
- Interesting analysis of the well-known hacker group: “Anonymous in Context: The Politics and Power behind the Mask” http://goo.gl/Ykg7YB
- Prasant Naidu reports: “Increased Presence of Terrorist Organizations on Social Media: Challenges for Social Networks” http://goo.gl/50N248
- How the FBI took down the Silk Road illicit drugs marketplace http://goo.gl/H5pu03
- "Online Reputation Management (ORM): A Quick Guide" by Chuck Price http://goo.gl/d1DxGm
- Counterfeiting attitudes: 16% of a representative sample of UK consumers said they buy fake medicines http://goo.gl/HNgpCx
- The Faces of Facebook - Mapping all 1.2 billion Facebook users' faces (click anywhere to zoom in) http://goo.gl/fzpFrn
- It's National Cyber Security Awareness Month; check out this selection of resources to help you stay safe online http://www.staysafeonline.org/ncsam/
- Google rolls out hashtag search in the US and Canada http://goo.gl/QD6uN9
- Is your smartphone spying on you? - Logging keystrokes using nothing but the sensors inside an iPhone http://goo.gl/NYXyUT
- Privacy often not important until it's too late: “How your personal information can be turned against you” http://goo.gl/t16cwm
- Running a “sextortionist" to ground: “How the FBI found Miss Teen USA’s webcam spy” http://goo.gl/vbgkFS
- "The power of metadata: Addiction, sex, and accusations can all be discovered" http://goo.gl/DJdfXQ
- No secure options? “Email can’t and shouldn’t be trusted, even if its encrypted and stored off shore” http://goo.gl/gM0ueL
- More than just 3D printed firearms: “The New World Of Digitized Guns” http://goo.gl/RaZWvV
- Using Google Analytics to track Gmail messages http://goo.gl/GXQe5B