

eForensics

Magazine

MAGAZINE

FINANCIAL FORENSICS

ANTI-MONEY LAUNDERING TOOLS AND TECHNIQUES

USING DIGITAL EVIDENCE

TO PROVE THE EXISTENCE OF A COMMON LAW MARRIAGE

CRYPTOCURRENCY IN DIGITAL FORENSIC INVESTIGATIONS

VOL.08 NO.05

ISSUE 05/2019, (90) MAY

ISSN 2300-6986

eForensics Magazine

TEAM

Editor-in-Chief

Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Managing Editor:

Dominika Zdrodowska
dominika.zdrodowska@eforensicsmag.com

Editors:

Marta Sienicka
sienicka.marta@hakin9.com

Marta Strzelec
marta.strzelec@eforensicsmag.com

Bartek Adach
bartek.adach@pentestmag.com

Senior Consultant/Publisher:

Paweł Marciniak

CEO:

Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Marketing Director:

Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

DTP

Dominika Zdrodowska
dominika.zdrodowska@eforensicsmag.com

Cover Design

Hiep Nguyen Duc

Publisher

Hakin9 Media Sp. z o.o.

02-676 Warszawa

ul. Postępu 17D

Phone: 1 917 338 3631

www.eforensicsmag.com

All trademarks, trade names, or logos mentioned or used are the property of their respective owners.

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the

word from the team

Dear Readers,

Money drives the world, doesn't it? In cybersecurity and cyber forensics fields there is a lot of discussion on fintech. Because of that, we decided to dedicate this month's publication to Financial Forensics.

In this publication you can read about anti-money laundering tools and techniques, forensic investigations and financial audits, forensic technologies to mitigate risks of financial crime and cryptocurrency in digital forensic investigations.

In addition to that we recommend you check out the articles "Using Digital Evidence to Prove the Existence of a Canadian Common Law Marriage" by Tyler Hatch, "Digital Forensic Integrity: Mental Health" by Rachael Medhurst & Emma Derbi, "Digital Forensics and Threat Hunting" by Gerard Johansen, and "Beacon - Dark Web Discovery for Data Breaches" from Echosec. Also, for beginners in the area of cyber forensics we have a wonderful introductory guide, written by Sudharshan Kumar.

Thanks to all authors, reviewers and proofreaders for participating in this project.

Have a nice read!

Regards,

Dominika Zdrowska

and the eForensics Magazine Editorial Team

05

AML TOOLS & TECHNIQUES

by Johan Scholtz

23

CRYPTOCURRENCY IN DIGITAL FORENSIC INVESTIGATIONS

by Chris Chiang

37

DIGITAL FORENSIC INTEGRITY: MENTAL HEALTH

by Rachael Medhurst & Emma Derbi

46

PROVING THE EXISTENCE OF A COMMON LAW MARRIAGE

by Tyler Hatch

55

DIGITAL FORENSICS AND THREAT HUNTING

by Gerard Johansen

67

FORENSIC TECHNOLOGIES TO MITIGATE RISKS OF FINANCIAL CRIME

by Florence Love Nkosi

75

BEACON - DARK WEB DISCOVERY FOR DATA BREACHES

from Echosec

82

FORENSIC INVESTIGATIONS AND FINANCIAL AUDITS

by Ranjitha R

87

CYBER FORENSICS FOR A BEGINNER

by Sudharshan Kumar

95

TRACE LABS - FINDING MISSING PERSONS THROUGH OSINT

Interview with Josh Richards

Anti-Money Laundering tools and techniques

by Johan Scholtz

Money laundering is a common term understood in layman's term as something that has to do with money washing or methods to conceal where the money came from by ensuring it changes hands so often and fast it is difficult to keep track of where it is going or coming from. The rise of online banking institutions, anonymous online payment services and peer-to-peer (P2P) transfers with mobile phones have made detecting the illegal transfer of money even more difficult. Moreover, the use of proxy servers and anonymizing software makes the third component of money laundering, integration, almost impossible to detect—money can be transferred or withdrawn leaving little or no trace of an IP address.

What is Money Laundering?

Money laundering is the process of making large amounts of money generated by criminal activity, such as drug trafficking or terrorist funding, appear to have come from a legitimate source. The money from criminal activity is considered dirty, and the process "launders" it to make it look clean. Money laundering is itself a crime. Key terms are also objective to conceal true ownership and origin of the proceeds, a respite to take control or a need to change the form of the proceeds.

One first has to understand why money laundering takes place – or rather why would anyone start doing this? Clearly, the motive behind money laundering hides behind the so-called washing of money,

and again, there are other factors or reasons driving this. Money washing or money laundering is a well-planned method to obfuscate or hide other streams of income from authorities. The money laundering culprits do not want to declare their income and do not want to pay taxes on their income.

First, the money in question has to be accepted or changed through some kind of banking system and often this is the most dangerous part for the criminals, as they need to bypass strict government regulations to deposit the money in a bank or financial institution.

People launder money because money can leave a traceable pathway to their fraudulent activity. The cash itself is susceptible to take-over from law enforcement authorities and therefore needs to be protected. In some countries, tax evasion is another main reason.

Figure 1 shows to what extent financial crimes are bypassing controllers at various levels. A concern is that more than 25 % of institutions have not yet implemented a detailed AML/CFT risk assessment to control this crime.

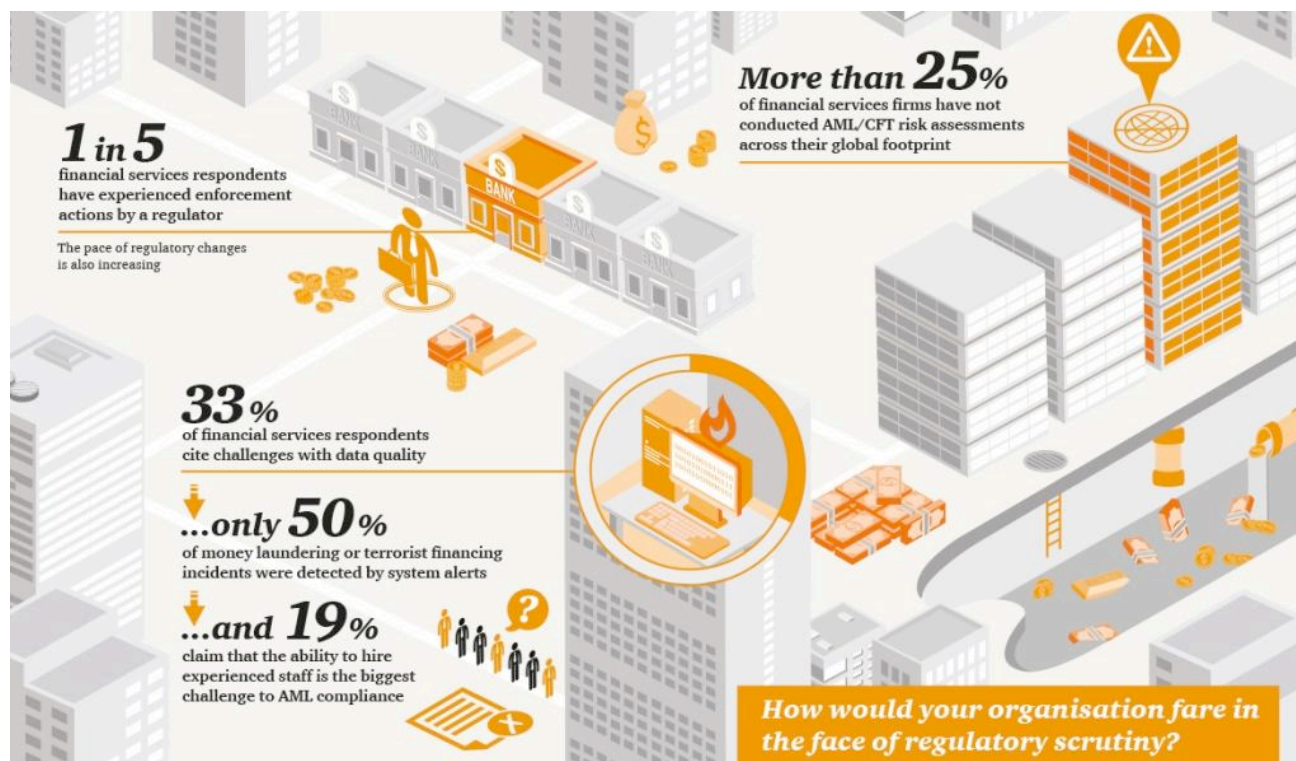


Figure 1. Infographic of Financial Crime. [1]

How Money Laundering Works

Money laundering is essential for criminal organizations that wish to use illegally obtained money effectively. Dealing in large amounts of illegal cash is inefficient and dangerous. Criminals need a way to

deposit the money in legitimate financial institutions, yet they can only do so if it appears to come from legitimate sources.

More precisely, according to the Vienna Convention [2] and the Palermo Convention [3] provisions on money laundering, it may encompass three distinct, alternative acts: (i) the conversion or transfer, knowing that such property is the proceeds of crime (ii) the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime; and (iii) the acquisition, possession or use of property, knowing, at the time of the receipt, that such property is the proceeds of crime. [4]

Price Waterhouse and Cooper (PWC) suggest the following tools to combat anti-money laundering [5]. Note that these are only a few policy compliance tools and does not necessarily identify the culprits. These tools have been developed by financial services, data, technology, risk and regulatory subject matter specialists and have gone through several iterations. They are designed to help customers meet their complex AML compliance challenges.

- Computer Assisted Subject Examination and Investigation Tool (CASEit®): A Web-based tool that facilitates AML compliance, AML transaction monitoring, trade surveillance, operational risk and anti-fraud case management.
- Customer Due Diligence Tool (CDD): Web-based tool that acts as the single data entry point and risk rating for all existing and new customer and account data in support of Know Your Customer (KYC) requirements. Additional customer and account information captured includes ultimate beneficial owners, officers/directors (non-individuals and financial institutions only), power of attorney, co-signers, and other related parties.
- Name/entity matching: Sophisticated matching and scoring tools and techniques that improve the searching of account and transaction information across systems, regions and business lines to create one view of the customer or to improve the name/entity screening (e.g. OFAC, PEP, etc.) and matching processes (e.g. 314a, subpoenas, NSL, ad-hoc searches, etc.)
- Suspicious activity detection tuning: Advanced methods and techniques that improve the efficiency and effectiveness of transaction surveillance technology. By analyzing the population of data,

institutions can identify trends and patterns and better determine which behaviours fall outside an acceptable range. Statistical analysis can be the first step in selecting appropriate rules and thresholds. Equally important is the reassessment of the monitored behaviours and thresholds over time. On-going analysis can be used to determine correlations and trends between productive and non-productive alerts allowing refinements that better target potentially suspicious activity, reducing overall review efforts.

- Know your customer quick reference guide: A user-friendly Web-based guide to anti-money laundering legislation and regulatory requirements for nearly 50 countries.[5]

The Three Stages of Money Laundering

The process of laundering money typically involves three steps: placement, layering, and integration.

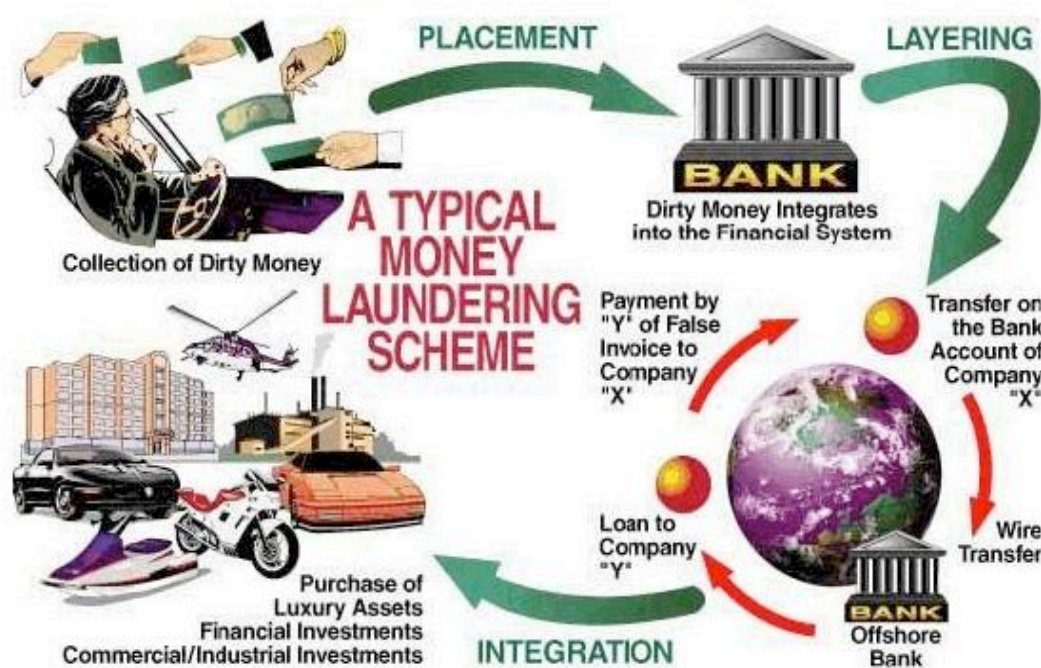


Figure 2. Three Stages of Money Laundering. [6]

During the *Placement* phase, the "dirty money" is placed into the legitimate financial system. This phase is also known for specific financial avoiding techniques, for instance, using the connected account of relatives, associates or shell companies – which do not exist anymore. In addition, several legitimate accounts might be opened in a different bank account and registered as not for profit or charity trusts. Lastly, a person might use techniques called smurfing, where they would deposit a large

amount of illegal manner into several bank accounts but using small amounts to do this. Movement of funds away from its source is the first step in the process. This step is the initial entry of the money or proceeds of a crime into the financial ecosystem. The cash is moved into circulation through banks, casinos, shops and other cash-heavy businesses (e.g. restaurants, night clubs). This stage is also where money launderers are the most exposed since introducing large amounts of cash and a high volume of small transactions (in order to stay under \$10K limits) into the financial system raises red flags.

In the *Layering* phase, the source of the money is concealed through a series of transactions and bookkeeping tricks, for instance, separating the illicit (criminal) origin of the illegal money through a complex web of financial transactions. The main objective of this phase is to make the source of fund and its ownership untraceable, through multiple layering of complex transactions. This is a complex step in any money laundering activities. After introducing the money into the financial system, the fraudster carries out a series of money laundering techniques, one transaction after another, all designed to hide what they are doing. During this step, the laundering organization adds layers, such as moving funds electronically across international borders, reselling assets, investing in overseas stock markets and diverting funds to offshore accounts, shell companies and paying front men. The disguise stage of the process represents the most challenging area of detection. Due to the many layers, it's hard to trace the funds, especially if the money is moved multiple times from one institution to another. Finding all of the individuals involved, and how they are linked and connected, requires lengthy forensic investigations and advanced correlation algorithms. One of the reasons why organized crime syndicates such as drug cartels have continued to flourish is because of their infiltration into hundreds of institutions. They coordinate with so many types of organizations across many countries that eliminating one institution will not hinder their practices.

Lastly, in the *Integration* phase, the now-laundered money is withdrawn from the legitimate account to be used for whatever purposes the criminals have in mind for it, thus giving a legitimate image for illegal money. This is the last stage of the laundering process. During this stage, it is very difficult to find the illicit origin of the money. After using the above methods of laundering, the illegal money is now circulated into the economy by way of investments, purchase of lands, expenditure or savings. [7]

Integration mainly tries to move the money back into the economy in such a way as to make it look like a legitimate business transaction with an audit trail by:

- Buying property – Use shell companies to buy a property where the revenue from the sale would be considered legitimate
- Providing loans – Criminals lend themselves their own laundered proceeds in an apparently legitimate transaction
- Faking invoices – Overstate their income, which comes from over-invoicing to allow inflow of illegally obtained money [8][9]

There are many ways to launder money, from the simple to the very complex. One of the most common techniques is to use a legitimate, cash-based business owned by a criminal organization.

For example, if the organization owns a restaurant, it might inflate the daily cash receipts to funnel illegal cash through the restaurant and into the restaurant's bank account. After that, the funds can be withdrawn as needed. These types of businesses are often referred to as "fronts."

Other money-laundering methods involve investing in commodities such as gems and gold that can easily be moved to other jurisdictions, discreetly investing in and selling valuable assets such as real estate, gambling, counterfeiting, and using shell companies (inactive companies or corporations that essentially exist on paper only). [10]

We note from Figure 3 that a very high percentage of 80%+ of illicit money laundering is through trade-based money laundering (TBML). This figure strengthens the global concern of monitoring and controlling how and where illicit trading still manages to escalate right under the noses of government and bank control.

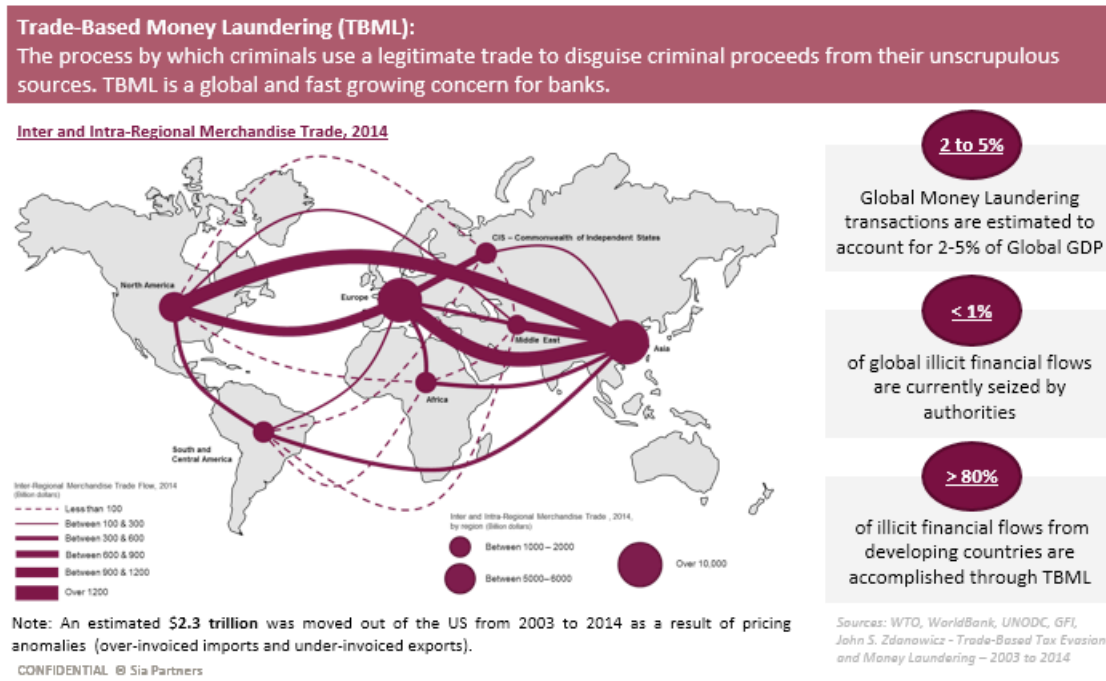


Figure 3. Trade Based Money Laundering – A Growing Concern. [11]

Banks are required to report large cash transactions and other suspicious activities that might be signs of money laundering. However, this is not an easy task, since mathematical equations and algorithms are not yet fool-proof, in detecting culprits.

Questions arise on how to use Artificial Intelligence (AI) or machine learning to detect financial inconsistencies in banks. For instance, the CEO at Danske Bank resigned when a report was published showing gross underestimated acceptance of fraudulent money laundering of around \$234 billion in value. “Danske Bank CEO Resigns on Heels of Report Detailing an Astounding \$234 Billion in Suspicious Transactions in Money Laundering Scandal”. [12]

Perhaps one reason for this situation was simply due to gross neglect when it comes to due diligence – investigating where the money came from and how the funds are redistributed. The misconduct came from non-resident account holders not living in Estonia at the time. Danske Chairman says ‘Large’ Part of \$234 Billion is Suspicious.

“Criminal complaints against Danske have so far suggested its Estonian unit was used to launder as much as \$9.1 billion between 2007 and 2015, with the illicit funds stemming mostly from Russia”. [13]

The Group Audit internal investigation concluded the Estonian branch was not conducting proper customer due diligence and could not possibly monitor the accounts using the current system. The

Group undertook a number of initiatives to address the issues in Estonia, but ultimately these inadequate AML procedures became the subject of harsh criticism by the FSA in Estonia". [14]

Trends and patterns should emerge from big data

The software which potentially may trace and inconsistencies are required for a final trace. Rohit [15], suggests using the extraction of hidden predictive information from large databases to trace illegal money/funds movement. Using a combination of the decision tree, clustering and neuron network approaches, one might succeed in the discovery of erratic fluctuations in a normal transaction.

All investigation methods are trying to detect accounting fraud; this can be done in applying a rule-based approach where essentially a notification is sent to the bank if irregular patterns come to the front after a typical dysfunctional behaviour from a client is detected – an unusual report based on the Bayesian network approach, which assigns a customer behaviour score based on transaction history. [16]

A clustering-based approach would detect any discrepancies that are not part of a set cluster grouping. When a strange pattern is obviously different from a set basic pattern, a warning would prompt activity from the bank. A classification-based approach will detect anomalies inside the data set. However, it would be difficult to investigate money movement as vast amounts of data needs to be classified, since some data sets would have a similar data transaction footprint as others in the account and might be difficult to specify with exactness as false-positives will occur. 34 % of respondents said they thought their organization's use of technology to combat fraud and/or economic crime was producing too many false positives. [17]

This finding reiterates the importance of AI to develop new algorithms and search specific groupings or segmentation as we see in the next section.

Segmentation

One problem with AI in finding patterns in meta-data is the high false positives. A possible guideline is suggested by [18],[19] to improve segmentation processes, even after the normal customer due diligence processes were conducted.

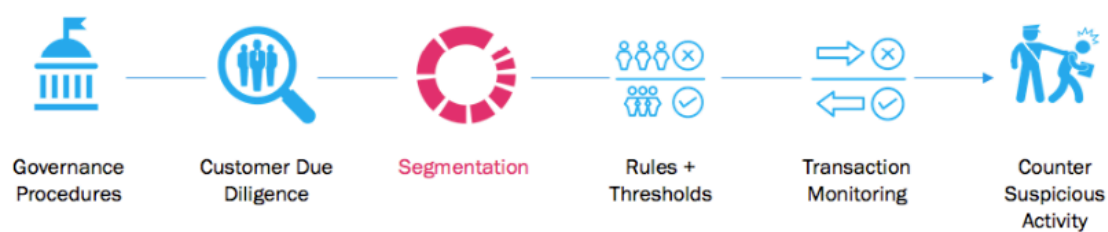


Figure 4. Segmentation.

Although segmentation should set a pattern or at least a platform in guiding selection and identification of possible irregularities, most processes are hampered by the transaction monitoring system (TMS) which is set to the government or independent agency regulations. In other words, if these regulations imposed by TMS are not closely monitored, a high false positive rate again negatively impacts the investigation of suspicious activities.

A select number of financial institutions have moved toward applying machine-learning-driven segmentation. While superior to hand-coded segments, machine-learning-driven segmentation practices struggle with some key challenges:

- The shortcomings of standard clustering methods such as K-means
- Segmenting client and transaction data separately
- Slow segment uptake into real-time transaction monitoring.

K-means is a powerful algorithm, but in this context, it has some shortcomings: scalability is significantly limited, the number of clusters must be defined beforehand and it can be subject to chaining, resulting in highly non-uniform clusters (such as a single cluster). [20]

Intelligent Segmentation

Intelligent segmentation combines unsupervised learning with supervised learners in an application that powers the categorization of customer data into segments/groups with similar characteristics so that appropriate rules and thresholds can be determined to flag suspicious transactions.

Intelligent segmentation uses unsupervised learning approaches encapsulated in Topological Data Analysis (TDA), a technique developed in Stanford's mathematics department with funding from DARPA and the National Science Foundation (NSF). [21]

TDA and machine learning automatically assemble self-similar groups of customers and customers-of-customers. AI software makes the selection of the appropriate algorithms to create candidate groups and tune the scenario thresholds within those groups until the optimal ones are identified. These groups are then put through a tuning process with additional algorithms to identify optimal groupings. A subject matter expert then adjusts the segmentation process per their specifications.

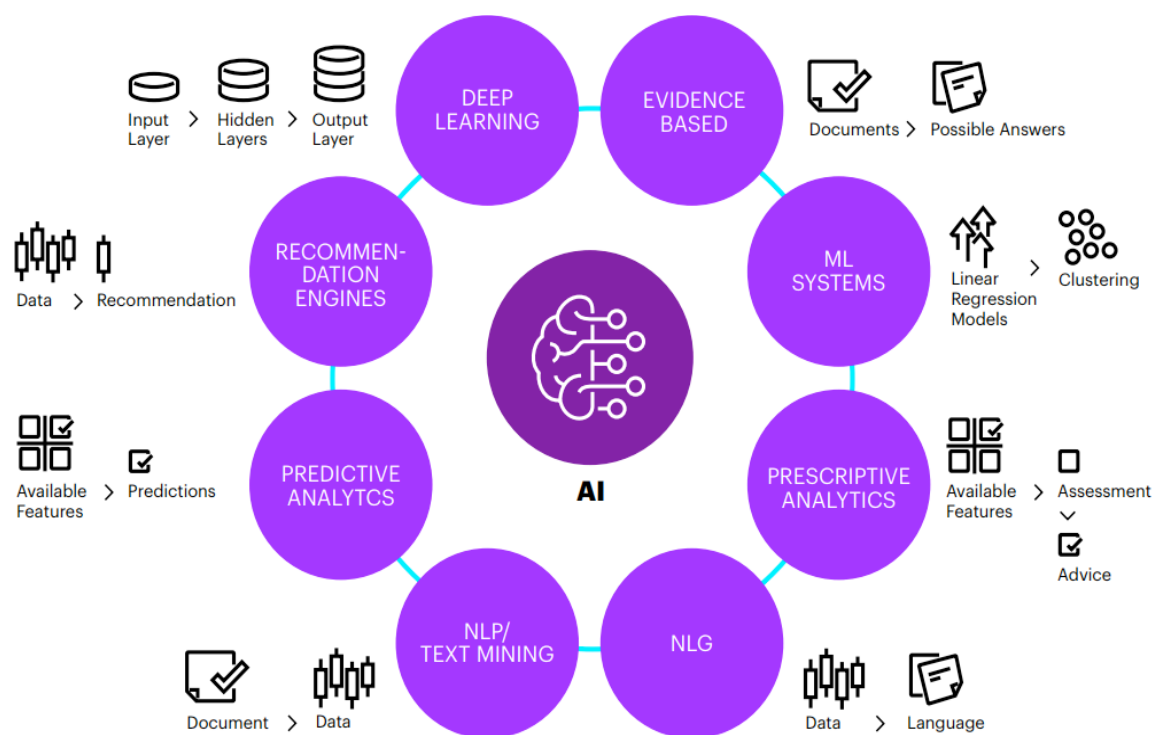
An AI Model-based approach would indicate any strange behaviour of the client to detect outlier or exceptional transaction records by using a modelling framework to analyse user behaviour and then to detect if the user model is coherent with these transactions.

AI could assist bank employees by sifting through large quantities of data and detecting strange patterns they may miss without help. That's because AI excels at examining massive amounts of information extremely quickly. As such, financial institutions often deploy AI to increase the productivity of human teams tasked with searching for things that could indicate money laundering occurrences.

As a result, it may take time to see the full effects of deploying AI to reduce money laundering, especially if algorithms get smarter with ongoing use. [21]

Figure 5 reiterates that several components require substantial meta-data processing; analysing patterns, or disruptions to identify expected customer behaviour, will take time to formulate. Under Predictive Analytics, available features and predictions are dependent on the discovery of meaningful data using natural language processing (NLP)/text mining produces. At this stage, even with AI processing, the enormity of the meta-data does not produce clear patterns.

It is important to notice that AI is only as good as the evolving algorithms match new data to assumed expectations and processes; this might take some time to gradually improve since vast amounts of (segmented) data need to be sifted to form predictions.



Source: The Artificial Intelligence Ecosystem, Narrative Science

Figure 5. A few components of AI Applications show high relevance to data investigations using AI. [22]

Digital Forensics, Bitcoin and AML discovery

Anonymity, of course, is one of the most important tools in the criminal's toolbox. For money laundering, in particular, the entire purpose of the criminal activity is to separate the perpetrator's identity from financial transactions.

New challenges to Digital Forensics, specific to identity intelligence, using AI and pattern recognition, is going to be a critical field within AML-tech. Large distributed systems that can process large amounts of hard drive data, mobile data and other data from sensors, will be crucial for identity management. To the same regard, digital transactions, particularly Bitcoin use for money laundering, are an upcoming trend. With Bitcoin, individuals do not have to rely on other intermediaries to facilitate the transfer. Individuals are privately becoming their own banks by holding their own private keys. Since cryptocurrencies make it hard to regulate such transfers, many people who want to evade taxes in their respective countries may start using Bitcoin. [23]

Anti-Money Laundering (AML) efforts, therefore, are understandably concerned about cryptocurrency. Complicating this story for the money launderers is the fact that Bitcoin itself is not truly anonymous. “While Bitcoin has a reputation for anonymity, the entire history of Bitcoin transactions is visible to all users,” explains Helene Rosenberg, Director of Cash Management, and Global Transaction Banking for Barclays US, in a recent white paper. “Therefore, the blockchain technology/ledger, combined with a monitoring tool, actually allows for increased visibility into potential clients’ activity – more so than would traditionally be available for MSBs [money service bureaus].” [24]

Since we are working with a vast data column and data from the bank might be incomplete, machine learning is only as good as the baseline we work from in finding differences. Unfortunately, we face the similarity of licit and illicit conduct, as many patterns of transactions associated with money laundering differ little from legitimate transactions.

They are recognizable only because of their association with criminal activities. (Foundations of Information Policy Massachusetts Institute of Technology). [25]. Other potential investigation procedures might be using artificial intelligence or machine learning to trace inconsistencies.

Preventing Money Laundering

Anti-money-laundering laws (AML) have been slow to catch up to these types of cybercrimes since most of the laws are still based on detecting dirty money as it passes through traditional banking institutions. Governments around the world have stepped up their efforts to combat money laundering in recent decades with regulations that require financial institutions to put systems in place to detect and report suspicious activity. The amount of money involved is substantial: According to a 2018 survey from PwC, global money laundering transactions account for roughly \$1 trillion to \$2 trillion annually or some 2% to 5% of global GDP. [26]

The Financial Services and Technology industries are finding the most value in Artificial Intelligence (AI) and Advanced Analytics. Figure 6 shows a need to invest more time into both Machine Learning and Predictive analysis as either shows a very low respective 19% and 18% use in combating fraud.

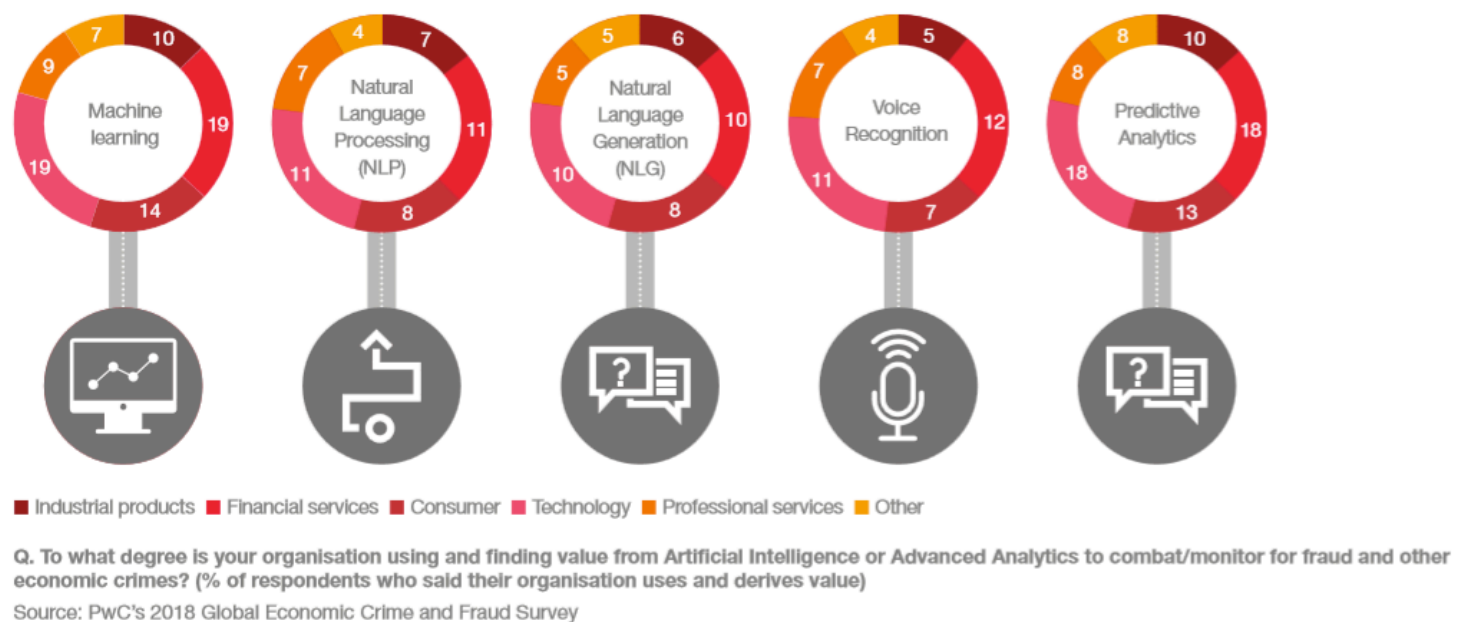


Figure 6. Industry acceptance of Artificial Intelligence. [26]

Cyber-Crime and Money Laundering: Contemporary Tools and Techniques.

The techniques used by money launderers are many and varied: they evolve to match the volume of funds to be laundered and the legislative and regulatory environment of the various jurisdictions in which they are laundered. [27]

Money laundering trends and techniques

Sophisticated money launderers usually seek the part of the financial sector that is the least resistant or weakest. For example, in a cash-based society that has lax legal and regulatory controls; little effort is required to disguise illicit cash or its ownership.

The criminal will fund his lifestyle in cash, or, where funds need to be transferred or surplus funds deposited or invested, the launderer will deal directly with the banks in order to abuse basic banking facilities.

By having the funds laundered through banks, launderers are attempting to legitimise their criminal monies. Where cash is not the norm and legal and regulatory controls are sound, greater effort is required on the part of launderers to disguise the criminal source of funds and also their beneficial ownership. Launderers might have to set up corporate structures and trusts (both onshore and offshore) and attempt to present an appearance of the legitimate commercial or financial enterprise as a

disguise. It will be an added advantage if such corporate structures can be set up in jurisdictions where legislation and regulatory controls are lacking or where there are strict confidentiality controls. It is important to note that the money laundering techniques used by criminals will evolve and change according to the development of products and services pertaining to banking and other financial sectors. There will also be cases in which launderers will develop methods/techniques that will be 'new' to the financial services industry. A case of digital forensics and AML discovery catch-up will then commence. [28][29]

Data Mining Techniques for Anti Money Laundering Examples:

- A terrorist organization uses wire transfers to move money to further its activities across borders - Source: FATF

A terrorist organization in country X was observed using wire transfers to move money in Country Y that was eventually used for paying rent for safe houses, buying and selling vehicles, and purchasing electronic components with which to construct explosive devices. The organization used "bridge" or "conduit" accounts in Country X as a means of moving funds between countries. The accounts at both ends were opened in the names of people with no apparent association with the structure of the terrorist organization but who were linked to one another by kinship or similar ties. There were thus the apparent family connections that could provide a justification for the transfers between them if necessary. Funds, mainly in the form of cash deposits by the terrorist organization, were deposited into bank accounts from which the transfers are made. Once the money was received at the destination, the holder either left it on deposit or invested it in mutual funds where it remained hidden and available for the organization's future needs. Alternatively, the money was transferred to other bank accounts managed by the organization's correspondent financial manager, from where it was distributed to pay for the purchase of equipment and material or to cover other ad hoc expenses incurred by the organization in its clandestine activities. [30]

- Money Launderers use the insurance industry to clean their funds - Source: FATF

Clients in several countries used the services of an intermediary to purchase insurance policies. Identification was taken from the client by way of an ID card, but these details were unable to be

clarified by the providing institution locally, which relied on the due diligence checks of the intermediary. The policy was put in place and the relevant payments made by the intermediary to the local institution. Then, after a couple of months had elapsed, the institution would receive notification from the client stating that there was now a change in circumstances, they would have to close the policy incurring the losses, and would thus request a reimbursement (by cheque). On other occasions, the policy would be left to run for a couple of years before being closed with the request that the payment is made to a third party. This reimbursement cheque was then often processed by the local financial institution without further question since the payment came from another reputable local institution. [30]

Extended interesting reading:

<http://www.terrorismanalysts.com/pt/index.php/pot/article/view/279/html> [31]



Unfortunately, investigators often get into the situation above, as high-up government officials may, or may not, know about illicit activities and they might have a share in the misconduct.... [32][33]

References

- [1] <https://1.bp.blogspot.com/-iPMpuC4842c/Wk1GUNGDoqI/AAAAAAAAAASk/BZZ-o8ExVbMMFLhEfVkJQ1TCnYfWtSdEEACLcBGAs/s1600/infographic-crime-02.jpg>
- [2] http://www.unodc.org/pdf/convention_1988_en.pdf
- [3] http://www.unodc.org/pdf/crime/a_res_55/res5525e.pdf
- [4] <https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm>
- [5] <https://www.pwc.com/us/en/industries/financial-services/financial-crimes/anti-money-laundering/compliance-tools.html>
- [6] UNODC – UN Office on Drugs and Crime: The Money Laundering Cycle. <http://www.unodc.org/indc/en/money-laundering/luandrycycle.html>
- [7] <https://www.bankeredu.com/aml-basics-sources-steps-and-methods-of-money-laundering/>
- [8] <https://www.datavisor.com/2016/09/22/dont-be-taken-to-the-cleaners-anatomy-of-money-laundering/>
- [9] https://www.moneylaundering.ca/public/law/3_stages_ML.php
- [10] <https://www.investopedia.com/terms/s/shellcorporation.asp>
- [11] http://en.finance.sia-partners.com/sites/default/files/post/visuels/sia_partners_-_alm_in_trade_finance_-_trade_based_money_laundering_-_a_growing_concern.png
- [12] <https://www.moneylaunderingnews.com/2018/09/danske-bank-ceo-resigns-on-heels-of-report-detailing-an-astounding-234-billion-in-suspicious-transaction-in-money-laundering-scandal/>
- [13] Frances Schwartzkopff and Peter Levring. September 19, 2018, 6:36 PM GMT+12 Updated on September 20, 2018, 1:07 AM GMT+12

- [14] <https://www.bloomberg.com/news/articles/2018-09-19/danske-bank-ceo-to-step-down-for-role-in-laundering-scandal>
- [15] Kamlesh D. Rohit Dharmesh B. Patel. Review On Detection of Suspicious Transaction In Anti-Money Laundering Using Data Mining Framework. IJIRST –International Journal for Innovative Research in Science & Technologyl Volume 1 | Issue 8 | January 2015 ISSN (online): 2349-6010
- [16] Nida.S. Khan 2013. Nida S. Khan, Asma S. Larik, Quratulain Rajput, Sajjad Haider, "A Bayesian approach for suspicious financial activity reporting", International Journal of Computers and Applications, Vol. 35, No. 4, 2013
- [17] <https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf>
- [18] A Much-Needed Intelligent Approach to Segmentation by GURJEET SINGH. August 10, 2017, in Compliance, Featured
- [19] <https://www.corporatecomplianceinsights.com/ai-transforming-anti-money-laundering-challenge/>
- [20] A Much-Needed Intelligent Approach to Segmentation by GURJEET SINGH. August 10, 2017, in Compliance, Featured
- [21] Leveraging machine learning within anti-money laundering transaction monitoring. 2017. Regan, S., Adams, H., Guiral, P., Choudri. S.
- [22] https://www.accenture.com/_acnmedia/PDF-61/Accenture-Leveraging-Machine-Learning-Anti-Money-Laudering-Transaction-Monitoring.pdf
- [23] <https://www.blockchain-council.org/blockchain/how-bitcoin-money-laundering-works/>
- [24] <https://www.forbes.com/sites/jasonbloomberg/2017/12/28/using-bitcoin-or-other-cryptocurrency-to-commit-crimes-law-enforcement-is-onto-you/#311e0fd23bdc>. Bloomberg, Jason. Dec 28 2017
- [25] <https://groups.csail.mit.edu/mac/classes/6.805/articles/money/ota-money-laundering/05ch4.pdf>
- [26] <https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf>
- [27] <https://www.coursera.org/lecture/forensic-accounting/money-laundering-basics-GA9J3>

[28] <https://aml-cft.net/money-laundering-trends-techniques/>

[29] <https://pdfs.semanticscholar.org/5afb/5296e3987c275b3f191d62f72325570a0fa5.pdf>

[30] http://www.fatf-gafi.org/media/fatf/documents/reports/2003_2004_ML_Typologies_ENG.pdf

[31] <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/279/html>

[32] <https://stears.s3.amazonaws.com/media/articleImages/mlm1.jpg>

[33] <http://thegabblor.com/>

About Johan

With more than 25 years' work experience, I have 15+ years' experience in the tertiary education of which the last 7+ years in lecturing roles. I completed a PhD. in Computer Science at The University of Adelaide, (awaiting approval) covering a broad range of computer science disciplines, especially research in semantics, ontology, provenance, sensors, and associations between domains with emphasis on knowledge engineering and flow models. Other interests: Research: Sensor Event discovery/ Environmental Sensor awareness. Sensor device



localization and tracking. Early Warning Sensor (EWS) system. Ontology development: Knowledge discovery and data mining. Provenance and workflow processes. Semantic query and data management methods. Digital Forensics: fragment traceability in the cloud. Completed a Masters Computer and Information Science (MCIS) at the Auckland University of Technology (AUT) (Research based thesis). Thesis: Digital Forensics discipline: "Towards an Automated Digital Data Forensic Model with specific reference to Investigation Processes" 2010.

Lectured in:

- Software requirements engineering
- Data mining and Knowledge Engineering
- Information Security
- Contemporary Issues
- Research methods I and II
- Integrating Information Technology and the Enterprise

Why Cryptocurrency Matters in Digital Forensic Investigations

by Chris Chiang

Investigators need to know something about cryptocurrency, because it has become the payment of choice for many criminal activities. It has been identified as a payment method in transactions involving fraud, illegal drugs, money laundering and child pornography.

Cryptocurrencies make it easier to conduct any transaction, and building with cryptographic protocols makes transactions secure and difficult to fake. Even though, the thief tried to launder the money, he wasn't patient enough to hide the tracks that forensic investigators can exploit. Fortunately, the cryptocurrency's blockchain records all. The trail of cryptocurrency addresses may link all that money to illegal drug sales. By identifying different types of virtual currencies, a digital forensic investigator will get a clear goal, and look for specific digital evidence in the computer or mobile to support unique investigations. Take one of popular email scams for example, the following public address is 18c74HRohRc781Fw34gDBN3TkQm94hi3q1. I got this email at 22:47 on Jan 21, 2019. From public online resources, I am curious if anyone paid the fraudster in bitcoins?

Hi, my prey.
This is my last warning.

I write you because I attached a virus on the web site with pornography which you have visited.
My trojan captured all your private data and switched on your camera which recorded the act of your solitary sex. Just after that the trojan saved your contact list.
I will erase the compromising video records and information if you send me 900 USD in bitcoin.

This is address for payment - 18c74HRohRc781Fw34gDBN3TkQm94hi3q1
(If you don't know what bitcoin / write to buy bitcoin in Google)

I give you 30 hours after you open my message for making the payment.
As soon as you read the message I'll see it right away.
It is not necessary to tell me that you have sent money to me. This address is connected to you, my system will erased automatically after transfer confirmation.
If you need 48h just Open the calculator on your desktop and press + + +
If you don't pay, I'll send dirt to all your contacts.
Let me remind you-I see what you're doing!
You can visit the police office but anybody can't help you.
If you try to deceive me , I'll know it immediately!
I don't live in your country. So anyone can not track my location even for 18 months.
bye. Don't forget about the shame and to ignore, Your life can be ruined.

One of the popular email scams to trick you.

Summary	
Address	18c74HRohRc781Fw34gDBN3TkQm94hi3q1
Hash 160	536c7eb511f6394621a86e58e5c5d606df61a56e
Transactions	
No. Transactions	4
Total Received	0.0004227 BTC

1914860ad5ef1e0348bc8c0a103ecf0ddfc6b0b6fbc5fa345e7d4642c4c423e1	2019-02-06 05:21:45
3JSnHsH2uJB2wxPxtk7k8NrVKWWhw347Szi	→ 18c74HRohRc781Fw34gDBN3TkQm94hi3q1 \$ 1.19
	\$ 1.19
9f92669e354d49786d9ce288835a7366442692dcf532dfd452df2b3d4d2dd3e0	2019-01-26 07:04:47
1PjvKNBjogKVaefvKRCdW8iQs9V2dpRJv7	→ 18c74HRohRc781Fw34gDBN3TkQm94hi3q1 \$ 2.30
	\$ 2.30

It looks like 2 people paid the fraudster in bitcoins.

Though it's not a large amount, it's still important to answer my next question— where's the real money? First one from 1PjvKNBJoGKVaefvKRCDw8iQs9V2dpRJV7 paid to the public address, and then someone sent coins to another two public addresses.

51dc94b39d2b5b85dae6495129caab98a7be3f94461c21a2926d2e0d76172502		2019-01-26 22:20:39
18c74HRohRc781Fw34gDBN3TkQm94hi3q1	→	18Suu42YFeGoc4upwRbpTsXhF1kTrEvgzZ 1HB1GxZCBbdbSjnTJuqtJu2e8XNLqDnAXM
		0.0001062 BTC 0.00027925 BTC
		-0.00027826 BTC
9f92669e354d49786d9ce288835a7366442692dcf532dfd452df2b3d4d2dd3e0		2019-01-26 07:04:47
1PjvKNBJoGKVaefvKRCDw8iQs9V2dpRJV7	→	18c74HRohRc781Fw34gDBN3TkQm94hi3q1
		0.00027826 BTC
		0.00027826 BTC

Now we are following on one of two public addresses, 1HB1GxZCBbdbSjnTJuqtJu2e8XNLqDnAXM. Let me call it 2nd public address. We found three more people sent coins to the 2nd public address. Not only that, the 2nd public address is linked to the 3rd public address, 3KnzC2XJRMD-JMf1iaNPTkCiAquKEFPU92X.

17672b46f78bdbaf6031f28adb2c4687699a4076201622d21d6776a039b3167		2019-02-17 07:00:15
12WDCCJwu8bR94dTKtJTEk3mZ6oxYqYdjh 1AHRDJ5CzZhsJptLfyEWKFzsTJZqkeBDoR	→	1A1V1bAtjvxFm33rsyZzWTJbCpGNrEPVJw
		\$ 343.73
		\$ 343.73
7b1f74170cc7654ae0f74c4d71b5dc1d981fa10ce114b0923619d537dd86ae64		2019-02-17 04:13:05
18c74HRohRc781Fw34gDBN3TkQm94hi3q1	→	1A1V1bAtjvxFm33rsyZzWTJbCpGNrEPVJw
		\$ 1.14
		\$ 1.14
1d1ef964881ac02ca28dab2034ef608579d60f63d28cc1a4a3f2c63232517c5a		2019-02-16 17:50:54
1LVdvayubZqiovNsowc26xkuX1CbzYvdm	→	1A1V1bAtjvxFm33rsyZzWTJbCpGNrEPVJw
		\$ 228.62
		\$ 228.62
7723531f4af96effc7956648d44b9451b6160bfd9f8e9c8c86ab433e212298c0		2019-02-18 02:37:04
1A1V1bAtjvxFm33rsyZzWTJbCpGNrEPVJw	→	1HAXBdjrv62cS5e2di6YK74Ni3GPGHMqrk 3KnzC2XJRMDJMf1iaNPTkCiAquKEFPU92X
		\$ 43.87 \$ 296.94
		\$ -344.55

The 3rd public address, 3KnzC2XJRMDJMf1iaNPTkCiAquKEFPU92X, is also linked to the 4th public address, 33X2qBtGRjqcEPVZhrDRJbNbMZLvdGEcha, as expected.

923459f345362237f9a2fbc27740357639befd61b23ff198076bc4cace4cd1a9	2019-02-18 08:46:16
3KnzC2XJRMDJMf1iaNPTkCiAquKEFPU92X	→ 33X2qBtGRjqcEPVZhrDRJbNbMZLvdGEcha
	\$ 14,484.92
	\$ -296.90
7723531f4af96effc7956648d44b9451b6160bfd9f8e9c8c86ab433e212298c0	2019-02-18 02:37:04
1A1V1bAtjvxFm33rsyZzWTJbCpGNrEPVJw	→ 3KnzC2XJRMDJMf1iaNPTkCiAquKEFPU92X
	\$ 296.90
	\$ 296.90

From the 4th public address, we found up to 170 possible victims there. Someone sent coins to the 5th public address, 1JezCi8oBs4DsKCrtbLDTH5sPwy6TjGCTa.

923459f345362237f9a2fbc27740357639befd61b23ff198076bc4cace4cd1a9	2019-02-18 08:46:16
3EpMhNC4ABGpnxBThCPnoaT32j2WA1GsvH 3KB3vcvPzqzUSg7vUW5LyGr8yEgAJhR9Le 3AC1693pp7SQp7BeZQpymeAno3dNBTZN3 3PvqVmLbHREExCREWuHCk7X1Suqk3SmKzj 3Bq7G3S7QAUa4vvED9iSz2Dhi4zV6do6QE 3688RGYhN1ntG5dcFBRXHTRVjqX84dDBRQ 3KnzC2XJRMDJMf1iaNPTkCiAquKEFPU92X 3LuHwxAX8hvAoVoFKMJcvurNj54Qn1wcu2 3BBLgMjKEMh3QjMtoU4xVLjwCDjxh1Ut 34k44LBeiUy3fFMbQoDqjNCY8mQga85Ji 382WSvs3nsSk3o8LForEKW8pgHvdVHFxA 38WLMmRvjaUoYz3dL1AacpxqnuMBwUhnc 35Lrgd1Zp9GsvLWcWZ5gdxqo4xgt4AFLxW 39iQHkeJ3c8Gbkx1wLdgb6a6S1aQkH8m8B 37stjXJ2RpFfKEQ6ig6nQ77oKmpWetM3Xa 3Q94aXQGrzxU25LMqjoFEuP3143ZWy6ZD 37fJDLZ41AB26ZxzFsz978U9qzGU2qrB3Q 3BAz3kZrBjirEDQtdMT84k9xL86dqFFnG9 3BQyvjJpn4S7kdYmNLM5y6wGeHbo5ux2z 3EEVgwCcJ8yzRyXk1JQvwwPX6xtZaWxvK5 36DmEgKuahEE33A5jBrRK77mVRM7j4gHj9 3DxWAe4zbFdLuBk5yQZizsrgoKVTDGFUo 37e6usBdKh1urgSLNFKprvnhkhyUhGwJfJ 3KeyTEtioeJPWR95yy1iCx3TFVBHJx6pu 3Hn9fLuwTQXhigifVcz23M7rGG8GUrqWZ 32UzKPoU7DKQaCLuZrAVgF3FyCQDQgVWbM 3L1EXmmvmNadYgC1zfuLKZrg4rStMtwS9L 3FWYeu2GoNHkohjwNs5ftwQMQV8h6n4UKC 39cWo6pfpnJU36oiyYcJ6TxCYKf9wstkVd 3LmQxdKreT7XksGpQgvSqKqme5HP6azSn 3DVafhMK4kveaGiiA7vsnP61R3MYIIPFn6zF	→ 33X2qBtGRjqcEPVZhrDRJbNbMZLvdGEcha
	\$ 14,479.99

I would like to stay in this stage. The 5th public address received up to USD \$11,839,449 from Jan 24, 2018 to May 31, 2019. Since the story does not end here for email scams, may we look into any public addresses in cryptocurrency wallets from computer or mobile as a digital evidence? It may provide an accessible alternative way to support fraud investigation.

b6839ee15ee3c596f225cfddefddc4a888964e5173fdbd95673c1ddce8285ea9		2019-02-19 09:13:43
33X2qBtGRjqcEPVZhrDRJbNbMZLvdGEcha	➔ 1JezCi8oBs4DsKCrtbLDTH5sPwy6TjGCTa	\$ 36,852.59
		\$ -14,479.99

Summary	
Address	1JezCi8oBs4DsKCrtbLDTH5sPwy6TjGCTa
Hash 160	c1a94754ccc46812ab84736da69b80cd451863a3
Transactions	
No. Transactions	598
Total Received	\$ 11,839,449.08

The 5th public address received USD \$11,839,449 until May 31, 2019.

3078a9b495e2d51af9d9948198ece0f355c01419411e1e5aa295d7d41f645224		2018-01-24 17:42:04
33VAxyerzXC3cF5KHJJ4z8Bgtj2ArLtp1r	➔ 1JezCi8oBs4DsKCrtbLDTH5sPwy6TjGCTa	\$ 827.75
		\$ 827.75

62d923a1e488259d5d5d00bad6f9ecf2354bdc33bed7eced97f9acb7fbcf2823		2019-05-29 09:01:18
3ESQMyeesFUupKV56TWccRmC3YvaxaAenKv	➔ 1JezCi8oBs4DsKCrtbLDTH5sPwy6TjGCTa	\$ 60,324.29
		\$ 60,324.29

The transaction records for the public address.

What is cryptocurrency?

The main issue of digital forensic investigation is to search suspicious operations that were made with the use of cryptocurrency, but each country decides differently how to deal with it. It's natural to find some ways of searching suspicious operations that could be directed to criminal fraud and illegal drugs according to different types of cryptocurrencies.

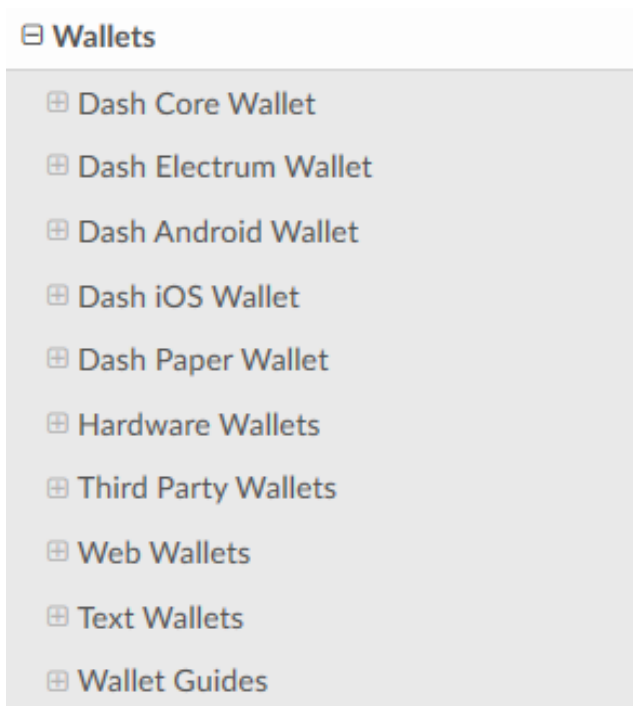
So the question is, "aren't cryptocurrencies, digital currencies and virtual currencies the same thing?"

- **Digital Currency:** Digital currency represents electronic money. It doesn't have a physical equivalent in the real world, but it acts in the same way. Therefore, it can be defined as the payment or exchange of money without a physical currency. They can be used to purchase goods and services. For example, online shopping by using credit card may be subjected to theft from hackers, and they may be exchanged for physical cash.
- **Virtual Currency:** All virtual currencies are digital, but are not issued by a bank. It may be operated with or without a trusted third-party. For instance, Linden dollar is a type of virtual currency for a gaming network. It is the official currency of a virtual gaming world, Second Life. But most notably for game coins, there are lots of local games like More Laozi (com.more.laozi) in Taiwan. Both are operated with a trusted third-party. If a virtual currency is built with cryptographic protocols, that's cryptocurrency. So cryptocurrencies such as Bitcoin are considered to be virtual currencies, and they may be not controlled by a trusted third-party.
- **Cryptocurrency:** Many cryptocurrencies operate as decentralized systems without a trusted third-party. It builds on blockchain technology that only exists online. Since it has a strong security, digital forensic investigators acknowledge that no institution is set aside to regulate them. It's still a way to find digital evidence, because people may be afraid of computer or software failure. Suspects may make a backup file on a computer, mobile or USB device.

The Timing for digital forensic investigation

Investigators try to get hidden cryptocurrency things on computers or mobile devices, such as transactions, wallet public addresses, wallet private keys, passphrases and other sensitive data.

A cryptocurrency wallet is a software program that stores public addresses and private keys. Different types of wallets are used for different purposes at various times. Any type of wallet is simply a combination of the private key and public address. Please note, a public key may generate as many public addresses as you like. It's based on how and where we store them, so a cryptocurrency wallet can be located in an USB device, Windows software, MacOS software, Linux software, a mobile app, a website or just a printable paper. Let's take Dash Wallet for example, it's compatible with both Android and iOS systems. In general, most popular hardware wallets allow us store more than 22 cryptocurrencies.



As an expert team, Frontline detective's note improves work efficiency for digital forensic investigators. It would be better to know the usage behavior of cryptocurrency wallet and wallet information from suspects. Generally speaking, a cryptocurrency wallet has multiple public addresses, a public key and a private key. Take Bitcoin for example, addresses are alphanumeric, public keys use a BASE58 character set. It means it doesn't contain characters that may be visually confused 0 (zero), O (capital o), I (capital i) and l (lower case L). Bitcoin addresses should be 34 characters long, but it can theoretically be as short as 26 characters.

3CYrVFJgzwwZHNBWJ28s7QzPgj2nXM2uTS



3CYrVFJgzwwZHNBWJ28s7QzPgj2nXM2uTS

One of Bitcoin's Public Addresses

The main difference between traditional finance is that there is no third-party for cryptocurrencies. Private key should be hosted on end user side, so users may manually do backup files on computer or cloud storages like Dropbox, Google Drive or Box.com. Private key may prove ownership of the wallet, that's why digital forensic investigators are tasked with presenting it to the court.

According to the crime scene and the usage behavior of a cryptocurrency wallet, digital forensic investigators may consider the following tips to perform a better forensic result:

1. Unlock the computer or mobile device to avoid getting locked again. For unusual phones, charging cable testing is required. It made a deep impression on Lee and me last week, however it's hard to find a replaced charging cable for some unusual phones.
2. Try to find out hot wallet and cold wallet. Most people have two wallets. Hot wallets are connected to the network, and cold wallets are not. Hot wallet is insecure, so they always keep small amounts of money.
3. Seizing the hardware or software wallet does not prevent cryptocurrency from being moved. Try to understand the usage behavior of a cryptocurrency wallet.
4. If your department has no cryptocurrency wallet for law enforcement use, please follow digital forensic process. Never transfer any coins to a personal cryptocurrency wallet.

5. If your department has a cryptocurrency wallet for law enforcement use, just follow up your regional standard operating procedure. Digital forensic processes might prove the transaction from A wallet to B wallet.

Sensitive cryptocurrency data in forensic investigation

There are many smart ways to keep cryptocurrency safe. Investigators have to collect key digital evidence from billions of rows of data on a computer, mobile or online platform. We realize we need something different- that's to say, a strategy.

- Hardware Wallet

Hardware wallet looks like an USB stick. If you are not familiar with it, there are many hardware wallet brands online such as Ledger or Trezor. Investigators try to get actual public addresses and private keys from within it. Some people have two or more hardware wallets to avoid losing all of their coins.

- Computer Software Wallet

Let's take Bitcoin Core for example. Initially, it's under the name "Bitcoin" by Satoshi Nakamoto, Bitcoin founder, and later renamed for "Bitcoin Core".

Download: <https://bitcoin.org/en/download>

Bitcoin Core supports Windows, MacOS, Linux, ARM Linux and Ubuntu, please select your chosen operating system to download the latest version.

Now we suppose we have obtained a forensically-sound and legally-defensible image, and we completely parsed collected data. Our primary goal is to get suspicious evidence. It will prompt us to access related financial transactions by wallet backup file and private key.

It's the default Bitcoin Core folder path:

Windows `C:\Users\{Username}\AppData\Roaming\Bitcoin`

MacOS `~/Library/Application Support/Bitcoin/`

Linux `~/Bitcoin/`

Other cryptocurrencies may set similar paths, but it's still possible to change default paths. Try the following alternative ways:

1. Type part of the filename you want to find, such as wallet name. In Bitcoin Core, we know the backup file keyword, Wallet.dat.
2. Sort by folder size. Blockchain may need more space to handle storage. It helps us discover unknown cryptocurrency wallets.
3. If your digital forensic tools support virtual machines, you may click HELP >> Debug Window to understand source path at Bitcoin Core software.

- Web Wallet

Web Wallet may be traced by web browsers. There are several ways to know if there are any suspicious activities.

- Web Histories
- Bookmarks
- Recently Visited Websites
- Cookies
- Login credentials










If there's no digital forensic software on hand, we may manually do an exercise first.

A search for "places.sqlite", it's a FireFox database file.

Source path:

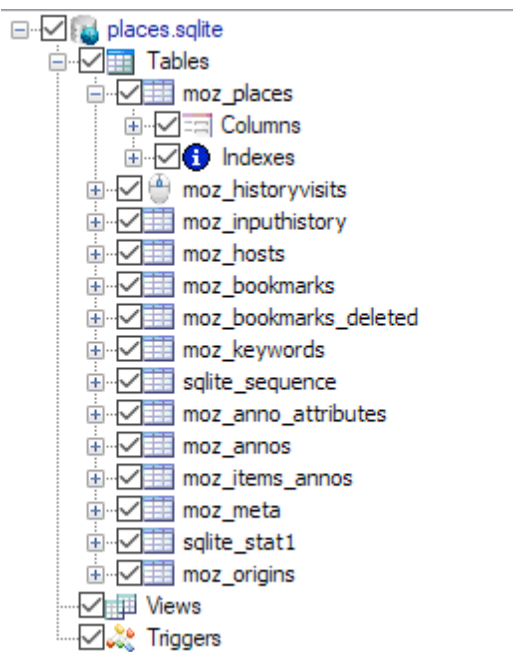
```
C:\Users\{username}\AppData\Roaming\Mozilla\Firefox\Profiles\
```

(AppData is a hidden folder by default, and you have to unhide it.)

 memory-report.json.gz	2018/9/11 下午 0...
 notificationstore.json	2019/5/17 上午 1...
 parent.lock	2019/5/23 上午 0...
 permissions.sqlite	2019/5/23 下午 0...
 pkcs11.txt	2018/8/31 上午 0...
 places.sqlite	2019/5/23 下午 0...
 places.sqlite-shm	2019/5/23 上午 0...
 places.sqlite-wal	2019/5/23 下午 0...
 pluginreg.dat	2019/5/21 上午 1...

Try to open it from any SQLite Repaired Tools and get following tables:

1. Moz_places
2. Moz_historyvisits
3. Moz_Bookmarks



- Mobile Wallet

Bitcoin, Litecoin and Darkcoin are popular cryptocurrencies to mobile app. The best practice to mobile wallet is physical acquisition and memory dump, and it may get expected forensic evidence files for

cryptographic wallets. For example, bitWallet is one of Bitcoin’s wallets. We got public keys and private keys from a file named “Wallets.v1”.








Private key is addressed in a .txt file for Litecoin, something looks like below.

T7jegh25d23s39fs19e34f8sdff4xs8s2.....	2019-05-24T20:11:12
--	---------------------

Particular interest to forensic investigator and law enforcement may be IP addresses and transaction hashes. Both might be found in the wallet.log files.

Listed Items	Examples
Sender’s Public Address	18c74HRohRc781Fw34gDBN3TkQm94hi3q1
Receiver’s Public Address	1HB1GxZCBbdbSjnTJuqtJu2e8XNLqDnAXM
Amounts	0.02 BTC
Fee	0.00001 BTC
Seen Peer Numbers	3
Time	07:59:12
Transaction Status	Spent Transaction

It’s worth mentioning that usage behavior is also a good point to confirm your findings. Take Coinbase for example, you might get more information on com.google.android.gms.measurement.prefs.xml, and following listed items may help your practice. If you have a timestamp issue, try to visit at www.epochconverter.com.

 coinbase-database	2019/5/22 _
 coinbase-database-shm	2019/5/22 _
 coinbase-database-wal	2019/5/22 _
 com.amplitude.api	2019/5/22 _
 com.amplitude.api-journal	2019/5/22 _
 google_app_measurement_local.db	2019/5/22 _
 google_app_measurement_local.db-journal	2019/5/22 _

Coinbase Application Folders.

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="gmp_app_id">1:242335961153:android:a804a0bfc04046cd</string>
  <string name="app_instance_id">6722f7ad256c3c47c5abe91c6c66a358</string>
  <long name="time_active" value="1266" />
  <boolean name="has_been_opened" value="true" />
  <long name="first_open_time" value="1558323023293" />
  <boolean name="deferred_analytics_collection" value="false" />
  <long name="app_install_time" value="1558322943000" />
  <boolean name="use_service" value="true" />
  <long name="health_monitor:start" value="1558492208408" />
  <long name="last_pause_time" value="1558493337844" />
  <long name="last_upload" value="1558323032937" />
  <string name="previous_os_version">5.1.1</string>
  <boolean name="start_new_session" value="false" />
</map>
```

Some Information for Coinbase Application.

Listed Items	Examples
Application Name	Coinbase
Application Version	6.25.2
Cryptocurrency Name	Bitcoin(BTC)
Installed Time	1558322943000
First Opened Time	1558323023293
Last Pause Time	1558493337844
Last Uploaded Time	1558323032937
Current Opened	True

Conclusion

Cryptocurrency is anything possible, but straightforward to investigation. All public addresses of Bitcoin are recorded and verified on the blockchain. Some countries are starting to regulate cryptocurrency markets, and exchange requires Identification cards or driver license verification before any transaction. However, Bitcoin is just one of many cryptocurrencies, it's not anonymous. By taking advantage of cryptocurrency, it helps prevent a large range of financial crime tomorrow.

About the Author



Chris Chiang is a Data Scientist, a Digital Forensic Investigator and a Digital Forensic Instructor for law enforcement agencies. His forensic practice courses were attended by thousands of participants from Prosecutors, Judicial Police Officers, to Investigators. Chris stepped into the spotlight during a child exploitation investigation on LinkedIn last year. Using a photo provided by Europol he was able to use AI to determine the name of a hotel that was relevant to the case, correctly predicting it was located in Asia, and not (as the general consensus was at the time) in Europe. You may follow him on LinkedIn at <http://linkedin.com/in/chris-chiang>

Digital Forensic Integrity: Mental Health

by Rachael Medhurst & Emma Derbi

Digital Forensics is the process of examining data that has been located upon digital devices. This will often leave Digital Forensic Investigators exposed to a range of illegal material that can affect the investigator's psychological state. This is often because the investigator will view nefarious content, write an expert witness statement, present this information in a Crown court and ultimately relive the evidence. This can be a highly emotional and stressful career for many. This article will be looking into what support is available, if any, the accessibility of support available, and if there is currently enough support while cybercrimes are continuously rising in this modern age. Using secondary and primary research from investigators, this will provide a highlighted understanding of whether the potential psychological damage caused has a detrimental impact on the integrity of Digital Forensic Investigations.

“Cybercrime is any kind of crime that involves a computer. That could be hacking, or it could be identity theft or child pornography. Cybercrime covers a wide range of different offences, all of which are punishable by law in the UK. We can divide cybercrime up into two categories: crimes that affect people and those that affect businesses” (Henshaw.S, 2018). Due to the sophistication of cyber-crimes currently occurring and on the increase, this has caused a surge for the demand of Digital Forensic Investigators to uncover vital evidence.

Forensic laboratories should adhere to the ISO 17025 standard. The 17025 standard is the international standard for the testing and calibration laboratories. Without this accreditation, the laboratory would be considered technically incompetent and should state this within their expert witness reports. The technical competency of employees is vital to uphold the integrity of Digital Forensic cases.



(AeroBlaze, 2017)

Additionally, Digital Forensic Investigators should be adhering to the ACPO guidelines throughout the investigation process. The four main principles include:

Principle One: *No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.*

Principle Two: *In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.*

Principle Three: *An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.*

Principle Four: *The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to" (Officers, 2012).*

The principles are in place to ensure the integrity of the data is maintained throughout the investigation. However, ACPO acknowledges within section 7.2. that there is a concerning aspect for

the welfare of investigators within digital forensics. ACPO Good Practice for Computer-Based Electronic Evidence suggests recommendations for individuals who are exposed to images of sexual abuse on a “regular” basis. These individuals should attend a psychological support scheme. The suggested support for forensic companies includes:

- A minimum of one session per year, which could be individual or group sessions.
- An option for 24-hour access to occupational help, if needed.
- Limit the exposure by restricting access to the environment.

(Officers, 2011)

Although there are frameworks and principles in place for the Business and Investigation aspect of Digital Forensics, the biggest asset to any company is its employees. Yet for such a demanding career path, there is currently no framework or guidelines in place to ensure the welfare of the employees. Therefore, forensic laboratories are not looking after the Human element of their business. For successful completion of a forensic investigation, all three elements should be in concurrence of each other equally. These elements are considered as Business, Investigation and Human.



(Three factors of a successful forensic investigation, 2019)

MFHA England states that *'1 in 6 workers will experience depression, anxiety or problems relating to stress at any one time'*. This represents the general working population, however, when working with such nefarious content this statistic is likely to increase dramatically. Additionally, MFHA England also stated *'15% of employees who disclosed mental health issues to their line manager reported being disciplined, dismissed or demoted'*. With this statistic available, this may cause employees to be scared to discuss their psychological needs with management and seek help (MHFA England, 2019).

Eric Oldenburg, Griffeye's Law Enforcement Liaison Officer stated 'Speaking for myself, I started to feel mentally stressed after about four years. I often came home from work mad and I didn't know why. My home life with my family suffered and my marriage was under a lot of stress – to the point where I almost got divorced. I also had physical issues' (Oldenburg.E, 2018).

With these statistics in mind, it is important to gather primary research. A questionnaire has been utilised to gauge their experience of support while working in this industry. A total of 16 digital forensic investigators have completed this questionnaire to provide an insight into the human element of digital forensics, below is a summary of responses from each question posed.

Question One: How long have you worked in the industry?

A total of 14 participants stated they have worked within the industry for 2+ years, the additional two were between 6 months to a year. This was important to establish and highlight if there is a correlation between the amount of time working in this industry and the impact this has on the investigator's psychological state.

Question Two: Which of the following types of cases do you work on?

Out of the 16 participants, 12 participants work on criminal cases and the additional 4 participants work on civil cases. Depending on the type of cases investigators complete, this would result in different effects.

Question Three: Has this type of work had a mental impact on your well-being? If so, how?

This question was a comment box which provided further information to be collected, all 16 participants completed this question. A total of 7 participants stated that completing these cases did

not have an impact on their mental well-being but often stated it made them more aware of crimes in the world and they became hardened to the material.

The additional 9 participants stated that this has affected their mental well-being, this was from the material viewed daily, but other factors raised included the stress of being accountable for every action and to work quickly but efficiently in this field.

Question Four: What support is available at your place of work?

All 16 participants completed this question with a range of answers, one common answer is the availability of counselling and psychological evaluations. Although counselling and psychological evaluations are provided in many companies, it appears to be limited to how often an investigator can seek this help. This variation between companies includes seeing a counsellor once every 3 months, to once every 12 months and then 6 free sessions a year. More concerningly, 4 participants stated that there are no counselling facilities for their mental well-being while working on these cases.

One participant stated that they were in the process of promotion and worried about if they asked their line manager for help for their mental health, then this would affect their chances of being successful in their promotion.

Question Five: Have you utilised this support? If so, what support?

Out of the 16 participants, 8 of these have received counselling and psychological assessments. However, several of these participants also stated the few sessions they received from their companies was not sufficient enough for the amount of content being viewed and had to seek private counselling to help minimise the impact. Another participant stated that the annual psychological assessments are a tick box exercise. Due to the tick box exercise, this places doubt in the validity of these psychological assessments.

The remaining 8 participants have not sought any support services from their company or personally for mental well-being relating to their career path. This may be because it is not available within their company or because they feel they do not require this support currently.

Question Six: Do you feel there is sufficient help available?

This question was posed as a multiple-choice question, the three answers provided were 'Yes', 'No', 'Could be Better'. In total, 5 participants stated 'Yes' there is enough support available, 4 participants stated 'No' there is not enough support available while the additional 7 thought that the support services 'Could be Better'. This highlights that 11 out of the 16 participants felt that currently there are not enough support services provided to digital forensic investigators.

Question Seven: What else would you like to see in place to help support your case?

After concluding from the participants what support is available and if they have sought this support, the next question is for further information on the additional services they would like implemented to help this well-being. Some of the suggestions include; mandatory counselling/supervision at least once a month, anonymous phone lines, break out rooms, gym, support from management instead of focusing on deadlines of cases, quarterly mental health assessments, trained management, less overtime (an adequately staffed team) and HR team equipped to deal with the emotional turmoil these cases can cause and a functional mental health unit.

From the suggestions mentioned, this does show that digital forensic investigators would like additional support services and facilitates made available to them to help them maintain well-being during their work life.

Question Eight: Do you feel like your psychological state impacts your ability to complete cases successfully?

After question seven highlighting several areas for improvement for the human element of the forensic industry. The next question has been posed to determine if the lack of support services available impacts the integrity of casework. All 16 participants completed this questionnaire, 9 out of the 16 participants stated that the lack of support for their mental well-being has had an impact on their casework due to concentration issues, the feeling of sadness and the stress of worrying not everything necessary for the case has been found.

The additional 7 participants stated that the emotional aspect of this career path has not affected their casework. This included one participant who stated that 'if anything, it drives me to do my best'.

Question Nine: Do you feel if you had more support with mental health this would improve your casework?

This question was a multiple-choice question, the answers available are 'Yes', 'No' and 'Not Sure'. All 16 participants completed this question, 7 of which stated 'Yes' with the correct support services available this would improve their casework; 4 participants stated 'No' the additional support services would not help them improve their casework and the final 5 stated that they are 'Not Sure' if this would help their casework.

Question Ten: Any further comments?

The final question posed was for any additional comments, some interesting comments have been mentioned in this section which included; "since experiencing the lack of support, I have now changed jobs due to such poor support for such a difficult job role" and "There needs to be more help for digital forensic investigators, not many people investigate such horrific crimes every day and deal with the stress that we have to deal with".

Other participants did not answer this question or thank us for the questionnaire. However, those topic comments highlight for those two participants a need for assistance that, unfortunately, is not being met currently.

From this questionnaire, a great amount of information has been provided from digital forensic investigators about their experience and services available. Although several participants didn't feel like viewing illegal content daily has had a psychological impact on them, over 56.25% of the 16 participants did feel like completing this job role has left them with psychological effects. Furthermore, a total of 11 participants stated that there was not enough support available for individuals in this job role. Therefore, 56.25% of investigators are experiencing psychological effects and 68.75% state there are not enough support services available to them. This would deem the question, with these effects and lack of support services, are these investigators working to the best of their ability to uphold the integrity of all forensic cases?

From the primary and secondary research, it has become clear that a guide should be in place for the human element to help reduce the impact of psychological damage. A recommended guide for Digital

Forensic Investigation has been constructed to help assist with maintaining investigators' well-being. Mental health is a very individual topic; therefore, not one method will work for all investigators. This should be used as a guide to help employees completing this work. The proposal incorporates different coping methods based on the primary research gathered from investigators that have experienced issues from their mental health.

Environment:
Gyms
Break out rooms

Management:
Support
Case load

Debriefing Sessions

Mental Health Guide

Mental Health Unit:
Health assessments
Counselling
Anonymous phone
lines 24/7

Activities:
Group days out
Company Sports
Team

**Reduce Excessive
Overtime**

The aim of this research was to highlight if there is a correlation between digital forensic support services and the integrity of casework being completed. Although there have been improvements with the annual psychological assessments and 24/7 anonymous phone lines suggested in ACPO, there is no current guide or enforcement of such facilities within any forensic company. This, therefore, highlights a potential issue as some workers may not be in the correct psychological state to deal with such emotional cases and demanding work life, which could result in errors. However, this would be minimised with the correct support available to investigators.

To establish if this correlation is a problem, 16 participants completed a questionnaire to gather information. This has highlighted that although not all investigators need additional support services, there is a large amount that does require additional support, which they believe will help the quality of

their forensic work. A framework cannot be created for the human element whereas it has been for the investigation and business aspects, each individual will vary with the support they require, if any. Due to this, a generalised guide has been created from the feedback acquired from investigators within the industry. This guide will not be used as a framework but as ideas and suggestions that can be implemented into businesses to help improve their employees' well-being.

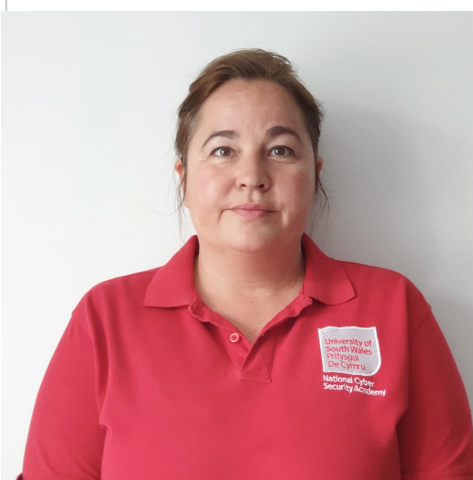
With the highlighted psychological state of, on average (according to the questionnaire), 56% of investigators struggling to deal with the content and 68% feeling further support services are required, are digital forensic companies failing their responsibility to the welfare of their employees and casework?

About Rachael

Rachael Medhurst is a graduate of the University of South Wales where she gained her Digital Forensic qualifications at both Bachelor's and Master's level. After graduating, Rachael became a Digital Forensic Investigator for a private firm that offered their assistance to a variety of forces throughout the country, while here she completed hundreds of cases and attended court as an Expert Witness. In the summer of 2018, Rachael decided to fulfill a role as a Digital Forensics and Cyber Security lecturer within the University of South Wales for their initiative BSc Applied Cyber Security program at the 'National Cyber Security Academy.



About Emma



Emma Derbi is a lecturer in Cyber Security at the University of South Wales. She received her BSc Hons Computer Forensics from the University of South Wales in 2018. She worked as a Cyber Security Engineer before becoming a Lecturer. When Emma is not lecturing, she spends her time being a mum raising her three children. Emma is currently researching new technology and how they can be forensically examined or open to vulnerabilities. She currently resides in Barry with her husband and family. She can be contacted at emmaderbi@outlook.com

Using Digital Evidence to Prove the Existence of a Canadian Common Law Marriage

by Tyler Hatch

Private digital forensics firms, as opposed to Government or Law Enforcement, investigate and produce evidence for people, businesses and those involved in civil legal disputes, primarily through their lawyers. The more that society uses technology, the more that lawyers and parties to legal proceedings turn to digital evidence to prove important and contentious aspects of their case. Legal proceedings involving couples who have ended their marriage, or a marriage-like relationship, engage private digital forensics firms often. In fact, in many cases, one of the parties will engage a private digital forensics firm *before* the relationship ends because they suspect their partner of cheating or otherwise betraying their trust.

In most cases, one party will engage a private digital firm after the relationship ends because the partner is spying on them (i.e., through spyware, keyloggers and GPS trackers), harassing them online through social media posts or by sending inappropriate or threatening text or communication app messages to them which get tendered as evidence before the Court.

This is nothing new, but my firm, located in Canada, was recently consulted by a lawyer acting for a party in a family law dispute for a unique investigation. Let me give you some context in order to understand the particular issue in this case.

Canadian law recognizes two relationships that give rise to legal rights and obligations – a legal marriage and a “common law” marriage. A legal marriage is defined by a Federal law that applies to all of Canada, but a common law marriage is defined by the applicable law in each Province and Territory in Canada. For example, in the Province of British Columbia, the Family Law Act defines the circumstances under which a common law marriage comes into existence.

A “common law” marriage is defined as a couple who has lived together in a marriage-like relationship for a continuous period of at least two years. That means that despite not having been formally married, living with a partner in a marriage-like relationship for a continuous period of at least two years may entitle them to rights in the property of the common law partner. Potentially, there could be a lot at stake if a party to a legal proceeding can prove to the Court that they were in a common law marriage with a partner who has a lot of property or earns a lot of money. Returning to the example from above, the lawyer that contacted us represented a lady who says that she lived with her partner in a marriage-like relationship for a continuous period of at least two years. Her partner said that they didn’t live together, were only casually “seeing each other” (i.e., not a marriage-like relationship) and were involved for far less time than two years. As is often the case in these situations, the two parties had completely different versions of the same set of circumstances. Digital evidence can play an important role in resolving conflicting testimony such as this. Through digital forensics examination of technology and devices, we can determine whose version of the truth is more consistent with the evidence. Accordingly, the lawyer asked me how I could assist in producing evidence that would show who was telling the truth. I found it interesting and accepted the challenge with great enthusiasm. My immediate focus was on examining any computer or mobile device that would show where the client was living and for how long they lived there. Clearly, geolocation data and wi-fi connection points would play an important part in this investigation. The client used a laptop and an Android smartphone and, therefore, had a Google account that we examined. While I am not at liberty to reference the client’s Google account due to confidentiality, I will take you on an exploratory journey of my own Google account to illustrate the many ways in which Google account evidence assisted in our investigation. By default, Google tracks GPS data of the account owner through connected devices such as smartphones, tablets and computers. That setting can be disabled if the account owner chooses to but it is enabled by default. Google accounts are private and, therefore, require the consent of the account

owner to access or a Court order to compel production. In our case, we used Magnet Forensics AXIOM Cloud tool to acquire the evidence from the Google account:

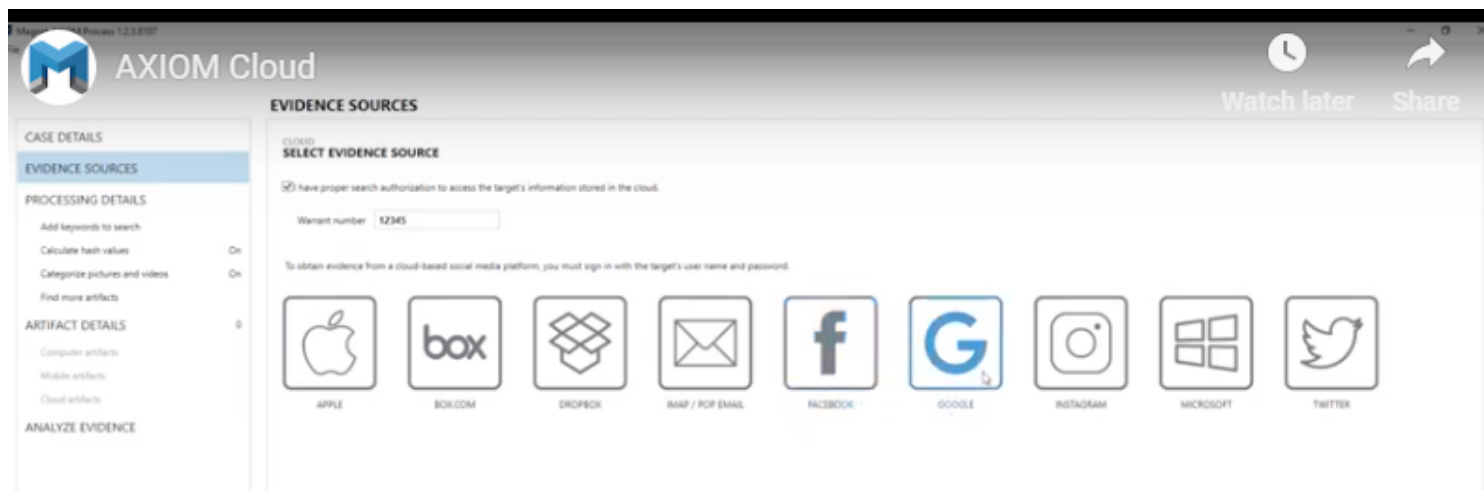


Figure 1 – Magnet Forensics AXIOM Cloud

This tool, and others like it, such as Oxygen Forensics® Detective and Cellebrite’s UFED Cloud Analyzer, acquires the entire Google account very thoroughly. In this scenario, the “Timeline” section of a Google account can be extraordinarily valuable if the subject of the investigation has had a Google account that has been recording data during the relevant period of time. In the case of my account, it has been in existence since about 2013 and has an enormous amount of location data to examine:

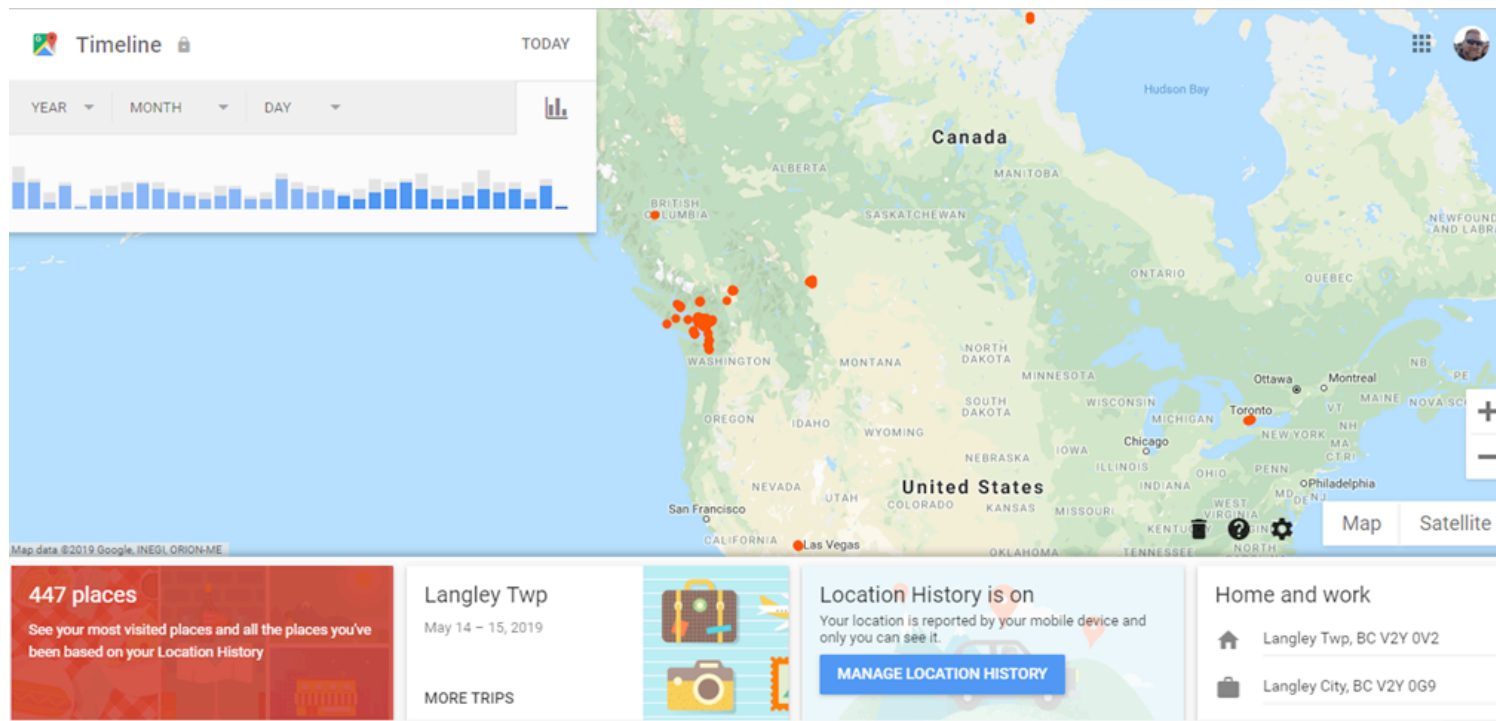


Figure 2 – “Timeline” Section of Google Account

Figure 2 is a summary of my own Google account Timeline and the 447 recorded locations that I’ve been to in the past several years are marked in red on the map. My home and work locations are also identified, which is important. It should be noted that the home and work information is set by Google automatically based on, presumably, your most frequently attended locations. In the upper left corner of Figure 2, we see that there is a filter available to examine in greater detail a particular date in the overall data set. For example, selecting the date of March 19, 2015, displays the following:

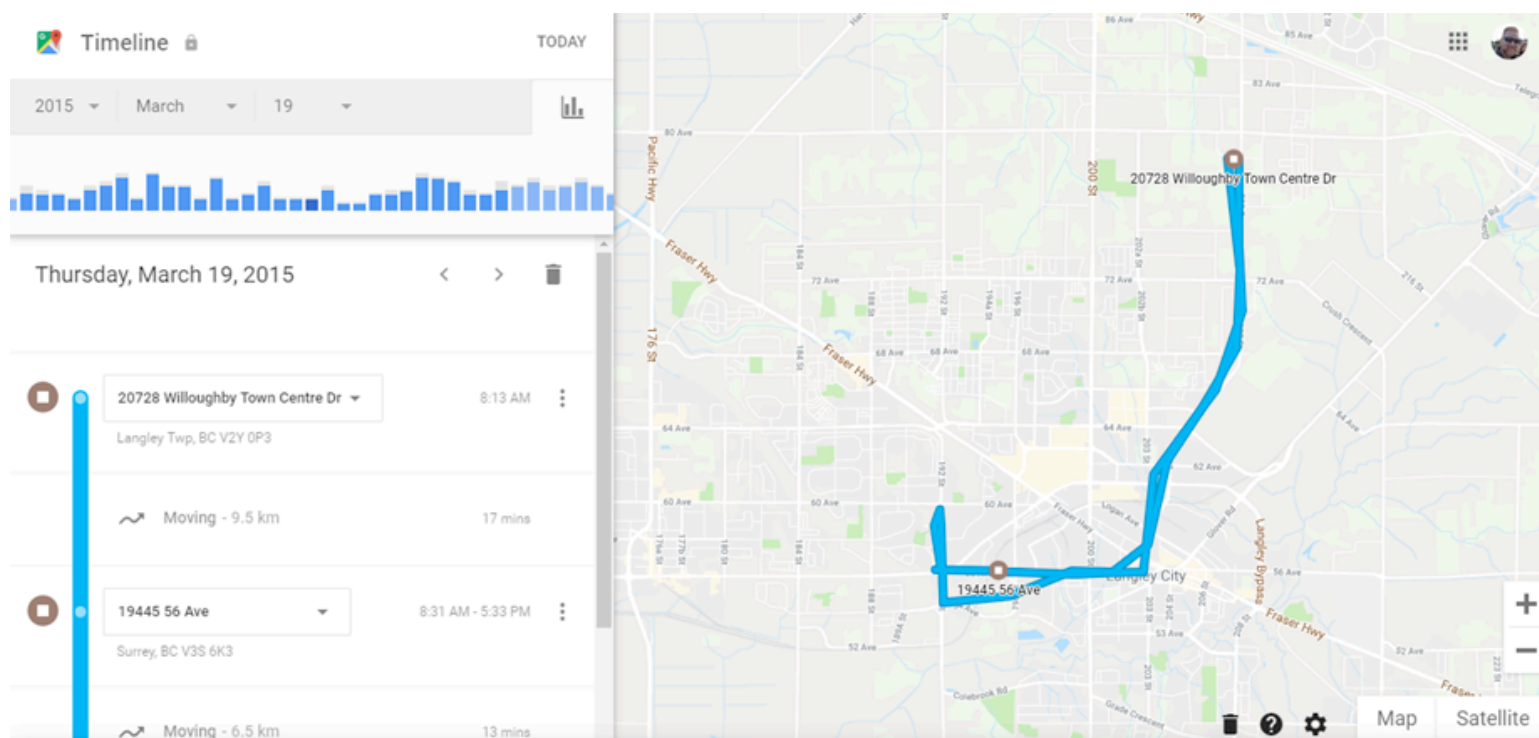


Figure 3 – Detailed Timeline View of Google Account Evidence for March 19, 2019

The location data is plotted on the map on the right side of the screen and on the left, there is detailed location information provided, including time and distance travelled. This evidence is clearly extremely valuable in determining an answer to the question of where a person was residing, when they were residing there and for how long.

As with all evidence, we must be cautious and verify it as much as possible prior to formulating a conclusion. Upon closer examination, there appeared to be many anomalies in the location evidence associated with my Timeline. In fact, there were four locations plotted on the map for which I have never travelled to. For ease of reference, I will illustrate the following two locations in Canada that my Timeline suggests I visited, but that I did not:

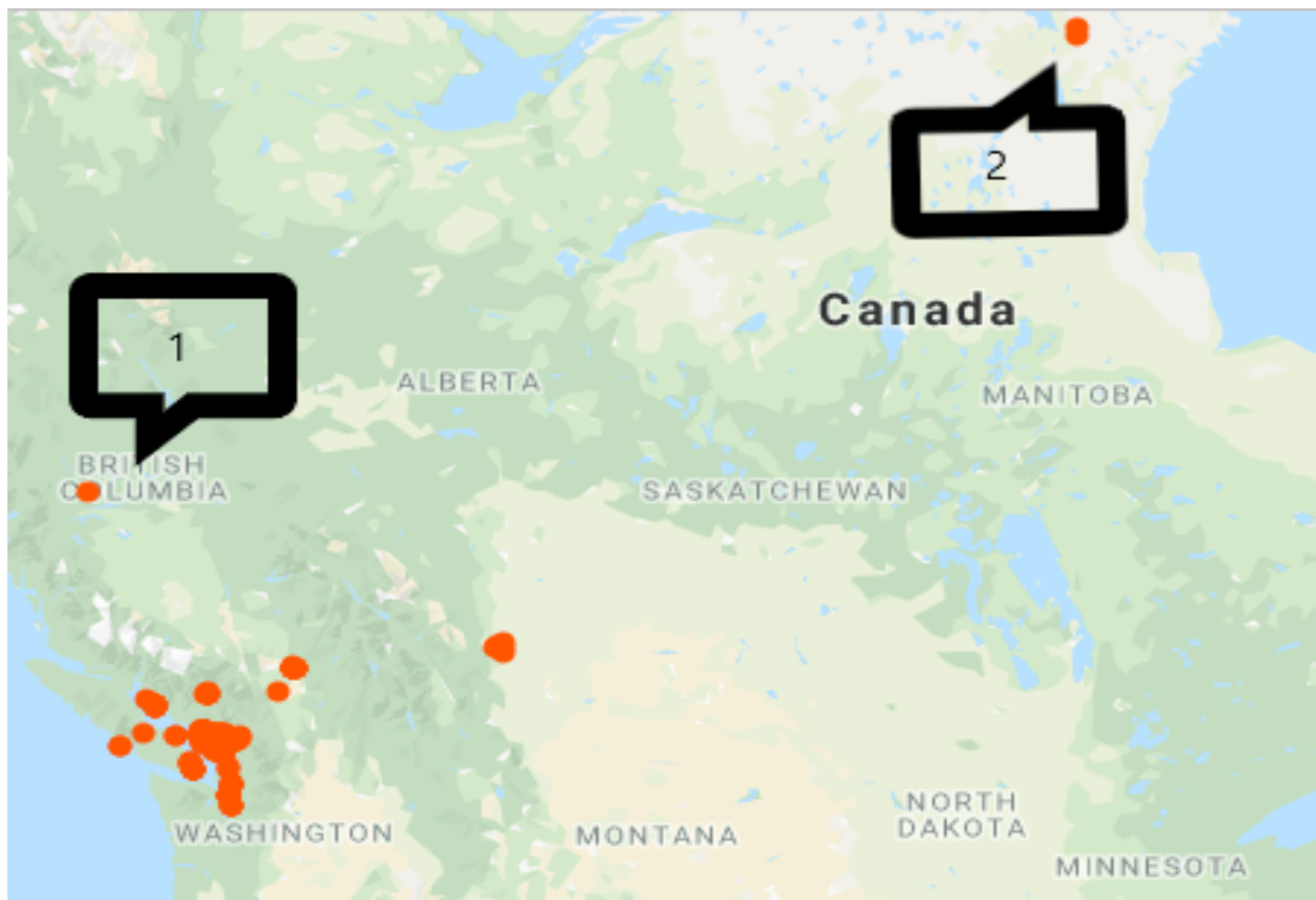


Figure 4 – Anomalous Locations from Google Account Timeline

Location #1 in Figure 4 is a location in Northern B.C., Canada, and location #2 in Figure 4 is a location in the Territory of Nunavut, Canada. As noted, I have never been to either place.

A closer examination of location #1 reveals the following details:

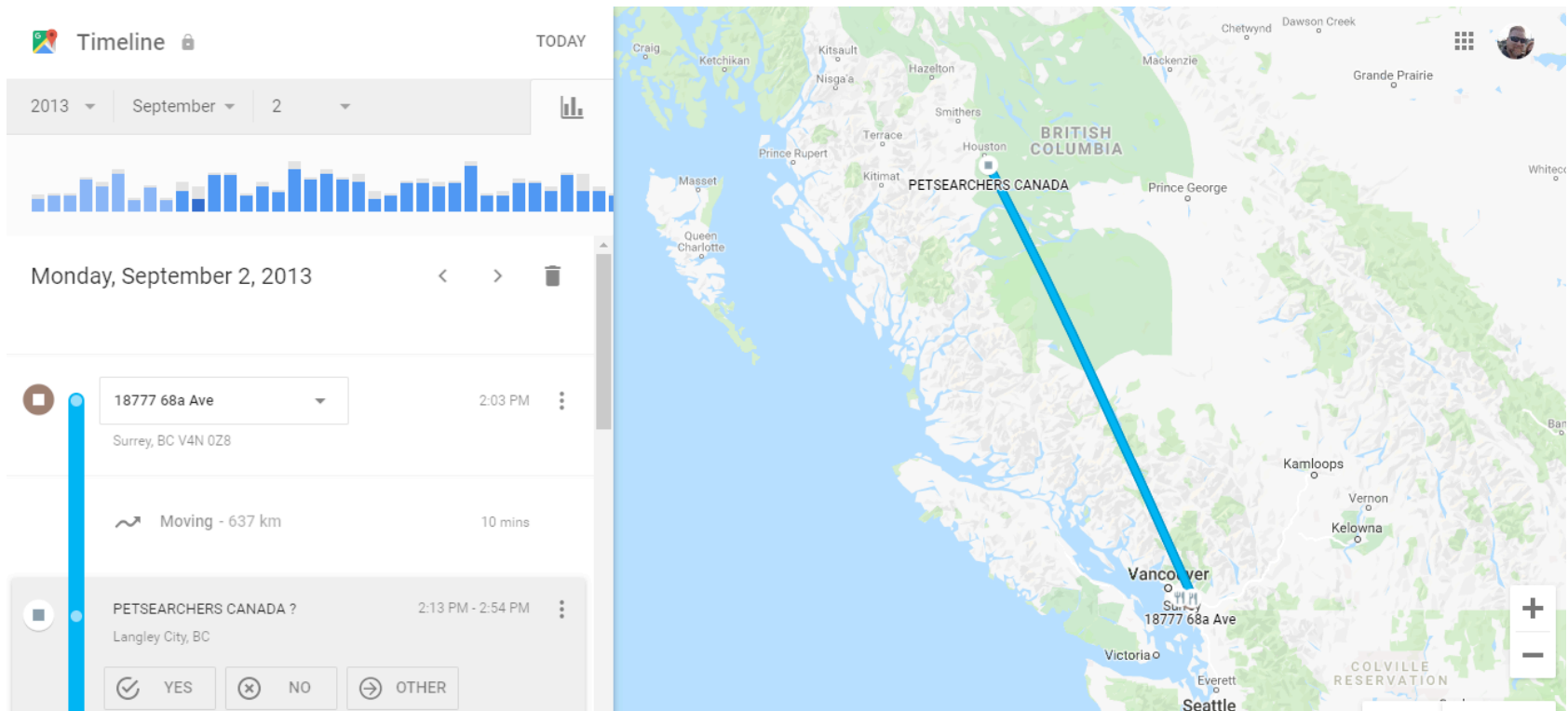


Figure 5 – Detailed view of Location #1 identified in Figure 4

Fortunately, it is fairly easy to dismiss these anomalies as unreliable data when we have a closer look. On the date in question for Figure 5, we welcomed our family dog, Buddy, to our home from Northern, B.C. He was there, not me, and it is unclear why Google indicates that I travelled between these locations. However, as it is indicated on the left side of the screen that the travel distance was 637 kms in a mere ten minutes, we can reasonably dismiss this as inaccurate information.

Similarly, a closer examination of location #2 from Figure 4 reveals the following details:

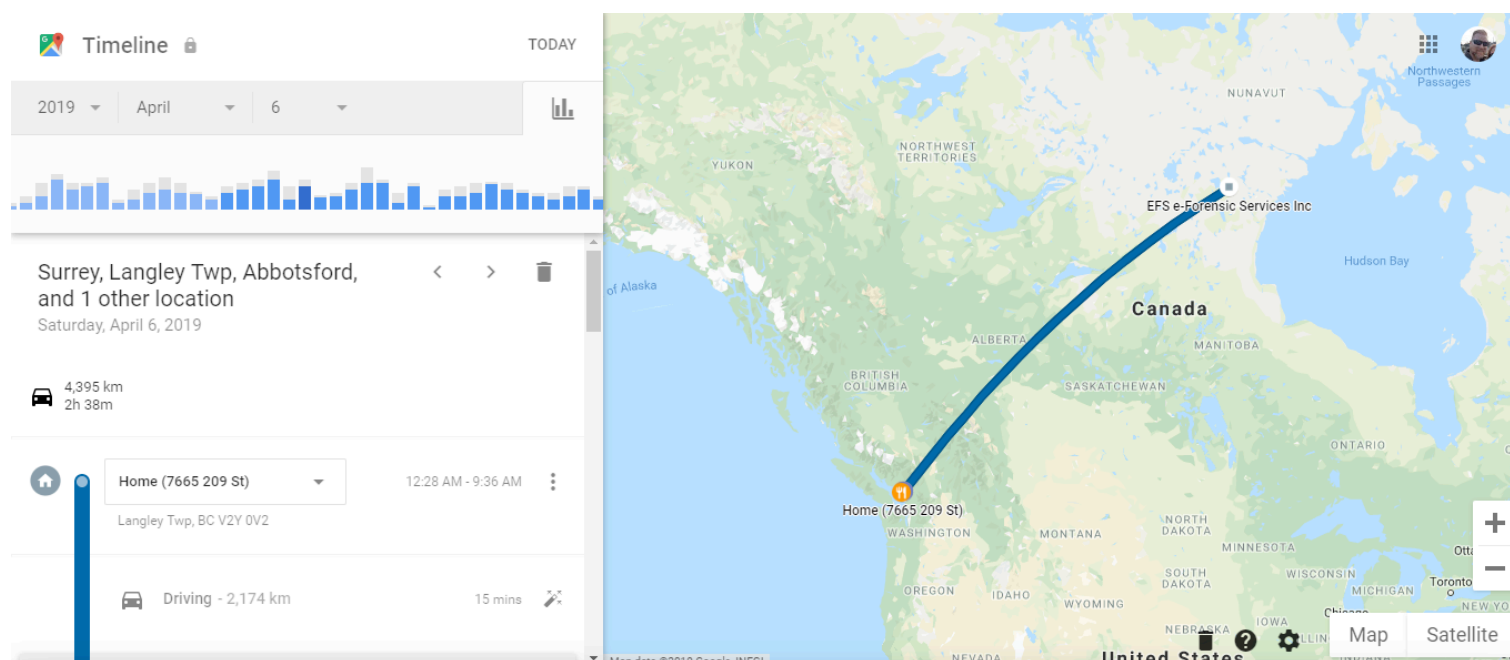


Figure 6 - Detailed view of Location #2 identified in Figure 4

The identified location, “EFS e-Forensics Services Inc.”, is incorrectly plotted on the map as being thousands of kilometers farther away than it actually is. Again, Google shows the distance and time travelled as being 2,174 kms in 15 minutes so we can be reasonably certain that it is an error and dismiss this information. This example illustrates the principle that all forensics examiners should examine data for inaccuracies and be prepared to explain them under scrutiny or cross-examination at trial. While Google account data is clearly one of the more comprehensive sources of evidence for this type of investigation, it is not the only one. In fact, there may be several others, depending on the device(s) available and the particular user. As mentioned, connections to wi-fi networks are common sources of evidence that are readily available to investigators when extracting data from smartphones as are other geolocation sources of evidence such as metadata from image and video files. The following illustrations from a typical Cellebrite iPhone 6s extraction are examples of potentially useful evidence:

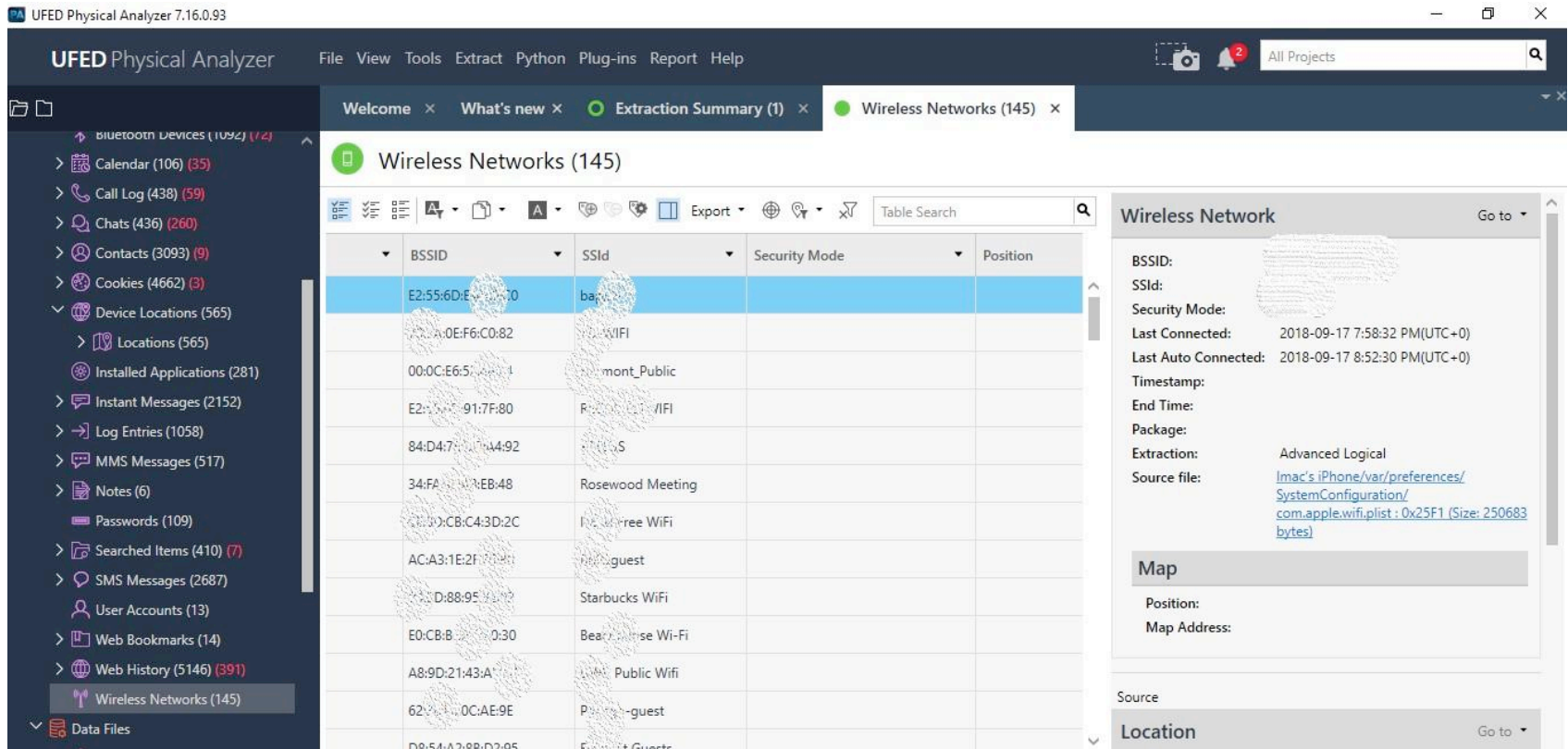


Figure 7 – Cellebrite Extraction Data of Connected Wi-Fi Networks from Target Device (Portions Redacted for Confidentiality)

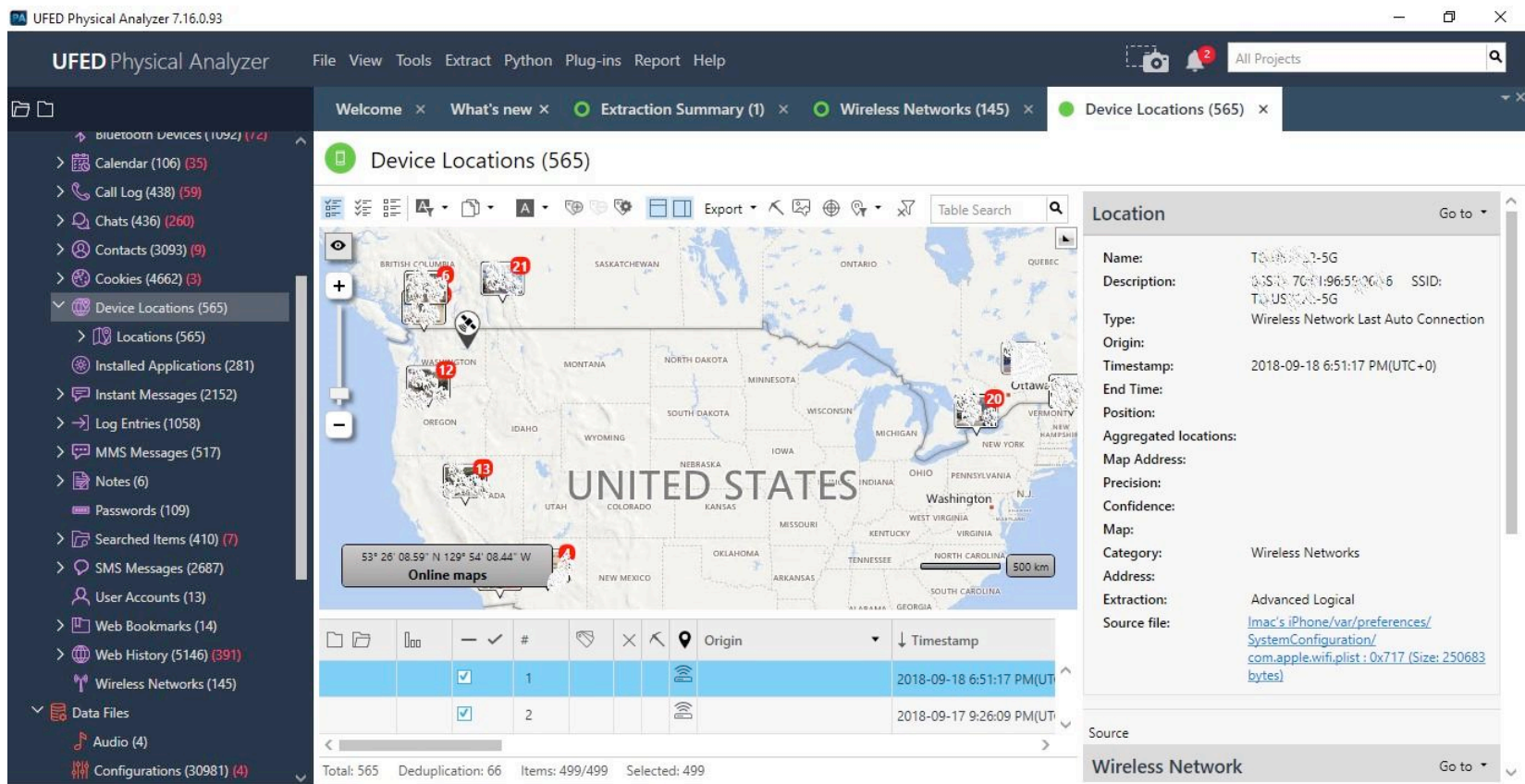


Figure 8 – Cellebrite Location Data Acquired from Sources on Target Device (Portions Redacted for Confidentiality)

Other potential sources of digital evidence to establish location, residence and duration of residence would be:

1. Apple Maps;
2. Waze (a Google traffic app);
3. Mileage Tracker apps, such as Microsoft's MileIQ, used to record business travel for tax purposes;
4. Health and Fitness Trackers that may record exercise activity such as jogging around one's neighbourhood;
5. Social Media posts that use a feature like Facebook's "check-in" to establish where one was, when and with whom; and
6. Many other sources from apps, cloud accounts and mobile devices.

One of the extraordinarily fun aspects of being a digital forensics investigator is that we get to use creativity and knowledge of technology to benefit our clients in the pursuit of the truth! Embrace your creativity and always keep up with the latest digital technology to stay on the cutting edge of digital investigations.

About the Author



Tyler Hatch is the founder and CEO of DFI Forensics Inc., a Canadian-based digital forensics and cyber security firm that services clients in North America. Tyler is a former practicing litigation lawyer with a keen investigative mind and a passion for digital forensics. Tyler is also a certified computer (CCFE) and mobile (CMFE) forensics examiner. Learn more at <https://dfiforensics.ca>

Digital Forensics and Threat Hunting

by Gerard Johansen

“When you don’t hunt the threat, the threat hunts you” - Eric O’Neil, National Security Strategist, Carbon Black

Introduction

With the release of Mandiant’s APT1 report, information security and incident response professionals were able to get a deeper understanding of the threat that nation state hacking, such as the Chinese PLA Unit 61398, represent to organizations. As time has charged on, security professionals have also seen the advent of nation state capabilities and tools in the hands of cyber-criminal gangs and even lone adversaries. This was brought to the forefront when the hacking group Shadow Brokers released the cache of tools that was pilfered from the United States National Security Agency (NSA). This in effect placed nation state capabilities in the hands of anyone with internet access, greatly increasing the threat to organizations worldwide.

Further demonstrating the threats that are present are various data breach studies that attempt to ascertain the amount of time it takes an organization to identify a data breach. The IBM/Ponemon Institute *2018 Cost of a Data Breach Study: Global Overview* report indicated that of the 477 organizations that experienced a data breach over the preceding 12 months took an average of 197 days to detect the breach. This equates to having a malicious actor or actors within the enterprise network for over half a year. It does not take a stretch of the imagination to conjure up what damage can be done in that time.

Coupled together, the ability of hackers at every level to utilize sophisticated attack tools and organizations' inability to detect equates to a significant risk. As a result, organizations and individual practitioners need to move to a more proactive approach in addressing these threats. One of these methods is the practice of Threat Hunting. What follows is an overview of this practice and examples of where digital forensic techniques can be utilized proactively to identify and eliminate threats.

Threat Hunting

In order to address the risks associated with an adversary having prolonged access to the network, many organizations have developed threat hunting programs. These programs often incorporate Security Operations Center (SOC), incident response or digital forensics personnel as these individuals often have the technical expertise and skills necessary to make threat hunting successful.

Before going any deeper though, it is necessary to formalize a definition of threat hunting. The security company Sqrrl defines threat hunting as; "the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions". Threat hunting is proactive in nature. The practice does not rely on preconfigured Intrusion Detection or Prevention alerts, but rather a combination of manual processes and automated assistance with the ultimate goal of finding malicious activity that has gone previously undetected. The heart of threat hunting is an active defense process that is led by human intelligence, leveraging automated and manual security tools, digital forensic techniques and threat intelligence to identify threats that have not been previously identified.

Threat Hunting Cycle

Like many aspects of digital forensics and incident response, there is a generally defined process to threat hunting. While there is no specific threat hunting process, there is a general work-flow as to how a threat hunt is initiated, conducted and concluded. Figure 1 visualizes one such process that guides threat hunters through the various stages in order to facilitate a successful hunt.



Figure 1 - Threat Hunting Cycle

Initiating Event

The threat hunt begins with an Initiating Event. This can be simply a security driven process or procedure that dictates that threat hunting is conducted on a periodic basis, say monthly or quarterly. Additional Initiating Events may include an alert from a government agency or other organization concerning a new or emerging threat. Figure 2 shows one such report below where the United States Federal Bureau of Investigation (FBI) has indicated new Indicators of Compromise (IOCs) associated with the Ryuk family of ransomware (<http://image.communications.cyber.nj.gov/lib/fe3e15707564047c7c1270/m/1/23a5f86b-847f-4425-af2c-0a9ea8d24d59.pdf>). Alerts such as these often serve as the driver behind initiating a threat hunt.



02 MAY 019

Alert Number
MC-000103-MW

**WE NEED YOUR
HELP!**

If you find any of these indicators on your networks, or have related information, please contact

**FBI CYWATCH
immediately.**

Email:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been **TLP:WHITE**: Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Indicators of Compromise Associated with Ryuk Ransomware

Summary

Unknown cybercriminals have targeted more than 100 US and international businesses with Ryuk ransomware since approximately August 2018. Ryuk encrypts files on network shares and an infected computer's filesystem. Once the victim has been compromised, the actors encrypt all the network's files and demand sums of up to \$5 million worth of Bitcoin (BTC) in exchange for a decryptor program. Ryuk's targets are varied and indiscriminate, but attacks focus on organizations with high annual revenues in hopes of extracting larger ransoms from the victims. While Ryuk is generally undiscerning about victims, attacks have had a disproportionate impact on logistics companies, technology companies, and small municipalities.

Figure 2 - FBI Flash Intel Report

Create Working Hypothesis

At this stage of the threat hunt cycle, there has been an initiation of the hunt. From here, the threat hunters will need to craft a Working Hypothesis. This hypothesis will be used to focus the threat hunt on those data and intelligence sources that are relevant to the threat. An over generalized hypothesis such as "there is an adversary that is in control of systems on the network" is not specific enough to be of use. This does not give the threat hunters a concrete focus area. A better hypothesis would be "An adversary has compromised the web servers in the DMZ and has established a Command and Control channel". This gives the threat hunters concrete focus areas in which to examine.

Often, a threat intelligence report or alert has initiated the threat hunt. In this case, the intelligence report can be used to craft the hypothesis to match the data contained within. For example, an examination of the FBI Flash report in Figure 3 shows specific information on how Ryuk is spread on an internal network. In this case, through the use of SMB.

The exact infection vector remains unknown as Ryuk deletes all files related to the dropper used to deploy the malware. In some cases, Ryuk has been deployed secondary to Trickbot and/or Emotet banking Trojans, which use Server Message Block (SMB) protocols to propagate through the network and can be used to steal credentials.

Figure 3 - FBI Flash Intel Detail

From here, the threat hunters can craft a hypothesis such as “An adversary utilizes a dropper to drop malware on an internal system. After the initial infection, the Ryuk malware attempts to move laterally via the Windows Server Message Block”. This hypothesis provides a concrete set of parameters that the threat hunters can use moving forward such as examining suspicious SMB connections between hosts.

In those threat hunts where the initiating event is not driven by a specific threat intelligence or alert, but maybe driven by a threat hunting schedule, one tool that is useful to craft a hypothesis is the MITRE ATT&CK Framework. This framework is a knowledge base of adversary Tactics, Techniques and Procedures (TTPs) that have been observed. This framework can be leveraged to create a hypothesis that matches realistic real-world attacks.

For example, one attack that is often seen by incident responders is the use of PowerShell for the delivery of malware as well as lateral movement. When examining the MITRE ATT&CK Framework attack “T1086” (<https://attack.mitre.org/techniques/T1086>), hunters are provided details about the attack, and adversary groups are utilizing this attack as well as data sources that can be leveraged for detection. From here, threat hunters can identify specific uses of PowerShell by groups and types of malware. This can be utilized to craft a hypothesis that allows threat hunters to focus on the malicious use of PowerShell and PowerShell Empire (<https://www.powershell empire.com>) within their environment.

Leverage Threat Intelligence

Timely and accurate intelligence on threat actors and more specifically, how these threat actors operate, is invaluable to threat hunters. When examining threat intelligence, the information can be broken down into three broad categories:

- **Indicators of Compromise (IOCs):** These are indicators that are found on compromised systems, often through digital forensic techniques, that indicate an adversary has successfully attacked and compromised the system. There are a broad range of IOCs ranging from IP addresses contained within the memory indicating Command and Control to registry key settings and event logs that indicate the execution of malware or other exploits.
- **Indicators of Attack (IOAs):** As opposed to IOCs, IOAs are indicative of an attack that may or may not have been successful. Similar to IOCs, there are a broad range of IOAs. For example, an unsuccessful brute force attack against an SSH login by an external IP address would be an indicator that an adversary is attacking a system.
- **Tactics, Techniques and Procedures (TTPs):** These are the methods that attackers will use to compromise a system. TTPs are generally higher-level descriptions rather than specific hash values for malware or IP addresses for command and control infrastructure, normally associated with IOCs. For example, TTPs for a fictitious hacking group called AtomicRabbit might be defined as a phishing email containing a PDF document with an embedded PowerShell script. This PowerShell script makes use of the PowerShell Empire suite of tools that downloads a second stage of malware that takes control of the system and establishes command and control.

Once a hypothesis is created, threat hunters should build an accurate dossier on what indicators and TTPs are available related to that hypothesis. Take for example the hypothesis concerning the execution of a Ryuk attack. The hypothesis is based on information indicating that a dropper such as Trickbot or Emotet are utilized to infect the system. A search of AlienVault's Open Threat Exchange reveals a number of up-to-date URLs that are associated with Emotet.

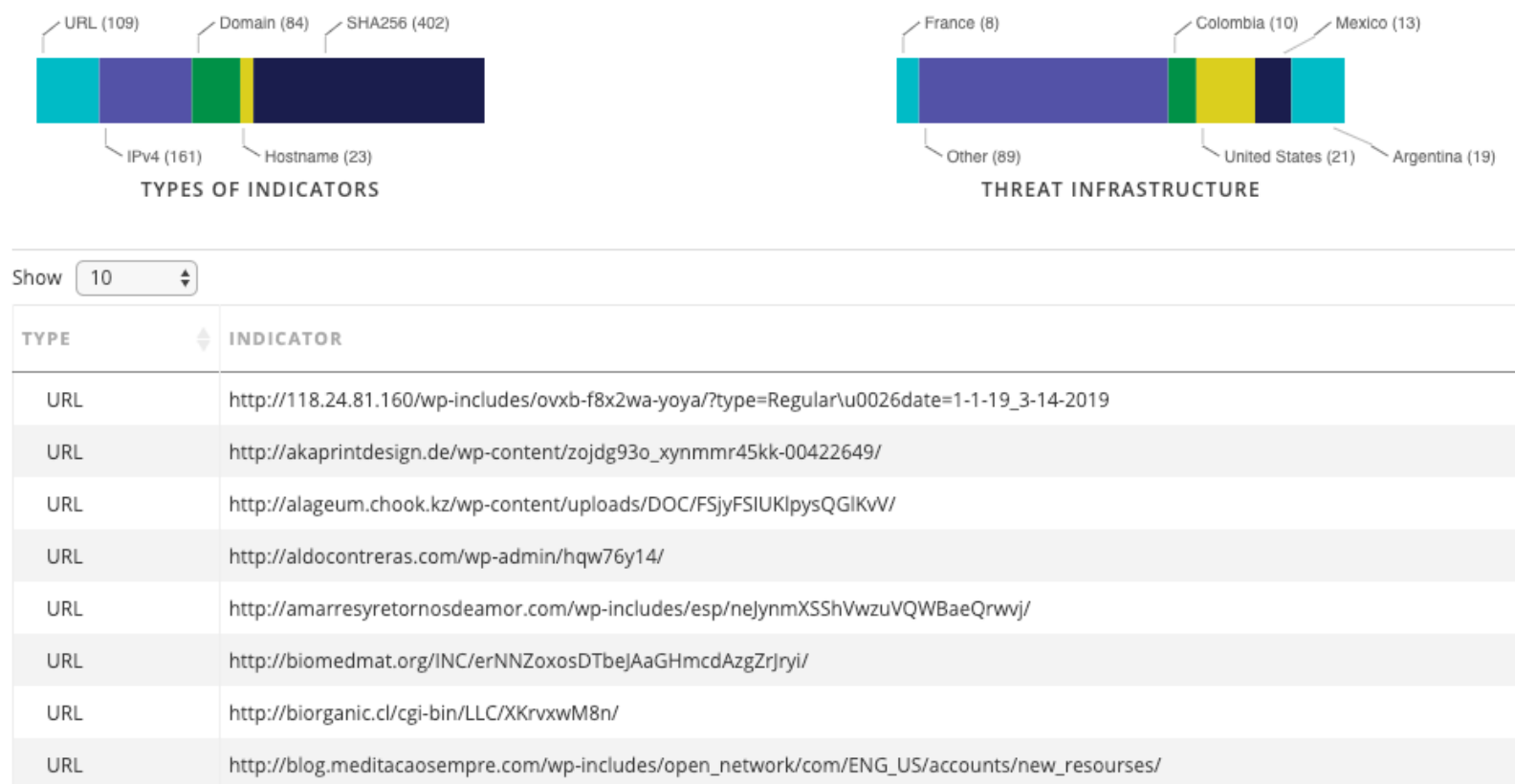


Figure 4 - Emotet Threat Intelligence

From here, threat hunters have specific IOCs associated with Emotet and Ryuk that can be leveraged as they move into the application of forensic techniques. Having accurate and timely threat intelligence allows threat hunters to fine tune their targeting of threats and produces better results.

Apply Forensic Techniques

Threat hunts require detailed examination of systems, logs and other evidence. As a result, threat hunters should have a solid foundation of digital forensics training and experience. Further, digital forensic examiners should proceed in examining digital evidence in the same manner they would if they had clear evidence a system has been compromised. This approach allows for detailed examination and reporting while maintaining the integrity of the evidence in the event that the threat hunt determines a compromise has occurred.

Although not an exhaustive list, the following are some of the digital forensic focus areas that are applicable during threat hunts:

- Log Analysis: Comprehensive logging of host and network activity is critical to facilitate a productive threat hunt. Windows Security Event logs are a treasure trove of data that can indicate malicious activity. For example, the Windows Sysinternal tool PsExec is used by threat actors to push malicious code to other systems on the network. Using the Windows Security Event IDs 4688 and 4689 along with a search for the term “psexec” can show threat hunters where this tool has been used in the environment. When discussing log analysis, there are too many specific use cases to address in this overview. One of the best approaches an organization can take to properly configure their security controls to facilitate deeper threat hunts is to configure their systems to log activity, aggregate those logs in a central location and implement some form of event management system on which to perform log reviews.
- Disk Artifacts: While system storage provides a wealth of evidence for much of a digital forensic examiner to address, the time necessary to fully examine a disk can be time consuming in threat hunting. Threat hunters should focus on a few key elements found on the disk as part of the threat hunt. First, the Pagefile is an excellent first step. Focusing string searches on several key words such as “Mimikatz”, “PowerShell” and “Meterpreter” along with regular expressions for URLs and IP addresses, threat hunters are able to ascertain if a system may have been compromised. Second, the Master File Table should be reviewed for entries indicative of attacks such as the addition of malware or hacking tools. Finally, the Prefetch files offer some evidentiary value in determining code execution.
- Memory Analysis: With the increased use of file-less malware, the running memory of high-risk systems such as web servers, domain controllers and file servers should be reviewed. The running memory represents a significant evidence source in threat hunting. Threat hunters can examine memory for suspicious processes, command and control connections and code execution among a host of other potential areas.
- Network Analysis: Network traffic is also a good source of evidence during threat hunts. Attacks that compromise internal systems will most likely have a lateral movement component to it. Having the ability to examine historical Netflow will allow threat hunters to identify lateral movement. Another source of evidence that can be leveraged are packet captures. Capturing network traffic at key points

such as firewalls, routers and switches can be evaluated for signs of command and control traffic, exploit traffic and other remote access techniques.

Threat hunters should not feel limited to these tools and techniques. Furthermore, examining existing processes, tools and techniques for areas where automation is possible will allow threat hunters to process more data, examine more systems, hunt for specific IOCs and focus their energies on new and emerging threats.

Identify New TTPs, IOCs, and IOAs

It is often the case that during a threat hunt, new IOCs, IOAs or TTPs are discovered. In general, the following are the top ten IOCs or IOAs that maybe identified during a threat hunt:

1. Unusual Outbound Network Traffic
2. Anomalies in Privileged User Accounts
3. Geographical Anomalies
4. Excessive Log-In Failures
5. Excessive Database Read Volume
6. HTML Response Sizes
7. Excessive File Requests
8. Port-Application Mismatch
9. Suspicious Registry or System File Changes
10. DNS Request Anomalies

Any additional indicators that are discovered indicating a potential compromise should be addressed with the appropriate incident response plan. Indicators may also indicate unsuccessful attacks and should be documented for the follow-on stage. Access to threat intelligence can help enrich any new indicators that are identified as well, providing additional context.

Enrich Existing Hypothesis

In general, the hypothesis that began the threat hunt is often not going to survive the entire threat hunt cycle unchanged. For example, a threat hunt team may be examining SIEM logs for signs of lateral movement via SMB. During the examination, they see a particular system that is attempting unsuccessfully to connect to a server. After an examination of that system, the team determines that at some point, a remote access tool has been installed. They further identify an IP address that the system beacons out to. Leveraging threat intelligence, they determine that the IP address is a known botnet. From here, the team removes the infected system from the network. The new IOC, the IP address and the malicious remote access tool, now serves as new data points and an updated hypothesis is created. The updated hypothesis will move the threat hunt team towards examining for indicators of a remote access tool that communicates with an identified botnet. From here, the cycle can begin again.

Making a Plan

Structuring a threat hunt does not require an extensive amount of planning but before a threat hunt can begin, there are a few questions that need to be answered. First, what is the team looking for? This is best addressed by a properly constructed hypothesis. Second, what evidence sources are available? Third, are there intelligence sources that can be leveraged?

Finally, based on the first two questions, what digital forensics or security tools are necessary to perform the hunt? A brief plan of action that answers these questions will often suffice for organizations that are just at the beginning of incorporating threat hunting into their security operations.

A concise plan can easily be written out with the following elements that address the questions necessary to conduct a hunt:

- **Hypothesis:** A brief one or two sentence statement that outlines the hypothesis. This provides everyone involved in the threat hunt a clear understanding of what to look for.
- **Sources:** The plan should include a listing of digital forensics sources that can be examined as part of the threat hunt.

- **Threat Intelligence:** Any specific threat intelligence that is relevant to the threat hunt should be included as part of the plan. The plan does not necessarily require a complete list of IOCs but should include those sources that can provide such detail.
- **Tools:** A list of digital forensic and security tools that are available for the threat hunt. These can be a combination of open source and commercial tools and should account for different tools in use by threat hunters.
- **Scope:** The scope in terms of systems or network segments should be clearly defined. An overly broad scope may require too much time to address. In the early stages of threat hunting within an enterprise, it is best to keep the scope smaller as this allows for a team to develop expertise and to make improvements to the process.
- **Timeframe:** The timeframe is largely dependent on the systems, evidence sources and tool set. The application of digital forensics to some areas of evidence are not based on a specific timeframe, for example, the analysis of running memory captures the state of the system at that date and time. Log reviews, on the other hand, require a specific time period. If, for example, there are only 90 days of logs available, the threat hunt team may specify that the last 90 days of logs are to be reviewed as part of the threat hunt.

Depending on the threat hunt, the plan can be very simple, such as the sample plan in Figure 5. Other, more complex threat hunts that involve a wider scope, timeframe, and personnel may require much more detailed planning and workflows. This ensures that personnel are working on their defined scope and systems without overlap. Finally, it ensures that all systems that should be part of the hunt are included.

Hypothesis	<ul style="list-style-type: none"> • An adversary has compromised a webserver in the DMZ and has placed a Remote Access Trojan to maintain control.
Sources	<ul style="list-style-type: none"> • Windows Event Logs, Memory Capture, Pagefile • IIS Logs, Master File Table
Threat Intelligence	<ul style="list-style-type: none"> • VirusTotal • Alien Vault OTX • US-CERT
Tools	<ul style="list-style-type: none"> • Event log review tool • Memory capture and analysis utility • File Search tools
Scope	<ul style="list-style-type: none"> • All Webservers in the DMZ
Timeframe	<ul style="list-style-type: none"> • Last 90 Days for Log Reviews

Figure 5 - Sample Threat Hunt Plan

Conclusion

Relying on passive detective controls is not addressing the threats to today's organizations. Threat hunting puts the security personnel into an active defense mode that drives quicker detection of adversaries, maximizes the security technology and optimization of the defensive measures. As threats rapidly evolve and change their Tactics, Techniques and Procedures, organizations will have to adopt the ability to hunt the threats because to not do so allows the threat to hunt them.

About the Author



Gerard Johansen, CISSP is an incident response professional with over a decade of experience in a variety of information security disciplines including digital forensics, incident response and threat intelligence integration. Prior to working in the private sector, Gerard spend 10 years working in state and federal law enforcement, including five years specifically within the digital forensics and cyber-crime investigation fields. Gerard has completed several training programs specifically addressing digital forensics and incident response and has also obtained the SANS GIAC Certified Forensic Analyst and the SANS GIAC Certified Threat Intelligence certifications. He is a graduate of Norwich University's Master of Science in Information Assurance where he focused study on vulnerability management and Incident Response. Gerard is currently an incident response

consultant for a major technology company.

Forensic technologies to mitigate risks of financial crime

by Florence Love Nkosi

The current technological advancements within the finance sector, together with the emergence of innovative technologies like mobile and internet banking, that have allowed for fast and effective transaction processing, at the same time have opened up increasing opportunities for criminal activity perpetrated through technology. Consequently, there has been a notable increase in the approach and sophistication of financial crimes committed through the use of technology, such as money laundering, terrorism financing, cybercrime, fraud, tax evasion, bribery and internal threats from employees.

INTRODUCTION

The current technological advancements within the finance sector, together with the emergence of innovative technologies like mobile and internet banking, that have allowed for fast and effective transaction processing, at the same time have opened up increasing opportunities for criminal activity perpetrated through technology. Consequently, there has been a notable increase in the approach and sophistication of financial crimes committed through

the use of technology, such as money laundering, terrorism financing, cybercrime, fraud, tax evasion, bribery and internal threats from employees. At least 49% of financial institutions and 37% of companies on average had reported being victims of financial crime (PwC, 2016). Interpol defines financial crime to be closely related to cybercrime as they are both committed via the internet and have a major impact on international banking and the financial sector (Interpol, n.d). Likewise, there has been an

acute increase in financial crime perpetrated using various computer accounting packages and information systems.

Financial institutions are continuously faced with the challenge to mitigate the risk of financial crime in order to avoid financial loss and getting a bad reputation. As technology advances, data of financial transactions can be easily hidden in the cloud and other devices, like smartphones and laptops, making it easy for criminals to distort evidence and hard for investigators to uncover details of the financial crime. It is very important for financial institutions to adapt quickly in order to stay ahead in the technology arms (Markson, Towey, & Welford, 2018), by implementing technologies that assist in timely detection and prevention of technologically perpetrated financial crime. Forensic technologies are key to uncovering fraud since they preserve and analyse all the necessary evidence that can be used in further investigation or presented in a court of law. As defined by IGI Global, forensic technologies are used for investigating and identification of facts surrounding a crime (IGI Global, n.d.), and are mainly used to preserve and analyse data in order to determine any outliers that are indicative of fraud.

Financial institutions need to focus on implementing technologies that help to investigate and mitigate financial crime, but are also robust enough to be used in forensic investigations. Technologies like Artificial Intelligence and Machine Learning, data analytics and blockchain technologies are among the tools that are being used to develop solutions that are key to preventing and detecting financial crime. Thus the article discusses these technologies and how they work as forensic technologies. Further to that, the article makes mention of a few known software solutions that have applied machine learning and data analytics to assist financial institutions mitigate the risk of fraud and other financial crimes.

MACHINE LEARNING (ML) AND ARTIFICIAL INTELLIGENCE (AI)

Machine learning uses algorithms to detect patterns, predict outcomes and potentially operate autonomously — to mine bank data and find anomalies (Goldstein, 2017). Machine learning can therefore be used to automate aspects of the review process, by building models based on gathered data to determine the likelihood of a transaction being fraudulent. Thus, forensic rules used to determine whether a transaction is fraudulent or not can then be

embedded into Machine Learning models to analyse and categorise transactions as they come.

In a way, this reduces the need for post-forensic analysis and allows for instant investigation and categorisation of a transaction as fraudulent or not right before it is processed. The significance of Machine Learning models is that they do not just focus on configured rules to categorise a transaction, but also take into consideration other relationships and qualities of the transactions that may be indicative of a financial crime. Thus, they detect those suspicious patterns and relationships invisible to experts. Furthermore, ML models can be configured to flag high risk transactions before they are processed, in a way, eliminating the risk of false positives and allowing for investigators to zero in on high risk transactions before they are processed.

Banks and other financial institutions are already making use of Machine Learning and Artificial intelligence in financial crime risk management activities like transactions monitoring in order to identify suspicious transactions. Machine learning offers efficient and agile solutions by transforming how financial institutions deal with financial crime. Nonetheless, financial institutions

need to adapt quickly in order to stay ahead of sophisticated technology tricks being used by criminals to avoid being caught.

DATA ANALYTICS

Data analytics tools can mine through digital data and identify hidden relationships and red flags thereby enabling banks to proactively identify potential fraudulent transactions before they manifest themselves years down the line (Deloitte, 2013). On the other hand, Forensic Data Analytics (FDA) relates to the ability to collect and use structured and unstructured data to identify potentially improper payments, patterns of behaviour and trends (EY, 2017). Thus FDA plays a critical role in detecting potential fraud. FDA is used to develop in-house resources that can detect potential fraud. However, advanced technologies that incorporate data visualization, statistical analyses and text mining concepts can also be incorporated into in-house developed software to make the tools more effective and efficient. Data analytics driven tools tackle large volumes of both historic and current data to determine patterns and relationships that are fraudulent in nature and could otherwise have gone unnoticed. Predominantly, banks have applied predictive analytics for behaviour

monitoring, network analysis, pattern recognition, and profiling to fight financial crime.

For forensic investigation purposes, data analytics provide a platform to extract data and perform an in-depth analysis in order to identify outliers that need investigation and remediation.

Data analytics is a significant tool for extracting the evidence needed during investigation and key in reporting the necessary details that may be required to be presented in a court of law. This may also be largely because most of the analytics tools are developed in-house by various banks and financial institutions to meet their particular requirements.

By far, data analytics provide a better ability to detect financial crime but also facilitate prevention of suspicious transactions by highlighting suspicious transactions. Integrating data analytics with continuous monitoring and analytics tools like ACL, further provide a rapid response to flagging fraudulent transactions in real time or near real time, thus allowing for thorough investigations to be conducted to ascertain the originality and authenticity of a transaction before it is finalised, in a way, saving millions of dollars that would have been lost. More so, there is a spectrum of analysis that can be deployed to detect fraud, that ranges from

point-in time analysis conducted in an ad hoc context for one-off fraud investigation or exploration, through to repetitive analysis of business where fraud is likely to occur (ACL, 2014).

BLOCKCHAIN

Blockchain technology appears to be a huge opportunity for the banking and financial sector to mitigate crime. The blockchain is a distributed ledger technology and verification system for financial transactions, thus blockchain uses a publicly-viewed ledger to record and keep track of transactions (Patel, 2018). For financial institutions, blockchain technology has enormous potential for internal controls, but also for improving regulatory compliance. Blockchain can also be explained as a secure shared distributed ledger through which banks can record transactions and work together to validate updates.

Blockchain technology provides a platform where a transaction can be authenticated by both people involved. Blockchain works by assigning cryptographic keys to the transaction between person A and B, which then creates a block that is validated by a distributed network before it is attached to the blockchain where it creates a permanent record of the transaction.

Thus, taking advantage of the blockchain provides increased power to detect and prevent fraudulent transactions by decentralizing the data, requiring multiple sources to validate a new piece of data before it is approved, plus making transmitted data unalterable, thereby greatly reducing the risk of fraudulent transactions.

Its ability to cryptographically sign transactions could be a much more authoritative means of recording transactions versus a relational database that can be accessed and manipulated. So far, it also provides customers and insurers with means to manage claims in a transparent, responsive and irrefutable manner. Blockchain-smart contracts can be beneficial to insurance, to reject multiple claims for one accident because the network would know that the claim has already been made. Undoubtedly, blockchain technology will continue to play a major role in regulatory reporting and identity management for financial institutions in the years to come.

Blockchain works as a many-in-one tool for managing risk of financial crime, by allowing a transaction to be vetted by both initiator and receiver, by adding the transaction to a block so that it is preserved for further investigations if need be. For forensic purposes, blockchain

maintains a definite trail of records that can be checked when the need arises.

ARTIFICIAL INTELLIGENCE AND DATA ANALYTICS APPLICATION FOR FORENSIC PURPOSES

Artificial Intelligence and data analytics are predominantly used in various software tools to mitigate the risk of financial crime through analysis and detection of potential fraudulent and financial crime transactions. Most of these tools are developed in-house and customised to meet the requirements and objectives of the particular institution. The overlaying forensic tools can be a combination of data analytics or AI together with other technologies like data mining, visualisation, continuous audit and monitoring tools among others. While data analytics apply specific rules to identify suspicious transaction, continuous monitoring techniques work to constantly test and flag transactions that are suspicious and could potentially be a financial crime. On the other hand, data mining techniques categorise already known patterns as fraud and explore new patterns and relationships susceptible to be financial crime.

Although there is a wide disbursement of forensic technologies being used to mitigate

financial crime, there is no particular tool that is dominating the market. The following tools apply various techniques to aid in mitigating financial crime:

E-discovery

E-Discovery and analysis tool applies cutting edge tools and techniques for dealing with high volumes of electronic data and makes it possible for investigators to undertake a comprehensive analysis of potentially fraudulent financial transactions. It offers standard forensics and unstructured data analytics designed to search, collect and investigate enterprise data to manage legal obligations and risk.

Computer Assisted Audit Tools (CAAT) is used as an analytical tool to detect fraud. CAATs include ACL, Idea analysis and Wiz Rule among others. ACL can be configured into financial systems with specific rules that classifies transaction as fraudulent or not based on previously identified fraud cases. CAATs are useful in investigating fraud as they simplify the process of extracting data, can analyse a large volume of data and identify exceptions that relate to fraud. Additionally, CAATS can be configured to flag incoming transactions that match previously known fraud patterns.

Pelican Secure

The Pelican Secure Fraud Prevention solution uses Machine Learning Artificial Intelligence technology to analyse patterns of behavior to identify and flag subtle anomalies that are indicative of fraud, supports real-time analysis of transactions and flags suspicious transactions before they are processed. In addition, it applied advanced analytics and reporting enabling efficient alert management system of suspicious transactions.

Feedzai and DataRobot

Feedzai is mainly used for fraud prevention and money laundering and is built on artificial intelligence and DataRobot. Feedzai customers benefit from having these models easily integrated into an end to end Omni channel platform purposely built for financial crime detection, including sub-10 millisecond latencies and high availability. (Businesswire, 2019). The flexibility of Feedzai allows for data cleaning, analysis, feature engineering, model training, and testing within the Feedzai platform. On the other hand, DataRobot is used to rapidly build and deploy learning models and create advanced AI applications.

FINAL THOUGHTS

The fight against financial crime in a constantly developing technological era has not been easy at all. As financial institutions and banks develop adequate solutions to tackle certain criminal techniques, criminals develop more sophisticated patterns. Thus, organisations need to change the manner in which they address financial crime risk by utilising the various technological innovations to improve how they fight financial crime. Thus, banks and financial institutions have to be on top of their game when it comes to deploying technologies that mitigate the risk of financial crime, all the while, implementing effective solutions that are sustainable, resilient and well competent to address the increased risk of financial crime. Financial institutions need to change the way they manage risk of financial crime by leveraging forensic technologies to conduct their financial crime investigations.

Artificial intelligence, data analytics, and blockchain technologies continue to revolutionize the landscape of financial crime mitigation, providing financial institutions with the ability to reduce the risk of financial crime. It is evident from the tools explored above that integrating these technologies is the way forward

in developing more reliable and effective tools. Forensic investigations of electronic crimes have become reliant on tools that combine Artificial Intelligence and data analytics to ensure more accurate results and reduce the risk of false positives. There is a need to explore further how other emerging technologies can complement already working technologies, in order to maximize the advantages of all the necessary technologies in completely mitigating the risk of financial crime. Nevertheless, criminals are also looking to break these new technologies, and banks and financial institutions ought to always stay abreast in their research and solutions.

While these technologies play a huge role in identifying high-risk transactions, compliance officers in the various institutions ought to follow up the alerts and ensure that necessary corrective measures have been enforced. It remains imperative for financial institutions to explore technologies that are effective and essential in mitigating financial crime, plus there is a need for continued research in how integrating the working techniques can increase accuracy and reduce false positives. When used appropriately, these technologies can greatly enhance the effectiveness, and at the same time reduce cost, of financial crime compliance and investigations.

About the Author



Florence Love Nkosi is a Master of Science in Computer Forensics and a Certified Information systems Auditor (CISA). Her specialities include: Information Systems Security, Information Systems Audit, information systems security management, computer forensics, data mining and analytics, including cyber security. She is currently working as a Principal Internal Auditor- Information systems with Malawi Ministry of Finance and Economic development-Central Internal Audit Unit. Florence likes baking during her free time.

Beacon – Dark Web

Discovery For Data Breaches

from Echosec

There are new data breaches happening every day. An organisation is never truly safe from a data breach as they can occur in a variety of ways. Popular examples include external threats that exploit poor technical implementations, or threats from internal employees leaking private information driven by an agenda. Many breaches happen because the data has been left exposed to the public by mistake and can be found on popular search engines.

Beacon

When data is stolen, it often lands on hacker message boards or the Dark Web. Beacon is a search engine designed to target these sources and find the data before it ends up in the wrong hands.

These sources include:

- **Surface Web** - Popular hacking message boards and paste sites.
- **Messaging Services** - Public or group messenger channels.
- **Dark Web** - Sites and marketplaces only accessible through the Tor browser.

Surface Web

Many data breaches result in information turning up on Surface Web hacking forums like BreachForums and RaidForums. The post below shows information about the Dailymotion breach, such as what

hashing algorithm was used for the passwords and it includes a link to a news article. The crucial piece of information here is the MediaFire link that lets you download the raw data from the breach.

The screenshot shows the Beacon search interface. At the top, the search bar contains the query: `("data breach" OR "database") AND "download"`. The search results are displayed in a list on the left and a detailed view on the right.

Search Results List:

- Database Requests 17** (raidforums.com) - (04-27-2018, 04:40 PM) Quote: : Name of the requested dat...
- Dailymotion Database leaked October 2016 - Free ...** (bitshacking.com) - In October 2016, the video sharing platform Dailymotion suf...
- Dailymotion Database leaked October 2016 - Free ...** (breachforums.com) - In October 2016, the video sharing platform Dailymotion suf...
- DailyMotion Database - Leaked, Download!** (breachforums.com) - (06-23-2018, 09:39 PM) Quote: : Hello, today I have s...
- Database Requests 17** (raidforums.com) - Hey guys, I'm looking for these data breach: https://linustec...

Thread Details:

- Thread Section Title: Account Dumps | Breach Forums
- Thread Participants: 1
- Thread Spam Score: 0.018

Thread Content:

In October 2016, the video sharing platform **Dailymotion** suffered a data breach. The attack led to the exposure of more than 85 million user accounts and included email addresses, usernames and bcrypt hashes of passwords.

Compromised data: Email addresses, Passwords, Usernames

Breach in the news:
<https://thehackernews.com/2016/12/dailymotion-database-leaked.html>

Password encoding: bcrypt

Download
<https://www.mediafire.com/file/hc9u...> Buy Threads, Replies, Reactions, Signatures, etc -
<http://...>

This information was discovered by performing a basic boolean search in the Beacon platform. The search above is for anything that includes the words "data breach" and "download", or "database" and "download". This means "download" must be in all results, but they can have either "data breach" or "database" in them, not always both.

Below is a post from another forum found in Beacon. This is from a recent leak called "Collection 1". This leak is comprised of around 2844 separate data breaches all put together. The data consists of both email addresses and passwords. There are over 773 million entries.

No download link is present here. Therefore, the download must be executed on the page itself. If a user was to download the data, they would navigate to the link shown and download it from there.

Forums, including RaidForums and many others, require users to create an account to download the raw data. Accounts are usually free, however, many of them require users to post comments and threads to gain access via credits. Credits can be used as currency to access more premium breach downloads.

BEACON ("data breach" OR "database") AND "download" **SEARCH** 6693 results

ADVANCED SEARCH Search by

breachforums.com
(06-23-2018, 10:08 PM) Quote: : Hello, today I have s;

WeHeartIt Database - Leaked, Download!
breachforums.com
(06-23-2018, 10:08 PM) Quote: : Hello, today I have s;

2,844 Collection Leaked, Download!
raidforums.com
Hello RaidForums Community, Today I have uploaded the 2,

DailyMotion Database - Leaked, Download!
breachforums.com
(06-23-2018, 09:39 PM) Quote: : Hello, today I have s;

Mate1.com | 2016 - Leaked, Download!
breachforums.com
Hello, today I have spent my own time to upload the Mate1.

Thread Section <https://raidforums.com/Forum-Databases>
Thread Section Title **Databases | RaidForums**
Thread Replies 11
Thread Participants 10

TRANSLATE EN

Hello RaidForums Community,
Today I have uploaded the 2,844 **Troy Hunt** Database Collection for you to download for free, thanks for reading and enjoy!
[Notes]
In February 2018, a massive collection of almost 3,000 alleged data breaches was found online. Whilst some of the data had previously been seen in Raid Forums, 2,844 of the files consisting of more than 80 million unique email addresses had not previously been seen. Each file contained both an email address and plain text password and were consequently loaded as a single data breach. **Troy Hunt** .
Compromised data: Email addresses, Passwords

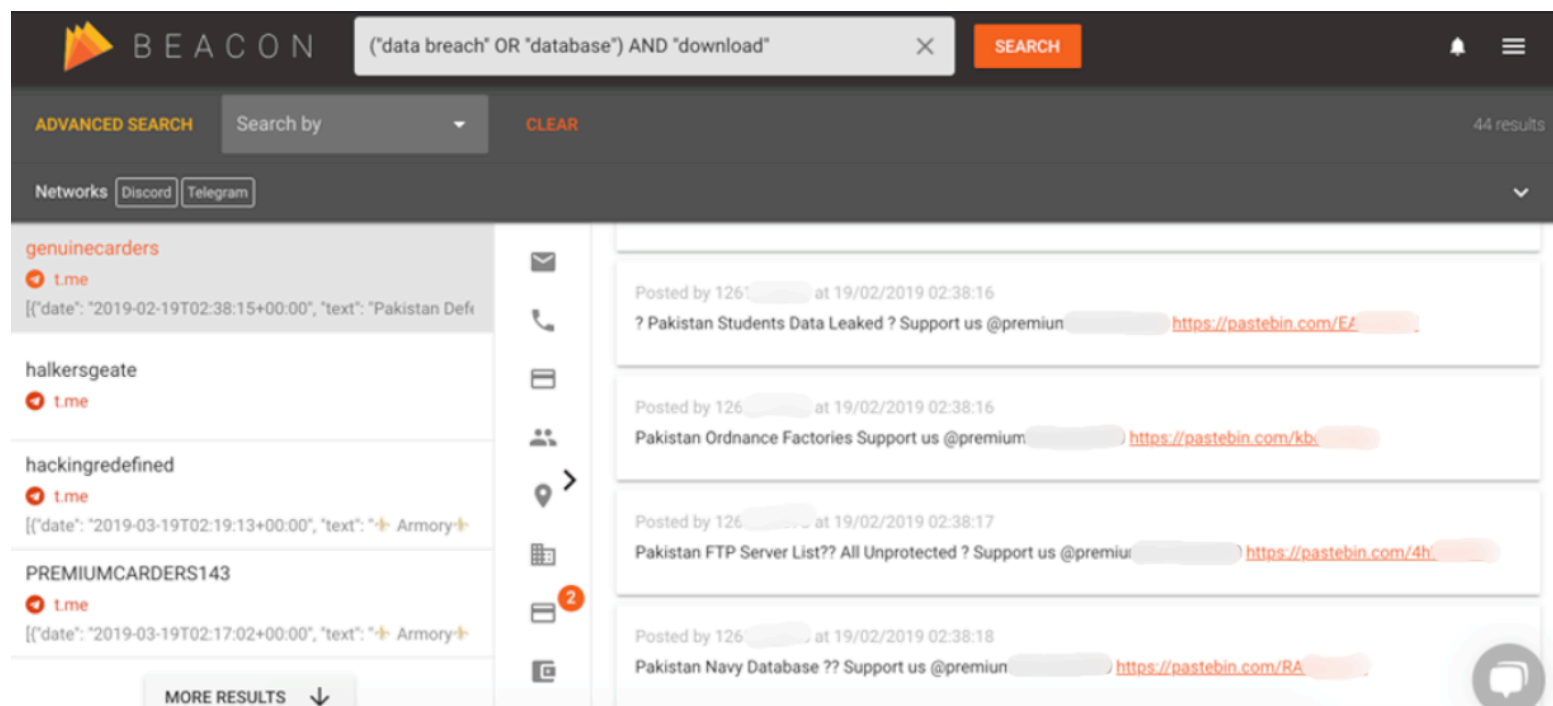
MORE RESULTS ↓

2,844 Collection Leaked, Download!

Site URL	https://raidforums.com/Thread-2-
Crawled	April 24th 2019, 9:43 am
Network	Open Web
Authors	
Language	English
Published Date	May 16th 2018, 8:03 pm
External Links	https://www.troyhunt.com/ive-just-added-2844-new-data-breaches-with-80m-records-to-have-i-been-pwned/
Site Type	discussions
Site Country	US
Site Categories	politics law_government_and_politics non_standard_content adult
Thread URL	https://raidforums.com/Thread-2-
Thread Section	https://raidforums.com/Forum-Databases
Thread Section Title	Databases RaidForums
Thread Replies	11
Thread Participants	10

Messaging Services

Among the sources Beacon accesses are Telegram and Discord. These are important because, unlike other sources, many users are unaware that others can read their posts. This results in them often discussing illegal activities between themselves.



For Discord and Telegram, Beacon shows all the metadata associated with each result. This includes:

- Direct URL to the data
- Dates of when the data was published
- When the data was crawled
- What language it is in
- Any links in the post that point to external websites
- The author of the data

Author's names can range from a username they have chosen, a unique user ID, or a generic term like "Anonymous" for users who choose not to identify themselves, like in the Telegram example below.

ANONYMOUS ZONE

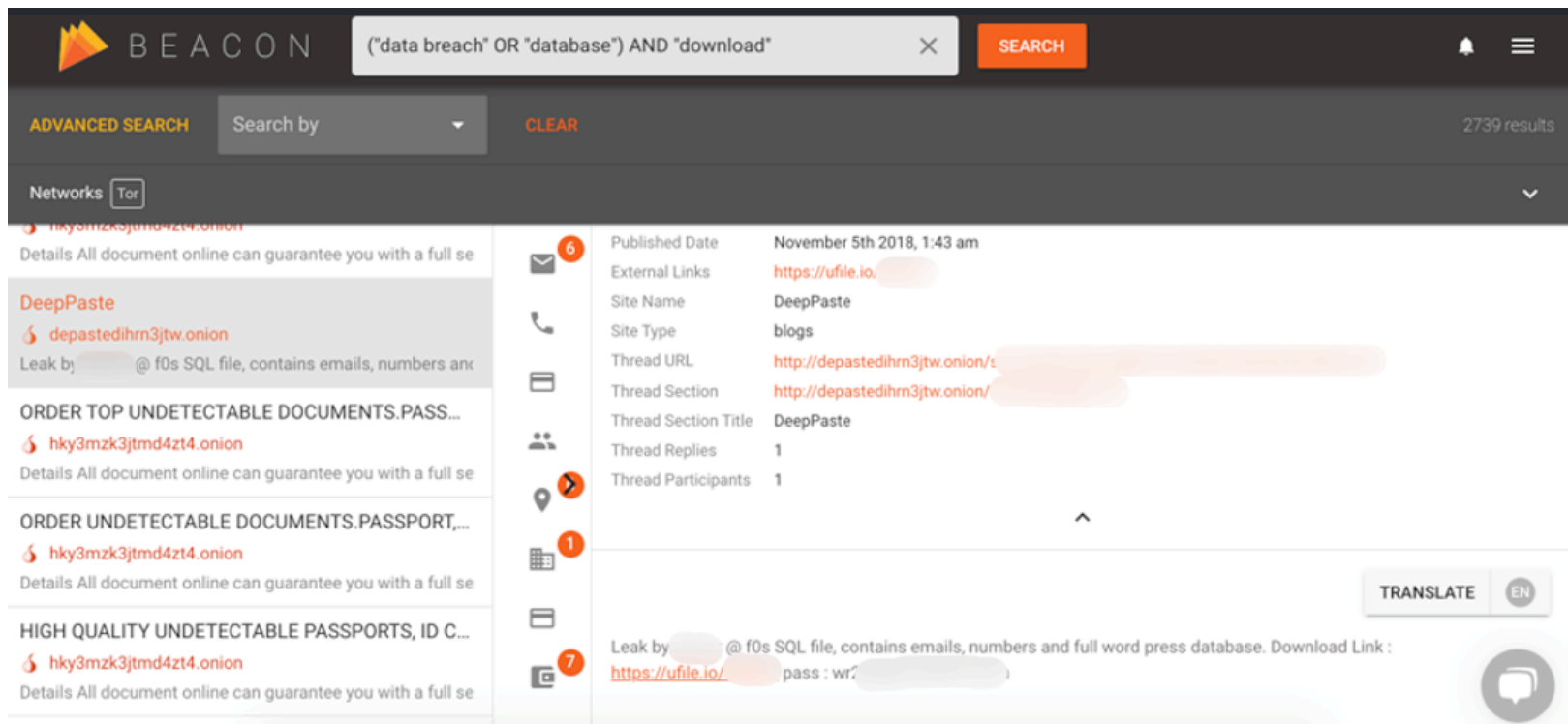
Site URL	https://t.me/
Crawled	May 24th 2019, 1:42 pm
Network	Telegram
Authors	Anonymous
Categories	hacking
Language	English
Published Date	May 24th 2019, 1:32 pm
Site Name	ANONYMOUS ZONE
Site Type	chat
Thread URL	https://t.me/
Thread Participants	1
Thread Spam Score	0.103

Beacon users can click through the external links shown in the metadata. One of the links in the example above displayed full names, personal email addresses, and dates of birth for people believed to be working in the Pakistan government.

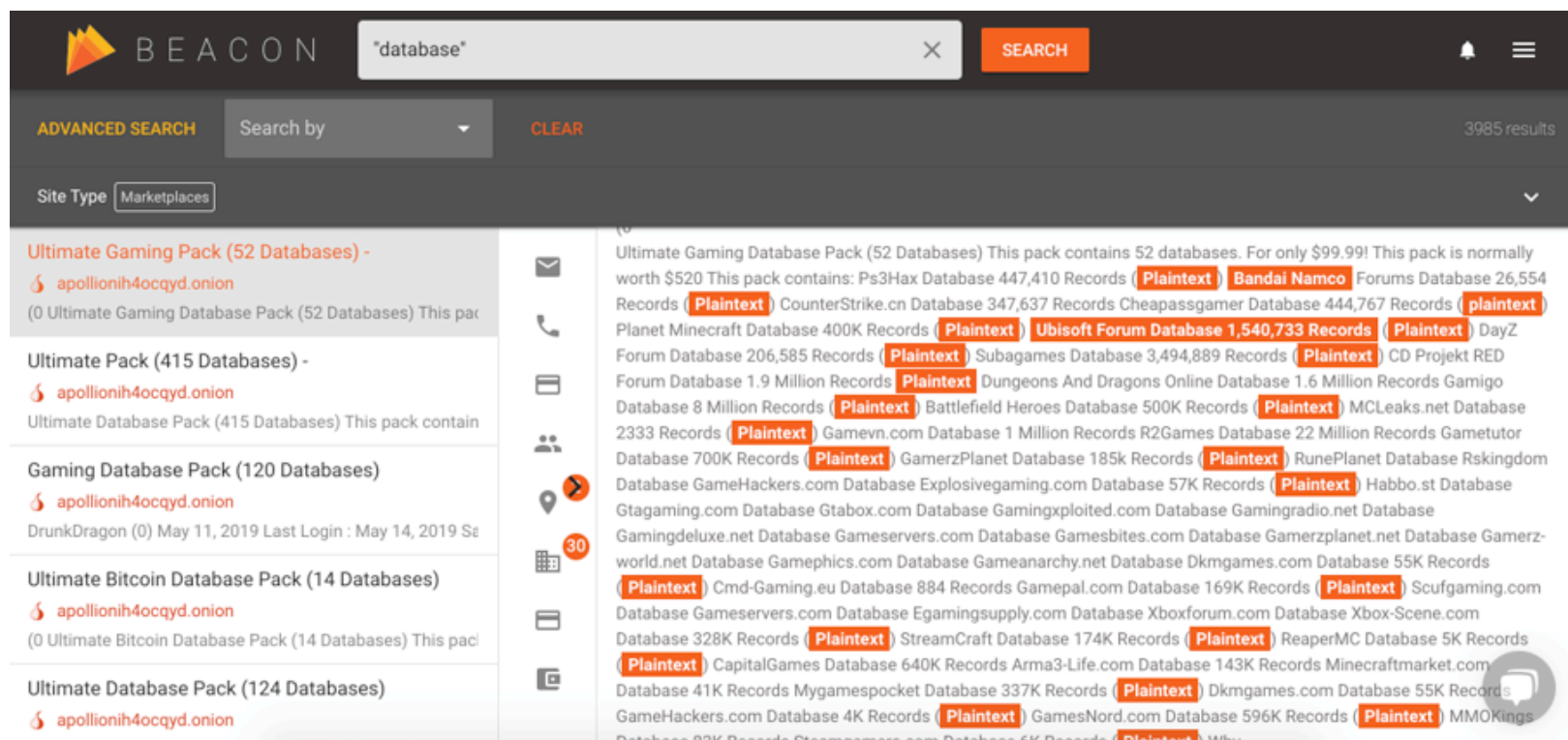
Full Name:	Email:	DOB
Ze	@gmail.com	1992-
us	@gmail.com	2012-
Kh	@yahoo.com	1993-
MU	@yahoo.com	1994-
Sh	@yahoo.com	1993-
Wa	@gmail.com	1995-
MU	@yahoo.com	1993-
m	@yahoo.com	1994-
Sh	@gmail.com	1992-

Dark Web

Below is an example of a Dark Web result on an onion website. It looks similar to the first result that was found on a normal hacking forum. It has some details about the data and then a link for downloading the breached data. This also displays the password needed to unlock the download.



The Dark Web is home to an array of marketplaces. Below shows people selling entire databases on a Dark Web market. Beacon users can narrow their searches to focus only on marketplaces, forums, or other specific areas of the Dark Web.



Conclusion

The Surface Web, messaging applications, and the Dark Web are all important sources because they each offer different information. While a variety of browsers and applications are often needed to access these sources, Beacon can do it all in one.

The built-in filters allow you to narrow down the results you need. Metadata allows you to view when the breaches were posted and often who posted them. Once a breach has been located, you can download it and search the raw data. This can help to assess the impact it will have on your organisation or yourself if you are looking for your data within another data breach.

An important factor of Beacon is that you can search the Dark Web without going on it yourself so that you remain safe. You don't need accounts on other platforms, like Telegram or Discord either, as Beacon does all the work for you.

For more information about Beacon, visit our website or contact us via email:

<https://www.echosec.net/>

support@echosec.net

About Echosec



Echosec is a web-based data discovery platform that helps organizations detect online data for threat intelligence. Aggregating and mapping content from hundreds of sources including social media, blogs, news, and the Dark Web (with Beacon), Echosec gives users instant visibility into any place on earth through a digital window. Echosec uses machine learning technology to recognize images and keywords so users get notified when specific content is posted. Beacon is the newest service offering from Echosec and is a dark web search platform.

Forensic Investigations and Financial Audits

by Ranjitha R

Forensic accounting is a challenging discipline that substantially interacts with auditing, economics, finance, information systems, and law.

Forensic accounting is a challenging discipline that substantially interacts with auditing, economics, finance, information systems, and law.

A forensic accountant will use accounting, consulting, and legal skills in engagements. A forensic accountant needs a working knowledge of the legal system and excellent quantitative analysis and communication skills to carry out expert testimony in the courtroom and to aid in other litigation support engagements.

A person just being an accountant is no longer enough to do this work—the person has to understand the legal system, and what the law says. He or she should have the expertise to interrogate and interview. It really is much more than dealing with the numbers. It's no longer just

basic fraud work. A forensic accountant reduces the complexity by distilling information and slicing away deceptions to help a judge or jury to see the essence of a financial dispute.

Forensic accountants provide perspective in situations evaluating whether accounting information is presented fairly without GAAP-based constraints, such as:

- Identification of financial issues.
- Knowledge of investigating techniques.
- Knowledge of evidence.
- Interpretation of financial information.
- Presentation of finding.

Forensic accountants are employed to seek, interpret, and communicate transactional and reporting event evidence in an objective, legally sustainable fashion, not only in situations in which there are specific allegations of wrongdoing, but also in situations in which interested parties judge that the risk of loss from wrongdoing is such that proper prudence requires legally sustainable evidence to support the conclusion that no wrongdoing is occurring.

A forensic audit looks at the details of a specific aspect of the records, trying to determine why everything does not or should not add up. Thus, a forensic audit is much more time-consuming and can be significantly more expensive than a regular financial audit.

Practitioners in each area have a broad understanding of business and industry trends; a thorough understanding of the issues, timing, and concerns of the auditing process; an understanding of the types of financial records and documents that should exist to support recorded amounts; and a shared concern about the impact of fraud on company operations.

Financial auditors are charged with performing an examination of a company's financial statements in accordance with Generally Accepted Auditing Standards (GAAS).

Forensic accounting investigators principally tackle two broad categories of financial fraud:

- Fraudulent accounting and reporting
- Misappropriation of assets.

Much of the forensic accounting investigator's work involves the retrieval, interrogation, and analysis of relevant information to answer specific questions about what, why, when, how, and by whom allegedly improper behavior may have occurred.

Lying to an auditor can also result in criminal sanctions. According to the U.S. Department of Justice, lying to auditors or a forensic accounting investigator can be considered obstruction of justice. Also, lying to any member of an audit team may trigger penalties under Sarbanes-Oxley (misleading an auditor).

Expert services are deemed to be advocacy in nature and are prohibited under the act and the rules adopted by the SEC. Forensic accounting investigative services are performed either in aid of the audit committee's or management's carrying out of its corporate governance responsibilities or in aid of the audit team's satisfying its responsibilities pursuant to GAAS and Section 10A of the Exchange Act (Section 10A). An auditing firm can continue to provide

forensic accounting investigative services for an audit client if services were already under way when a government investigation commenced so long as the auditor controls its work.

In addition, forensic accounting investigative services related to a violation of internal policy or procedures are appropriate; so, too, is investigation of whistleblower allegations.

Further, the auditors may already be performing investigative procedures if they were the first to detect a suspected fraud and are therefore well placed to conduct forensic accounting investigative work in the event of an investigation, assuming that they utilize professionals specially trained for such work. The auditing team in place may enable a forensic services team to be deployed more quickly and effectively.

Forensic accounting investigators normally have few predetermined boundaries. They often develop the scope of an inquiry with input from various sources—including counsel, the responsible committee of the board of directors, management, the independent auditors, and the company's internal audit group.

Auditors, in contrast, set the scope of the audit, based on risk factors determined after consideration of relevant information, including

books and records, management input, and other data such as industry norms. The auditors benefit from cumulative knowledge based on prior work and advance planning.

While the auditor places at least some reliance on management representations, the forensic accounting investigator usually places little or no specific reliance on management representations.

Staffing and executing an audit is necessarily different from staffing and executing a forensic investigation. Most financial audits delegate work among staff, based on the complexity of the tasks. On the other hand, it is more typical than not in forensic accounting investigation that the more senior, more experienced personnel both direct and execute substantial portions of the scope.

A financial auditor does not ordinarily create work product under an attorney privilege or report findings to a lawyer; audit working papers are, on the whole, not privileged. On the other hand, most forensic work is customarily structured to be performed in a privileged environment because of the likelihood of related litigation.

In most forensic accounting investigation engagements, the forensic accounting inve-

stigator uses knowledge, skills, education, training, and experience to advise the client as to a menu of recommended forensic procedures. After a discussion that may include input from various parties involved in the investigation, the client determines the scope, nature, and timing of the forensic procedures to be performed. Because the client sets the scope, it is appropriate for the forensic accounting investigator to receive indemnification and liability protection from the client.

Financial auditors on the other hand may offer an opinion (qualified, unqualified, disclaimer of) in an audit, negative assurance in a review, or no assurance in a compilation or application of agreed-upon procedures.

CONCLUSION

The future of international forensic accounting investigation assignments can be among the most challenging, intricate, and interesting. The field of forensic accounting investigation is advancing worldwide, with more sophisticated challenges to address and resolve and with more sophisticated tools at hand. The field will be, and deserves to be, a gathering place for outstanding auditors who have looked at the conceptual and practical challenges of forensic

accounting investigation and looked also at the personal demands of the field.

REFERENCE

1. Forensic Accounting As A Tool For Fraud Detection And Prevention, Jumah Gabriel, 2019
2. Assessing internal audit reliability Okodo, Aliu & Yahava, 2019
3. Forensic Accounting In The World: Past And Present Jūlija Liodorova, 2018
4. Financial Accounting Fraud Detection Using Business Intelligence, Shirley Wong Sitalakshmi Venkatraman, Melbourne Polytechnic, Victoria, Australia, 2015.
5. The Impact Of Forensic Investigative Methods On Corporate Fraud Deterrence In Banks In Nigeria Benjamin Ezugwu Onodi, Tochukwu Gloria Okafor, Onyali Chidiebele Innocent, 2015
6. Empirical Analysis On The Use Of Forensic Accounting Techniques In Curbing Creative Accounting, Ngozi Ijeoma, [Nnamdi Azikiwe University, Awka Unizik](#), Department of Accounting, 2015

About the Author



I am a post graduate in MTech Computer Science and Engineering with specialization in Cyber Forensics and Information Security from CUSAT, Cochin, Kerala, India. I am settled in Thiruvananthapuram, Kerala, India. My hobbies do include reading, writing articles, poems, and also preparing tutorials.

Cyber Forensics for a beginner

by Sudharshan Kumar

Cyber forensics requires a proper triaging done to prioritize the investigation to be followed. Based on such effective triaging, cyber forensics could be divided into three steps, viz., Identifying, Preserving and Investigating.

Getting started

“We can all see, but can you observe?” is an interesting quote from a book called **Everyone Lies**. The phrase might sound simple, but it holds a very deep meaning. Each and every one of us have the equal opportunity to get all the needed data from around us. But the question is, **“are we intellectual enough to see the bigger detail even in the smaller data?”**

Forensics is basically an art of identifying the sources for details, gathering evidence, aggregating and correlating this evidence to deduce the perpetrators. Forensics has always been a more sophisticated methodology ever since the crimes have rooted in the history of the world. Crimes may be of various forms and factors, depending upon the subject under attack – physical or digital crimes. The first known cyber attack was on the optical telegraphy-based data network known as **Semaphore**. The incident happened in **1834**, where the attack was related to the stock exchange data theft.

In the modern world, we have moved into the cyber space where all our day-to-day activities are directly or indirectly dumped into the internet. This has eventually urged the criminals to take advantage of the anonymity of the cyberworld. The more advanced our technologies have grown, the more the attack surface has expanded for the cyber-criminals to exploit the minor loose ends in these systems.

Cyber Forensics – A defensive approach

The threat to digital information is gearing up at an alarming rate as every day we see breaches reported attributing cyber-attacks to the business institutions. Based on today's threat landscape, there is no organization that could consider itself to have completely made off from cyberattacks.

Investigation in Cyber Forensics, also known as the digital post-mortem, sometimes requires a reverse engineering approach that needs the backtracking skills to get the fingerprints, preserve them and analyse these data. The contribution of the digital forensics would be the insights for the **RCA (Root-Cause-Analysis)** performed, where the **IoCs (Indicators of Compromise)** are identified which will further escalate to a level where the first successful point of entry could be traced to picturize and categorize the successful attack.

IoCs help to run a quick status check/full malware scan to verify whether our network and endpoints have been compromised or not. Usual IoCs include – **malicious domains contacted (CnC servers), malicious IPs, hash values of malware files**, etc.

Based on the firm and credible evidence, the necessary patching and preventive mechanisms could be implemented to reduce the attack surface an attacker could take advantage of.

Steps in Cyber Forensics

Cyber forensics requires a proper triaging done to prioritize the investigation to be followed. Based on such effective triaging, cyber forensics could be divided into three steps, viz.,

- **Identifying**
- **Preserving**
- **Investigating**

Identifying:

Once the information security incident/breach has occurred, the first level of investigation will begin with the identification and collection of raw data from various data sources within the crime scene. For instance, if there has been a hard drive involved in the incident, then the hard drive needs to be accounted as an important piece of evidence for the case.

It is essential that a cyber security analyst needs to have the intellect to identify the different sources of data that could contribute to the effective investigation and forensics. If there has been a breach into a network infrastructure, the different data sources are the various log sources such as the proxies, IDS, IPS, firewalls and other network devices within the infrastructure. It is crucial that every organization must have event logging deployed, which greatly bolsters the investigation.

Preserving:

Once the data sources are identified, the evidence should be taken into control and no access to the evidence should be entertained until submitted to the court of law and the final judgement is made on the case. Preserving the evidence and artefacts plays a very crucial role as it is the base of any allegations made on a suspect.

Every organization, government or a financial institution needs to maintain archives for a specified period of time, which is a plethora of data about the entities of that organization. This is required because of the fact that this information plays a pivotal role when an audit is done or when, in our case, an investigation needs data from the past.

When it comes to cyber forensics or general forensics for that matter, the better approach is to proceed investigation by taking a perfect copy of the evidence. This allows the original evidence to be preserved intact and any trial-and-error based investigations might be carried out over the replica of the original evidence.

For example, consider the evidence to be a storage device – a hard drive partition that contains the evidence that a particular confidential document has been stored unauthorized. In this case, the cloning of the data source/evidence/target is done, which involves obtaining an exact disk image file of the original target – the hard disk drive partition. It is to be noted that replicating the evidence to a disk image file does not mean the copying or backing up of the original evidence. The disk image file will be an exact replica of the original evidence where the hash value for both the original drive partition and the disk image file will be an exact match. The disk image files and file hashes can be generated using various imager tools such as Sleuthkit-Autopsy, FTK imager, etc.

The hash matching would greatly help to ensure that the original evidence has not been tampered after the evidence has been collected and preserved with access restrictions. The hash value could be

considered as a fingerprint derived for every file/folder based on several algorithms such that the integrity of the file/folder/application could be validated.

This hash value check could also be used to make sure that any data transmitted by a trustable source is not tampered in transit by any MITM (Man-In-The-Middle) attacks by a malicious attacker. There are some application vendors that provide the pre-calculated hash values (MD5, SHA1 or SHA256) to help the end users validate the hashes for the applications after the download is complete.

Hash values:

In cryptography, the data or a message is encrypted using a specific algorithm called a hashing function, which renders an output of a specific size. There are various hashing functions/algorithms used and some of them are:

- MD5 (Message-Digest algorithm)
- SHA1 (Secure Hashing Algorithm 1), SHA256.

Calculating MD5 hash value of a file:

There are several commands to determine the hash values of files in both Windows and Linux environments. The commands to calculate the file hash value are as follows.

For Windows:

From the Windows command prompt, change the working directory to the path where the file is placed. Then enter the command -> **"certutil -hashfile <filename> md5"**.

```
C:\Users\████████\Pictures\Desktop_Background>certutil -hashfile ironman-movies.png md5
MD5 hash of ironman-movies.png:
711806548279e96fd3e53af45e67f817
CertUtil: -hashfile command completed successfully.
```

For Linux distributions:

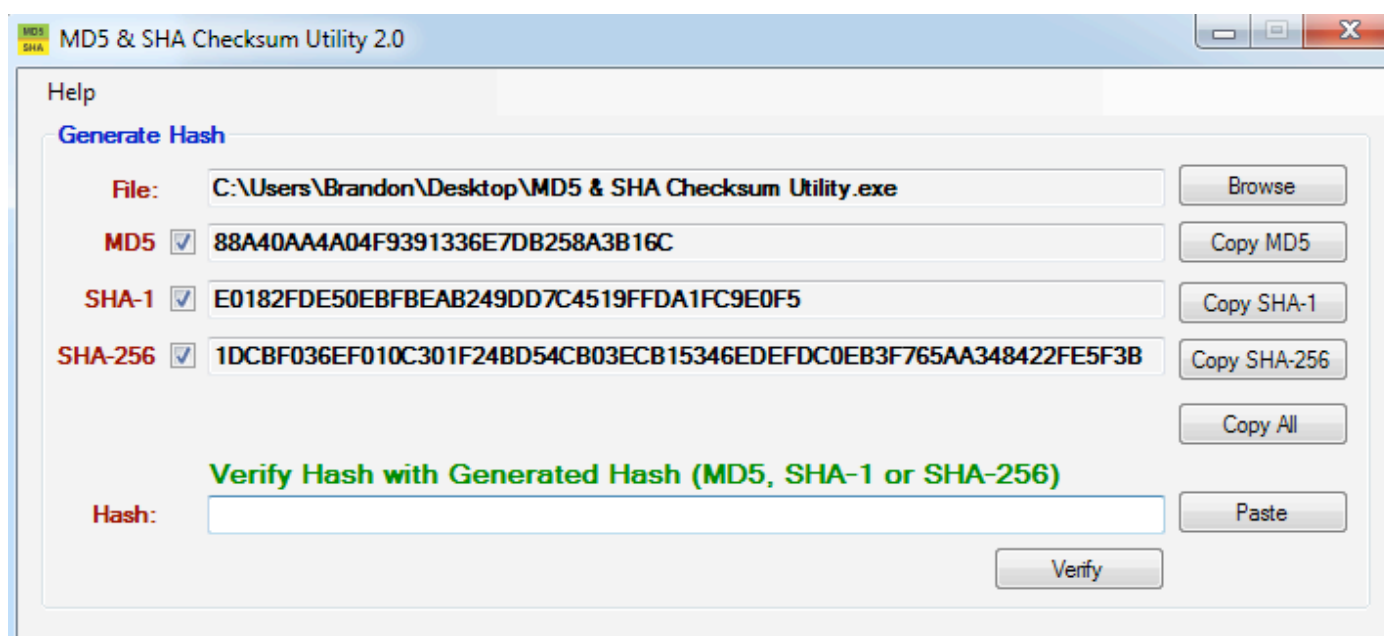
From the Linux terminal, simply use the command **"md5sum <filename>"** to determine the MD5 hash value of a file.

```
[TonyStark@server-1 ~]$md5sum test.txt
d41d8cd98f00b204e9800998ecf8427e test.txt
```

Similarly, in the case of a Linux distribution, the SHA256 hash values and hash-checks could be done using the command **sha256sum <filename>** as follows.

```
[TonyStark@server-1 ~]$ls
123 folder1 test.txt
[TonyStark@server-1 ~]$sha256sum test.txt
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 test.txt
[TonyStark@server-1 ~]$
```

Whereas, for a Windows machine, there are multiple tools to perform checksum for a particular file to determine hash values and perform hashchecks. One such tool for Windows is **“MD5 & SHA Checksum Utility”** (Utility Download link: <http://raylin.wordpress.com/downloads/md5-sha-1-checksum-utility>).



Investigating:

The most interesting part of the cyber forensics is the investigation of the collected logs and evidence. The investigation of the evidence is simply taking apart the target and analysing the core functionalities of it so as to picturize the attack scenario.

The analysis might be done over the malware/malicious application or on the storage devices that are pivotal evidence in a cyber-crime. When it comes to the forensic investigation/post-mortem of a malware or the malicious application, there are two ways to start the analysis, viz.,

- **Static analysis**
- **Dynamic analysis**

Static analysis:

Any malware is a complex code that contains a malicious routine scripted to aid the attacker in successfully exploiting the system. This piece of code might be an entirely standalone application/file/program or a sub-routine that is wrapped within an application that appears legitimate.

In order to analyse this malicious application, we need to first extract the source code of the application to further proceed with the code analysis. This process where the application is reverse engineered to get the source codes and the code level analysis is done to identify the logic/algorithm behind the malicious code is called the Static analysis. This method works best when we have effective tools to reverse engineer the application into binaries and codes or we already have the source-codes. The challenge here is that the open source applications might easily give away the codes but the licensed applications have a strong bundled application difficult to crack.

Static analysis requires the reverse engineering tools and a strong knowledge on code analysis. One of the interesting open source tools released in recent times for reverse engineering is the **"Ghidra"** software reverse engineering (SRE) framework developed by the NSA.

Ghidra is available for download from the Github. The NSA developed SRE tool is a java-based framework that features a very user-friendly GUI with features to backtrack the viruses, malware or applications to study their behaviour.

On a serious note, the reverse engineering technique is a very precise, specialized, time consuming process where, say for example, an executable bundle is unzipped to extract the components, which are the libraries and code snippets that are the core of the front-end application (in other words, the executable file). To put it in simple terms, a java application is an executable file (.exe file – a Windows

application program) in a zipped, compressed bundle that consists of the class files or **bytecodes**. These bytecodes are obtained by compiling the original java source code using a java compiler.

Furthermore, apart from the code analysis, which requires skills such as java source code reviews, reverse engineering also deals with the assembly level routines and instructions. This drills down to the instruction sets handled by the processor, where the memory buffers, registry values, and pointers are studied to understand the core of the application and its behaviour at the binary level.

The most notorious ransomware attack – Wannacry – had a kill switch where the ransomware checks for a certain URL if it is a live website. Once the website with the particular URL is live in the internet, the ransomware shuts itself down. This was discovered by a cyber security researcher by reverse engineering the malware strain.

Dynamic analysis:

In contrast to the static analysis, which involves the reverse engineering of the malicious software and codes being analysed, the dynamic analysis deals with the testing/analysis of the malware in a runtime environment.

This analysis is pretty interesting where the compromised system affected by a malware is immediately isolated from the network to spare other endpoints in the network from getting infected. Once isolated, the forensic analysis is either done by testing the behaviour of the malware within the affected PC/laptop or by running the malicious code in a contained, sandbox environment.

The sandboxed environment simulates a real-time system that runs an operating system and hence the malware does not recognize the closed test setup and gets executed, which will be recorded in the sandbox container to study the malware behaviour.

Always think out-of-the-box!

Though we have structured step-by-step analysis techniques, there is never a limit or restriction to bring in new ideas and workarounds to improve the existing techniques when it comes to cyber forensics. There have been a lot of interesting cyber security related incidents and crimes where the evidence and

artefacts inspire us to deep dig into the related data sources. Let me highlight one of the interesting facts from the cybersecurity related incidents I had come across.

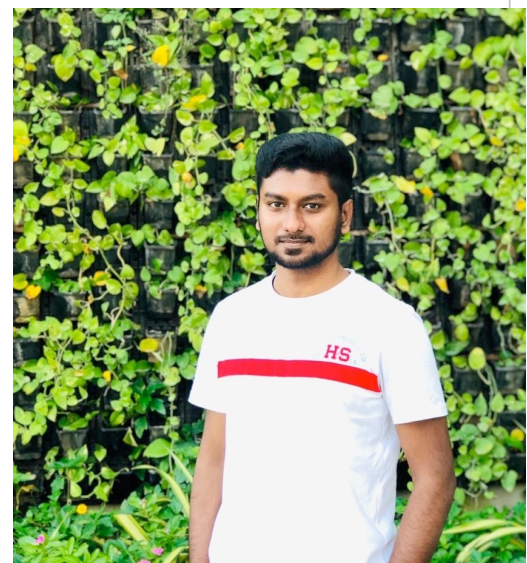
Slack space

The slack-space is the unused storage space that could contain some of the juicy information when analysed. Every hard disk drive consists of circular storage disks called platters. These platters have logical segments called sectors of a particular size that store the data. If the file size is less than the size of the allocated sector, then the remaining unused space becomes the "Slack space". When the data stored in that sector is deleted, the sector only re-allocates that space to new data to occupy. If the new data copied to the same sector space is less than the previous data, then the difference between the old data and the new data will become the leftover slack-space, which will still hold the old data until new data of same size requests a reallocation.

Reference: <https://whatis.techtarget.com/definition/slack-space-file-slack-space>

About the Author

Sudharshan Kumar is currently pursuing his Masters in Cyber Forensics & Information Security while working as a Cyber Security professional. As a Cyber Security enthusiast, Sudharshan is interested in keeping himself updated on the latest Cyber Security news and he is curious about the latest exploits. He spends his free time playing with exploits and analyzing them. Active threat hunting and Application Security are areas of Sudharshan's interests. He has a CEH certification and more certifications on the pipeline. Apart from professional interests, he also likes photography.



Trace Labs - Finding missing persons through the use of crowd sourced OSINT

Interview with Josh Richards

[eForensics Magazine]: Hello Joshua Richards! Thank you for agreeing to the interview, we are honoured! How have you been doing? Can you tell our readers something about yourself?

[Joshua Richards]: Hi, it is great to be speaking with you today! I have been doing great thanks, I am near the end of my first year in university studying Applied Cyber Security, only a couple more pieces of work to finish and then a nice summer holiday where I can focus on a lot more OSINT related work again. I also have a part time job with Echosec so I am definitely excited to keep working with them and looking forward to doing whatever I can to help them develop even more.

Where did you learn how to use OSINT for such purposes?

I only learnt about this idea after I had found Trace Labs. At first, coming into this kind of work, I seemed to be surrounded by the more negative

side where there are people finding information, some in very creative ways, that could be used for such good reasons, but instead they choose to leak this information online for malicious purposes. I never wanted to be a part of that life, but I did love finding information more than anything, so I had to find something I could use it for. Then I found Trace Labs, which gave me the opportunity to use my information gathering skills, but for a very good reason, and I loved it, so have continued on with it ever since, and have met a lot of incredible people along the way.

Can you tell us more about the non-profit organisation you work with, Trace Labs?

The main aim of Trace Labs is to use OSINT to help the police locate real missing persons so that they can be returned to their families. So far, we have two ways of doing this. One is normal everyday operations where we will create a new channel in our Slack community, and any

information you find on that person can then be added to the channel so that everyone can try help and the information can be handed over to the police when we are happy that we have done all we can. The second is in the form of a Capture The Flag. CTF events are usually done with hacking, where you have to hack into something to get specific answers to obtain the flags. However, ours is unique because now you are finding flags or information that we don't yet know about. This is why we always have a range of great judges who see the submissions coming in, verify that the information is real and what we want, and can then assign points to that team afterwards. At the end of the event, all information is put together and sent to the relevant authorities. Some prizes are also given to the winning team like a Hunchly license and an IntelTechniques virtual training subscription. Some of our more important rules are that we only find information on people who have a public police report out stating that the police are asking for the public's help as we don't want to start searching for someone who isn't really missing. The other is that we do OSINT only, zero touch, so you can go to social media profiles, but cannot send them friend requests to try get more information that way or anything else that would be considered contact. We don't

want to interfere with the police investigations at all so this is the best way.

Where did the idea of founding Trace Labs come from? Do you know?

I personally had nothing to do with creating it to start with, that was Robert Sell. He has done a lot of work with search and rescue teams in Canada like Coquitlam Search & Rescue, which he has been a part of for over ten years. This has allowed him to see the large impact these missing persons have on their families and everything else that comes along with these complex cases. Rob also has over twenty years experience in IT and has a big interest in social engineering and OSINT so it made sense to mix the two and use OSINT to try help locate these missing persons. Having people on the ground is crucial, but looking for information online is just as important as it could lead directly to them much more quickly than a ground search could. It gives real insight into their lives and can point us in a better direction rather than a completely random search.

How many missing persons have you found thanks to open source intelligence?

Sadly, it is hard for us to know. We gather our information, and send it over to law enforcement. Sometimes they may give a reply,

sometimes they won't, so maybe our information has been used to find missing persons, or at least some good leads, but we just don't know about it.

We do have some good examples of findings from teams in our CTF events though. One team found that a missing person had a second Instagram account, and they had been posting on it recently, a year after they were reported missing. They also had some location tags on the posts, so we had a new location and recent pictures of the person, these would not have been found without OSINT being conducted. Another involved a team finding that a missing person's boyfriend had some court records for the same date she had gone missing, so they looked into the boyfriend and found some social media accounts, and the missing person was seen in some of his pictures after the date she was reported missing. All this information was handed over to the police for them to deal with, we only find the information, we don't act on it, that is for the police to do. These are just two examples of how OSINT has helped to track down missing persons.

Can you tell us about a case that was really challenging for you while working with Trace Labs?

I suppose this question can be seen in two ways. The cases we do can certainly be challenging because they are always different. We could be looking into a teenager who may have a lot of social media for us to find and maybe forum accounts where we can get a better insight into their lives. We could then be looking into an elderly person who has a little online footprint apart from official public records. There could be a young child who has gone missing where they may not have anything to find on them specifically so we have to try come up with other ways. So there are always challenges in that aspect. The other way this could be seen is emotionally. I personally don't get emotionally attached to any of the cases, but some people do. There was one where we found a lot of information on them, and they had posted to a forum telling a story about how they had witnessed a friend being harmed very badly, and they also talked about self harm and were giving tips on how to cover it up. So while we found a lot of information on this person, it could still be challenging in that aspect to some people because it can be hard to read these types of things. An important thing to remember is with

missing persons cases, anything is possible, they could have run away on purpose, they could be the victim of a crime, they could have harmed themselves. It is very sad but the number of missing persons is only increasing, so it is important to understand this.

How did you find out about Trace Labs? Are there other non-profit organizations that find missing persons and help them getting back to their families?

I was always trying to find new ways for me to use OSINT for good reasons, but it was very difficult for me to find anything at the time. At one point, I made a Twitter account just for OSINT related things. I don't remember exactly, but I believe someone retweeted a tweet from Trace Labs, so I looked into it and registered. I helped out on one case and it was really interesting so I have continued on with it ever since. Regarding other non-profits, there is likely quite a lot, I don't personally know of many, though. There is 'Missing People' in the UK who work closely with the police and families of the missing persons to try help locate them. They put up posters, do fundraising events, and more. The main difference here is, of course, that they work with the families and try to find all they can to help through those ways, while Trace Labs

only uses OSINT and doesn't contact anyone in the family or friend's groups. There may be some other groups that I don't know about who do some similar things, but to my knowledge, Trace Labs was the first to ever do an OSINT CTF that involved finding real missing persons, so Trace Labs is certainly doing some unique events that really are helping, and we hope to expand this more, of course.

Could our readers join Trace Labs? If so, how?

Of course. If you want to learn more about Trace Labs, we have a website that you can go to for resources and reading material: (<https://www.tracelabs.org/>). If you do want to join us, simply hover over the 'Accounts' tab on the website and click on 'Register'. Once you have registered, your application will be sent off to Robert so that he can look over it and accept it. Once accepted, you will be emailed a link to our Slack community, which is what we use to communicate. There are channels for missing persons operations, some general ones for speaking to other people with common interests. I have met some incredible people, and it all started here in this Slack. There are also other opportunities like if you want to be a judge in our CTF events, that can be arranged, we have trainings to help with that and we are always

looking for new ideas and things we can do to go even further with Trace Labs. As I mentioned previously, there are normal operations, and there are the CTFs. If you only want to take part in the CTFs, or only normal operations, that is quite common and is completely fine. We would still recommend you join the Slack so you can be aware of what is going on and we always use it as the communication method for CTFs and operations anyway so it is worth being in.

What are your plans for the future? Can you tell us what you are currently working on?

Our hopes for the future are to keep developing things like our relationships with law enforcement so that we can be even more confident handing information over to them and knowing that they are making use of it, as this isn't always the case currently. We are always looking for events we can attend to host CTFs in. So far we have done them in big events like Defcon, BSides, and more. I also introduced them to my university so we did one recently in the University of South Wales, which was an incredible experience, it went very well. We are also working with Saigar to build the first dedicated OSINT CTF platform for missing persons. Most other platforms are made for the generic CTFs that have specific answers, which makes it challenging for us to use

them. When we have one for our specific needs, it will make everyone's CTF experience much better and will help us manage the information that is so important for the police and families of the missing people.

Do you have any thoughts or experiences you would like to share with our audience? Any good advice?

If you are interested in OSINT at all, whatever level you are at, Trace Labs is an amazing way to practice, learn more, and meet amazing new people. You also get to put your practice into something that really means a lot to the families out there who have missing family members and friends. I can confidently say that I wouldn't be where I am now without Trace Labs, it can open up a lot of possibilities for you, and you will be doing something very rewarding at the same time. As a reminder, our website is (<https://www.tracelabs.org/>) so please feel free to read more about us and register if you are interested in helping out in any way.