Security Visualization Intelligence Model for Law Enforcement Investigations

Jeffery Garae[1], Ryan K. L. Ko[2], Mark Appearly[3] and Silvino J. Schlickmann[4]

[1] Cyber Security Lab, Department of Computer Science, The University of Waikato, Hamilton. NZ
[2] Cyber Security Lab, Department of Computer Science, The University of Waikato, Hamilton. NZ
[3] Department of Computer Science, The University of Waikato, Hamilton. NZ
[4] Interpol - IGCI, Singapore. Singapore
[1] jeff.garae@gmail.com; [2] ryan@waikato.ac.nz;
[3] mapperle@waikato.ac.nz; [4] s.schlickmannjunior@interpol.int;

Abstract. Data analytic methods and techniques have proven crucial in aiding law enforcement investigations and day-to-day operations. However, the rise of cyber-attacks across transnational jurisdictions creates a challenge to share information across law enforcement agencies. Malware, Bitcoin and social media datasets are some examples. Security visualization is a solution to facilitate information sharing across jurisdictions comfortably in enhancing investigations without revealing the underlying sensitive raw data therefore, reducing the time spent on analysing and processing such large dataset. In this paper we introduce the ``Security Visualization Intelligence (SVInt) framework'', a visualization intelligence model for investigations and situation awareness deployed for the international law enforcement domain. We provide an effective user-centric visual method of analysing, sharing and exchanging complex datasets using visualization to aid law enforcement investigations. Attribution and evidence preservation without revealing the underlying raw data is the primary goal for SVInt. The SVInt framework provide visualizations of Bitcoin transaction relationships and threat map visualization showing top malware threats using geo-locations. It also provides expendable visualization features for future investigation demands. Finally, we provide possible future work within the law enforcement security visualization domain.

Keywords: Visualization, Forensics Visualization, Security Intelligence, Block chain, Bitcoin, Malware Attacks, Transnational cyber-attacks.

1 INTRODUCTION

Law enforcement investigations often face a challenge of analyzing data collected on a day-to-day basis. The complexity contributes to slowing down the entire investigation process. Investigators and cyber security specialists are continually exploring the best methods and tools [1], [11] to help them analyze and understand the nature of the data with the intention of obtaining useful insights [2], [9], [12], [3], [10], [32]. However, "International law enforcement organizations" frequently have the challenges of: (1) attributing back to the source of attack and (2) data sensitivity and privacy issues, especially for the case of transnational cyber-attacks [14]. The trust complications for sharing and exchanging information with other countries becomes the challenge which results in slowing down investigation processes. There needs to be a method of sharing the data/information comfortably with other countries involved by maintaining the integrity, authenticity and without revealing the details of the underlying raw data. Security visualization has proven to be a critical solution to this challenge in helping crime analysis [2]. In this paper we propose our 'Security Visualization Intelligence (SVInt)' framework, a visualization intelligence model for investigations and awareness which can be used within the law enforcement domain particularly enhancing investigations among countries involved in transnational cybercrime. We provide the SVInt framework with a block chain visualization and threat Intelligence platform. It is an added feature to the existing in-house Bitcoin block chain explorer (Analytics tool) [24]. SVInt provides the visual analytical options for the Bitcoin block chain explorer and an existing manual in-house weekly threat report [7], [8]. With the need and nature of law enforcement investigations, SVInt is a centralized visualization intelligence

framework that enhance and facilitate investigations among different countries involved in cybercrime investigations. The framework has been adopted by the INTERPOL Global Complex for Innovation (IGCI) and currently has two visualization features: the Blockchain Relationship visualization and the threat-map visualization.

2 OBJECTIVES

In this paper we:

1) Provide an evaluation on existing visualization standards within the law enforcement sector, then present a new security visualization standard.
2) Provide an assessment and evaluation on existing block chain visualization platforms against our Blockchain Explorer Visualization.
3) Present the Security Visualization Intelligence (SVInt), that aims to aid investigation process for law enforcement particularly for attribution purposes.
4) Highlight the attribution and evidence-preservation security visualization intelligence (SVInt) model for investigations, information sharing, exchange and awareness.

2.1 Key Contributions

Figure 3 shows a summary of the test results based on the speed metric. The accuracy metric showed that the CBIR technique was 98% accurate, the CBII technique 35% accurate (based on the meta-data provided), and the HBIR was 78% accurate. These results are expected with the CBIR and CBII techniques and the time costs reported in figure 3 are consistent with the literature values. The HBIR was remarkably accurate given the limitations reported above. This indicates that the extremities of CBIR and CBII can be moderated by HBIR to offer a more balanced working solution. The HCI aspects of the tool were not tested within the time frame of the research period but are the focus of further testing.

2.2 The Need for Security Visualization

Existing methods of carrying out analytical investigation and reporting within law enforcement day-to-day operations can be confusing and tedious, and often affects getting the message across to targeted audiences. Data/information loss is a critical factor during the process of reporting security events or presenting them and most importantly whether the report can be admissible to the courts. The complexity of analysing large datasets collected (social media posts, images, physical evidences, application logs, system logs and network logs) effectively during investigations is an ongoing security challenge for security experts. Security Visualization is a potential solution for law enforcement reporting. It can simplify complex amount of data (evidences, work processes, etc.) into simple, clear and efficient quick-to-action visual representation that automatically has effective impact on all targeted audiences (CEOs, researchers, technical specialists, and law enforcement officers). Understanding the concept of representing effective security visualization, requires known examples and use-cases which are discussed in Subsection 1.4.

2.3 Forensic Frameworks and Tools

Law enforcement agencies are in need for forensics frameworks and tools that help them analyse data to identify useful insights that could help them solve criminal cases. Memory forensics methodologies and tools examining what is left in the main memory after a private browsing session and forensics of intrusions examining digital processes are some of the existing frameworks and tools [27], [28]. Intelligence and forensics tools directed towards mobile platforms such as MSAB's XRY framework and Cellebrite's Mobile forensics data extractions tool have aid investigators with investigations [29], [4], [30], [31]. Other open-source frameworks such as STIX which in cooperates CybOX are addressing information sharing based on feedbacks and active participation from organizations, and experts across a broader security spectrum [10], [32]. However, these tools are for data extractions and not specially for visualization, situational awareness, information sharing and exchange with the intension of attribution and evidence preservation.

Blockseer, an open source Bitcoin block chain tool and ecosystem, has graphing and visualization features [6]. It basically allows users to look up Bitcoin addresses and examine relational connections between transactions with address tagging capabilities. Elliptic, a commercial block chain intelligence

platform provides actionable intelligence to financial and law enforcement agencies [5]. It has visualization capabilities to display complex transaction history on specific Bitcoin transaction addresses, mapping them to all payment history relationships made in the past. To provide effective visualizations for law enforcement uses, the importance of having a security visualization standard is crucial and this brings in the need to develop a security visualization standard which will be discussed in the next section of this paper.

3 A Security Visualization Standardization Model for Law Enforcement

While there are other methods aiding law enforcement investigations and operations, the application of security visualization can minimize the time spent on investigations and other work processes. There is a need to create a set of visualization standards that can be used as key indicators in various visualization processes. For example, the current use of INTERPOL's 'International Notice System (Fig.1)' is a good start for such visualization standards, where the colour RED in red notices indicates 'Wanted Person', YELLOW notices indicate 'Missing Person' and so on [15], [13]. This helps law enforcement users instantly see and understand the purpose of such alerts when received at the National Central Bureaus (NCBs) in different member countries.

In this paper we initiate the need to develop a security visualization standard for the law enforcement sector. While the INTERPOL's type of notices are well known around the world, it indicates a good start with the use of visualization. Supposed the use of these colours from the types of notices are reused when visualizing cyber-attacks but adding more standards to it, such as a change of shape from the existing rectangle to a circle, then a 'red circle' in security visualization for cyber-attacks would indicate the presence and identity of malware attack. A 'green circle' could indicate normal network/system/web/file status. A 'yellow circle' could indicate suspicious network packets/system/web/file. Implementing such security visualization standard would over a period, be useful to the law enforcement particularly, with the reduced time spent on analysing or viewing security reports from investigations. Based on these suggestions for a law enforcement visualization standard, the idea of a centralized SVInt framework to use visualizations to assist investigations across jurisdictions. The SVInt framework design will now be discussed.

4 Security Visualization Intelligence Framework Design

Fig. 1: Interpol International Notice System.

SVInt is a web-based centralized security visualization intelligence framework, designed to address attribution, evidence preservation, situation awareness, information sharing and exchange without revealing the underlying raw sensitive data. Fig.2 shows the entire 'Security Visualization Intelligence' model with the following components: (1) bitcoin Blockchain visualization, (2) threat report visualization and (3) options for future visual platform to be incorporated into the SVInt Model. It is built using Hyper Text Markup Language (HTML), JavaScript (CoffeeScript), Cascading Style Sheets (CSS), Bootstrapping, and D3.js (A Java Scripting Visualization Library) [19], [20], [21], [22]. Each visualization components are discussed in the following subsections.

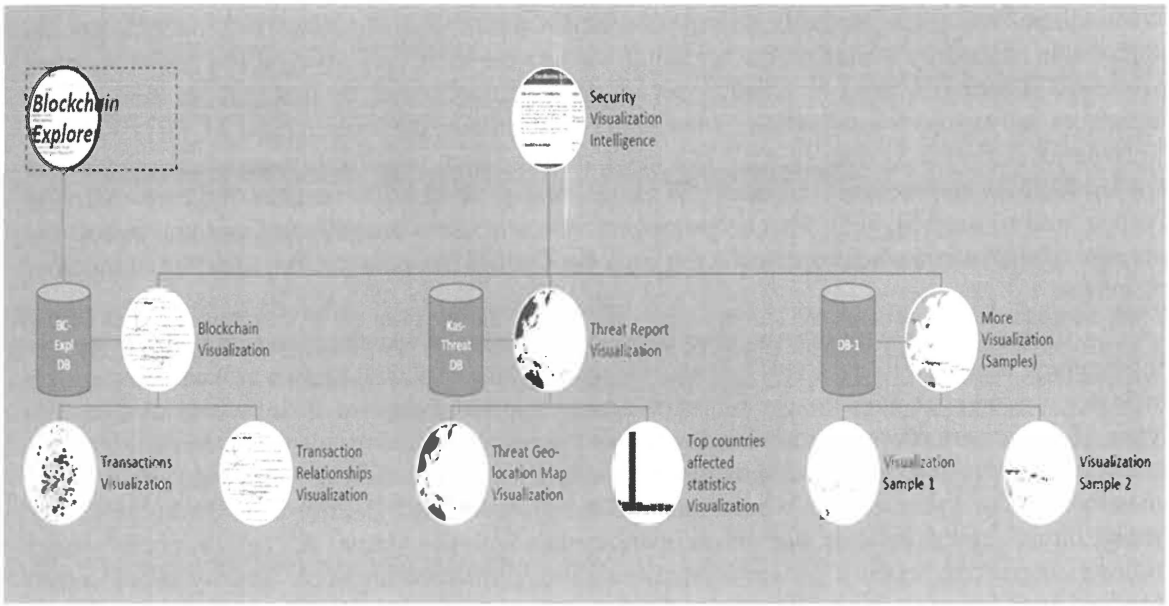
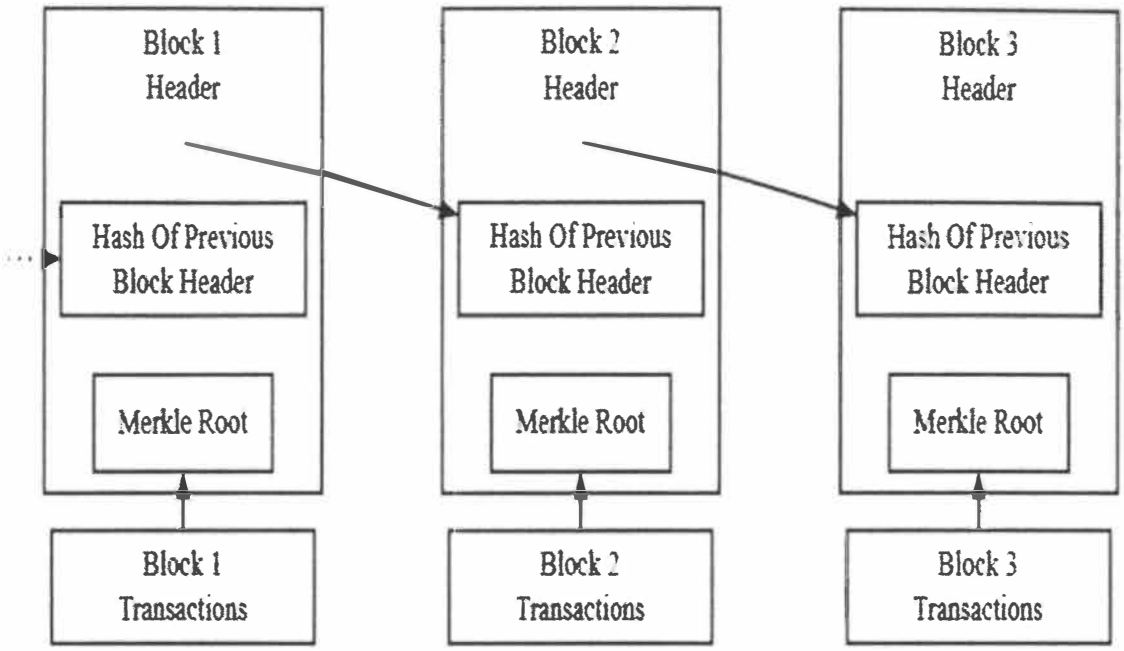


Fig 2. Security Visualization Intelligence Model Overview.

4.1 Bitcoin Blockchain

Although this paper's main focus is on security visualization, having a clear understanding of the Bitcoin block chain infrastructure will help users better understand how the Bitcoin visualization will work. In brief, a block chain provides the Bitcoin's public ledger, which contains timestamped record of transactions in an orderly manner [23]. The core reason for this implementation methodology is to avoid and protect against duplicated spending and prevent modification of previous transaction records. Fig.3 shows a simplified Bitcoin block chain design. More information on the implemented Bitcoin Blockchain Explorer has been described in the paper "Blockchain Explorer: An Analytical Process and Investigation Environment for Bitcoin" which will be presented at the ecrime 2017 (Electronic Crime Research) symposium [24], [25].

Fig.3. shows how transactions are processed from one Bitcoin block to another block. Note each block header contains the 'hash of the previous block header' to maintain and chaining the blocks together. Storing the hash of the previous block's header prevents the transaction from modification without modifying the block that records it as well as the all other following blocks [25].



Src:: https://bitcoin.org/en/developer-guide#block-chain-overview

Fig 3. SVInt: Simplified Bitcoin Blockchain Design.

4.2 Blockchain Visualization Design

Fig.4 shows the Blockchain visualization design. It relies on an external Blockchain Explorer [24] to provide the data for visualization purposes and it is a Bitcoin suspicious-tag centric, where relationships of known Bitcoin suspicious address tags (Bitcoin transaction Address) are visualized. It serves two core purposes: (1) an overview of Bitcoin transaction flow visualization and (2) Bitcoin transaction relationship visualization showing bitcoin movement and correlation between input and output transaction identifiers (TXIDs).

1) Overview Bitcoin Transactions Visualization: Based on user input queries, a visual overview is displayed of all transactions related to specific suspicious-tags between different wallet ID addresses, Bitcoin exchanges and Bitcoin Market places. This visualization (Fig.4) provides the user with various visualization features such as: Layouts (Force-Directed visualization, Wallet Addresses, and Relationships), Filters (all transactions, popular transactions and Obscure transactions) and Sort (by addresses and Links (relationships to other addresses)).
2) Bitcoin Transaction Relationships Visualization: The Bitcoin transaction relationships visualization option gathers for all past Bitcoin transaction relationships, hoping to reveal insights from the visualizations. Based on the suspicious tags, the visualization will be able to show predictable future transactions between various Bitcoin address wallets. This aims to connect the dots between known suspicious tags to new investigation leads for criminal activities using Bitcoins. The visualization model extracts data based on how the Bitcoin blockchain handles input and output transactions within the Blocks. Fig.5.

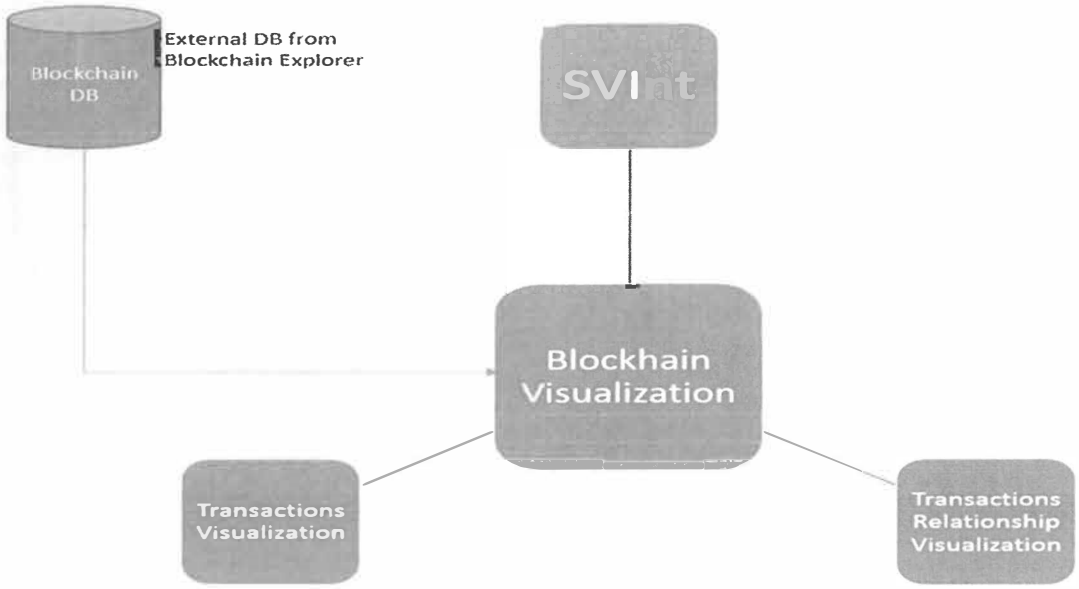


Fig 4:. SVInt: Blockchain Visualization Design.

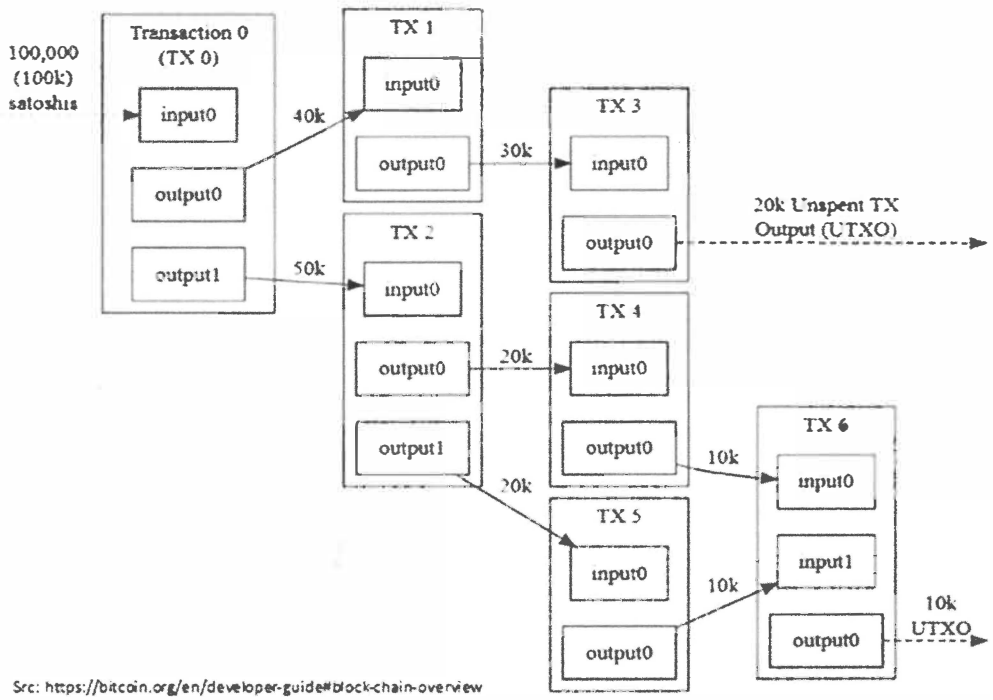


Fig 5:. Bitcoin Transaction-To-Transaction Payments Bookkeeping Design.

4.3 Threat Report Visualization Design

Figure 6 shows the threat report visualization design. It is a geo-location threat map visualization showing the top countries affected with cyber-threats in weekly and monthly intervals [17], [16]. The cyber-threat visualization provides two visual features as shown in Fig.9 and in Fig.10. These visualizations are designed with the intention of reducing the time spent on reading cyber-threat logs, therefore improving the way investigations are carried out.

The current threat report visualization model is design and implemented using HTML, D3.js, and predefined geo-location coordinates for visualization purposes. Datasets are structured in the form of .json (JavaScript Object Notation) .tsv (Tab Separated Values) and .csv (Comma

Separated Values) file formats. This allows D3.js to easily call and use the datasets efficiently. In terms of processing the data and visualizing from the threat report, the current method is static where the front end of the model reads directly from static report files and produces the threat map visualization.

4.4 More Visualization Design

With the idea of having a centralized security visualization intelligence framework, it is design to allow additional features (Fig.2 - More Visualization) purposely to harmonize future security visualizations platforms to allow law enforcement personnel's to effectively carry out their investigations with a one-stop security visualization framework that offers multiple purposes. This is because the SVInt framework is a central security visualization framework with the aim of providing attribution and situational awareness for law enforcement.

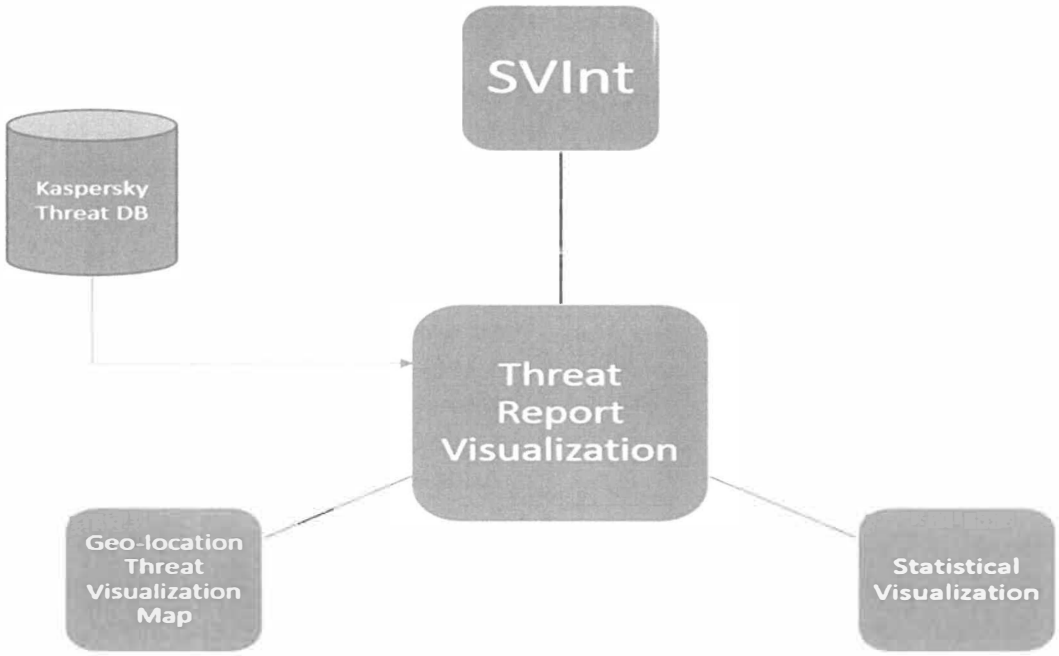


Fig. 6 Threat Report Visualization Design

4.5 Datasets

The SVInt model relies on external datasets of which were provided by the Blockchain Explorer (an in-house Bitcoin ledger) and the Kaspersky Lab's weekly and monthly threat reports received by emails (.xml and .xlsx files) All datasets are anonymized, standardized and transformed into either .csv, .tsv and .json formats for visualization [14].

5 SVINT MODEL VISUALIZATION

This section provides results of the SVInt model and explain how and why the visualizations are implemented. The key idea of the SVInt model is to provide a central security visualization model to aid law enforcement investigations. With this objective, the web-based security visualization model shows a central visualization home page with different visualization features that allows an investigator or law enforcement analyst to utilize fully when carrying out investigations. Fig.5 shows the Bitcoin block chain visualization page with the visualization options an investigator can select to visualize different Bitcoin transactions. Fig.7 shows the malware threats collected

using Kaspersky Lab's Web Antivirus (WAV) and Mail Anti-virus (MAV). These threat reports show weekly and monthly cyber-threats affecting users around the world. A geo-location visualization is to reduce the time spent on trying to understand the threat report if it was in a .xlsx or .xml file format. In addition, a statistical visualization feature (Fig.10) is added into the threat map visualization to provide statistical analysis on cyber-threats affecting users on a weekly and monthly time frame in specific countries.

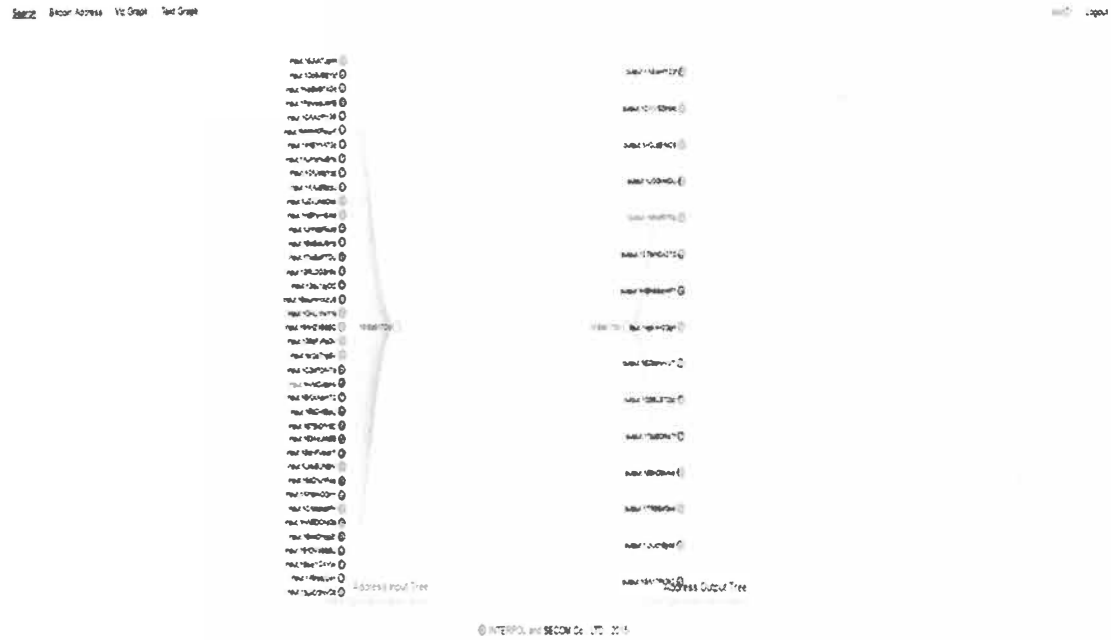


Fig 7:. Blockchain Visualization of Bitcoin transactions

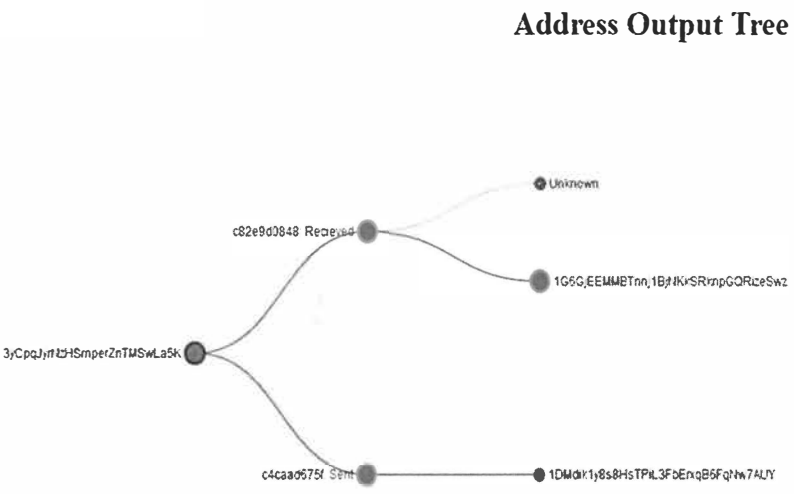


Fig 8:. Blockchain Visualization of Bitcoin Transaction Relationships.

Overall, SVInt provides a security visualization model that facilitates faster working processes during an investigation. With the given options of visualization, investigators can request for a variety of data abstracts depending on a given security event that is of interest to investigators. For example, a visualization showing all Bitcoin within a given length of time or date; weekly malware threats and/or monthly malware threats in the top 10 countries in the world.

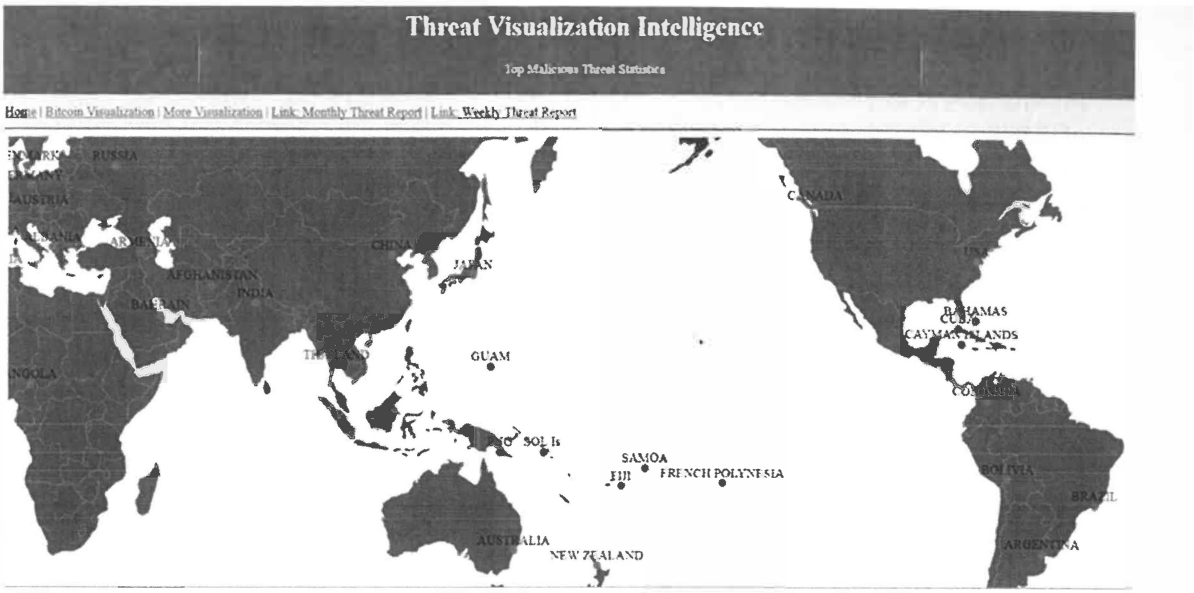


Fig 9:. Malware Threat Geo-location Visualization

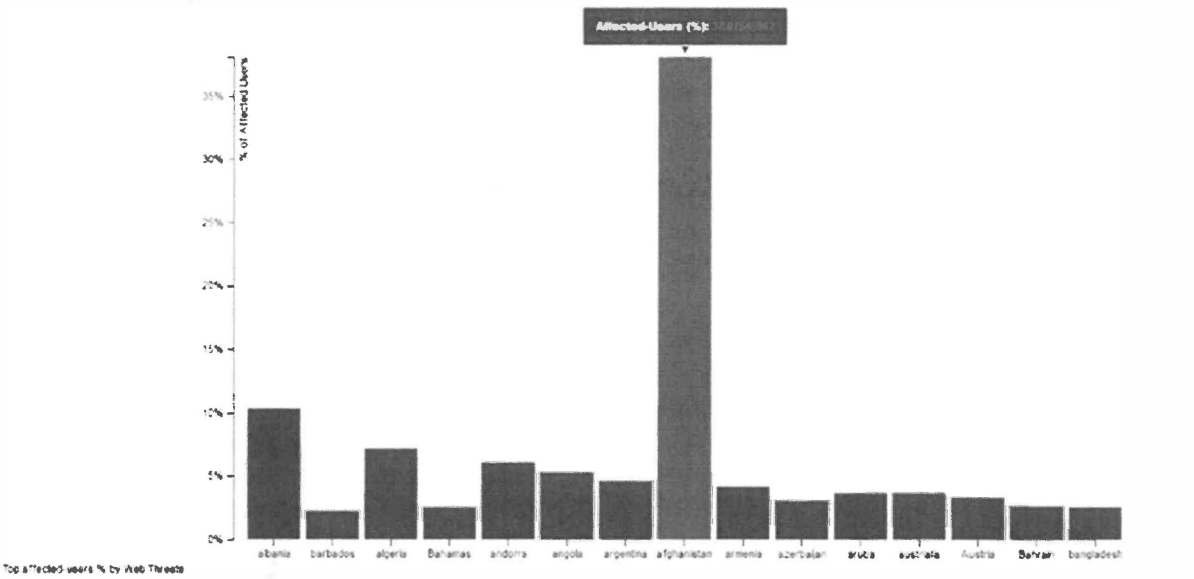


Fig 10:. Threat Report Statistical Visualization.

6 SVINT FRAMEWORK PURPOSE

As we have seen in Section IV, this framework is purposely implemented to aid law enforcement investigators in their investigations and during their day-to-day operations. The core aim is to provide a situational awareness method to the law enforcement sector around the world and assist them with confidence and trust-relationship of sharing and exchanging information/data to other countries involved in a certain investigation without revealing the underlying raw data. This framework serves the purpose of aiding investigators to effectively carry out their investigation with the use of simple security visualizations, i.e. simple visualization types and methods that investigators would spend minimal time to analyse a given visualization for useful insights.

6.1 Threat Report Visualization Features and Aspects

For the Blockchain visualization. The use of colours, links and circle sizes are for representation of different Bitcoin addresses. Different colours show distinctive wallet addresses and circle sizes shows the frequency of transactions made to other wallet addresses. The links represents the relationship of a particular Bitcoin transaction to the next wallet address.

Based on the size of the Bitcoin data extracted from the Blockchain explorer, the Blockchain visualization will show all bitcoin transactions from that given dataset. With the 3 different Blockchain visualization layouts, users can select "BTC Relationships" to visualize different Bitcoin transactions based on the user queries. This layout aims to deliver a one-to-one relationship among different Bitcoin wallet addresses and Bitcoin suspicious-tags.

As shown in Fig.7, the Blockchain Visualization is a 'Force-Directed Visualization, built using Hypertext Markup Language (HTML), Javascript (JS), CoffeeScript (a little language that compiles into JavaScript) and D3.js (A JavaScripting Visualization Library) [6], [7]. In order to use D3.js and CoffeeSscript within the HTML codes, links to the sources are added to the HTML codes as shown below:

1. < scriptsrc = " js=libs=d3:v2: js" >< =script >
2. <scriptsrc=" js=libs=co f f ee□script: js"><=script >

The Bitcoin block chain Visualization is designed to accommodate two parts: (1) general visualization of Bitcoin transactions based on suspicious transaction identifiers (TXIDs) tags and classifying them in various clusters and categories (Fig.7) and (2) a Bitcoin transaction relationship Visualization (Fig.8).

6.2 Threat Report Visualization Features and Aspects

The main objective of the threat report visualization is to provide law enforcement users with a clear understanding of security events derived from weekly and monthly Kaspersky Labs threat reports. It reduces the time spend on reading the malware threat logs (.xml &.xlsx files). Having the opportunity to observe malware threat reports a quick-to-action visual representation does help investigators to understand threats better. The key idea of visualizing various weekly and monthly threats and categorizing them according to 'top countries affected', will eventually show malware patterns. Such identification along with known intelligence could link to an organized cybercrime, and which attributes back to the people who are behind certain malware attacks. Below are the visualization features:

1. A geo-location malware threat map to show top malware threats around the world (Fig.9).
2. A user-affected statistical visualization to show most users-affected ranked into top countries affected (Fig.10).

7 EVALUATION AND VALIDATION

The research objective is to develop a security visualization intelligence framework that could facilitate information sharing and situation awareness amongst several law enforcement agencies. Based on the SVInt model assessment and evaluation process, a challenge encountered while visualizing the bitcoin transaction relationship was due to the default nature of how the block chain ledger works. Because we have identified that SVInt has potentials and strengths in moving forward into full implementation. The strengths and potentials identified for law enforcement benefits are:

1. The ability to anonymize the underlying raw data brings in the need to visualize, discuss and share information with other law enforcement agencies around the world.

2. SVInt was able to simplify the complex datasets into simple visual representations which are understandable by investigators.
3. Using visualization to act as a central security intelligence framework for law enforcement has able to capture the interest of law enforcement investigators to use the framework and process the data collected from various investigations.

Although there are existing frameworks and tools that address law enforcement investigations, their focus is targeted towards analysing the data and discovering potential crime related information that would be useful in the court of laws [26]. SVInt provides similar features however it goes beyond those purposes and facilitates information sharing and situational awareness for attribution purposes in forensics investigations amongst law enforcement agencies such as INTERPOL. However, due to policies and investigation confidentiality and information integrity, our findings were not fully reported.

7.1 Bitcoin Blockchain Visualization

A further analysis and evaluation of the Blockchain Visualization platform is to evaluate against existing Bitcoin tools. This will help identify the strengths and weakness of the tool. We look at Elliptic (a commercial Bitcoin visualization explorer) and Blockseer (an open source Bitcoin explorer). The Elliptic explorer tool is an exploration tool providing users with all the bitcoin links and highlighting known transaction IDs that have been involved with some form of Cybercrime. Blockseer have similar features but leverage on diagram visual platforms to present intelligence. The SVInt: Bitcoin visualization utilizes known suspicious transaction IDs and tags them for intelligence search during the visual analytics process. A challenge for the all bitcoin visualization including the SVInt: Bitcoin visualization, is the ability to visualize the relationship between the processes of payment due to how Bitcoin Block chain operate. Once a payment is about to be made, the wallet ID creates bitcoin transaction IDs (TXIDs) based within the bitcoin block node to handle payment. When the payment it made, that specific transaction node (TXID) is destroyed. Therefore, Attribution and tracking such links and relationships among Bitcoin payment is a current challenge. However, if the data has been logs during that process, SVInt Bitcoin Visualization can visually represent every transaction associated with the payment.

8 CONCLUSION

Attribution and evidence-preservation are critical during law enforcement investigations. Current methods of information sharing tools threatens the integrity of the evidence by revealing the sensitive underlying raw data during investigations. This can jeopardize the evidence collected of not worthy of being admissible into the courts. The centralized security visualization intelligence (SVInt) framework the means of sharing information across different parties while the underlying raw data remains preserved and untouched. It utilizes the Bitcoin block chain tool to visualize relationships between suspicious known transaction address tags that are involved in cybercrime activities. Moreover, it also presents a threat visualization feature utilizing the geo-location capability to visually identify malware attacks around the world on a weekly and monthly time frame.

This analytical visual intelligence method helps users to quickly understand security events faster. Secondly, the SVInt framework provides the investigators with the capabilities of visualizing monthly and weekly cyber threats to connect the dots between various malware attacks that are associated with known intelligence. Finally, the SVInt framework has been designed in a way that it would allow additional visualization features to the central framework, therefore making law enforcement investigators to easily toggle between various types of visualization from the central framework and utilize it for their investigations.

For future work, there is a need to fully develop SVInt framework and push it out to all law enforcement agencies in various countries to help them investigations. Secondly, further

enhancing the Bitcoin transaction relationship visualization to predict future transactions between various wallet addresses. In addition, develop visualization capabilities to show Bitcoin transaction provenance to show possible malicious attempts on the bitcoin block chain. Finally, expand the security visualization capabilities into visualizing correlations among multiple models such as the malware attacks and bitcoin payment flow to investigate and attribute possible links between organized crime offenders and the flow of bitcoin payments.

ACKNOWLEDGEMENT

The authors wish to thank the members of the IGCI Research & Innovation Directorate (IC) and Digital Forensic Lab (DFL) Team, Kaspersky Labs, Madan Mohan Oberoi, Steve Honnis, Christian Karam, Costel Ion, Thoshinobu Yasuhira, Elijah Moss Kipsoi, Margaret Samuel, Hiroki Kuzuno (Secom), STRATUS (Security Technologies Returning Accountability, Trust and User-Centric Services in the Cloud - (https://stratus.org.nz), a science investment project funded by the New Zealand Ministry of Business, Innovation and Employment (MBIE).) and the University of Waikato. This work was supported in part by INTERPOL Global Complex for Innovation (IGCI), STRATUS, University of Waikato (UoW) and the New Zealand and Pacific Scholarship programme (NZAid).

REFERENCES

[1] Stasko, C. Grg, and Z. Liu, Jigsaw: Supporting Investigative Analysis through Interactive Visualization, Information Visualization, vol. 7, no. 2, pp. 118132, Jun. 2008.

[2] H. Chen, H. Atabakhsh, C. Tseng, B. Marshall, S. Kaza, S. Eggers, H. Gowda, A. Shah, T. Petersen, and C. Violette, Visualization in Law Enforcement, in CHI 05 Extended Abstracts on Human Factors in Computing Systems, New York, NY, USA, 2005, pp. 12681271.

[3] D. K. Rossmo, Geographic Profiling, in Encyclopedia of Criminology and Criminal Justice, G. Bruinsma and D. Weisburd, Eds. Springer New York, 2014, pp. 19341942.

[4] Cellebrite - Mobile Forensics Products - Extraction. [Online]. Available: http://www.cellebrite.com/Mobile-Forensics/Products. [Accessed: 30-Apr-2016].

[5] Elliptic Enterprise Limited, Elliptic, Elliptic, 2017. [Online]. Available: https://www.elliptic.co/. [Accessed: 07-Feb-2017].

[6] Blockseer, BlockSeer — Features, 2015. [Online]. Available: https://www.blockseer.com/features. [Accessed: 07-Feb-2017].

[7] dfrws, Program, dfrws, 25-May-2016. [Online]. Available: http://dfrws.org/conferences/dfrws-usa-2016/schedule/program. [Accessed: 07-Feb-2017].

[8] DFRWS USA 2016, dfrws, 02-Jan-2016. [Online]. Available: http://dfrws.org/conferences/dfrws-usa-2016. [Accessed: 07-Feb-2017].

[9] J. Xu and H. Chen, Criminal Network Analysis and Visualization, Commun. ACM, vol. 48, no. 6, pp. 100107, Jun. 2005.

[10] Casey, Eoghan, Greg Back, and Sean Barnum. "Leveraging CybOX to standardize representation and exchange of digital forensic information." Digital Investigation 12 (2015): S102-S110.

[11] H. Chen, D. Zeng, H. Atabakhsh, W. Wyzga, and J. Schroeder, COPLINK: Managing Law Enforcement Data and Knowledge, Commun. ACM, vol. 46, no. 1, pp. 2834, Jan. 2003.

[12] H. Chen, J. Schroeder, R. V. Hauck, L. Ridgeway, H. Atabakhsh, H. Gupta, C. Boarman, K. Rasmussen, and A. W. Clements, COPLINK Connect: information and knowledge management for law enforcement, Decision Support Systems, vol. 34, no. 3, pp. 271285, Feb. 2003.

[13] Notices / INTERPOL expertise / Internet / Home – INTERPOL [WWW Document], n.d. URL http://www.interpol.int/INTERPOLexpertise/Notices (accessed 3.30.16).

[14] Research / Cybercrime / Crime areas / Internet / Home - INTERPOL. [Online]. Available: http://www.interpol.int/Crimeareas/Cybercrime/Research. [Accessed: 02-Aug-2016].

[15] INTERPOL, 2015. International Notices System. INTERPOL, n.d. Notices / INTERPOL expertise / Internet / Home - INTERPOL [WWW Document]. INTERPOL Notices. URL http://www.interpol.int/INTERPOL-expertise/Notices (accessed 3.28.16).

[16] Kaspersky Security Bulletin 2014. Predictions 2015 - Securelist [WWW Document], n.d. URL https://securelist.com/analysis/kaspersky-securitybulletin/67864/kaspersky-security-bulletin-2014-predictions-2015/ (accessed 3.30.16).

[17] Kaspersky Security Bulletin 2015. Overall Statistics for 2015 - Securelist [WWW Document], n.d.
URL https://securelist.com/analysis/kaspersky-securitybulletin/73038/kaspersky-security-bulletin-2015-overall-statisticsfor-2015/ (accessed 3.30.16).
[18] NATO, n.d. The history of cyber-attacks - a timeline [WWW Document]. NATO Review Magazine. URL http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm (accessed 3.30.16).
[19] Ashkenas, J., 2009. CoffeeScript [WWW Document]. URL http://coffeescript.org/ (accessed 3.31.16).
[20] Bostock, M., n.d. D3.js - Data-Driven Documents [WWW Document]. URL https://d3js.org/ (accessed 3.31.16).
[21] Bostock, M., n.d. Force-Directed Graph [WWW Document]. URL ttp://bl.ocks.org/mbostock/4062045 (accessed 3.31.16b).
[22] Bostock, M., Ogievetsky, V. and Heer, J., 2011. D data-driven documents. Visualization and Computer Graphics, IEEE Transactions on, 17(12), pp.2301-2309.
[23] B. Project, Developer Guide - Bitcoin, Bitcoin is an innovative payment network and a new kind of money, 2017. [Online]. Available: https://bitcoin.org/en/developer-guide#block-chain-overview. [Accessed: 23-Mar-2017].
[24] H. Kuzuno and C. Karam, Blockchain Explorer: An Analytical Process and Investigation Environment for Bitcoin. The twelfth Symposium on Electronic Crime Research (eCrime) 2017, April, 2017.
[25] S. by Baunfire.com, Agenda — APWG, Unifying the Global Response to Cybercrime, 26-Apr-2017. [Online]. Available: http://www.antiphishing.org/apwg-events/ecrime2017/agenda. [Accessed: 23-Mar-2017].
[26] Cross-jurisdictional Criminal Activity Networks to support border and transportation security. / Marshall, Byron; Kaza, Siddharth; Xu, Jennifer; Atabakhsh, Homa; Petersen, Tim; Violette, Chuck; Chen, Hsinchun. IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC. 2004. p. 100-105.
[27] Sohl, Eli, Curtis Fielding, Tyler Hanlon, Julian Rrushi, Hassan Farhangi, Clay Howey, Kelly Carmichael, and Joey Dabell. ”A Field Study of Digital Forensics of Intrusions in the Electrical Power Grid.” In Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, pp. 113-122. ACM, 2015.
[28] Ghafarian, Ahmad, and Syed Amin Hosseini Seno. ”Analysis of Privacy of Private Browsing Mode through Memory Forensics.” International Journal of Computer Applications 132, no. 16 (2015).
[29] J. Lessard and G. Kessler, Android Forensics: Simplifying Cell Phone Examinations. ECU Publications Pre. 2011, Jan. 2010. [30] V. L. L. Thing, K.-Y. Ng, and E.-C. Chang, Live memory forensics of mobile phones, Digital Investigation, vol. 7, Supplement, pp. S74S82, Aug. 2010.
[31] MSAB - The Pioneers of Mobile Forensics, MSAB. [Online]. Available: https://www.msab.com/. [Accessed: 30-Apr-2016].
[32] Barnum, Sean. ”Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX).” MITRE Corporation 11 (2012).