OPEN ACCESS 78

ISSN 2460-9056
http://socj.telkomuniversity.ac.id/ijoict/

Intl. Journal on ICT
Vol. 6, No. 2, Dec 2020. pp. 78-87
doi: 10.21108/IJOICT.2020.00.530

A Forensic Analysis Visualization Tool for Mobile Instant Messaging Apps

Ong Wee Sern [1], Nurul Hidayah Ab Rahman [1*]

[1]*Fakulti Sains Komputer dan Teknologi Maklumat, Universiti Tun Hussein Onn Malaysia*
86400 Parit Raja, Batu Pahat, Johor, Malaysia.

[*] hidayahar@uthm.edu.my

Abstract

Instant Messaging applications become the main tools to communicate with the others because they are free to use whenever there is internet connection. Therefore, evidence artefacts of IM apps which acquired from mobile devices (storage) would provide significant clues about an incident through digital forensics analysis activities. In this study, we demonstrate the role of visualization to facilitate forensic analysis goal in interpreting metadata of evidence of interest to answer who, what, why, when, where, and how an incident occurred. Two mobile Instant Messaging (IM) applications (i.e. WhatsApp and Line) were deployed as a case study. Subsequently, a tool – W*W Visualizer – was designed and developed with the aims to analyze and visualize the connection of evidence metadata, text frequency and word count, and display report of analysis activities. The tool is developed by adopting Object-Oriented Software Development Model with Visual Studio platform and C# language were used to develop the system. Our findings show that W*W Visualizer could transform the data of the chat database into a visual form, for example graph, chart and word cloud. The tool also allows the user to perform search feature such as searching based on keyword and timestamp from the IM chat history. It is expected that outcomes from this study would significantly influence digital forensics practitioners in analyzing and interpreting evidence data, and judicial authorities in understanding the presentation of evidence.

Keywords: Forensic analysis, Instant Messaging apps, Mobile forensics, Visualization

I. INTRODUCTION

The number of smartphone users are getting larger with the increasing number of users from 2.1 billion in year 2016 to around 2.5 billion in year 2019 [1]. The features capability of Instant Messaging (IM) applications such as WhatsApp, Viber, LINE, and WeChat are moving beyond text messages to video and voice calls, sharing media, documents and location posed overwhelming adoption among smartphone users.

The sophisticated features and popularity of communication apps, however, could be exploited as a platform for cybercrime activities including spread scam messages and malicious software, conduct cyber harassment and recruiting criminal members. Therefore, evidence artefacts of IM apps which acquired from mobile devices (storage) would provide significant clues about an incident through digital forensics analysis activities. Examples of key evidence artefacts are chat history, texts or emails, pictures or video recordings, phone number lists and call log.

Mobile forensics is a process to gather digital evidence from the information retrieved from the storage of mobile phone or smartphone [2]. Example of mobile phone forensics are taped conversations, texts or emails, pictures or video recordings, phone number lists and call log. Extraction of data from mobile phone can be done either physical extraction and/or logical extraction depending on the compatibility between forensic tools and smartphones [3]. It is important to obtain important information from mobile phone so that they can be used as

Received on 14 Oct 2020. Revised on 15 Nov 2020. Accepted on 16 Nov 2020. Published on 21 Nov 2020.

evidence in criminal, civil and even high profile cases [4]. However, the extracted raw databases of those applications are not in a human readable state.

This study is, therefore, aims to enhance evidence analysis by integrating information visualization approach to facilitate evidence interpretation and presentation. Visualization can be either symbolically or graphically that can ease users to spot patterns and correlations across a large dataset [5]. WhatsApp and Line are two IM apps that are deployed as a case study to demonstrate the tool's functionalities. Both apps are selected due to the popularity and at the Top 4 ranking of usage rank. WhatsApp Messenger, as an example, has been downloaded more than 100 million from Google PlayStore while Line Messenger hit more than 11 million downloads at the time of this study undertaken.

The objectives of this study are to design, develop and test a tool to visualize information from WhatsApp and Line chat database in facilitating digital forensics analysis. It should be noted that this tool does not involve forensic acquisition process and LinePay analysis.

This paper is organized into the following sections: Section 2 provides the review of this study background that includes visualization and forensic analysis. Section 3 describes the design and development of W*W tool. Section 4 presents findings and discussion and finally Section 5 concludes this study.

II. LITERATURE REVIEW

This section discusses the concept of visualization, issues in the forensic analysis of IM apps, and review of related work.

A. Visualization

James and Cook [6] highlighted visual analytics as a "science of analytical reasoning to synthesize information and derive insight from massive, dynamic, ambiguous, and often conflicting data; detect the expected and discover the unexpected; provide timely, defensible, and understandable assessments; and communicate assessment effectively for action", while intelligence visual analytics is a concept that combines visual interaction with automated analytical methods to identify the relationships of a dataset [7]. The aim is to apply visualization process as an aiding tool in processing data for analytic discourse that includes multidisciplinary areas such as analytical reasoning technique, visual representation, data representation and transformation, and techniques to disseminate analytical result [6], [8].

A proposed model by Card et al. [9] on non-computational visualization of abstract data is the most influential reference model for information visualization that transforms the raw data to views involving the human in the interaction processing. The transformation starts with data transformation processes, which transform multiple raw data into relations or sets of relations (data table). The mapping of the data tables to visual structures is the second step of the transformation process. The last step of the reference model transforms static graphical presentation by involving humans' interaction to produce distinct perspective of visual structures and provide an interactive visual environment. The time and correctness of the task completion are the two important elements for determine the effectiveness of visualizations.

B. Challenges of Instant Messaging Applications Forensic Analysis

Forensic analysis is one of the phases in digital forensics that is undertaken after evidence collection and examination. It involves "analyzing the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination" [10].

The challenges of forensic analysis involving mobile communication apps can be broadly discussed into three that includes (1) an increasingly used of the apps as a platform to launch cyber incidents; (2) difficulty in investigating and interpreting unstructured form of evidence data; and (3) the need to provide better understanding among legal communities during forensic presentation.

Taking cyber harassment incidents in Malaysia as an example, it has been noted as the third most dangerous threat after fraud and intrusion by the CyberSecurity Malaysia [11]. An example of a notable incident is a man was arrested under Section 233 of the Communications and Multimedia Act 1998 by the Malaysian police after

sharing an insulting photo of the former Malaysia's Prime Minister in a WhatsApp group, and caused the suspect's smartphone was seized as the evidence [12].

Searching for admissible evidence would involves extracting both textual and non-textual unstructured data (e.g. image, video, audio and documents) from IM apps. However, the form of unstructured data or massive data could lead to difficulty in forensic examination phase as well as time consuming. Although investigators are usually carried out cross analysis between different forensic software tool, but it lack of advanced visualization techniques to facilitate evidence analysis [13].

Results from the evidence analysis such as events reconstruction will then be presented to the judicial authorities. However, experience and training in handling electronic evidence could posed a gap between forensic practitioners and judiciary [14]. This also indicates the need for judicial authorities to be prepared with the growth of digital evidence in both volume and complexity. It also has been pointed out that the application multimedia technology is positively influenced the understanding of digital forensics [14].

C. A snapshot of related work

In the context of digital forensics, visualization can be applied to aid forensic analysis and interpretation as well as providing rapid and cost-effective investigations. For example, a graph-based feature analysis model is proposed by Wang et al. [15] to reduce and classify original criminal record where visualization techniques allow investigators to visually analyze the associations between features and criminals for better understanding on the activities or possibilities. Heuser et al. [16] presented DroidAuditor that applied graph-based presentation to visualize behavior graph in analyzing application-layer privilege escalation attacks in Android platform. Koven et al. [17] demonstrated visual email search and triage by integrating approaches from intelligent pre-processing and a context aware visual search, and display results that presents an integrated view of diverse information contained within emails. Similarly, Stadlinger and Dewald [18] provides interactive graph visualization of email data supported by statistical information, to assist investigators in identifying suspicious communication patterns.

Focusing on network forensics, Kotenko et al. [19] proposed an approach for network forensics based on different views on the network traffic, in which traffic were classified into slices and the slices were represented by different visualization model (e.g. bar chart, parallel coordinates, and triangular coordinated). Wijk [20] examined visually encoding traffic based on environmental knowledge to discover (un)desired traffic patterns for ransomware dynamic behavioral analysis.

Using cyber scammers as a case study, Koven et al. [21] demonstrated Beagle, a visual analytics tool that provides tagging capabilities to externalize knowledge built by investigators as addition to data querying, coordinated views, content extraction and summarization of email's data. A study by Lapso [22] applied visualization to present whitelisting system state in Windows forensic memory through simultaneous representation of the hierarchical and associative relationships and eliminating items of little interest from view.

Tassone, Martini and Choo [13] proposed three-stage forensic data storage and visualization life cycle in which first stage is data decoding, second stage is data storage in database, and third stage is visualization of the stored data.

Existing studies show that information visualization is a relatively mature area and have been integrated into digital forensics area. However, there are still lack of studies to forensically visualize evidence artefact from instant messaging applications. With the increasing use of emerging technologies, there is an urgent need to adopt the visualization to facilitate forensic analysis activities for the instant messaging applications.

III. SYSTEM DESIGN AND DEVELOPMENT OF W*W VISUALIZER

Object Oriented Software Development model was adopted from Singh and Malhotra [23] as development model in this study. It consists of four phases as follows:

i. System analysis - to define and analyze the requirements necessary by using modelling. Other key activities are selecting appropriate visualization model and conducting dataset collection to be used during Implementation.
ii. System design – to describe the interaction and relationship between classes are modelled into use case diagrams, sequence diagram, activity diagram and class diagrams by using Unified Modelling

Language (UML). Algorithm design has been carried out to transform the visualization model into algorithm, then code.

iii. Implementation - to implement all the features and develop the proposed tool according to the previous analysis and design. The proposed tool is developed by using C# programming language through Microsoft Visual Studio platform.

iv. Testing – to undertake system functional testing and users acceptance testing. System testing involves both functional and non-functional requirements.

A. Selection of Visualization Model

Selecting appropriate visualization model is a key to facilitate the evidence interpretation as well as improving the investigation time. In this section, examples of the visualisation model are discussed that include bar chart, word cloud, timeline, timespan and pie chart.

The Bar Chart - can either be horizontal or vertical - is used to show discrete, numerical comparisons across categories. Bar chart is therefore useful to present numerical IM metadata such as the number of the messages and frequent contact number from both single and group chat history.

A Timeline is used to display a list of events in chronological order in a graphical way. In W*W Visualization, Timeline presents the timestamp of users' activities such as chat conversation, sharing media, documents and video calls.

A Word Cloud, also known as a Tag Cloud, is used to display how frequently words appear in each body of text through the size of each word. The word size presents its frequency proportional. In this study, the word cloud shows the most frequent words the user used to represent the most frequent conversations of the user.

Pie Chart displays the proportions and percentages between categories, by dividing a circle into proportional segments. The full circle represents the total sum of all the data, which equal to 100%. In W*W, the pie chart shows the proportion of contacts' conversation in a group chat.

Timespan represents a time interval that is measured as a number of days, hours, minutes, seconds, and fractions of a second. The time intervals are usually measured in days because of the consistency. This study applies the timespan to show the duration of the conversation.

The visualization technique is chosen based on the type of data that need to be visualized. The example of function of each visualization technique is shown in Table 1.

TABLE I
SUMMARY OF VISUALIZATION TECHNIQUE AND FORENSIC ANALYSIS INTEREST

Visualization Technique	Examples of forensic analysis interest
Bar Chart	Shows the number of the messages, images, videos, voice messages and locations the user sent.
Timeline	Shows the time and the number of messages and files the user sent.
Word Cloud	Shows the most frequent words the user used or the most frequent conversation of the user.
Pie Chart	Shows which user write the most in a group chat.
Timespan	Shows how the duration of conversation.

B. Dataset collection

A pre-defined dataset was designed for WhatsApp and Line applications (apps). The dataset consists of 100 chat messages and 3 chat groups to both apps. Steps for collecting the pre-defined dataset were adopted and consistent in previous studies by [24], [25].

The simulations of common IM activities were undertaken that involved text chat, voice messages, video messages, sharing locations and images. Subsequently, databases for WhatsApp and Line were acquired using the forensically-sound mobile acquisition technique.

IV. W*W VISUALIZER: FINDINGS AND DISCUSSION

This section discusses the relation of the developed W*W modules with forensic analysis activities, and testing results that have been conducted. It should be noted that the acquisition of the IM apps' database is not in the scope of this study.

*A. The Role of W*W Visualizer in Forensic Analysis*

Analyzing digital evidence artefacts is a key to derive clues for events reconstruction. The integration of visualization in W*W Visualizer would demonstrate the use of visualization in facilitating forensic analysis activities.

Visualization of evidence artefact is commenced with users selecting to visualize evidence artefact from either WhatsApp or Line app. Subsequently, users need to import `msgstore.db` database if they choose Whatsapp app while `naverline.db` need to be imported for Line. As a result, list of the imported database tables appears where users can browse each of table.

Figure 1 presents the main page of W*W Visualizer. The summary of database is shown at the bottom of the main page presenting some details of the database, for example, the total number of messages, number of contacts, total number of images, videos and audio messages. The Menu section provides the Top Five Most Frequent Contact, Most Frequent Word and Frequency of Users in Group Chat in a visualization form that will be generated at the right bottom corner.

For example, the Top Five Most Frequent Contact is displayed in a bar chart form that illustrates contacts' name and their total number of chats (see Figure 1). Similarly, the Top Five Most Frequent Users from group chats also present the contacts' name and total number of chat conversations. This feature assists investigators to identify salient contacts and infer their relations.

Fig. 1. Main Page of W*W Visualizer

The Most Frequent Words is displayed in a word cloud form that tabulates the frequent words used from the whole chat conversations (see Figure 2). The use of word cloud would facilitate investigators to have a quick view of the noticeable words being used in the IM communications, as echoed in a study by [26].

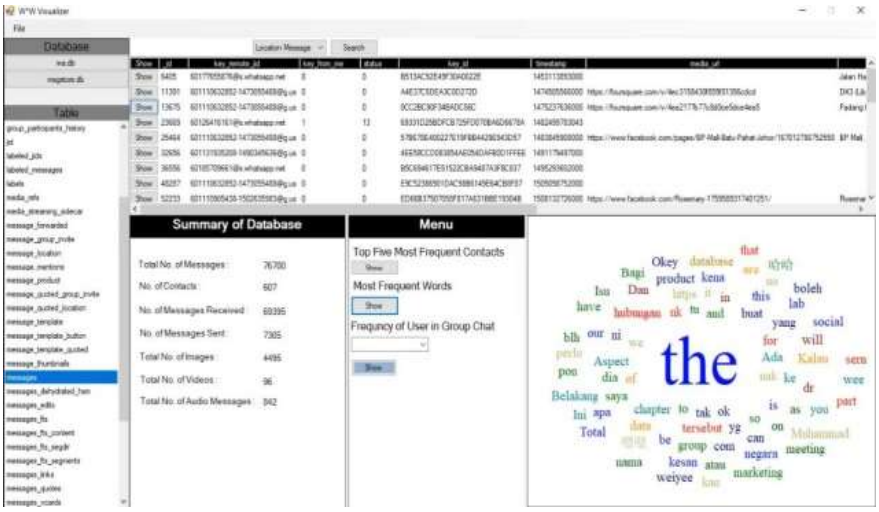

Fig. 2. Interface of Most Frequent Words

Other significant features involve searching through entire chat tables using Keyword, Timestamp, Phone Number, and Location. Keyword search is the most common technique used in forensic analysis as demonstrated in [17], [18]. In W*W Visualizer, a list of related chats that contains the inserted keyword is displayed (see Figure 3). Besides conversation, the chat list includes other significant metadata such as timestamp and phone number.

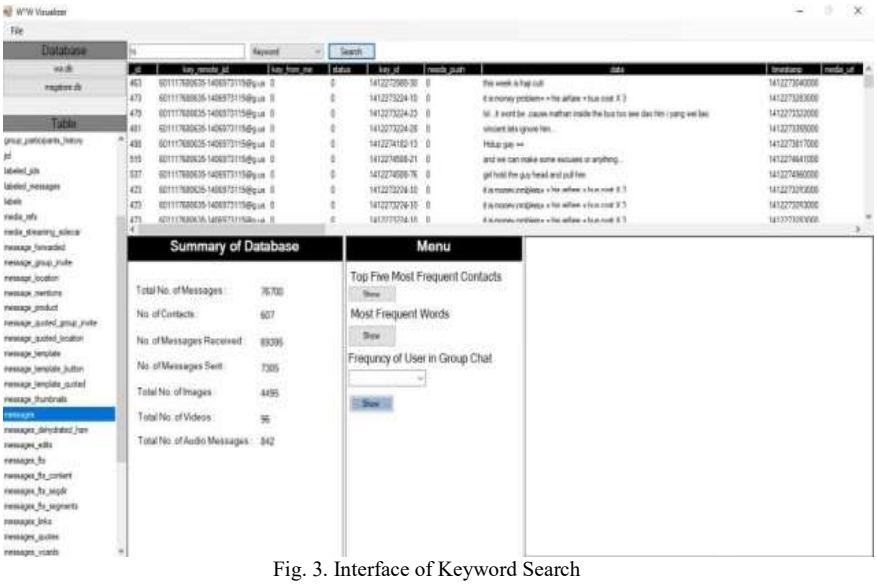

Fig. 3. Interface of Keyword Search

The importance of timestamp metadata in reconstructing events have been noted in previous studies [27]–[29]. As consistent with previous studies finding, W*W Visualizer provides timestamp search that enables users to select a specific date or time and subsequently display list of chats within the range of selected timestamp (see Figure 4).

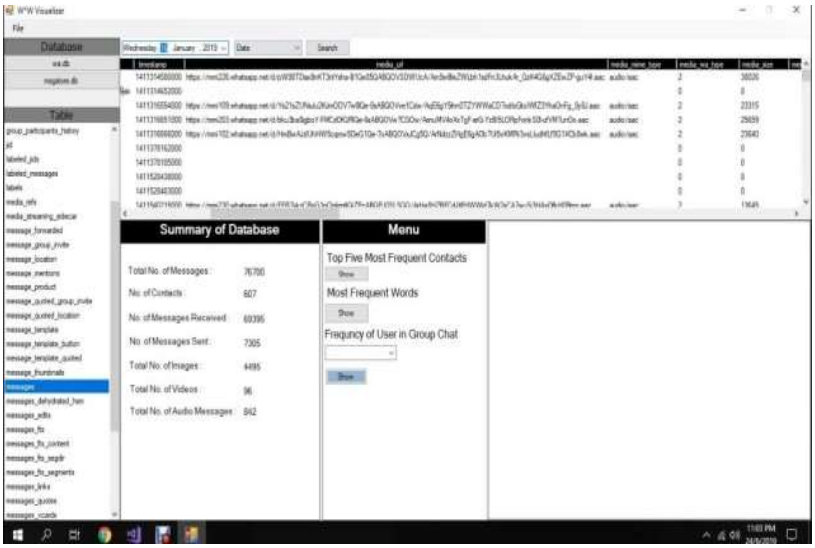

Fig. 4. Interface of Timestamp search

Sharing location is a common feature in any popular IM apps and would be one of the key metadata in an investigation. Investigating locations from raw data of IM database, however, would present investigators with GPS coordinates in which need to be manually search using other applications (e.g. Google Maps). Therefore, W*W Visualizer enables a pop-up map from GPS coordinates (see Figure 5). This feature is further indicates that visualization could influenced in minimizing tedious works and time taken, as echoed in Teerlink and Erbacher [30], and Koven et al [17].

Fig. 5. Interface of Map Display from GPS Location

W*W Visualizer demonstrates the role of visualization to reconstruct the chronology of events through evidence of interest such as contacts, timestamp, and chat history metadata. The features are in-line with studies in IM forensic analysis that highlight the correlation of multiple artefact (e.g. contacts list, timestamp, text history) from IM apps database to reconstruct the message chronology [25], [29], [31].

*B. Testing of W*W Visualizer*

We undertook system functional testing and user acceptance testing. In system functional testing, test plans were designed to examine if all functions work as intended. The test shows that all functions working properly. As an example, Table II presents the result from Main Page testing.

TABLE II
TEST CASE FOR MAIN PAGE INTERFACE

No.	Test Cases	Expected Output	Actual Output
1	Refresh the page after the user inserted database	The page is refreshed, and the data is shown.	The page is refreshed, and the data is shown.
2	Search bar	The user can perform search of metadata from the database.	The user can perform search of metadata from the database.
3	Visualize Function	The data is converted into graphs and word cloud.	The data is converted into graphs and word cloud.
4	Display summary of database	The system shows the display summary of database.	The system shows the display summary of database.
5	Export result into PDF file	The system exports the result into PDF file.	The system exports the result into PDF file.

A user acceptance test was carried out with 20 potential users comprise the third-year students in Bachelor of Computer Science (Information Security), Universiti Tun Hussein Onn Malaysia. The group is selected due to their (at least) minimum 3 years of experience in digital forensics and information security as well as programming practices. This test is carried out to examine two parts, namely: (1) all modules are well-functioned and (2) meet the aim of forensic analysis.

Our results show that all respondents are agree that W*W Visualizer is well-functioned while Table III presents results from the part no (2). Respondents are needed to give score based on the scale from 1(Strongly Disagree) through 5 (Strongly Agree).

TABLE III
USERS REVIEW RESULTS

No.	Description	1	2	3	4	5
1	The visualization of the data can facilitate the investigators.	0	0	2	14	4
2	The type of graphs and visualization method are suitable.	0	0	1	13	6

The first description examine if the visualization of the data can facilitate the investigators. 4 respondents (20%) strongly agree with the statement, 14 respondents (70%) agree with the statement while 2 respondents neither agree nor disagree with the statement. The second description examine if the type of graphs and visualization models are suitable. 6 respondents (30%) strongly agree with the statement, 13 respondents agree with the statement while 1 respondent neither agree nor disagree with the statement. Overall, the results indicate positive acceptance of W*W Visualizer from respondents.

V. CONCLUSION AND FUTURE WORK

In this study, we have demonstrated the design and development of W*W Visualizer, and testing results are discussed. Therefore, objectives of this study are successfully achieved. More importantly, the presented visualization features in W*W Visualization could facilitate investigators to reconstruct events of when, what, where, who, how, and which an incident or a crime took place.

We identified two major limitations in this study. First limitation is W*W Visualizer is only able to generate a few types of chart and the chart is pre-determined. Second limitation is the generated timestamp in W*W Visualizer is in the epoch format instead of data time. Taken the limitations into account, future work could consider the following improvements:

- Generate more types of visualization model to display evidence metadata - the model can be displayed in a dynamic approach in which users are able to select the model.
- W*W Visualizer could integrate more IM apps database.

It is expected that outcomes from this study would significantly influence digital forensics practitioners in analyzing and interpreting evidence data, and judicial authorities in understanding the presentation of evidence.

DATA AND COMPUTER PROGRAM AVAILABILITY

Data and program used in this paper can be accessed in the following site https://github.com/nurulh/W-W-Visualizer.

ACKNOWLEDGMENT

The authors express appreciation to the Ministry of Higher Education (MOHE) and Universiti Tun Hussein Onn Malaysia (UTHM). This research is supported by the Fundamental Research Grant Scheme (FRGS) grant (Vot 1640). Authors would like to thanks to anonymous reviewers for their feedback.

REFERENCES

[1] Statista, "Number of smartphone users worldwide from 2014 to 2020 (in billions)," 2018. .

[2] S. Alhidaifi, "Mobile Forensics : Android Platforms and WhatsApp Extraction Tools," *Int. J. Comput. Appl.*, vol. 179, no. 47, pp. 25–29, 2018.

[3] K. Curran, A. Robinson, S. Peacocke, and S. Cassidy, "Mobile Phone Forensic Analysis," in *Crime Prevention Technologies and Applications for Advancing Criminal Investigation*, 2016, pp. 250–262.

[4] R. V. Dharaskar, "Mobile Forensics : An Overview , Tools , Future trends and Challenges from Law Enforcement Perspective," in *6th international conference on e-governance, iceg, emerging technologies in e-government, m-government*, 2008, pp. 312–323.

[5] S. Lowman and I. Ferguson, "Web History Visualisation for Forensic Investigations," pp. 1–15, 2011.

[6] J. James and K. A. Cook, "A Visual Analytics Agenda," *IEEE Comput. Graph. Appl.*, vol. 26, no. 1, pp. 10–13, 2006.

[7] M. C. Hao and U. Dayal, "Intelligent Visual Analytics Queries," in *IEEE Symposium on Visual Analytics and Technology*, 2007, pp. 1–8.

[8] D. Keim *et al.*, "Visual Analytics : Definition , Process and Challenges," in *Information Visualization - Human-Centered Issues and Perspectives*, Springer, 2008, pp. 154–175.

[9] S. K. Card, J. D. Mackinlay, and B. Scheiderman, *Readings in Information Visualization: Using Vision to Think (Interactive Technologies)*, 1st Editio. 1999.

[10] K. Kent, S. Chevaliar, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," 2006. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf. [Accessed: 30-Mar-2014].

[11] F. H. Rashid, "Cyberbullying among top five online threats," *News Straits Times*, 2017. [Online]. Available: https://www.nst.com.my/news/exclusive/2017/05/236873/cyberbullying-among-top-five-online-threats. [Accessed: 09-Jan-2019].

[12] N. Claudia, "Man Arrested After Posting Picture Insulting Najib on WhatsApp Group," *World of Buzz*, 2016. [Online]. Available: https://www.worldofbuzz.com/man-arrested-posting-picture-insulting-msia-pm-whatsapp-group/. [Accessed: 09-Jan-2019].

[13] C. Tassone, B. Martini, and K.-K. R. Choo, "Forensic Visualization: Survey and Future Directions," in *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, Elsevier Inc., 2017, pp. 163–184.

[14] N. D. W. Cahyani, B. Martini, and K.-K. R. Choo, "Do Multimedia Presentations Enhance Judiciary's Technical Understanding of Digital Forensic Concepts? An Indonesian Case Study," in *Proceedings of Hawaii International Conference on System Sciences (HICSS 2016)*, 2016, pp. 5617–5626.

[15] W. B. Wang, M. L. Huang, J. Zhang, and W. Lai, "Detecting criminal relationships through SOM visual analytics," *Proc. Int. Conf. Inf. Vis.*, vol. 2015-Septe, pp. 316–321, 2015.

[16] S. Heuser, M. Negro, P. K. Pendyala, and A.-R. Sadeghi, "DroidAuditor: Forensic Analysis of Application-Layer Privilege Escalation Attacks on Android," in *Financial Cryptography and Data Security*, 2016, pp. 260–268.

[17] J. Koven, E. Bertini, L. Dubois, and N. Memon, "InVEST: Intelligent visual email search and triage," *Digit. Investig.*, vol. 18, pp. S138–S148, 2016.

[18] J. Stadlinger, A. Dewald, J. Stadlinger, and A. Dewald, "A Forensic Email Analysis Tool Using Dynamic Visualization," vol. 12, no. 1, 2017.

[19] I. Kotenko, M. Kolomeets, A. Chechulin, and Y. Chevalier, "A visual analytics approach for the cyber forensics based on different views of the network traffic," vol. 2, no. June, pp. 57–73, 2018.

[20] V. Wijk, "Eventpad : Rapid Malware Analysis and Reverse Engineering using Visual Analytics Eventpad : Rapid Malware Analysis and Reverse Engineering using Visual Analytics," 2018.

[21] J. Koven, C. Felix, H. Siadati, M. Jakobsson, and E. Bertini, "Lessons Learned Developing a Visual Analytics Solution for Investigative Analysis of Scamming Activities," *IEEE Trans. Vis. Comput. Graph.*, vol. 25, no. 1, pp. 225–234, 2018.

[22] J. A. Lapso, "Whitelisting System State in Windows Forensic Memory Visualizations," Air Force Institute of Technology, 2016.

[23] Y. Singh and R. Malhotra, *Object-Oriented Software Programming*. PHI Learning Pvt. Ltd., 2012.

[24] G. Grispos, W. B. Glisson, and T. Storer, "Using smartphones as a proxy for forensic evidence contained in cloud storage services," in *Proceedings of the 46th Annual Hawaii International Conference on System Sciences*, 2013, pp. 4910–4919.

[25] N. D. W. Cahyani, N. H. Ab Rahman, W. B. Glisson, and K.-K. R. Choo, "The role of mobile forensics in terrorism investigations involving the use of cloud storage service and communication apps," *Mob. Networks Appl.*, 2016.

[26] N. Diakopoulos, M. Naaman, and F. Kivran-swaine, "Diamonds in the Rough : Social Media Visual Analytics for Journalistic Inquiry," in *IEEE Symposium on Visual Analyics and Technology*, 2009, pp. 115–122.

[27] A. Ariffin, C. D'orazio, K.-K. R. Choo, and J. Slay, "iOS forensics: How can we recover deleted image files with timestamp in a forensically sound manner?," in *Proceedings of the 8th International Conference on Availability, Reliability and Security*, 2013, pp. 375–382.

[28] N. H. Ab Rahman and K.-K. R. Choo, "A Survey of Information Security Incident Handling in the Cloud," *Comput. Secur.*, vol. 49, pp. 45–69, 2015.

[29] C. Anglano, "Forensic Analysis of WhatsApp messenger on Android smartphones," *Digit. Investig.*, vol. 11, pp. 1–13, 2014.

[30] S. Teerlink and R. F. Erbacher, "Foundations for Visual Forensic Analysis," in *Proceedings of the 7th IEEE Workshop on Information Assurance*, 2006, no. June, pp. 21–23.

[31] C. Anglano, M. Canonico, and M. Guazzone, "Forensic analysis of the ChatSecure instant messaging application on android smartphones," *Digit. Investig.*, vol. 19, pp. 44–59, 2016.