A Survey of Forensic Analysis and Information Visualization Approach for Instant Messaging Applications

Shahnaz Pirzada[1], Nurul Hidayah Ab Rahman[2], Niken Dwi Wahyu Cahyani[3], Muhammad Fakri Othman[4]
Centre for Information Security Research, Universiti Tun Hussein Onn Malaysia, Parit Raja, Malaysia[1, 2]
School of Informatics, Telkom University, Bandung, Indonesia[3]
Application & Research on Multimedia, Universiti Tun Hussein Onn Malaysia, Parit Raja, Malaysia[4]

***Abstract*—Instant messaging applications, including WhatsApp, Viber, and WeChat, are moving beyond text messages to videos and voice calls, which are proportioned to current media, files, and locations. In this study, we surveyed existing forensic visualization and forensic analysis techniques for instant messaging applications, with the aim of contributing to the knowledge in the discussion of these research issues. A total of 61 publications were reviewed after searching various academic databases, including the IEEE, ACM Digital Library, Google Scholar, and Science Direct during the last five years. Our observation from research trends indicates that both forensic analysis and information visualization are relatively mature research areas. However, there is a growing interest in forensic visualization and automated IM forensic analysis. We also identified the lack of discussion on forensic selection criteria in existing forensic visualization works and the needs of benchmarking the evaluation method of automate forensic analysis tools.**

***Keywords*—Forensic analysis; forensic visualization; instant messaging apps; mobile forensics; and mobile communication apps**

I. Introduction

Mobile Instant Messaging (IM) applications (apps) are becoming essential for smartphone users in their daily communication activities. As reported by Statista [1], the number of smartphone subscriptions worldwide in 2021 surpassed more than seven billion. Some of the most widely used IM apps include LINE, WhatsApp, WeChat, and Facebook Messenger [2]. As an example, WhatsApp has been upgraded beyond a basic messaging app to support more sophisticated features such as end-to-end encryption, deleting sent messages, and enable disappearing messages. These features, however, could be exploited by cybercriminals targeting IM apps for criminal activities.

According to a Norton report, malware, keylogging, and social engineering are the top three potential cybersecurity risks related to IM apps [1]. This is consistent with a report by Kaspersky, which showed that 341,954 attempts to follow phishing links were blocked in 2021, with 90% links coming from WhatsApp [2]. Furthermore, phishing statistics reported by PurpleSec identified that WhatsApp is one of the top three most impersonated brands in phishing attacks [3], [4].

In the context of smartphones, the acquisition of digital evidence involves mobile forensic techniques [7]. The acquired artifacts can be valuable, as these include various significant metadata, such as application data, communication data, location data, and browsing history data. These data are, however, produced in unstructured data - raw data that are not in the organized data model form. The unstructured data could be challenging for forensic examination activities, for instance time-consuming and increase investigation cost [8], [9].

Therefore, there has been significant interest in examining appropriate approaches to expedite digital forensic analysis activities. One of the potential approaches is the use of forensic visualization. It is a common practice for digital forensic investigators to perform cross-analysis using various forensic software, but there is a lack of advanced visualization approaches to facilitate evidence analysis [5]. It also has been pointed out that the application of multimedia technology in presenting digital evidence could increase judicial understanding [6], [7], [8].

In this study, we explored the literature on forensic analysis of mobile applications, information visualization, and forensic visualization. The contributions of this work are twofold: (1) to provide insights into digital forensic analysis and the development of its automated tools, forensic analysis of IM apps, and forensic visualization to assist forensic analysis, and (2) to discuss the research trends and future research directions for these areas, including the potential of incorporating forensic visualization in IM forensic analysis. The knowledge gaps are identified from this study such as the needs of evaluation benchmarking and the lack of forensic selection criteria in the existing studies.

The remaining sections of this survey paper are organized as follows: Section II presents the review methodology while in Section III, associated works addressing forensic analysis and the techniques of visualization and mobile forensic analysis are discussed. Section IV reviews existing work in forensic analysis of IM apps. Section V discusses the role of forensic visualization in forensic analysis. Section VI presents the discussion on the research trends of forensics visualization and mobile forensic analysis techniques for future works. Section VII concludes this study.

II. Review Methodology and Process

A literature survey in forensic analysis, forensic visualization, and information visualization was performed by adopting the method used in [9] and [10] (see Fig. 1).

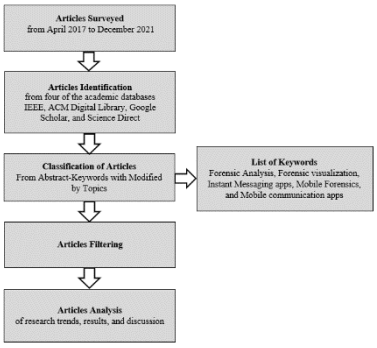

Fig. 1. Data collection method

To obtain a fair overview of the literature on forensic analysis and information visualization, we surveyed materials published in the English language over the past five years (i.e., April 2017 to June 2022). A total of 61 publications were located after searching various academic databases, including the IEEE, ACM Digital Library, Google Scholar, and Science Direct.

The search words used were different in each case, such as "digital forensics", "forensic analysis", "intelligent visual analytics digital evidence", "mobile forensics", and "information visualization". For the search in Title, Abstract, and Keywords, quotation marks were entered and modified by topic, such as "forensics visualization", "information visualization in digital forensics", "forensic analysis in visualization", and "forensic analysis in mobile application". We filtered the articles from the search results to include "digital forensics", "forensic analysis", and "visual analytics". We utilized the term "Web of Science" in title, abstract, and keyword searches in Advanced Search, and searched within Topics. Furthermore, we defined the document type as "articles" with no restrictions for all search results, and we only looked at journal publications.

III. Digital Forensics Analysis

Forensic analysis is one of the phases in digital forensics, which 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." [11]. More importantly, forensic analysis encompasses the gathering of evidentiary materials, evidence interpretation, results validation, and evidence presentation in an intelligible manner [12].

As discussed in [13], event reconstruction includes the combination of temporal, functional, and relational analyses of available evidence artifacts. Temporal analysis includes searching for other events that occurred around similar timestamps as those of one or more events already identified as related to the case being investigated. Functional analysis involves understanding what actions were possible within the environment of the offense and how the offender's toolkit works. Relational analysis involves studying how the various systems involved in a compromise relate to each other and how they interact.

String and keyword search, file filtering, and timeline analysis are examples of commonly used techniques in forensic analysis. String and keyword searching techniques can be used to filter out words, phrases, strings, and keywords that provide clues when searching for evidence. It is one of the primary features used in both commercial and non-commercial forensic tools, (e.g. Magnet Axiom, Autopsy). It has also been widely validated in academic forensic investigation studies, such as those analyzing web URL information [14]. Nowadays, the conventional keyword searching technique might be limited in a large volume of data, as it could lead to false negative or false positive and requires background knowledge about the case [15]. Therefore, studies such as [16] and [17], have examined the use of the semantic-based approach for text clustering with the aim of improving the performance and accuracy of forensic analysis.

Another technique, known as file filtering, can be applied as digital sieving of important files from irrelevant files by utilizing cryptographic hashes to screen the hash values of target files. For example, when using the MD5 Hash (and/or SHA-1 Hash) and Known File Filter options to process evidence, a hash value for each item is generated. The hash value of each file item inside the evidence is computed, and known files are filtered for the freshly computed hash value data [18]. The file filtering technique is significant in forensically examining file systems, for example, examining file similarities, as in [19], and examining file types, as in [20]. A limitation of this technique, however, is that it cannot be applied to corrupted files.

The timeline analysis technique is a chronological analysis of incidents to display all occurrences in a chronological sequence. However, emerging computing pose various factors that must be considered to generate a unified timeline, such as different time zone settings, timestamp interpretations, clock skew, and syntax [21]. Therefore, manual timestamp inspections may no longer be adequate to support investigations. Some recent studies have applied other scientific methods to enhance temporal analysis such as visualization approach, such as using graph-based and ontology-based approaches [22], [23] and highlighting patterns in the timeline analysis [24], [25], [26].

It is unlikely that a single method of data analysis is applied when examining digital evidence, as the evidence could have multiple interactions. The applied methods of data analysis can be mixed, depending on the complexity of a system's architecture. For example, Carrier [27] presented data analysis based on layers, in which physical storage media analysis was the bottom layer. The next layers comprised volume analysis, memory analysis, file system analysis, and database analysis, while application analysis was the top layer. In a work by [28], the authors demonstrated system analysis, operating system analysis, application analysis, network analysis, device analysis, and Shim cache analysis to present Windows registry

forensics. Analyzing cloud apps on Android mobile devices, [29] demonstrated the analysis of app files in private storage, external storage, app database, and app account data and analyzed apps using the static and dynamic analysis approach. X. Zhang et al. [30] performed IoT botnet forensics by applying network traffic analysis, servers' disk analysis, servers' memory analysis, and database analysis. As described in these works, the configurations and deployments of systems architectures can vary. Undertaking the tasks manually may result in advertent or inadvertent mistakes and biases. The advancement of computing infrastructures and the interconnection of devices have made the tasks more complex and time-consuming. Hence, the automation of the tasks is essential to improve the efficiency of forensic analysis.

B. Metrics of Automated Forensic Analysis Tools

The development of automated forensic analysis tools is a developing field with a wide range of scientific techniques applied in many cyber forensics areas to keep pace with evolving computer generations [31]. Ayers [32] proposed seven metrics for computer forensic tools that are absolute speed, relative speed, reliability, accuracy, completeness, auditability, and repeatability.

Absolute speed, which refers to the elapsed time required to complete analysis tasks. Relative speed, which involves the average rate at which the tool can process evidence compared with the rate at which data can be read from the original evidential media. Reliability, which includes the proportion of tests that the tool executes successfully, as in performing without crashes and providing outputs in the intended format. Accuracy, which refers to the proportion of analysis results that are correct. Completeness, which concerns the proportion of evidence artifacts present in a forensic image that are identified and reported by the tool. Auditability, which includes the proportion of results that are fully auditable back to the original evidence data. Repeatability, which involves the proportion of tests that ran as stipulated in every aspect. Table I summarizes the applied forensic tools metrics in existing works related to forensic analysis tools.

TABLE I. A SUMMARY OF FORENSIC TOOL METRICS USED

Metric	**A. Singh et al.** [28]	**Lin et al.** [33]	**Kumar et al.** [34]	**Subedi et al.** [35]	**Anglano et al.** [36]
Absolute speed	√	√ (efficiency)	-	-	-
Relative speed	-	-	-	-	-
Reliability	√	-	-	-	-
Accuracy	-	√	√	√	√
Completeness	√	√	-	-	√
Auditability	-	-	-	-	-
Repeatability	√	-	-	-	√ (fidelity)
Other metrics	-	effective	-		effectiveness, generality, repeatability

In practice, it is unlikely for a study to include all the specified metrics in a tool due to the limited scope, time, and tool functionality. It has been observed that completeness and accuracy are the most applied metrics. The metrics are consistent with digital evidence principles by the RFC 3227 [37].

There are also other studies that proposed new or additional metrics to evaluate forensic tools. For example, Lin et al. [33] used the effective metric to evaluate their tool's efficacy in locating the source of the evidence artifact. Additional metrics proposed by Anglano et al. [36] are (1) effectiveness, which is the ability to correlate users' actions with the generated data, and (2) generality, which is the ability to analyze any mobile application on as many different Android devices as possible. It is observed that this work defined the repeatability metric as the ability to provide to a third party the possibility of replicating the same set of experiments. Considering the repeatability definition by Anglano et al. [36], we argue that all works shown in Table I are repeatable because detailed methodologies were provided. Furthermore, it is essential for academic work to provide a repeatable methodology for comparison with other similar research works. Other notable observations are that: (1) aforementioned studies used the same term to discuss different evaluations, such as Anglano et al. [36] using the "effective" term to discuss correlation ability, while Lin et al. [33] used the term to discuss the ability to locate data, and (2) the studies used different terms to describe the same evaluation, for example, Anglano et al. [36] using "fidelity" as a term to discuss repeatability.

IV. FORENSIC ANALYSIS IN MOBILE COMMUNICATION APPS

Examining IM apps is one of the continuous research works in mobile forensics. In addition, new updates of apps' features pose challenges for mobile forensics practices [38]. In this section, we describe the basic concepts of mobile forensics, and recent works involving the forensic analysis of mobile IM apps are reviewed.

A. Forensic Analysis of Mobile Instant Messaging Apps

Forensic analysis of mobile IM apps has received considerable attention and is rapidly emerging in recent years. For example, Anglano et al. [39] performed an in-depth analysis on how to decode, interpret, and correlate the data generated by users, using Telegram Messenger as a case study. The experiments involved user account information, contacts, chats, message exchanges, phone calls, and deleted information. The proposed methodology of this work was evaluated based on completeness, repeatability, and generality. It should be noted that analysis tasks were conducted manually and involved the evaluation of sources. The study's event reconstruction includes temporal and relational analyses. In a similar vent, Akinbi and Ojie [40] demonstrated forensic analysis of Conversation and Xabber apps on Android smartphones. The study discussed the results obtained from the completeness of recovered data, the sources of data, and timeline analysis to present the chronology of chat logs, message contents, and deleted files.

Riadi and Firdonsyah [41] compared mobile forensics tools' effectiveness on four IM apps, which were Short Message Service, Blackberry Messenger (BBM), LINE, and WhatsApp. The applied tools in this study were Andriller, Oxygen Forensic Suite, WhatsApp DB/Key Extractor, and Metasploit. The experiments were conducted on Android smartphones and an Android smartwatch. Tool effectiveness was evaluated using the success rate percentage of artifact extraction, in which Oxygen Forensic Suite showed the highest success rate at 57.14% on BBM and WhatsApp, while Smartwatch achieved 42.85% success rate on SMS and LINE. Additionally, the completeness of the recovered artifacts was evaluated using the percentage of artifact extraction.

Due to concerns over privacy, the features of encrypted chat and end-to-end encryption have been updated in some IM apps. These pose another dimension in forensic analysis of investigating possible ways to recover data from encrypted databases. For example, [42] examined the encryption status of WhatsApp, Facebook Messenger, LINE, and Hangouts on Android smartphones. The study compared encrypted and unencrypted databases between rooted and unrooted smartphones. The results of the recovered data from unencrypted databases were presented in terms of the point of origin of data, database structures, and data completeness. Rathi et al. [43] performed forensic analysis tasks on four encrypted Android IM applications, which were WeChat, Telegram, Viber, and WhatsApp. It was demonstrated that encrypted WeChat and Viber databases can be acquired from rooted devices, WeChat database can be decrypted using the IMEI number and the phone identifier encryption key, WhatsApp messages can be acquired from unrooted devices, WeChat data can possibly be retrieved from unrooted devices by downgrading the app version, and Telegram data were irretrievable from unrooted devices. However, with the current version of the WeChat application, the approaches used in their study are no longer valid [44]. Although this study did not directly specify the evaluation method, it has been observed that the forensic analysis result was presented based on the completeness criterion. The analysis tasks were undertaken manually and involved the evaluation of evidence sources.

Also focusing on the decryption methodology for forensic analysis, [45] investigated Wickr and Private Text Messaging apps on both rooted and unrooted Android smartphones, as well as jailbroken and non-jailbroken iOS smartphones. The results of this study showed that the proposed method was able to decrypt the databases of both apps and examine the encrypted databases' structure. The verification method of recovered user-entered password was used to decrypt the entire data. The method was evaluated based on the efficiency of estimated password recovery time. It is observed that this work focused on cryptographic contribution, as there was no discussion on data completeness and sources of evidence.

There are studies that attempted to compare recovered data from volatile and non-volatile memories. Focusing on Android LINE Messenger, [46] examined data remnant through the simulation of user activities, such as installation, uninstallation, logins, conversations, file transfer, and other LINE activities. The findings of the study showed that evidence artifacts from the LINE app can be recovered from both volatile and non-volatile memories. Similarly, their study attempted to analyze the artifacts using the evaluation metrics of evidence sources and completeness. Agrawal and Tapaswi [47] conducted the forensic analysis of the Android Google Allo messaging app. The study demonstrated manual analysis tasks on device images. An interesting observation is that this study applied inferential statistics to evaluate the completeness metric. The recovered files were evaluated based on the point estimation value, while margin of error was used to calculate confidence limits. Another study that applied the inferential statistics concept was conducted in [48]. The study demonstrated the residual data of Android Kik Messenger on the NAND flash memory and the heap memory. The results of this study were presented by comparing the count and the average number of recovered messages between the NAND memory and the RAM memory.

Considering the extensive manual tasks of forensic analysis, some studies have proposed the development of automated tools. Barradas et al. [49] demonstrated forensic analysis tasks on eight messaging apps, which were Facebook Messenger, WhatsApp, Viber, Signal, Twitter, Telegram, Hangouts, and Trillian. The proposed tool, called RAM Analysis System (RAMAS), was designed based on the file-carving approach to extract potential evidence artifacts from physical memory. This study simulated common user activities on messaging apps. The performance of RAMAS was measured using the analysis time metric by varying the memory image size and the number of modules. The results indicated that reducing the set of strings improved the elapsed time, while running several modules in parallel resulted in a sub-linear time for analysis completion. The tool also supported event reconstruction tasks by applying the timeline analysis technique.

Nizam et al. [50] presented a tool to automate keyword indexing to assist the forensic analysis of WhatsApp. The main module of the tool involved loading a list of keywords from selected crime categories and uploading WhatsApp chat text files. Subsequently, a text-matching algorithm was executed, and a keyword count that showed the number of found keywords in the chat files was generated. The tool was tested using software engineering properties, which were application functionality testing and user acceptance testing. No event reconstruction feature was observed in this tool.

Using WhatsApp and LINE as case studies, [51] proposed a tool that applied the information visualization approach to support forensic analysis activities. Using visualization techniques, the tool was able to visualize key information, such as total number of messages, number of contacts, top-most frequent contact, top-most frequent words, and location map. Event reconstruction was supported by this tool using the timeline analysis approach. As in [50], this tool was evaluated through functionality testing and user acceptance testing.

A notable observation found from these works is that the simulation of user activities on the studied apps was used to elicit the generation of artifacts. The recovered artifacts from IM apps were mainly associated with user account information, contact information, chat histories, message exchanges, media exchanges, phone calls, app database, and deleted information.

Furthermore, analysis results from rooted and unrooted Android devices or jailbroken and non-jailbroken iOS devices presented significant differences involving encrypted data. Most of the studies examined recovered artifacts on device images manually, except for a few studies that used proposed automated tools. We also note that results from the metrics of origin of artifact and completeness of recovered artifact were the two predominantly reported forensic analysis results. Evaluation metrics, however, varied in these studies, and several studies did not directly specify their metrics. We discuss our further observation of the trends of studies on forensic analysis of IM apps in Section V.

V. An Overview of Information Visualization

Information visualization is the process of displaying data as graphical markings on a computer screen or other media, to enhance people's ability to recognize visual patterns, such as watching, browsing, discriminating, and comprehending data [33]. Information visualization (InfoVis) is considered as a mature area, as evidenced in a study by Rees and Laramee [52], which surveyed over 23,000 pages of information visualization books. The study also highlighted that InfoVis research papers were cited in many areas, including networks, finance, healthcare, and security.

Data types in InfoVis can be classified into multi/high-dimensional, relational, sequential/temporal, geospatial, and textual [53]. Multi-dimensional and high-dimensional data are presented in a table-like form, where the rows denote data objects, while the columns denote data dimensions, attributes, features, or descriptors. Relational data refers to the common case of binary relations and are represented as graphs. Sequential and temporal data concern the serial order of data points in a sequence, for instance, the time series data. Geo-spatial data involves creating maps of the real world to visualize spatial and non-spatial relationships among the data. Textual data are inherently multivariate data sources, for example, text corpora as a semi-structured source of information integrated with approaches (e.g., semantic, text-mining) to transform raw texts into structured data sources.

Sorapure [54] discussed four key elements in InfoVis for improving data interpretation, which are text, image, data, and interaction. Text is often included as titles, labels, annotations, explanations, and other commentaries. Significant functions of text are guiding interpretation, providing explanation, establishing context, and facilitating navigation. The image element concerns generating and maintaining users' interest by selecting the most effective ways to convey information. Data literacy is important in enabling users to formulate questions and make decisions informed by the data. It involves creating arguments based on the data, effectively using tools to manipulate and represent the data, and being able to communicate with the data. Interactions include activities from users, such as selecting, exploring, reconfiguring, encoding, abstracting, filtering, and connecting, to establish interactions with InfoVis.

The application of InfoVis in many different fields further indicates that it is a reliable approach to support data interpretation and decision-making tasks. In the context of digital forensic analysis, interpreting gathered evidence is the key to establishing connections in crime investigations. With the use of intelligent computing and decision-support frameworks, InfoVis has a significant role in assisting forensic analysts in digital evidence analysis activities [55].

A. Role of Visualization for Forensic Analysis

The use of information visualization techniques in digital forensics has received considerable interest in the digital forensics' community. Existing works applied information visualization to visualize forensic data using various case studies, such as mobile phones, network data, IoT data, and Windows system files.

A study in [56] demonstrated how visual representation could support faster and more accurate decision-making during real-time digital forensics investigations. The Nested Blocks and Guidelines Model (NGBM) was adopted to design the visualization interactions in this study. Using fileless malware as a case study, the usability of the proposed tool was evaluated through the tool's components, such as investigation timeline, network activity, read/write entropy, and system performance. Examples of the used data were "time series", "IP Address"," Windows Event Logs", "PowerShell Events", and "Syslog", while the involved visualization methods were line charts, ellipses, area charts, and time series.

Tassone et al. [5] proposed a proof of concept to visualize digital forensics datasets that consisted of three stages of visualization lifecycle, which were decode, store, and visualize. Three visualization techniques were used, namely treemap, geographic map plot, and word cloud. This study used three case studies to represent the XRY mobile forensics dataset to evaluate tool utility. The treemap technique was used to visualize SMS messages, the geographic map technique was used to map locations from a coupon app, and the word cloud technique was applied to visualize data from a text-based communication app. The three case studies were able to demonstrate the utility of the tool.

Kotenko et al. [57] proposed a visual analytics approach for network forensics to analyze network traffic. The proposed approach consisted of two stages, which are data slice classification and the selection of an information visualization model. The visualization model can be determined from data types, such as numerical (e.g., pie chart, bar chart), tree (e.g., TreeMaps), planar (e.g., Voronoi Maps), semi-structured (e.g., Chord diagram), unstructured (e.g., graph), and a combination of data types and models. The usability of the proposed tool was evaluated using a case study of an SSL-strip attack that involved 200584 network packets in the files. The model was demonstrated in a three-hour training lab session, in which the result showed that 8 out of 10 students were able to solve the use-case within the lab session using the proposed visual analysis tool.

Also investigating network traffic data, [58] applied a 3D model and the use of time-based information as a display third axis, combined with a computer network topology in a single interactive data. The proposed tool, Scanmap3D, was evaluated based on its effectiveness to solve questions from network forensics challenges. The results were compared with other

tools that applied traditional statistical and 2D graphical analysis approaches.

Implementing Windows Jump List, [59] presented a graphical digital forensics tool, known as Jump List Analyzer. The study applied statistical charts (e.g., histogram) to visualize attributes, such as AppID, time, zoom, CustDest file, recorded file, and GUI interface. The tool was demonstrated to support forensic investigations of users' background and behavior analysis. Compatibility, friendliness, and functionality were the three applied metrics to evaluate the Jump List Analyzer. A comparison with other tools suggested that the proposed tool can effectively visualize large volumes of data.

Analyzing an online social network, [60] proposed a forensic analysis model that included evidence acquisition, evidence solidification, evidence analysis, and evidence visualization. Evidence analysis used semantic analysis method in natural language processing, and it involved text analysis, hot word frequency analysis, and physical locations. Sina Microblog was used to demonstrate the proposed tool's feasibility. Web page files, such as HTML text data, CSS files, JavaScript files, and images, were the involved metadata. However, there was no detailed information on InfoVis.

Applying the use of 3D and 2D models, [61] proposed a drone forensic framework to investigate the post-flight investigation of drone activities. The authors applied 3D visualization models to visualize three specific parameters, which were roll, pitch, and yaw along the flight path, while other parameters, which were drone-controller communication, signal type, battery, altitude, number of satellites used, and speed at each point of time, were visualized using 2D models. Each parameter value was logged based on the timestamp. Graphs and charts, such as line charts, were utilized for the 2D models. This study measured forensic visualization aspects based on performance and responsiveness. The study indicated that the tool could manage the visualizations of sensor data without interruptions.

Focusing on cloud computing's containers and Virtual Machines (VMs), [62] applied InfoVis to visualize the bytes contained in a virtual machine file for rapid incident response. The extracted data were visualized using two-dimensional colorized visualization. The proposed visualization method was evaluated based on relative speed and accuracy using a series of *t*-tests for significant difference. A total of 42 participants were involved in the test, in which they were divided into test and control groups. Results showed that members of the test group did not have to wait to access the test data, and accuracy rates were relatively equivalent between the groups.

X. Zhang et al. [63] proposed an automated knowledge-sharing forensic platform by applying the ontology-based approach. The proposed method involved five layers: collection, extraction, analysis, visualization, and abstraction. A timeline-based visualization panel was used to display the investigated metadata. The platform would allow forensic investigators to create schemas based on the results of their forensic investigation. However, the authors did not further discuss the applied visualization model, which might be due to the study focusing on the knowledge-sharing approach.

Chow and Ab Rahman [64] demonstrated a mobile forensic visualization tool that visualized metadata from the Android data partitions of different models. Examples of data visualization were frequent message texts, top contacts, call duration, and location maps. Tool usability was evaluated through application functionality testing and user testing. In a similar study, [51] presented a tool to visualize WhatsApp and WeChat metadata. Examples of data visualization were chat history, timeline of chats, frequent contacts, and location maps. It was observed that the visualization models and evaluation methods used in this study were similar to those of [64]. Both studies highlighted the use of forensic visualization to enhance forensic analysis tasks for mobile forensics.

Shidek et al. [65] demonstrated timeline graph visualization to display data from WhatsApp chat conversations. The utility of the tool was evaluated through questions derived from forensic analysis goals: what cyber incident occurred, who was involved in the incident, and where, when, and how the incident occurred. Also applying timeline graph visualization, [66] presented a visualization-based approach to support malware investigations on the Internet of Things environment. This study applied the data mining method to preprocess DLL files and assign weights to represent malicious and benign files. It was evaluated using a questionnaire survey for academicians and industry practitioners. The respondents were asked about visualization evaluation, user experience, and time performance. A *t*-test was used to examine the significant difference for performance evaluation.

Fig. 2 and Fig. 3 summarize the results from the literature survey of forensic analysis of IM apps. Further discussion of the findings is in the next section.

	Chang and Chang [2]	Agrawal and Tapaswi [51]	Al-Rawashdeh et al. [52]	Barradas et al. [53]	Nizam et al [54]	Ong and Ab Rahman [55]
Forensic analysis tasks	**M**	**M**	**M**	**A**	**A**	**A**
Evaluation metrics	**Origin of data, data completeness**	**Point of estimate value, margin of error**	**Count of recovered messages, average no. of recovered messages**	**Analysis time**	**Functionality testing, user acceptance testing**	**Functionality testing, user acceptance testing**
Evaluation method	**QL**	**QN**	**QN**	**QN**	**QL & QN**	**QL & QN**
Event reconstruction/ Analysis method	**N**	**N**	**N**	**Y /temporal**	**N**	**Y / temporal**
M = manual analysis; A= automated analysis; QL = qualitative; QN = quantitative; Y = Yes; N = No						

Fig. 2. Summary of studies in forensic analysis of IM apps (first part)

	Anglano et al. [44]	Riadi et al. [75]	H. Zhang et al. [47]	Rathi et al. [48]	Kim et al. [50]	Güneş Eriş and Akbal [76]
Forensic analysis tasks	**M**	**M**	**M**	**M**	**M**	**M**
Evaluation metrics	**Completeness, repeatability, generality**	**Artifact extraction percentage, tool success rate**	**Origin of data, data completeness**	**Origin of data, data completeness**	**Password recovery time**	**Origin of data**
Evaluation method	**QL**	**QN**	**QL**	**QL**	**QN**	**QL**
Event reconstruction/ Analysis method	**Y / temporal and relational**	**N**	**N**	**N**	**N**	**Y / temporal and relational**
M = manual analysis; A= automated analysis; QL = qualitative; QN = quantitative; Y = Yes; N = No						

Fig. 3. Summary of studies in forensic analysis of IM apps (second part)

VI. Results and Discussion

In this section, we present the results of, and insight on, forensic analysis of Instant Messaging (IM) apps and forensic visualization for forensic analysis.

A. Forensic Analysis of Instant Messaging Apps

The findings are summarized into methods of forensic analysis tasks, evaluation metrics, evaluation methodologies, and event reconstruction methods.

Fig. 2 and Fig. 3 present most of the studies manually analyzed forensic artifacts of IM apps, while three studies demonstrated the use of automated tools to perform forensic analysis tasks. A closer inspection of the table shows that the evaluation metrics for manual forensic analysis were different from those for automated forensic analysis. Origin of data and completeness were the most applied metrics to evaluate manual forensic analysis. For automated forensic analysis, tool performance and tool functionality were the two applied metrics.

Our examination of evaluation methodologies shows that the qualitative methodology was more predominant to be applied in manual forensic analysis studies. This is likely related to the most applied evaluation metrics. For example, the evaluation metric of origin of data is more meaningful in a qualitative way rather than quantitative. Mixed methodologies, on the other hand, are observed as the major selection of research designs evaluating automated forensic analysis tools.

It is identified that very few studies used manual analysis method and generate event reconstruction. This is an unexpected finding, since event reconstruction is the outcome of forensic analysis. A likely explanation is that extensive manual tasks might demotivate the research works from including event reconstruction in their research questions. This was echoed by Kang et al. [67], who highlighted that event reconstruction in manual analysis is limited to personal knowledge, prone to human errors, and time-consuming. In contrast, two out of the three studies that used automated forensic analysis included event reconstruction. This further supports the benefit of automating forensic analysis tasks, which is expediting event reconstruction.

As evidenced by the number of publications from 2017 until 2021, it can thus be suggested that IM forensic analysis has received significant interest from the forensics community, and the research on automated IM forensic analysis is growing. Therefore, we argue that automating IM forensic analysis to facilitate forensic analysis tasks is a promising research area. This is supported by a previous study by Anglano et al. [36], which indicated that the automated forensic analysis of mobile apps has recently received interest and that their proposed tool was able to achieve greater artifact coverage than did previous studies.

B. Research Trends of Forensic Visualization for Forensic Analysis

The research trends were summarized based on InfoVis data types, visualization techniques, case studies, and the number of publications (see Table II). The InfoVis data types were adopted from [53], while the list of visualization techniques was adopted from a survey conducted in [68].

TABLE II. Trends of Forensic Visualization Applications to Support Forensic Analysis

InfoVis Data Types	Forensic Visualization Techniques	Case Studies	References
Relational	Bar Chart	Network Traffic, Windows OS, Intelligent Transport System	[62], [63], [69]
	Pie Chart	Network Traffic, Electronic Mail System	[57], [60]
	Histogram	Windows OS, Electronic Mail System	[59], [60]
	Treemap / Graph	Mobile Apps (SMS), Network Traffic, Windows Diagnostic Log	[5], [57], [70]
Multi-dimensional and high-dimensional	Colorization table, RGB Binary	Container and Virtual Machine, Malware detection	[62], [71]
Text	Word cloud	Mobile Apps (text-based communication apps), Android Operating System, Instant Messaging Apps	[5], [64], [51]
Geo-spatial	Geographic maps	Mobile Apps, Android Operating System, Instant Messaging Apps	[5], [64], [51]
Sequential and temporal	Time-based/ timeline	Windows OS, Cloud Computing, Internet of Things (IoT), Electronic Mail System, WhatsApp Artifact, Android Operating System, Instant Messaging Apps, Container and Virtual Machine	[64], [72], [51], [59], [60], [65], [62]

From Table II, we can see that forensic visualization was applied in various case studies, including recent computing trends, such as the Internet of Things. This finding accords with an earlier observation in [52], which showed various applications of InfoVis. Similarly, it indicates the generality of forensic visualization for incorporation into investigations of various digital infrastructures.

It is observed that each study incorporated more than one forensic visualization technique. Furthermore, most of the related studies demonstrated the selection of techniques based on data types, for example in [64], [57], [61], and [66]. This further indicates that different data types may require different visualization techniques. Therefore, we argue that the feature of the selection of visualization techniques must be incorporated in forensic visualization tools to ensure effective evidence interpretation.

Charts and graphs are the major visualization techniques applied, and relational is the most studied data type. This might be related to the usage flexibility of charts and graphs to visualize the relational data type. It can be argued that various types of charts and graphs are significant in providing evidence interaction, as well as interpretation, to users. For instance, [61] demonstrated that various parameters of drone flight data and sensor data can be visualized using various types of charts.

This is also consistent with the list of visualization techniques from a previous survey conducted in [68].

Time-based visualization is the second-most applied visualization technique. This is an unsurprising finding since timeline analysis is a major aspect of forensic investigations. The importance of timeline and its connection with digital forensics investigations were also echoed in the studies by [25] and [23]. Timeline analysis is not limited to examining the time of an incident, but it is also applicable to many other purposes, for instance, event correlation and time zone determination.

Word cloud and geographic maps were also applied as case studies involving mobile forensics data. This is, therefore, not surprising because most smartphone apps comprise textual and geo-spatial data. For example, the three case studies of [5], [64], and [51] used the word cloud to visualize textual data from communication and IM apps. This indicates that the metadata from smartphones involved enormous text-based data. Therefore, applying a word cloud can help analysts quickly understand the patterns of text-based data in relation to forensic investigations. Furthermore, incorporating geographic maps into the tool would expedite investigators in assessing geospatial data without manually examining the data using external map applications.

Another important finding is the evaluation methods of the proposed approaches. Table III summarizes the evaluation methods observed in the surveyed studies. The most applied method is performing technical simulations to evaluate tool usability, followed by conducting user testing to evaluate the tool, and using a focus group to solve forensic challenges. This shows that evaluation methods for visual analysis tools are relatively not mutually exclusive. Therefore, there is a need for benchmarking evaluation methods in this research area.

TABLE III. EVALUATION METHODS OF FORENSIC VISUALIZATION

Evaluation method	References
Technical simulations (e.g., case studies) to evaluate tool usability	[56], [59], [60], [61], [63]
User testing to evaluate tool functionality and performance	[64], [51], [62], [66]
Focus group to solve forensic challenges	[57], [58], [65]

In relation to the automated forensic tools metrics proposed by Ayers [32], speed (absolute and relative), reliability, accuracy, and completeness are the evaluation metrics used in existing studies. This is in line with our finding from automated IM forensic analysis tools, which show that performance and functionality are the most applied metrics. It should be noted that these studies might use different terms to describe the metrics. The result suggests that the existing tools were validated based on widely recognized metrics of computer forensics.

Despite the benefits of forensic visualization, most of the previous studies provided limited discussion on the selection criteria of forensic visualization techniques in relation to forensic analysis. This reflects the finding in [68] that most existing applications do not meet all forensic selection criteria. Forensic selection criteria include the following [68]: meaning, where the interpretation of evidence remains unaltered by the visualization technique used; errors, which is the ability to identify and account for errors to prevent evidence from being questioned; transparency, which is the ability to examine and verify all the data; and timeline, which shows users the events that occurred within a specific timeframe. These criteria are important to ensure the analysis results are valid and admissible in court of law. This observation suggests a knowledge gap(s) that needs to be addressed to highlight the significance of forensic visualization.

VII. CONCLUSION AND FUTURE WORKS

In this study, a literature survey was conducted to examine state-of-the-art IM forensic analysis and forensic visualization techniques. It appears from our literature survey that both forensic analysis and InfoVis are relatively mature research areas. However, there is a growing interest in forensic visualization and automated IM forensic analysis. This brings various research opportunities to fill up the knowledge gaps. For instance, there is a need to benchmark evaluation methods and metrics in both areas. Furthermore, there is a lack of discussion on forensic selection criteria in existing forensic visualization works.

Therefore, our next research work will be conducted on the automated forensic analysis of IM applications by integrating the forensic visualization approach. Statistical analysis and machine learning algorithms would be incorporated to utilize the forensic selection criteria in forensic visualization. It is expected that the outcomes of this study will significantly aid digital forensics practitioners in analyzing and interpreting evidence data and aid judicial authorities in understanding the presentation of evidence.

ACKNOWLEDGMENT

The first author is currently a PhD student at Universiti Tun Hussein Onn Malaysia. This research was supported by the Ministry of Higher Education (MOHE) through Fundamental Research Grant Scheme (FRGS/1/2020/ICT07/UTHM/03/1). The authors would like to thank the anonymous reviewers for their constructive and generous feedback.

REFERENCES

[1] "Instant Messaging Security." https://www.nortonlifelockpartner.com/security-center/instant-messaging-security.html (accessed Jun. 15, 2022).

[2] Securelist, "Kaspersky spam and phishing report for 2021 | Securelist," Kaspersky, 2021. https://securelist.com/spam-and-phishing-in-2021/105713/ (accessed Jun. 15, 2022).

[3] "2022 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends | PurpleSec." https://purplesec.us/resources/cyber-security-statistics/ (accessed Jun. 15, 2022).

[4] "WhatsApp hijack scam continues to spread - BBC News." https://www.bbc.com/news/technology-57357301 (accessed Jun. 15, 2022).

[5] C. F. R. Tassone, B. Martini, and K. K. R. Choo, "Visualizing Digital Forensic Datasets: A Proof of Concept," J Forensic Sci, vol. 62, no. 5, pp. 1197–1204, 2017, doi: 10.1111/1556-4029.13431.

[6] H. Henseler and S. van Loenhout, "Educating judges, prosecutors and lawyers in the use of digital forensic experts," DFRWS 2018 EU - Proceedings of the 5th Annual DFRWS Europe, vol. 24, pp. S76–S82, 2016, doi: 10.1016/j.diin.2018.01.010.

[7] N. D. W. Cahyani, B. Martini, and K. K. R. Choo, "Using multimedia presentations to enhance the judiciary's technical understanding of

digital forensic concepts: An Indonesian case study," Proceedings of the Annual Hawaii International Conference on System Sciences, vol. 2016-March, pp. 5617–5626, 2016, doi: 10.1109/HICSS.2016.695.

[8] N. D. W. Cahyani, B. Martini, and K. K. R. Choo, "Using multimedia presentations to improve digital forensic understanding: A pilot study," in ACIS 2015 Proceedings - 26th Australasian Conference on Information Systems, 2015, pp. 1–9.

[9] W. Xiong and R. Lagerström, "Threat modeling – A systematic literature review," Comput Secur, vol. 84, pp. 53–69, 2019, doi: 10.1016/j.cose.2019.03.010.

[10] 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, doi: 10.1016/j.cose.2014.11.006.

[11] H. D. Karen Kent, Suzanne Chevalier, Tim Grance, "Guide to integrating forensic techniques into incident response (NIST Special Publication 800-86)," 2006.

[12] J. Benoit, "Best Practice Document: Forensic Analysis and Incident Handling," 2016.

[13] E. Casey, Digital Evidence and Computer Crime, Second edi. San Diego, CA,: Elsevier Academic Press, 2011.

[14] G. Horsman et al., "A forensic examination of web browser privacy-modes," Forensic Science International: Reports, vol. 1, p. 100036, 2019, doi: 10.1016/j.fsir.2019.100036.

[15] B. Almaslukh, "Forensic analysis using text clustering in the age of large volume data: A review," International Journal of Advanced Computer Science and Applications, vol. 10, no. 6, pp. 71–76, 2019, doi: 10.14569/ijacsa.2019.0100610.

[16] P. Joseph and J. Norman, "Identifying Forensic Interesting Files in Digital Forensic Corpora by Applying Topic Modelling," in Advances in Distributed Computing and Machine Learning, Singapore: Springer, 2021, pp. 411–421.

[17] M. Hina, M. Ali, A. R. Javed, F. Ghabban, L. A. Khan, and Z. Jalil, "SeFACED: Semantic-Based Forensic Analysis and Classification of E-Mail Data Using Deep Learning," IEEE Access, vol. 9, pp. 98398–98411, 2021, doi: 10.1109/ACCESS.2021.3095730.

[18] "Computer Forensics: Forensic Techniques, Part 2 [Updated 2019] - InfosecResources," INFOSEC, 2019. https://resources.infosecinstitute.com/topic/computer-forensics-forensic-techniques-part-2/ (accessed Nov. 21, 2021).

[19] H. M. Elgohary, S. M. Darwish, and S. M. Elkaffas, "Improving Uncertainty in Chain of Custody for Image Forensics Investigation Applications," IEEE Access, vol. 10, no. 1, pp. 14669–14679, 2022, doi: 10.1109/ACCESS.2022.3147809.

[20] I. A. Alnajjar and M. Mahmuddin, "The Enhanced Forensic Examination and Analysis for Mobile Cloud Platform by Applying Data Mining Methods," Webology, vol. 18, no. August 2021, pp. 47–74, 2021, doi: 10.14704/WEB/V18SI01/WEB18006.

[21] M. Khanafseh, M. Qatawneh, and W. Almobaideen, "A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics," International Journal of Advanced Computer Science and Applications, vol. 10, no. 8, pp. 610–629, 2019, doi: 10.14569/ijacsa.2019.0100880.

[22] N. A. Adderley, "Graph-based Temporal Analysis in Digital Forensics," AIR FORCE INSTITUTE OF TECHNOLOGY, 2019.

[23] N. Adderley and G. Peterson, "Interactive temporal digital forensic event analysis," IFIP Adv Inf Commun Technol, vol. 589 IFIP, pp. 39–55, 2020, doi: 10.1007/978-3-030-56223-6_3.

[24] S. Bhandari and V. Jusas, "An ontology based on the timeline of Log2timeline and psort using abstraction approach in digital forensics," Symmetry (Basel), vol. 12, no. 4, pp. 1–24, 2020, doi: 10.3390/SYM12040642.

[25] H. Henseler and J. Hyde, "Technology assisted analysis of timeline and connections in digital forensic investigations," in CEUR Workshop Proceedings, 2019, vol. 2484, pp. 32–37.

[26] H. Arshad, A. Jantan, G. K. Hoon, and I. O. Abiodun, "Formal knowledge model for online social network forensics," Comput Secur, vol. 89, p. 101675, 2020, doi: 10.1016/j.cose.2019.101675.

[27] B. Carrier, File system forensic analysis. Addison-Wesley Professional, 2005.

[28] A. Singh, H. S. Venter, and A. R. Ikuesan, "Windows registry harnesser for incident response and digital forensic analysis," Australian Journal of Forensic Sciences, vol. 52, no. 3, pp. 337–353, 2018, doi: 10.1080/00450618.2018.1551421.

[29] B. Martini, D. Quang, and K.-K. R. Choo, "Conceptual Evidence Collection and Analysis Methodology for Android Devices," in Cloud Security Ecosystem, R. Ko and K. K. . R. Choo, Eds. Waltham, MA: Syngress, an Imprint of Elsevier, 2015, pp. 383–400.

[30] X. Zhang, O. Upton, N. L. Beebe, and K. K. R. Choo, "IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers," Forensic Science International: Digital Investigation, vol. 32, p. 300926, 2020, doi: 10.1016/j.fsidi.2020.300926.

[31] T. Wu, F. Breitinger, and S. O'Shaughnessy, "Digital forensic tools: Recent advances and enhancing the status quo," Forensic Science International: Digital Investigation, vol. 34, p. 300999, 2020, doi: 10.1016/j.fsidi.2020.300999.

[32] D. Ayers, "A second generation computer forensic analysis system," Digit Investig, vol. 6, pp. S34–S42, 2009, doi: 10.1016/j.diin.2009.06.013.

[33] X. Lin, T. Chen, T. Zhu, K. Yang, and F. Wei, "Automated forensic analysis of mobile applications on Android devices," Digit Investig, vol. 26, pp. S59–S66, 2018, doi: 10.1016/j.diin.2018.04.012.

[34] A. Kumar, K. S. Kuppusamy, and G. Aghila, "FAMOUS: Forensic Analysis of Mobile devices Using Scoring of application permissions," Future Generation Computer Systems, vol. 83, pp. 158–172, 2018, doi: 10.1016/j.future.2018.02.001.

[35] K. P. Subedi, D. R. Budhathoki, and D. Dasgupta, "Forensic analysis of ransomware families using static and dynamic analysis," Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018, pp. 180–185, 2018, doi: 10.1109/SPW.2018.00033.

[36] C. Anglano, M. Canonico, and M. Guazzone, "The Android Forensics Automator (AnForA): A tool for the Automated Forensic Analysis of Android Applications," Comput Secur, vol. 88, pp. 1–15, 2020, doi: 10.1016/j.cose.2019.101650.

[37] D. Brezinski and T. Killalea, "Guidelines for Evidence Collection and Archiving," Internet Engineering Task Force, 2002. https://datatracker.ietf.org/doc/html/rfc3227 (accessed Jun. 01, 2022).

[38] F. Alief, Y. Suryanto, L. Rosselina, and T. Hermawan, "Analysis of autopsy mobile forensic tools against unsent messages on whatsapp messaging application," in International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), 2020, pp. 26–30. doi: 10.23919/EECSI50503.2020.9251876.

[39] C. Anglano, M. Canonico, and M. Guazzone, "Forensic analysis of Telegram Messenger on Android smartphones," Digit Investig, vol. 23, pp. 31–49, 2017, doi: 10.1016/j.diin.2017.09.002.

[40] A. Akinbi and E. Ojie, "Forensic analysis of open-source XMPP/Jabber multi-client instant messaging apps on Android smartphones," SN Appl Sci, vol. 3, no. 4, pp. 1–14, 2021, doi: 10.1007/s42452-021-04431-9.

[41] A. F. Imam Riadi, "Forensic Analysis of Android Based Instant Messaging Application," in 12th International Conference on Telecommunication Systems, Services, and Applications (TSSA), 2018, pp. 1–6.

[42] H. Zhang, L. Chen, and Q. Liu, "Digital Forensic Analysis of Instant Messaging Applications on Android Smartphones," 2018 International Conference on Computing, Networking and Communications, ICNC 2018, pp. 647–651, 2018, doi: 10.1109/ICCNC.2018.8390330.

[43] K. Rathi, U. Karabiyik, T. Aderibigbe, and H. Chi, "Forensic analysis of encrypted instant messaging applications on Android," 6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1109/ISDFS.2018.8355344.

[44] R. Chanajitt, W. Viriyasitavat, and K. K. R. Choo, "Forensic analysis and security assessment of Android m-banking apps," Australian Journal of Forensic Sciences, vol. 50, no. 1, pp. 3–19, 2018, doi: 10.1080/00450618.2016.1182589.

[45] G. Kim, S. Kim, M. Park, Y. Park, I. Lee, and J. Kim, "Forensic analysis of instant messaging apps: Decrypting Wickr and private text messaging

data," Forensic Science International: Digital Investigation, vol. 37, p. 301138, 2021, doi: 10.1016/j.fsidi.2021.301138.

[46] M. S. Chang and C. Y. Chang, "Forensic analysis of LINE messenger on android," Journal of Computers (Taiwan), vol. 29, no. 1, pp. 11–20, 2018, doi: 10.3966/199115992018012901002.

[47] V. Agrawal and S. Tapaswi, "Forensic analysis of Google Allo messenger on Android platform," Information and Computer Security, vol. 27, no. 1, pp. 62–80, 2019, doi: 10.1108/ICS-03-2017-0011.

[48] A. M. Al-Rawashdeh, Z. A. Al-Sharif, M. I. Al-Saleh, and A. S. Shatnawi, "A Post-Mortem Forensic Approach for the Kik Messenger on Android," 2020 11th International Conference on Information and Communication Systems, ICICS 2020, pp. 79–84, 2020, doi: 10.1109/ICICS49469.2020.239559.

[49] D. Barradas, T. Brito, D. Duarte, N. Santos, and L. Rodrigues, "Forensic analysis of communication records of messaging applications from physical memory," Comput Secur, vol. 86, pp. 484–497, 2019, doi: 10.1016/j.cose.2018.08.013.

[50] S. H. S. Nizam, N. H. Ab Rahman, and N. D. W. Cahyani, "Keyword Indexing And Searching Tool (KIST): A Tool to Assist the Forensics Analysis of WhatsApp Chat," International Journal on Information and Communication Technology (IJoICT), vol. 6, no. 1, p. 23, 2020, doi: 10.21108/ijoict.2020.61.481.

[51] W. S. Ong and N. H. Ab Rahman, "A Forensic Analysis Visualization Tool for Mobile Instant Messaging Apps," International Journal on Information and Communication Technology (IJoICT), vol. 6, no. 2, pp. 78–87, 2020, doi: 10.21108/IJOICT.2020.00.530.

[52] D. Rees and R. S. Laramee, "A survey of information visualization books," Computer Graphics Forum, vol. 38, no. 1, pp. 610–646, 2019.

[53] M. Behrisch et al., "Quality Metrics for Information Visualization," Computer Graphics Forum, vol. 37, no. 3, pp. 625–662, 2018, doi: 10.1111/cgf.13446.

[54] M. Sorapure, "Text, Image, Data, Interaction: Understanding Information Visualization," Comput Compos, vol. 54, p. 102519, 2019, doi: 10.1016/j.compcom.2019.102519.

[55] I. Krak, O. Barmak, and E. Manziuk, "Using visual analytics to develop human and machine-centric models: A review of approaches and proposed information technology," Comput Intell, vol. 1, no. 9, pp. 75–98, 2020, doi: 10.1111/coin.12289.

[56] F. Böhm, L. Englbrecht, and G. Pernul, "Designing a decision-support visualization for live digital forensic investigations," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 12122, Springer, 2020, pp. 223–240. doi: 10.1007/978-3-030-49669-2_13.

[57] 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," J Wirel Mob Netw Ubiquitous Comput Dependable Appl, vol. 9, no. 2, pp. 57–73, 2018, doi: 10.22667/JOWUA.2018.06.30.057.

[58] D. Clark and B. Turnbull, "Interactive 3D visualization of network traffic in time for forensic analysis," VISIGRAPP 2020 - Proceedings of the 15th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications, vol. 3, pp. 177–184, 2020, doi: 10.5220/0008950601770184.

[59] S. K. Weng and J. Y. Tu, "A visualization jump lists tool for digital forensics of windows," KSII Transactions on Internet and Information Systems, vol. 14, no. 1, pp. 221–239, 2020, doi: 10.3837/tiis.2020.01.013.

[60] R. Lu and L. Li, "Research on forensic model of online social network," 2019 IEEE 4th International Conference on Cloud Computing and Big Data Analytics, ICCCBDA 2019, pp. 116–119, 2019, doi: 10.1109/ICCCBDA.2019.8725746.

[61] A. Renduchintala, F. Jahan, R. Khanna, and A. Y. Javaid, "A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework," Digit Investig, vol. 30, no. 2019, pp. 52–72, 2019, doi: 10.1016/j.diin.2019.07.002.

[62] J. Shropshire and R. Benton, "Container and VM visualization for rapid incident response," in Proceedings of the Annual Hawaii International Conference on System Sciences, 2020, pp. 6397–6406.

[63] X. Zhang, K. K. R. Choo, and N. L. Beebe, "How Do i Share My IoT Forensic Experience with the Broader Community? An Automated Knowledge Sharing IoT Forensic Platform," IEEE Internet Things J, vol. 6, no. 4, pp. 6850–6861, 2019, doi: 10.1109/JIOT.2019.2912118.

[64] C. X. Quan and N. H. Ab Rahman, "A Mobile Forensic Visualization Tool for Android Data Partition," in Applied Information Technology And Computer Science, 2021, vol. 2, no. 2, pp. 37–52.

[65] H. Shidek, N. D. W. Cahyani, and A. A. Wardana, "WhatsApp Chat Visualizer: A Visualization of WhatsApp Messenger's Artifact Using the Timeline Method," International Journal on Information and Communication Technology (IJoICT), vol. 6, no. 1, pp. 1–9, 2020, doi: 10.21108/ijoict.2020.61.489.

[66] I. Ahmad, M. A. Shah, H. A. Khattak, Z. Ameer, M. Khan, and K. Han, "FIViz: Forensics investigation through visualization for malware in internet of things," Sustainability (Switzerland), vol. 12, no. 18, pp. 1–23, 2020, doi: 10.3390/SU12187262.

[67] J. Kang, S. Lee, and H. Lee, "A digital forensic framework for automated user activity reconstruction," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 7863, Berlin, Heidelberg: Springer, 2013, pp. 263–277. doi: 10.1007/978-3-642-38033-4_19.

[68] C. Tassone, B. Martini, and K. K. R. Choo, "Forensic Visualization: Survey and Future Research Directions," in Contemporary Digital Forensic Investigations of Cloud and Mobile Applications, Syngress, 2017, pp. 163–184. doi: 10.1016/B978-0-12-805303-4.00011-3.

[69] D. Gürdür and L. Sopjani, "Visual Analytics to Support the Service Design for Sustainable Mobility," 2018 IEEE Conference on Technologies for Sustainability, SusTech 2018, pp. 4–9, 2019, doi: 10.1109/SusTech.2018.8671353.

[70] S. Park and S. Lee, "DiagAnalyzer: User behavior analysis and visualization using Windows Diagnostics logs," Forensic Science International: Digital Investigation, vol. 43, p. 301450, Sep. 2022, doi: 10.1016/j.fsidi.2022.301450.

[71] O. J. Falana, A. S. Sodiya, S. A. Onashoga, and B. S. Badmus, "Mal-Detect: An intelligent visualization approach for malware detection," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 5, pp. 1968–1983, May 2022, doi: 10.1016/j.jksuci.2022.02.026.

[72] S. C. Sathe and N. M. Dongre, "Data acquisition techniques in mobile forensics," in Proceedings of the 2nd International Conference on Inventive Systems and Control, ICISC 2018, 2018, pp. 280–286. doi: 10.1109/ICISC.2018.8399079.