A Systematic Review of Published Articles, Phases and Activities in an Online Social Networks Forensic Investigation Domain

Aliyu Musa Bade[1]
Department of Computer Science, Yobe State University
Damaturu, Nigeria

Siti Hajar Othman[2]
School of Computing, Universiti Teknologi Malaysia
Johor Bahru, Malaysia

***Abstract*—The purpose of this paper is to retrieve, evaluate and analyse the available published articles in five (5) relevant online databases from 2011 to 2021 and also critically identify the phases and activities involved in an Online Social Networks Forensic Investigation based on bibliometric analysis and Degree of confidence respectively in order to know the evolution in the research domain. A systematic literature review (SLR) technique was adopted by the author to search using pre-defined keywords. Only scholarly articles published between 2011 and 2021 written in English were included in the search. The total of 316 subscribed documents were collected from the five (5) online databases based on the search criteria although twenty-nine (29) are duplicates. ScienceDirect has the highest number with 189 documents and the year 2020 with the highest published articles. Six (6) phases and forty-three (43) activities were identified. According to a review of the recovered publications, no previous research has been done to statistically retrieve, evaluate and analyse the level of work that has been done in the domain of OSNFI, as well as the phases and activities involved in the forensic investigation of an online social networks crime.**

***Keywords*—Forensic; investigation; model; online social networks; bibliometric analysis; degree of confidence**

I. Introduction

Digital forensics has been studied for a decade, but it still appears to be a very young science, with many issues remaining unclear and ambiguous [1]. It is the science of collecting, preserving, examining, analysing, and presenting relevant digital evidence for use in legal proceedings [2]. The entire field of digital forensics investigation is still lacking in fundamental agreements which may be as a result that the field is relatively young [3]. It is a procedure, and not just one process, but a set of tasks and procedures that occur during the course of an investigation [2]. There is a lack of consistent definitions and language when it comes to the core parts of digital evidence investigation [4].

Millions of people use online social networks on a daily basis [5], which has facilitated new ways of connecting and sharing knowledge [6]. It has also resulted in a rise in excessive criminal activities [7], with criminals becoming more advanced in attempts to exploit technology to avoid detection and conduct crimes [6]; such as malware distribution, fraud, harassment, cyberbullying and cyberstalking. They also use online information to commit traditional crimes such as theft, kidnapping, and murder. Furthermore, they use the information as tools to assess and gain access to their victims [8].

Forensics is used on social media platforms like Facebook, MySpace, Twitter, and LinkedIn. It is well known as social media forensics, and it's a subset of digital forensics and network forensics [9]. Online social networks are Web-based services which enable individuals to create a public or semi-public profile within a confined system [6], articulate a list of other users with whom they share a link, and display and traverse their list of connections as well as those created by others within the system [10]. Different SNSs, like Facebook, Twitter, and LinkedIn, are used to connect people and enable them to communicate with one another [5]. People build personal profiles from various social networking sites to share their thoughts, photographs, images, emails, and instant messaging [11], as well as to find old friends or people with common interests or problems through various social networking sites [12].

Rapid technological development can cause issues for users of the technology. The more advanced people's lives become, the more advanced crime becomes [13]. Social media platforms are becoming increasingly popular, with Facebook managing above thirty-one (31) million users in United Kingdom, Twitter managing fifteen (15) million, and LinkedIn having 10 million. With the proliferation of mobile phones, the use of social network services (SNS) has skyrocketed, this SNS stores a variety of data, including user conversations, user location information, personal networks, and user psychology which can be valuable evidence in a digital forensics investigation of an incident [14]. Other uses of social networking sites include, general chatting, broadcasting breaking news, setting up a date, tracking election results, planning disaster response, humour, and serious analysis [11].

There are five (5) sections in this thesis. The following is a synopsis of the contents of each section: Section 1 – Introduction: this section provides a summary of the research study as well as explanations for the findings that led to the contributions of this review. The review objective is briefly stated in Section 2, and the methodology of the systematic literature review (SLR) used throughout the review process is discussed in Section 3. Section 4 includes a discussion based on the data gleaned from the review process. Finally, Section 5 brings this review to a conclusion.

II. Objective of the Review

The review looks into information from significant published sources on the available publications in the domain of an online social network forensic investigation, as well as the phases and other activities involved in the investigation process. According to the literature review, there are no SLR type publications on the topic of online social network forensic investigation. As a result, the goal of this review is to find out the amount of work that has been carried out and published in the domain of an Online Social Network Forensic Investigation. In addition, to identify the numerous phases and activities that can be employed in the investigation of an online social network forensic crime. These objectives are important because variety of DFIMs exist, but majority of which take related methods [15]; [16]. They fail to address the fundamental differences and unique needs of online social networks [17]. However, because there is no universal way [10]; [18] in many cases, investigators conduct automated forensic investigations mostly using different methods [19].

III. Methodology

The SLR is a step-by-step process that enables researchers to create their own search procedure**.** This review was carried out in accordance with the technique for conducting SLRs as proposed by [20]. It is used in identifying the required information from the selected articles. This method was chosen because it makes it easier to capture, summarise, synthesise, and critically comment on any of the topics reviewed. The SLR process consists of the following steps:

Step 1: Define the research questions.

Step 2: Determine the data sources and search process.

Step 3: Inclusion and exclusion criteria.

Step 4: Results of searching and data extraction.

Step 5: Discussion.

The total of three hundred and sixteen (316) articles linked to online social network forensic investigation were retrieved using the SLR approach from five (5) credible online journals. These online databases are: Scopus, Web of Science, IEEEXplore, ScienceDirect and Association for Computing Machinery (ACM) Digital Library.

A. Research Questions

RQ1. What are the available published articles in Scopus, Web of Science, IEEEXplore, ScienceDirect and Association for Computing Machinery (ACM) Digital Library in the domain of an Online Social Networks Forensic Investigation model from 2011 to 2021?

RQ2. What are the phases and activities involved in an Online Social Networks Forensic Investigation model Domain based on the Degree of Confidence?

B. Data Sources and Search Process

Five (5) online databases were accessed (Scopus, Web of Science, IEEEXplore, ScienceDirect, Association for Computing Machinery (ACM) Digital Library) and all available documents were retrieved based on the search key "[All:online] AND [All:social] AND [All:network] AND [All:forensic] AND [All:investigation] AND [All:model] AND [PublicationDate:(01/01/2011 TO 31/12/2021)". All articles which include any of the search term (online, social, network, forensic, investigation, model, publication date from 01/01/2011 to 31/12/2021) were retrieved. All articles from 2011 to 2021 were included in the search. This time frame was chosen because it would allow for the retrieval of a sufficient number of articles on the subject and the detection of a research trend. Despite that, the articles retrieved are relatively considered less considering the importance of the domain even though it's young.

C. Inclusion and Exclusion Search Criteria

Only empirical research based on published literature in the field of online social network forensic investigation were evaluated. The search parameters were configured to retrieve only items authored in English and published between January 1, 2011 and December 31, 2021. Interviews, news, periodicals, correspondence, conversations, comments, letters to the editor, summaries of tutorials, meetings, workshops, panels, and poster presentations were all eliminated from the search.

We excluded the aforementioned categories of publications since we only sought to identify papers in the field of online social network forensic investigation, the majority of which could be found in full-text and peer-reviewed journal articles. Journal articles are discovered to go through review processes that ensure that only proven evidence is available.

Journals published more matured research when compared to other sources. Only full-text studies were chosen the availability of thorough assessment methods as opposed to articles that are only available in abstract form. Also, peer-reviewed articles were chosen since they determine the credibility and dependability of studies.

D. Search Results

A number of literature works dealing with the topic of an online social network forensic investigation are listed in Table I. The article list is divided into four (3) vertical categories and serves as a broad overview with the; (i) Name of online Database(s), (ii). Total document retrieved, and (iii) Categorization by Year of publication. Tables III and IV presents the selection of the OSNFIM development phases based on degree of confidence (DoC) and the OSNFI phases and their activities respectively. Fig. 1 shows the retrieved articles according to the year of publication, Fig. 2, Fig. 3 and Fig. 4 shows the Network, Overlay and Density visualizations of available OSNFIM documents on one of the online database (Scopus) based on bibliometric analysis. Fig. 5 shows the OSNFIM development phases based on DoC while Table III shows the list of Items, Links, Total link strength, Occurrence and Average publication year of every cluster.

IV. Data Extraction

Based on the search term used in the five (5) relevant online databases, the total of three hundred and sixteen (316) documents were retrieved. ScienceDirect has the highest number of retrieved documents of one hundred and eighty-nine (189) and the year 2020 with the highest number of published articles as presented in Table I.

TABLE I. ANALYSIS ON THE AVAILABLE JOURNALS IN THE DOMAIN OF OSNFIM

S.no	Name of online Database(s)	Total document retrieved	Categorization by Year of publication										
			2021	2020	2019	2018	2017	2016	2015	2014	2013	2012	2011
1	Scopus	30	2	3	6	2	6	3	2	3	1	0	2
2.	Web of Science	14	2	3	3	2	1	1	1	0	1	0	0
3.	IEEEXplore	12	0	1	2	2	1	3	1	0	0	0	2
4.	ScienceDirect	189	31	31	35	19	19	22	8	8	7	5	4
5.	Association for Computing Machinery (ACM) Digital Library	71	8	18	9	10	7	6	7	1	2	2	1
Summary		**316**	**43**	**56**	**55**	**35**	**34**	**35**	**19**	**12**	**11**	**7**	**9**

There are some duplicates among the 316 papers that have been retrieved. Scopus has retrieved a total of 31 documents, 12 of which are duplicates. ScienceDirect has three (3) articles, IEEEXplore has eight (8) articles, and Web of Science has one (1) article. The total number of documents retrieved from IEEEXplore is 21, although ten (10) of them are duplicates. In Scopus, there are eight (8) papers, while in Web of Science, there are two (2) papers. The total number of documents obtained by Web of Science is 14, although three (3) of them are duplicates. Two (2) in IEEEXplore and one (1) in Scopus. ScienceDirect has retrieved a total of 189 documents, three (3) of which are duplicates and all of which are in Scopus. There are 71 documents in the Association for Computing Machinery (ACM) Digital Library, but only one (1) is duplicated in Web of Science.

V. DISCUSSION

This section contains a detailed discussion in order to answer the research questions that have been posed:

RQ1.What are the available published articles in Scopus, Web of Science, IEEEXplore, ScienceDirect and Association for Computing Machinery (ACM) Digital Library in the domain of an Online Social Networks Forensic Investigation from 2011 to 2021?

The total of 316 subscribed documents were collected among which ScienceDirect has the total highest number with 189 documents and the year 2020 with the highest published journals as shown in Table I and Fig. 1 which both can relatively considered as less considering the importance of the domain even though it's young. Also, most of the documents retrieved are not related to the domain of interest while some are duplicates. But they were accessed due to the search term used will involves all documents having any of the word (online, social, network, forensic, investigation, model) appeared in it. After sorting the relevant/not relevant articles, it can be concluded that not up to 30% of the 316 documents retrieved were relevant to the domain of interest and twenty-nine (29) articles are duplicates as presented in Table II.

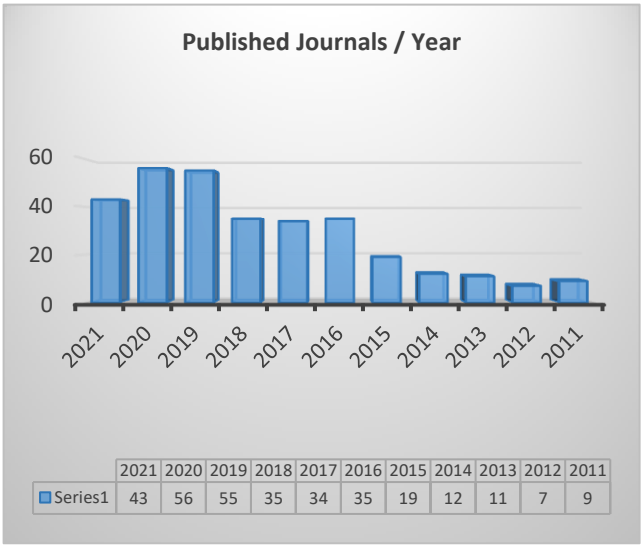

Fig. 1. Published Articles According to Year.

Therefore, more research has to be conducted and published in the domain of online social network forensic investigation (OSNFI) considering how technology is rapidly developing and crimes are increasing and becoming advanced day by day due to how people are becoming addicted to the use of social networking sites. This will help in creating awareness to the users and also help other researchers working in the domain.

TABLE II. EXTRACTION OF RELEVANT/NOT RELEVANT AND DUPLICATE DOCUMENTS

Name of Database	Total document retrieved	Relevant	Not Relevant	Total Duplicate
Scopus	30	7	23	12
IEEE	12	1	11	10
Web of Science	14	5	9	3
ScienceDirect	189	10	179	3
ACM	71	4	67	1
Summary	**316**	**27**	**289**	**29**

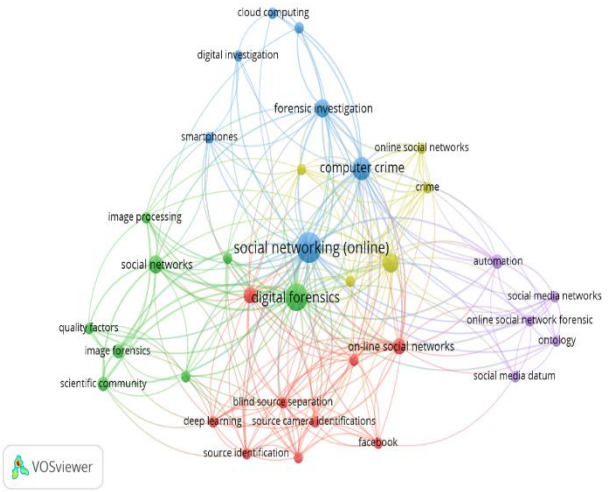

Fig. 2. Network Visualization of Available OSNFIM Documents on Scopus Database based on Bibliometric Analysis.

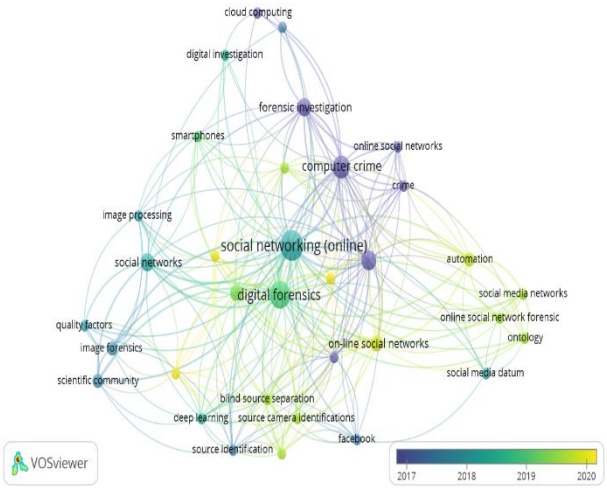

Fig. 3. Overlay Visualization of Available OSNFIM Documents on Scopus Database based on Bibliometric Analysis.

In 1926, Alfred Lotka introduced bibliometrics when he examined patterns of author output and presented the first criteria for bibliometrics [21]. Bibliometrics is a field of scientific inquiry that is gaining increasing interest from the scientific world and has swiftly grown and has been used to various academic domains. It is an excellent technique to retrieve, evaluate and statistically analyse quantifiable data in scholarly literature and also the merits of a certain topic area or a particular publication which can be used through its indicators to better reflect the evolution of a given research direction [22].

VOSviewer was used to conduct a co-occurrence analysis based on all keywords as the unit of analysis and Full counting method. The full counting technique indicates that each co-authorship, co-occurance, bibliographical coupling, or co-citation link gets the same weight. The parameters were used in order to analyse the retrieved documents so as to have a clear perspective in the domain of OSNFIM as presented in Fig. 2, Fig. 3 and Fig. 4. A total of thirty (30) documents were retrieved from the scopus online database after using the search term "[All: online] AND [All:social] AND [All:network] AND [All:forensic] AND [All:investigation] AND [All:model] AND [PublicationDate:(01/01/2011 TO 31/12/2021)". After conducting the analysis, thirty-four (34) item were generated based on five (5) clusters as in Table III.

The circles in Fig. 2 and Fig. 3 indicate the level of work which has been carried out and published in a specific area of research. It can clearly be seen that social networking (online) and digital forensic has the biggest circles based on the analysis. The domain of interest which is the online social network forensic investigation has one of the smallest circles even among its cluster. Therefore, this obviously indicates that not much work has been carried out in the domain even though it is considered young but very important.

RQ2. What are the phases and activities involved in an Online Social Networks Forensic Investigation Model Domain based on the Degree of Confidence?

Several models and frameworks have been proposed by [6]; [10]; [15]; [2]; [5]; [16]; [14]; [23]; [24]; [11]; [13]; [7]; [25]; and [17], but very few were designed with OSNFI in mind.

However [6]; and [10] proposed a digital forensic investigation model for online social networking and a digital forensic investigation model and its application design. Even though they tried in the automation of the entire process, there are some activities which requires manual handling which can decrease the dependability and credibility of evidence in criminal proceedings [10], added Iteration in all the investigation process and that can sometimes be very difficult tracing back at the source of the information collected [23]; [24]; [13]; [5] and [25], focused more on a particular platform or content rather than the entire OSN. Such platforms includes: WhatsApp, Cloud, Messenger, Imaging and Game.

Fig. 4. Density Visualization of Available OSNFIM Documents on Scopus Database based on Bibliometric Analysis.

TABLE III. ITEMS, LINKS, TOTAL LINK STRENGTH, OCCURRENCE AND AVERAGE PUBLICATION YEAR

Item	Links	Total link strength	Occurrence	Avg. Pub. Year
Cluster 1				
Blind source separation	15	21	02	2019.50
Cameras	21	34	04	2019.25
Deep learning	17	19	02	2018.50
Facebook	13	14	02	2017.50
Information systems	15	18	02	2014.50
Online social networks	**23**	**39**	**04**	**2019.75**
Source camera identification	15	21	02	2019.50
Source camera identifications	15	21	02	2019.50
Source identification	15	17	02	2017.50
Cluster 2				
Digital forensic	**21**	**81**	**11**	**2018.91**
Image enhancement	14	16	02	2020.00
Image forensic	**09**	**18**	**03**	**2017.67**
Image processing	12	15	02	2018.00
Quality factor	08	13	02	2018.00
Scientific community	09	18	03	2017.67
Sensor pattern noise	15	18	02	2020.00
Social networks	**17**	**32**	**05**	**2018.20**
Cluster 3				
Cloud computing	**05**	**06**	**02**	**2017.00**
Computer crime	**25**	**48**	**08**	**2016.62**
Digital investigation	**06**	**07**	**02**	**2018.50**
Forensic investigation	**18**	**33**	**05**	**2017.00**
Smartphones	**10**	**13**	**02**	**2019.00**
Social networking (online)	**33**	**92**	**14**	**2018.14**
Social networking sites	**06**	**08**	**02**	**2017.50**
Cluster 4				
Crime	11	16	2	2015.50
Electronic crime countermeasures	25	46	6	2016.50
Iterative methods	15	19	2	2019.50
Online social networks	11	16	2	2015.50
Online social network (OSN)	16	19	2	2020.50
Cluster 5				
Automation	14	24	3	2019.67
Online social network forensic	9	14	2	2019.50
Ontology	9	14	2	2019.50
Social media datum	7	8	2	2018.00
Social media networks	9	14	2	2019.50
Summary: Items = 34, Cluster = 5, Links = 247 and Total Link Strength = 406				

One of the best OSN models were those presented by [18]; and [17]. They both proposed a semi-automated and automated model for the domain of OSN. The author in [18] proposed a comprehensive digital forensic investigation process model that includes: acquisition and analysis of digital evidence. Iteration process is considered in their proposed model but the process is too common and non-specific. A digital forensic investigation process model for online social networks (FIMOSN) was presented by [17]. The model comprises of seven (7) phases and focused on automating the whole process activities. The model considered Iteration at a reasonable stage which is after analysis phase and before presentation but the evaluation process is entirely manual and this can slow the investigation process.

There are quite a number of models which recommend different phases and activities for the forensic investigation of online social networks. But for the purpose of coming up with a unified number and terms for this research, a total of five (5) models are randomly selected. According to [17], forensic investigation for online social networks consist of seven (7) phases; Pre-investigation, Incident specification, Extraction, Preservation, Analysis, Iteration and Presentation. [24] suggested six (6) phases; Identification, Preservation, Collection, Examination, Analysis and Presentation, [13] presented four (4) phases; Preparation, Incidence response, Laboratorium process and Presentation, [6] recommended four (4) also; Preliminary, Investigation, Analysis and Evaluation. Therefore, the Degree of Confidence (DoC) is used to calculate the number of frequency of each term as demonstrated in Table IV and Fig. 5.

Degree of confidence is calculated by dividing the frequency of the number of times a phase appears in the models chosen by the total number of R1models. The following is how DoC is calculated:

$$\text{Degree of Confidence} = \frac{Frequency\ of\ Phase}{Total\ number\ of\ R1\ models} = \text{n\%} \quad (1)$$

Based on the Degree of Confidence (DoC), there are five (5) categories of phases well-defined and they are as follows:

- Very Strong (100 - 70%)
- Strong (69 - 50%)
- Moderate (49 - 30%)
- Mild (29 - 11%)
- Very Mild (10 - 0%)

After applying the DoC formula, it can be seen from Fig. 5 that, analysis and presentation phases has the Very Strong DoC of 100%.

$$DoC\ (Analysis) = \frac{5}{5} * 100 = 100\%$$

$$DoC\ (Presentation) = \frac{5}{5} * 100 = 100\%$$

Preservation phase has a Strong DoC of 60%

$$DoC\ (Preservation) = \frac{5}{5} * 100 = 60\%$$

TABLE IV. SELECTION OF OSNFIM DEVELOPMENT PHASES BASED ON DOC

S/No.	Phases	R1 Models					Frequency	DoC (%)
		[17]	[24]	[13]	[15]	[6]		
1.	Preliminary	✓	×	×	×	✓	2	40
2.	Preparation	×	×	✓	×	×	1	20
3.	Identification	×	✓	×	×	×	1	20
4.	Investigation	×	×	×	×	✓	2	20
5.	Incident Specification	✓	×	×	×	×	1	20
6.	Incidence Response	×	×	✓	×	×	1	20
7.	Acquisition	×	×	✓	✓	×	2	40
8.	Triage	×	×	×	✓	×	1	20
9.	Preservation	✓	✓	✓	×	×	3	60
10.	Collection	×	✓	×	×	×	1	20
11.	Examination	×	✓	×	×	×	1	20
12.	Analysis	✓	✓	✓	✓	✓	5	100
13.	Evaluation	×	×	×	×	✓	1	20
14.	Iteration	✓	×	×	×	×	1	10
15.	Presentation	✓	✓	✓	✓	✓	5	100

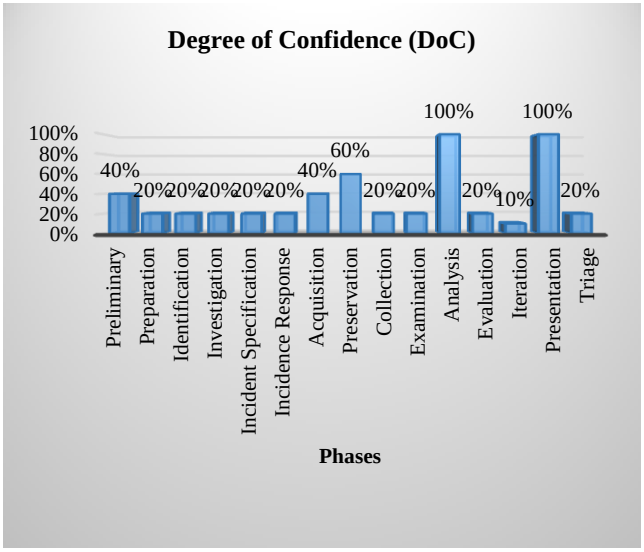

Fig. 5. OSNFIM Development Phases based on DoC.

Acquisition and Preliminary phases has moderate DoC of 40% each, Preparation, Identification, Investigation, Examination, Identification, Incident specification, Incident response and Collection phases has a Mild DoC of 20% while Iteration and Triage phases has a Very Mild DoC of 10%.

Any phase that is having the *DoC* as; Very Strong (100 - 70%), Strong (69 - 50%) or Moderate (49 - 30%) is selected while those with Mild (29 - 11%) or Very Mild (10 - 0%) were rejected. However, *iteration* phase was among the selected phases despite having the *DoC* of Very Mild (10%). It was selected because most of the previous models presented are adopting conventional practices; they are intended to offer guidance and a list of activities for human investigators. The method of automated investigation of OSNs is fundamentally iterative, investigators must continue to broaden the data collection process if the need arises [17]. Therefore, a total number of six (6) phases were selected and they are as follows:

1) Preliminary: This stage stresses two things: first, proper incident reporting, and second, formal authorization for investigation.

2) Acquisition: This is the procedure of obtaining information from any online social network.

3) Preservation: This is the secure keeping of property without altering or changing the content of data.

4) Analysis: This is the process of conducting an automated data sorting and filtering in order to obtain the most important data, which contains potential evidence.

5) Iteration: is a new round of data extraction with a wider scope.

6) Presentation: The investigators will choose relevant and appropriate evidence to present in court.

TABLE V. OSNFI PHASES AND THEIR ACTIVITIES

OSNFI Phases	Activities
Preliminary	▪ Infrastructure readiness ▪ Incident notification ▪ Authorization ▪ Acknowledgment ▪ Construction ▪ Notification ▪ Survey
Acquisition	▪ Identify Incident Parameters ▪ Identify Social Network sources ▪ Formulate PIEZ ▪ Initialize Parser ▪ Initiate Automated Extraction by using Parser ▪ Identification ▪ Searching ▪ Filtering ▪ Capturing ▪ Survey ▪ Transport ▪ Storage
Preservation	▪ Preserve a forensic copy of Data Set
Analysis	▪ Perform automated Analysis ▪ Sort and filter the data relevant to the inquiry ▪ Formulate hypotheses ▪ Examine the Data ▪ Test the Hypothesis ▪ Conclusion ▪ Reporting
Iteration	▪ Formulate new hypotheses ▪ Identify the Involvement of new Entities ▪ Outline the Secondary Information Extraction Zone ▪ Repeat Steps
Presentation	▪ Select Relevant Evidence ▪ Attach Suitable Metadata ▪ Add Visualizations ▪ Record Sequence of Steps ▪ Present the Evidence ▪ Conclusion ▪ Review ▪ Decision ▪ Interpretation ▪ Documentation ▪ Investigator ▪ CourtOfLaw

Therefore, because there is no any uniform method for conducting the investigation of an online social network crimes, these six (6) phases can be adopted in order to create a uniformity in the process of conducting the investigation.

Table V clearly defined the actions in each phase. A total of forty-three (43) activities were identified across the six (6) phases. These actions are regarded as the steps that must be completed in each phase in order to fulfill the investigation's goal.

VI. CONCLUSION

Due to the quick technology advancement, online social network forensic investigation is an essential young domain that requires considerable attention. Based on the findings of this study, it appears that, despite its importance and high demand, little work has been published in the field. Based on the search keyword, only 316 papers were obtained from five (5) online databases (Scopus, Web of Science, IEEEXplore, ScienceDirect, and Association for Computing Machinery (ACM) Digital Library). After categorizing the articles into relevant and non-related categories, it was discovered that only about 30% of the 316 documents obtained were relevant to the topic of interest, with twenty-nine (29) being duplicates. This is an indication that more work has to be conducted in the domain of OSNFI. In addition, five (5) R1 models were utilised to identify the various phases and activities that can be used in the investigation of an online social network forensic crimes and based on the level of confidence, a total of six (6) phases and forty-three (43) activities were extracted (DoC).

REFERENCES

[1] Pilli ES, Joshi RC, Niyogi R. Network forensic frameworks: Survey and research challenges. Digit. Investig. [Internet] 2010;7:14–27. Available from: http://dx.doi.org/10.1016/j.diin.2010.02.003.

[2] Baca M, Cosic J, Cosic Z. Forensic analysis of social networks (case study). Proc. Int. Conf. Inf. Technol. Interfaces, ITI 2013;219–23.

[3] Cohen F. Journal of Digital Forensics , Security and Law Column : Putting the Science in Digital Forensics. 2011;6.

[4] Kohn MD, Eloff MM, Eloff JHP. Integrated digital forensic process model. Comput. Secur. [Internet] 2013;38:103–15. Available from: http://dx.doi.org/10.1016/j.cose.2013.05.001.

[5] Kale S, Sahu PA. Forensic Imaging for Online Social Networks. 2014;3:166–70.

[6] Zainudin, M N, Merabti, Madjid, Llewellyn-jones, David. A Digital Forensic Investigation Model for Online Social Networking. 2010;1–6.

[7] Lu R, Li L. Research on forensic model of online social network. 2019 IEEE 4th Int. Conf. Cloud Comput. Big Data Anal. ICCCBDA 2019 2019;116–9.

[8] Arshad H, Jantan A, Hoon GK, Butt AS. A multilayered semantic framework for integrated forensic acquisition on social media. Digit. Investig. [Internet] 2019;29:147–58. Available from: https://doi.org/10.1016/j.diin.2019.04.002.

[9] Chang C-P. Knowledge Production from Social Network Sites - Using Social Media Evidence in the Criminal Procedure (Title of the Thesis) Knowledge Production from Social Network Sites - Using Social Media Evidence in the Criminal Procedure. 2014.

[10] Mohd Zainudin N, Merabti M, Llewellyn-Jones D. Online social networks as supporting evidence: A digital forensic investigation model and its application design. 2011 Int. Conf. Res. Innov. Inf. Syst. ICRIIS'11 2011.

[11] Montasari R. Digital Forensic Investigation of Social Media , Acquisition and Analysis of Digital Evidence. 2019;2:52–60.

[12] Kleinberg JM. Challenges in mining social network data. 2007;13:4–5.

[13] Rahman D, Rahadhian, Riadi I. Framework Analysis of IDFIF V2 in WhatsApp InvestigationProcess on Android Smartphones. Int. J. Cyber-Security Digit. Forensics 2019;8:213–22.

[14] Jang YJ, Kwak J. Digital forensics investigation methodology applicable for social network services. Multimed. Tools Appl. 2015;74:5029–40.

[15] Haggerty J, Casson MC, Haggerty S, Taylor MJ. A framework for the forensic analysis of user interaction with social media. Int. J. Digit. Crime Forensics 2012;4:15–30.

[16] Abdalla A, Yayilgan SY. A Review of Using Online Social Networks. 2014;8531:3–12.

[17] Arshad H, Omlara E, Oludare I, Aminu A. Computers & Security A semi-automated forensic investigation model for online social networks. Comput. Secur. [Internet] 2020;97:101946. Available from: https://doi.org/10.1016/j.cose.2020.101946.

[18] Montasari R. A comprehensive digital forensic investigation process model Reza Montasari. 2016;8:285–302.

[19] Valjarevic A, Venter HS. A Comprehensive and Harmonized Digital Forensic Investigation Process Model. J. Forensic Sci. 2015;60:1467–83.

[20] Kitchenham B, Pearl Brereton O, Budgen D, Turner M, Bailey J,

Linkman S. Systematic literature reviews in software engineering - A systematic literature review. Inf. Softw. Technol. [Internet] 2009;51:7–15. Available from: http://dx.doi.org/10.1016/j.infsof.2008.09.009.

[21] Ahmad P, Asif JA, Alam MK, Slots J. A bibliometric analysis of Periodontology 2000. Periodontol. 2000 2020;82:286–97.

[22] Wang X, Xu Z, Škare M. A bibliometric analysis of Economic Research-Ekonomska Istraživanja (2007–2019). Econ. Res. Istraz. [Internet] 2020;33:865–86. Available from: https://doi.org/10.1080/1331677X.2020.1737558.

[23] Chen L, Xu L, Yuan X, Shashidhar N. Digital Forensics in social networks and the cloud. 2015;1132–6. Available from: https://doi.org/10.1109/ICCNC.2015.7069509.

[24] Anwar N, ImamRiadi. Forensic Investigation Analysis of WhatsAppMessenger Smartphone Against WhatsApp Messenger Smartphone Forensic Investigation Analysis Against Web-Based WhatsApp. 2017;3:1–10.

[25] Taylor DCPJ, Mwiki H, Dehghantanha A, Akibini A, Kwang K, Choo R, et al. Science & Justice Forensic investigation of cross platform massively multiplayer online games : Minecraft as a case study. Sci. Justice [Internet] 2019;59:337–48. Available from: https://doi.org/10.1016/j.scijus.2019.01.005.