Journal of Computer Science

Original Research Paper

Investigating Cybercrimes with Digital Forensics

Maha Helal, Mohammed Alamri and Hazzaa Alshareef

College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia

Article history
Received: 09-05-2024
Revised: 11-07-2024
Accepted: 26-07-2024

Corresponding Author:
Maha Helal
College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia
Email: mhelal@seu.edu.sa

Abstract: Digital forensics has gained a high degree of attention recently due to the benefits it has to offer in investigating cybercrimes by analyzing and presenting digital evidence. It aims to highlight any correlations related to such crimes. Since digital forensics techniques are capable of providing robust and credible evidence, they have been used in different contexts and are accepted by law enforcement agencies. Social media forensics, a subdomain of digital forensics, has also been widely used to investigate digital crimes and suspicious activities on social media platforms. In addition to the challenges associated with digital forensics, such as anti-forensics, social media forensics also faces several obstacles, such as privacy and big data issues. This research proposes a dynamic methodology that utilizes digital forensics techniques to improve the investigation of cybercrimes committed on social media platforms. The proposed methodology offers a high level of flexibility, including choosing the type of crime, the platform used, and the investigation scenario. As part of the contribution of this research, the proposed methodology is used to detect suspicious activities associated with the COVID-19 pandemic. Various techniques and tools are used to evaluate the methodology such as VADER for tweet classification and other tools for collecting and extracting tweets' information and correlation. The results indicate that the methodology is simple and capable of handling the digital evidence collected, as well as identifying credible relations between the data. The proposed methodology could also be extended in many ways to handle other challenges and limitations associated with digital forensics in general and social media forensics in particular.

Keywords: Cybercrime, Digital Forensics, Digital Evidence, Anti-Forensics, Social Media Forensics, Text Sentiment

Introduction

As a branch of forensic science, digital forensics aims to examine digital evidence to extract useful insights that can help in solving cybercrimes (Maurya and Jain, 2024). The goal of digital forensics is to investigate what was done, when it was done, and who did it (Casino *et al*., 2022). According to Al-Dhaqm *et al*. (2021), digital evidence can be categorized as follows: (1) Computer Forensics includes analyzing digital evidence located in various devices and storage mediums such as PCs and operating systems as well as in the traces of installed applications and their related logs. Mainly, activities in this category include analyzing evidence from removed data after restoring it from the storage medium of the user's devices (Hassan, 2019). (2) Mobile Forensics handles collected data from various mobile devices such as smartphones (Alatawi *et al*., 2020). (3) Network Forensics involves examining and analyzing collected data from computer networks to detect possible intrusions. The collected data can be analyzed in real time or saved for future analysis. However, this category differs from other forensic categories by handling volatile data only (Hassan, 2019). (4) Database Forensics aims to answer the following questions: What, when, why, where, and how database tampering has happened and by whom (Chopade and Pachghare, 2019).

The process steps of digital forensics depend on the type of investigation (Kyung-shick *et al*., 2022; Horsman and Sunde, 2022). However, in general, all investigating types consist of the following three main phases.

Collecting: This phase is affected by the status of the device, whether it is on or off. If the device is off, limited data can be collected. However, it is crucial that the data collected

are identical to the original data. To achieve this, disk imaging tools can be used to build an identical copy of the original set of data. Once this is accomplished, the analysis can commence. Alternatively, volatile data and real-time analysis can be conducted if the device is on (Kävrestad, 2020). However, the collecting stage is associated with certain challenges, such as integrity, scalability, and data ownership issues (Soltani and Seno, 2017).

Analyzing: This phase initiates once the required data are collected from the different parts of the compromised system. The aim is not to prove whether or not a person is guilty, however; it is to provide a complete overview of the incident. Kävrestad (2020) recommends basing a basic analysis on the following: (1) Accounting for all the data; (2) Logging the device installation date, version of the operating system, and the list of users; (3) Recording information regarding the time zone; and (4) Noting the network drive maps.

Presenting: It is crucial to capture and document the detailed steps of the process of the investigation and examination of the evidence by providing this information in a final report. This includes reporting on both technical and legal evaluations. According to Varol and Sönmez (2017), two main challenges of reporting in digital forensics include: (1) Demonstrating that throughout the investigation process, evidence integrity has been taken into account. (2) Ensuring that all conducted operations are clear, transparent, and repeatable.

The handling of digital evidence is critical since the aim is to make it credible and acceptable in a court, for example. The handling task will be more difficult in some forms of digital evidence such as audio and video (Pedapudi and Vadlamani, 2023). This can be achieved by building the digital investigation steps carefully and according to logic by using the tools in the correct way. In general, any digital evidence accepted in court should follow basic rules, including the relevancy to the case and justifiability, which means explaining all the steps and methods used in presenting and demonstrating the digital evidence. Several frameworks and tools used in digital forensics have been reviewed and discussed (Dubey *et al*., 2023), where Abulaish and Haldar (2020) assert the importance of rigid digital evidence-handling procedures.

Digital forensics can be used and applied in various fields including governmental, private, and financial institutions and the investigation of crimes. For instance, Alotaibi *et al*. (2023) designed a methodology that uses digital forensics in Unmanned Aerial Vehicles (UAVs). The investigation of cybercrimes committed on social media platforms can also benefit from digital forensics. It is necessary to find methods and techniques that enable digital evidence collected from social media platforms to be accepted by the courts for the purpose of solving digital crimes, such as cyberbullying and identity theft (Soomro and Hussain, 2019; Khan *et al*., 2024).

Social media has become a medium for law enforcement units to prevent crime, as they can use such platforms to investigate digital crime or collect data about persons involved in crimes (e.g., witnesses, suspects, and victims). Therefore, social media forensics is considered an interdisciplinary field that intersects with digital forensics, big data, and data science. With regard to the processes applied in social media forensics, consist of data collection, data analysis, data visualization, and relation finding (Horsman and Sunde, 2022).

Even though social media forensics provides an alternative method of investigating digital crime, it bears with it a set of challenges that are faced by law enforcement agencies and academic researchers (Powell and Haynes, 2020). These challenges can be categorized into two types: Big data-related limitations and privacy and legal issues. First, the amount of information is enormous and is continually growing during the processing of the data collection phase. This generates noise and low-quality data which requires filtering, which also raises further challenges (Goswami and Kumar, 2017) Moreover, the challenges become more difficult when considering that there is not a unified standard method for investigating the variant types of social media platforms and the data generated by them, which causes further challenges such as the heterogeneity of the data.

Second, privacy and legal issues occur because social media providers are not willing to share users' activities with law enforcement agencies, for the purpose of maintaining user privacy. Hence, social media providers may refuse to cooperate. However, court orders could be issued to force social media providers to share victims' or suspects' data, such as subscriber information, dates of connection, and IP addresses. The challenge becomes more complicated in international cases.

Another considerable challenge in digital forensics facing investigators is anti-forensics (Yaacoub *et al*., 2022). Anti-forensics science aims to make forensics analysis more difficult by using mechanisms to mislead the process of investigation. These mechanisms affect collecting of digital evidence by concealing or deleting them which increases the amount of time and effort needed in the analysis process (Hassan, 2019). To achieve this aim, a set of existing tools are used to destroy digital evidence by modifying it and altering its availability which impacts the scientific validity of the evidence when used. In practice, anti-forensics approaches differ based on the purpose needed which includes artifact wiping, data hiding (e.g., steganography and encryption), and trail obfuscation (Kadhim *et al*., 2019; Majed *et al*., 2020).

Main Contribution of the Research

This study proposes a dynamic methodology utilizing digital forensics techniques for the purpose of improving

the investigation of incidents on social media platforms. The proposed methodology offers the flexibility of choosing the type of crime, the platform used, as well as the investigation scenario. Hence, applying the methodology will help in increasing the robustness and credibility of digital evidence, especially that taken from social media platforms. Therefore, the summary of the research contribution is as follows:

- Reviewing the literature and highlighting the related work
- Proposing a dynamic methodology utilizing digital forensics techniques
- Validating the proposed methodology and discussing the findings

Related Works

Arshad *et al*. (2020) present an event-based knowledge model that aims to define all objects involved in the incident and find any relation and correlation between them. As a result, the collected information will be filtered to choose the most related to the incident. The proposed model also defines objects that are involved in event-based knowledge on social media (e.g., event, object, subject, time, sub-event, and interaction). The implementation of their model achieved an extraction of evidence which led to a strong investigation.

In their study, Pasquini *et al*. (2021) discuss digital forensics analysis techniques in three stages: (1) Source identification and integrity verification on media uploaded on social networks; (2) Platform provenance analysis allowing the identification of sharing platforms; and (3) Multimedia verification algorithms that assess the credibility of media objects in relation to their associated textual information. In the first stage, the authors discuss traditional multimedia forensics that aims to verify the integrity of the collected data as well as identify its source. In the second stage, the identification of the platform's objects and the extraction of information is accomplished. The authors examined the ability of machine learning in particular to analyze images. In the third stage, they address the challenge of images and videos appearing alongside other forms of textual information and the misinformation that might be caused. The authors state that a main limitation in digital forensics analysis is related to the availability of the datasets and how realistic the data is. The authors conclude that this field remains a subject of interest and challenge for researchers, especially as videos contribute more to the transfer of information and there is greater difficulty in analyzing them and applying the rules of digital forensics.

Al-khateeb and Agarwal (2020) state that social media platforms contain many online deviant groups that disseminate fake propaganda in accordance with negative objectives. The authors provide a set of methods that utilize the Maltego tool to find any hidden correlations among (1) Twitter accounts and a set of websites/blogs (2) Websites/blogs and other websites/blogs; or (3) To infer ownership of a set of websites/blogs. These methods have been examined on a number of items of cyber propaganda in three different case studies. Other techniques have also been used and tested to analyze social media content and distinguish whether the content is considered to be suspicious and for the purpose of circulating fake news (Riadi *et al*., 2020).

Other work, presented by Rocha *et al*. (2017), states that there are a number of reasons that complicate the process of identifying social media users during the investigation process such as the use of public Wi-Fi hotspots, pre-paid SIM cards, distributed networks. Their work introduced a new method, Authorship Attribution, which aims at finding the ownership of social media content by detecting the writing style (tweets). Extracting the identity of such an author from the text of a tweet faces many challenges, such as the size of the tweets when they are very short. In addition, the problem becomes more difficult when the tweet includes unconventional punctuation, abbreviations, and characters based on signifiers common in Internet culture.

Shu *et al*. (2017) discuss the phenomenon of fake news on social media and review many of the algorithms that detect it. The authors believe that the detection of social media fake news faces many challenges which require further investigation. They provide several definitions of fake news and provide the unique characteristics of it on social media. According to Ghani *et al*. (2019), Social Network Analysis (SNA) is defined as the process of finding social relations between different objects within social media platforms. Stieglitz *et al*. (2014) divided the analytics process of SNA into several steps: Discovery, collection, preparation, and analysis. SNA aims to combine different data analysis techniques on social media. It became a field of interest in academic research and business. However, it differs from traditional analytics in various aspects, including volume, velocity, variety, and veracity (Stieglitz *et al*., 2018).

Materials and Methods

This research proposes a methodology that aims to improve the process of investigating digital crimes. Usually, building such a methodology relies on three main factors: (1) The type of crime; (2) The platform used; and (3) The investigation scenario. Since there are

many cybercrimes that can occur on social media platforms, this research mainly focuses on suspicious activities as a form of cybercrime.

Regarding the chosen platform, there are several different platforms on social media (e.g., Facebook, X [still called Twitter when this research was being conducted], YouTube, and Snapchat). Each of these platforms has a structure that is distinct from the others and has different types of data. It is not possible to build a methodology that can work with all these platforms at the same time. For instance, creating a methodology that relies on text analysis will not work well on a platform such as YouTube since it relies heavily on video content. Therefore, for this research, the Twitter platform was used to build the methodology. Regarding the third factor, this research introduces the following scenario: Searching in a specific topic, hashtag, or case, and then through this topic it is possible to search for suspicious activities (fake news, racism, etc.). More precisely, topics relating to the COVID-19 pandemic were chosen as part of the investigation scenario for the purpose of detecting any possibility of fake news propaganda that could have a negative impact on social stability. At the time of the preparation of this research, a very high number of people had become infected with COVID-19. The number of COVID-19-related fatalities has also increased dramatically. The pandemic's statistics were reflected in social media content and have become a new field for researchers and data analysts. The following four topics (#Hashtags) related to the COVID-19 pandemic were chosen: #Covid19, #Vaccine, #Astrazeneca, and #Sputnikv.

As mentioned earlier, social media forensics consists of four main processes/phases, as shown in Fig. (1). As presented in Fig. (1), the investigation consists of four main phases:

- Phase 1: Collect data from the social media platform
- Phase 2: Analyze the data using a text sentiment engine to classify them into positive or negative
- Phase 3: Visualize the results
- Phase 4: Analyze the results to extract relationships and insights

Regarding the text tweet classification process, the Valence Aware Dictionary and Sentiment Reasoner (VADER) is applied. It is an analysis tool commonly applied to examine sentiment expression on social media (Khan and Srivastava, 2024). After collecting the tweets, the classification process is started using the VADER Sentiment library to classify the tweets as negative and positive. If the tweet is negative, the author information (including author ID, location, and join date) of this tweet is extracted. Fig. (2) Presents the process of classifying tweets using the aforementioned technique.

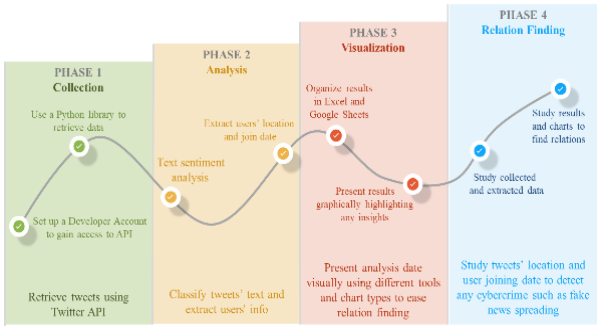

Fig. 1: Investigation process

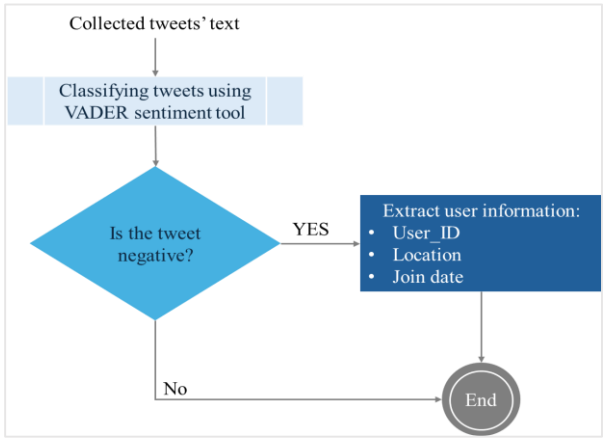

Fig. 2: Tweets' classification process using VADER to extract user information from negative tweets

Finally, with regard to the tools and technical requirements, this research chose "Google Colab" from among a number of Python compilers. "Google Colab" enables Python code to be written and executed in the browser with zero configuration required. This tool has several useful features, such as its free access to GPUs and ease of sharing. Similarly, there are many libraries that are available for use in research, such as VADER sentiment analysis and goepy. This research mainly used Tweepy, which is an open-source library hosted on GitHub that allows Python to interact with the Twitter API. Furthermore, this tool is beneficial for simple automation and creating a Twitter bot.

After defining the topics, the platform used, the investigation scenario, and the tools, the following investigation processes were performed.

Data collection: Collect 2,500 tweets from the selected topics above (hashtags).

Data analysis: Analyze all tweets, classify them, and extract information about the tweets' users (location and joining date) from negative tweets only.

Data visualization: Visualize the results in order to find relationships.

Relation finding: Analyze results to report if suspicious activities have been detected.

Results and Discussion

This section presents the results of analyzing the data collected from the four selected topics (hashtags). It also provides the findings and a detailed discussion based on the chosen investigation scenario, as outlined below:

- Percentage of negative and positive tweets in each hashtag, whereby the focus is on negative tweets
- User location (coordinates or country) analysis results
- Join date results
  - If the user created the account before the year 2020, it is considered an old account (i.e., a genuine account)
  - If the account was created after the year 2020, it is considered a new account (i.e., a suspicious account)

#Covid19

The results indicate that positive tweets (22%) are almost equal to negative tweets (21%), as presented in Fig. (3). Regarding the location analysis, it was found that the users' locations were distributed broadly as tweets were published from different countries. Fig. (4) Demonstrates the tweets' locations graphically. As for the users' join date, it was found that around 75% of all accounts were created before 2020, as shown in Fig. (5). As a result, it is apparent that no suspicious activities were detected for this hashtag at the time the tweets were collected.

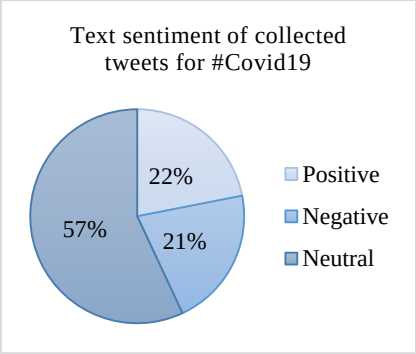

Fig. 3: Text sentiment of collected tweets for #Covid19

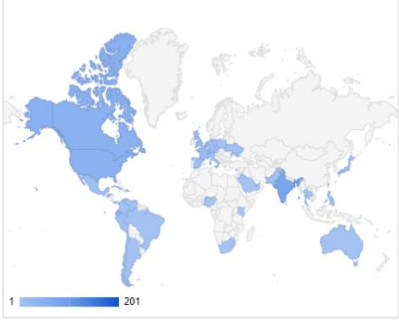

Fig. 4: Tweets' location distribution for #Covid19

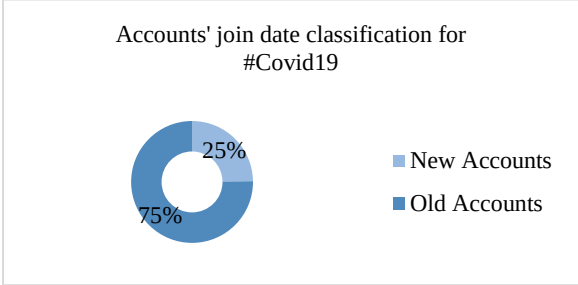

Fig. 5: Accounts' join date classification for #Covid19

#Vaccine

As presented in Fig. (6), there is a slightly higher percentage of positive tweets (36%) than negative tweets (30%). It was found that the users' locations were distributed broadly and tweets were published from different countries, as shown in Fig. (7). It was also found that around 83% of all accounts were created prior to 2020, as shown in Fig. (8). As a result, this indicates that no suspicious activities were detected for this hashtag at the time the tweets were collected.

#AstraZeneca

The results show that there are slightly fewer positive tweets (9%) than negative tweets (12%), as presented in Fig. (9). As shown in Fig. (10), the users' locations were distributed broadly, whereby tweets were published from different countries. Around 83% of all the accounts were created before 2020, as indicated in Fig. (11). These results suggest that no suspicious activities were detected for this hashtag when the tweets were collected.

#Sputnikv

For this hashtag, the results indicate that the positive tweets (9%) almost equal the negative tweets (7%), as presented in Fig. (12). The location analysis found that the users' locations were distributed broadly and the tweets were published from different countries, as shown in Figs. (13-14) shows that 94% of all accounts were created before 2020. This indicates that no suspicious activities were detected for this hashtag when the tweets were collected.

According to the results for all the data collected from the four chosen topics (hashtags) and after applying the investigation scenario, it is apparent that the proportion of positive tweets is either equal to or slightly higher than that of negative tweets. Regarding the location distribution of the collected tweets, it was found that the distribution was across different countries. However, it is worth noting that the location feature of some tweets had been disabled, which placed a limitation on analyzing the location of these tweets. Logically, it is very important to determine this indicator (location) if suspicious activities, such as disseminating fake news, take place, as such actions are usually planned and implemented in the same geographical location.

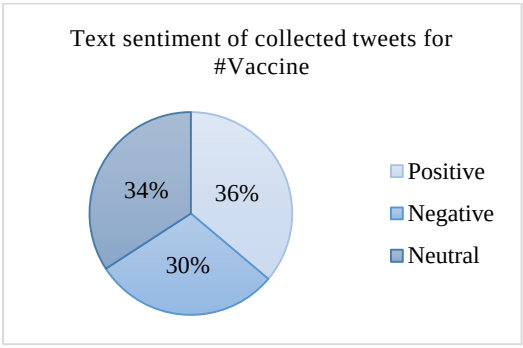

Fig. 6: Text sentiment of collected tweets for #Vaccine

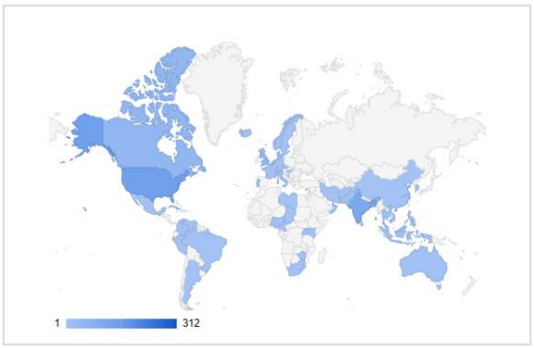

Fig. 7: Tweets' location distribution for #Vaccine

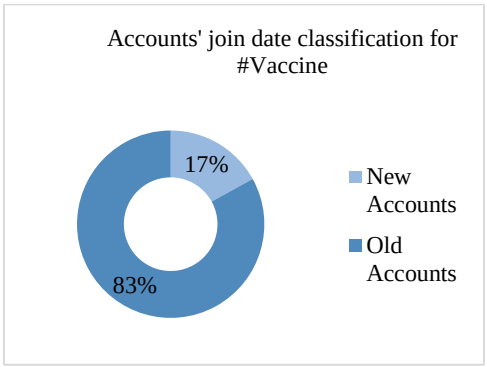

Fig. 8: Accounts' join date classification for #Vaccine

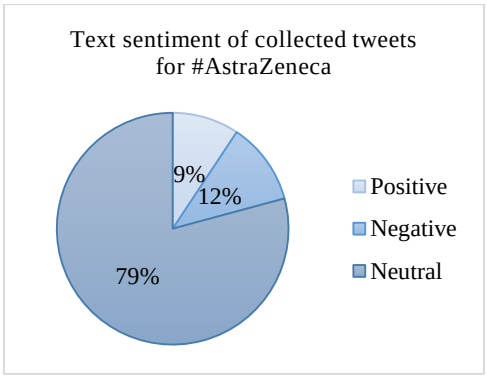

Fig. 9: Text sentiment of collected tweets for #AstraZeneca

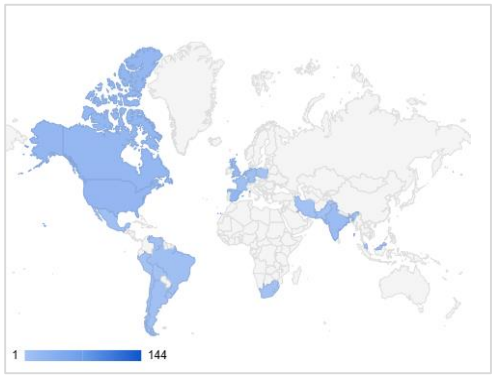

Fig. 10: Tweets' location distribution for #AstraZeneca

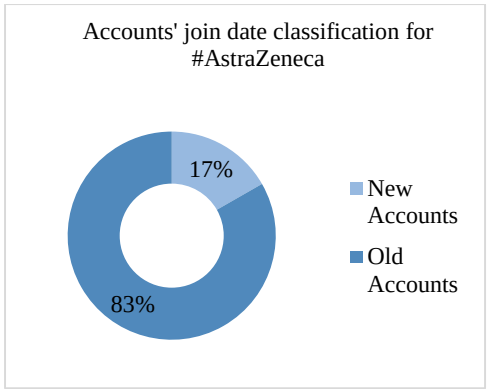

Fig. 11: Accounts' join date classification for #AstraZeneca

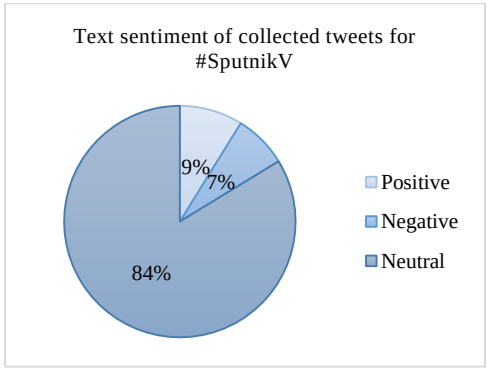

Fig. 12: Text sentiment of collected tweets for #SputnikV

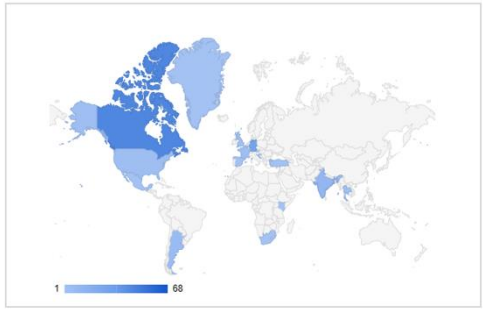

Fig. 13: Tweets' location distribution for #SputnikV

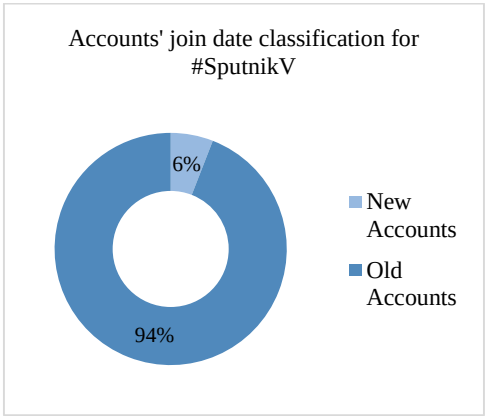

Fig. 14: Accounts' join date classification for #SputnikV

Moreover, creating new accounts is one mechanism for increasing the spread and dissemination of fake news. As presented above, it is clear that the percentage of old accounts (i.e., those created before 2020 when the pandemic hit) was much higher compared with the percentage of new accounts, by at least two-thirds. Therefore, it is evident that no suspicious activities were detected.

Conclusion

Digital forensics is considered one of the modern methods for investigating cybercrimes by supporting law enforcement agencies and investigators to build robust and credible digital evidence to be used in the courts. Several processes are performed in digital forensics, mainly collecting, analyzing, and presenting results for the purpose of discovering correlations in relation to such crimes. However, in some contexts, these processes could include other processes, such as data visualization and relation finding.

Social media forensics is an interdisciplinary field that applies the techniques of digital forensics and data analytics in collecting and analyzing digital evidence from social media platforms. It supports investigation efforts in relation to digital crimes and suspicious activities that may occur on social media platforms, such as fake news dissemination.

This research proposes a flexible methodology that uses digital forensics techniques to support identifying suspicious activities on social media platforms. This methodology relies on the selection of three main factors: (1) The type of crime (suspicious activities, in this research); (2) The platform used (Twitter in this case); and (3) The investigation scenario. Different tools and methods were used in this research, such as a text sentiment method for the purpose of classifying the collected tweets and finding relations between them.

Experimental results indicate that the analysis of tweets collected from the chosen topics (hashtags) did not show any suspicious activities. This finding was made after comparing negative tweets with positive tweets and the distribution of the tweets' geographical location (countries). Twitter user account creation dates were also analyzed to detect if these accounts had been initially created to spread fake news related to the chosen topics.

The challenges involved emerged clearly through this research and can be summarized under many headings, such as big data challenges, privacy and legal issues, and a lack of tools, algorithms, and methodologies. Since social media forensics is a developing field, there are different directions in which this research can be extended. First, increasing the dataset size as well as extracting more parameters from collected tweets, such as age and gender, would improve the investigation and relation finding. Second, to validate the flexibility of the proposed methodology, different and a broader range of hashtags and topics as well as types of cybercrimes could be analyzed. Finally, other platforms, such as YouTube or Instagram, could be selected to examine the usability of the methodology.

Acknowledgment

The authors of this manuscript would like to express their appreciation and gratitude to their university for supporting this research.

Funding Information

The authors have not received any financial support or have any funding to report.

Author's Contributions

Maha Helal: Analysis and interpretation of data, investigation, conceptualization, methodology, original draft preparation, and approval of the version to be submitted and any revised version.

Mohammed Alamri: Acquisition of data, software, design, investigation, and approval of the version to be submitted and any revised version.

Hazzaa Alshareef: Conceptualization, reviewing editing and approval of the version to be submitted and any revised version.

Ethics

This study is original and innovative and contains unpublished material. There are no ethical issues involved and none of the authors have any conflicts of interest to disclose.

References

Abulaish, M., & Haldar, N. A. H. (2020). Advances in Digital Forensics Frameworks and Tools: A Comparative Insight and Ranking. In *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools and Applications* (pp. 165–191). IGI Global. https://doi.org/10.4018/978-1-7998-2466-4.ch010

Alatawi, H., Alenazi, K., Alshehri, S., Alshamakhi, S., Mustafa, M., & Aljaedi, A. (2020). Mobile Forensics: A Review. *2020 International Conference on Computing and Information Technology (ICCIT-1441)*, 1–6. https://doi.org/10.1109/iccit-144147971.2020.9213739

Al-Dhaqm, A., Ikuesan, R. A., Kebande, V. R., Razak, S. A., Grispos, G., Choo, K.-K. R., Al-Rimy, B. A. S., & Alsewari, A. A. (2021). Digital Forensics Subdomains: The State of the Art and Future Directions. *IEEE Access*, *9*, 152476–152502. https://doi.org/10.1109/access.2021.3124262

Al-khateeb, S., & Agarwal, N. (2020). Social Cyber Forensics: Leveraging Open Source Information and Social Network Analysis to Advance Cyber Security Informatics. *Computational and Mathematical Organization Theory*, *26*, 412–430. https://doi.org/10.1007/s10588-019-09296-3

Alotaibi, F., Al-Dhaqm, A., & Al-Otaibi, Y. D. (2023). A Conceptual Digital Forensic Investigation Model Applicable to the Drone Forensics Field. *Engineering, Technology & Applied Science Research*, *13*(5), 11608–11615. https://doi.org/10.48084/etasr.6195

Arshad, H., Jantan, A., Hoon, G. K., & Abiodun, I. O. (2020). Formal Knowledge Model for Online Social Network Forensics. *Computers & Security*, *89*, 101675. https://doi.org/10.1016/j.cose.2019.101675

Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., & Patsakis, C. (2022). Research Trends, Challenges and Emerging Topics in Digital Forensics: A Review of Reviews. *IEEE Access*, *10*, 25464–25493. https://doi.org/10.1109/access.2022.3154059

Kyung-shick, C., Sinchul, Back, & Toro-Allvarez, Marlon Mike. (2022). *Digital Forensics and Cyber Investigation*. Cognella, Incorporated. ISBN-10: 1516536371.

Chopade, R., & Pachghare, V. K. (2019). Ten years of Critical Review on Database Forensics Research. *Digital Investigation*, *29*, 180–197. https://doi.org/10.1016/j.diin.2019.04.001

Dubey, H., Bhatt, S., & Negi, L. (2023). Digital Forensics Techniques and Trends: A Review. *The International Arab Journal of Information Technology*, *20*(4), 644–654. https://doi.org/10.34028/iajit/20/4/11

Ghani, N. A., Hamid, S., Targio Hashem, I. A., & Ahmed, E. (2019). Social Media Big Data Analytics: A Survey. *Computers in Human Behavior*, *101*, 417–428. https://doi.org/10.1016/j.chb.2018.08.039

Goswami, A., & Kumar, A. (2017). Challenges in the Analysis of Online Social Networks: A Data Collection Tool Perspective. *Wireless Personal Communications*, *97*(3), 4015–4061. https://doi.org/10.1007/s11277-017-4712-3

Hassan, N. A. (2019). Windows Forensics Analysis. In *Digital Forensics Basics* (pp. 179–245). Apress. https://doi.org/10.1007/978-1-4842-3838-7_7

Horsman, G., & Sunde, N. (2022). Unboxing the Digital Forensic Investigation Process. *Science & Justice*, *62*(2), 171–180. https://doi.org/10.1016/j.scijus.2022.01.002

Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive Survey of Image Steganography: Techniques, Evaluations and Trends in Future Research. *Neurocomputing*, *335*(28), 299–326. https://doi.org/10.1016/j.neucom.2018.06.075

Kävrestad, J. (2020). *Fundamentals of Digital Forensics* (2nd Ed.). Springer International Publishing. https://doi.org/10.1007/978-3-030-38954-3

Khan, A., Chen, Y.-L., Hajjej, F., Ahmed Shaikh, A., Yang, J., Soon Ku, C., & Yee Por, L. (2024). Digital Forensics for the Socio-Cyber World (DF-SCW): A Novel Framework for Deepfake Multimedia Investigation on Social Media Platforms. *Egyptian Informatics Journal*, *27*, 100502. https://doi.org/10.1016/j.eij.2024.100502

Khan, M., & Srivastava, A. (2024). Sentiment Analysis of Twitter Data Using Machine Learning Techniques. *International Journal of Engineering and Management Research*, *14*(1), 196–203. https://doi.org/10.5281/zenodo.10791485

Majed, H., Noura, H. N., & Chehab, A. (2020). Overview of Digital Forensics and Anti-Forensics Techniques. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 1–5. https://doi.org/10.1109/isdfs49300.2020.9116399

Maurya, M., & Jain, V. (2024). Digital Forensics and Cyber Investigation. *International Journal of Innovative Research in Technology and Science*, *12*(2), 363–365.

Pasquini, C., Amerini, I., & Boato, G. (2021). Media Forensics on Social Media Platforms: A Survey. *EURASIP Journal on Information Security*, *2021*(1), 4. https://doi.org/10.1186/s13635-021-00117-2

Pedapudi, S. M., & Vadlamani, N. (2023). Digital Forensics Approach for Handling Audio and Video Files. *Measurement: Sensors*, *29*, 100860. https://doi.org/10.1016/j.measen.2023.100860

Powell, A., & Haynes, C. (2020). Social Media Data in Digital Forensics Investigations. In *Digital Forensic Education,* (Vol. 61, pp. 281–303). Springer International Publishing. https://doi.org/10.1007/978-3-030-23547-5_14

Riadi, I., Sunardi, & Widiandana, P. (2020). Investigating Cyberbullying on WhatsApp Using Digital Forensics Research Workshop. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(4), 730–735. https://doi.org/10.29207/resti.v4i4.2161

Rocha, A., Scheirer, W. J., Forstall, C. W., Cavalcante, T., Theophilo, A., Shen, B., Carvalho, A. R. B., & Stamatatos, E. (2017). Authorship Attribution for Social Media Forensics. *IEEE Transactions on Information Forensics and Security*, *12*(1), 5–33. https://doi.org/10.1109/tifs.2016.2603960

Shu, K., Sliva, A., Wang, S., Tang, J., & Liu, H. (2017). Fake News Detection on Social Media: A Data Mining Perspective. *ACM SIGKDD Explorations Newsletter*, *19*(1), 22–36. https://doi.org/10.1145/3137597.3137600

Soltani, S., & Seno, S. A. H. (2017). A Survey on Digital Evidence Collection and Analysis. *2017 7th International Conference on Computer and Knowledge Engineering (ICCKE)*, 247–253. https://doi.org/10.1109/iccke.2017.8167885

Soomro, T. R., & Hussain, M. (2019). Social Media-Related Cybercrimes and Techniques for Their Prevention. *Applied Computer Systems*, *24*(1), 9–17. https://doi.org/10.2478/acss-2019-0002

Stieglitz, S., Dang-Xuan, L., Bruns, A., & Neuberger, C. (2014). Social Media Analytics. *Business & Information Systems Engineering*, *6*, 89–96. https://doi.org/10.1007/s12599-014-0315-7

Stieglitz, S., Mirbabaie, M., Ross, B., & Neuberger, C. (2018). Social Media Analytics – Challenges in Topic Discovery, Data Collection and Data Preparation. *International Journal of Information Management*, *39*, 156–168. https://doi.org/10.1016/j.ijinfomgt.2017.12.002

Varol, A., & Sonmez, Y. U. (2017). Review of Evidence Analysis and Reporting Phases in Digital Forensics Process. *2017 International Conference on Computer Science and Engineering (UBMK)*, 923–928. https://doi.org/10.1109/ubmk.2017.8093563

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Advanced Digital Forensics and Anti-Digital Forensics for IoT Systems: Techniques, Limitations and Recommendations. *Internet of Things*, *19*, 100544. https://doi.org/10.1016/j.iot.2022.100544