Digital Forensic Investigation Tools for Cases Related to Social Media and Cybersecurity

Asma Ibrahim Hijan

Bachelor of Computer Science, King Khalid University, Saudi Arabia

Email: asma.hijan@gmil.com

Abstract:

The entire world has moved into the digital realm as a result of the quickening pace of technological development. However, this change has also led to an increase in cybercrimes and security breach occurrences, which endanger user security and privacy. As a result, this study sought to examine how digital forensics, a significant advancement in cybersecurity, is used to combat cybercrime. The most recent developments in digital forensics, such as cloud forensics, social media forensics, and IoT forensics, have been examined in this study. With the use of these technologies, cybersecurity experts can protect data while identifying fraudsters by using the digital footprints that data processing and storage leave behind.

Technical, operational, and personnel-related issues are among the specific dangers to digital forensics that have been identified by the research. These systems' high level of complexity, volume of data, chain of custody, personnel integrity, and the validity and accuracy of digital forensics are all significant barriers to their widespread adoption. However, the research has also noted the use of artificial intelligence, intrusion detection, and USB forensics as significant prospects for digital forensics that can make the processes simpler, more effective, and safe.

Keywords: Digital forensics, Data security, Cybercrime, Data theft, Security attack

1. Introduction

The emergence of Web 2.0 technologies and the rapid advancement in the digital arena have significantly altered the global paradigm. These days, more and more people participate in internet exchanges, give to open projects, and post information about their Chapter online. However, the anonymity and ease with which any of these can be carried out cause concern over veracity and trust (Gollub, 2013). Particularly, the development of digital technologies has given rise to new strategies for committing computer crimes. In addition, the accessibility of networks and highly optimized data transfer have prompted security worries. Every day, malicious approaches, tools, and software are developed and executed to threaten both public and private networks while also exploiting data storage to obtain valuable information (Aminnezhad & Dehghantanha, 2014).

Digital forensics has received a lot of attention in resolving cybersecurity concerns to counter this new threat. According to, the science of displaying, documenting, analyzing, storing, and identifying information and evidence from electronic and digital devices while protecting user privacy is known as digital forensics. In addition, it recreates and explains the sequence of events using scientific methods. Digital forensics tries to use such illicit artifacts as evidence by analyzing, examining, and recording these sequences (Dezfouli & Dehghantanha, 2014).

Social networks undeniably power the modern world, and as digital technologies have advanced, cybercrime has also advanced, considerably influencing the creation of new strategies, tools, and attacks that allow attackers to breach even well-controlled environments (Sharma et al., 2019).

To combat the growing number of cyber anomalies, security professionals, researchers, and law enforcement organizations use digital forensics. To gather digital evidence, these professionals use scientific techniques including identification, validation, interpretation, and documentation on digital devices like RAM, phones, memory cards, floppy disks, and flash drives. However, as digital forensics tools progress, hackers are also taking use of anti-forensics technologies to either delay or entirely destroy digital evidence (Wazid et al., 2013).

1.1. Study problem

The rapid growth of social media platforms and their integration into various aspects of our lives has given rise to new challenges in the realm of cybersecurity. As social media becomes increasingly prevalent, it becomes a prime target for cybercriminals seeking to exploit vulnerabilities, commit fraud, engage in harassment, or perpetrate other malicious activities. Digital forensic investigations play a crucial role in uncovering evidence, identifying perpetrators, and providing legal support in social media-related cybersecurity cases.

However, the field of digital forensics faces challenges in effectively investigating and analyzing social media-related incidents due to the dynamic nature of social media platforms, their vast amount of user-generated content, and the complexity of extracting and preserving digital evidence. Therefore, there is a need to evaluate and assess the existing digital forensic investigation tools specifically designed for social media-related cybersecurity cases.

1.2. Study question

1- What are the current challenges faced by digital forensic investigators when conducting investigations related to social media in the context of cybersecurity incidents؟

2- What are the existing digital forensic investigation tools available for analyzing social media-related evidence in cybersecurity cases, and what are their strengths and limitations؟

3- How effective are the existing digital forensic investigation tools in handling social media-related evidence in cybersecurity cases? What are their capabilities, features, and limitations؟

4- Are there any specific requirements or improvements needed in digital forensic investigation tools to enhance their effectiveness in social media-related cybersecurity cases?

1.3. Study Objectives:

1- Assess the current challenges and limitations faced by digital forensic investigators when conducting investigations related to social media in the context of cybersecurity incidents.

2- Identify and evaluate existing digital forensic investigation tools specifically designed for analyzing social media-related evidence in cybersecurity cases.

3- Analyze the capabilities, features, and limitations of the identified digital forensic investigation tools in handling social media-related evidence.

4- Determine the effectiveness of the existing tools in addressing the challenges posed by social media in cybersecurity investigations.

5- Identify specific requirements and improvements needed in digital forensic investigation tools to enhance their effectiveness in social media-related cybersecurity cases.

1.4. Study Importance:

1- Enhancing Investigation Capabilities: The study of digital forensic investigation tools for social media-related cybersecurity cases is crucial for enhancing the capabilities of investigators. By understanding the strengths and limitations of existing tools, researchers can identify areas for improvement and develop more effective methodologies and techniques to investigate social media-related incidents.

2- Addressing Emerging Threats: Social media platforms are constantly evolving, and cybercriminals adapt their tactics accordingly. By focusing on digital forensic investigation tools for social media-related cases, this study addresses the emerging threats and challenges posed by cybercrime on these platforms. It helps in staying ahead of cybercriminals and developing strategies to effectively investigate and mitigate social media-related cybersecurity incidents.

3- Preserving Digital Evidence: Social media platforms generate vast amounts of user-generated content, making it challenging to extract and preserve digital evidence. This study emphasizes the importance of digital forensic investigation tools in accurately collecting, analyzing, and preserving social media-related evidence. It contributes to the development of best practices for maintaining the integrity and admissibility of digital evidence in legal proceedings.

4- Informing Decision-Making: By evaluating the capabilities of existing digital forensic investigation tools, this study provides insights that can inform decision-making processes. Investigators, forensic analysts, and cybersecurity professionals can make informed choices about the tools they employ in social media-related cybersecurity cases, ensuring efficient and effective investigations.

2. Methodology

Approach and Relationship to the Study:

The approach followed in this study is a combination of literature review, tool evaluation, data analysis, and requirement analysis. The study begins with a comprehensive review of existing literature to establish a foundation of knowledge and identify key challenges, tools, and methodologies in the field of digital forensic investigation for social media-related cybersecurity cases. This literature review helps inform the research questions and objectives of the study.

Following the literature review, the study identifies and selects digital forensic investigation tools specifically designed for analyzing social media-related evidence in cybersecurity cases. These tools are then applied to relevant datasets or case studies that involve various social media-related cybersecurity incidents. The evaluation process assesses the tools' effectiveness in extracting, analyzing, and preserving social media-related evidence.

The results obtained from the tool evaluation are analyzed to identify patterns, trends, and gaps in the capabilities of the tools. This analysis forms the basis for the requirement analysis, where specific requirements and improvements needed in digital forensic investigation tools for social media-related cases are identified.

The approach followed in this study is closely aligned with the research questions and objectives. It allows for a systematic evaluation of existing tools, an analysis of their strengths and limitations, and the identification of areas for improvement. By combining literature review, tool evaluation, data analysis, and requirement analysis, the study provides a comprehensive assessment of digital forensic investigation tools for social media-related cybersecurity cases.

3. Literature Review

The literature review conducted for this study aimed to explore existing research, publications, and articles related to digital forensic investigation tools for cases involving social media and cybersecurity. The review sought to establish a foundation of knowledge and identify key challenges, tools, and methodologies in the field. The following sources were consulted:

1- Casey, E. (2018). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.

Casey's book provides a comprehensive overview of digital evidence and computer crime, including chapters dedicated to social media forensics. It covers various aspects of digital forensic investigations, including evidence acquisition, analysis, and preservation, with a focus on the challenges and complexities associated with social media platforms.

2- Marrington, A., & Clark, D. (2019). Digital forensics: Challenges and future research directions. Digital Investigation, 29, S88-S96.

This research article discusses the challenges faced in digital forensics, including those specific to social media investigations.

It explores the need for advanced tools and techniques to handle the vast amounts of data generated by social media platforms and identifies areas for future research and development.

4. Digital Forensics

Digital forensics is the practice of collecting, analyzing, and preserving digital evidence to investigate and respond to cybersecurity incidents. It involves the application of forensic techniques and tools to examine digital systems, networks, and data in order to identify the source of an attack, assess the extent of the compromise, and gather evidence for legal or disciplinary actions, Examples of tools used (Forensic Toolkit, Cellebrite UFED, DEFT, OpenPuff).

4.1. Digital forensics and its role in cybersecurity

The role of digital forensics in cybersecurity is multifaceted and vital to effectively respond to and mitigate cyber threats. Here are some key aspects of its role:

1- Incident response: Digital forensics is an integral part of incident response procedures. When a cybersecurity incident occurs, such as a data breach or a network intrusion, digital forensic techniques are used to identify the attack vector, determine the scope of the compromise, and gather evidence to understand the attacker's methods and motives. This information helps organizations contain the incident, remediate vulnerabilities, and prevent future attacks (Casey, 2011).

2- Attribution and threat intelligence: Digital forensics can aid in attributing cyber-attacks to specific individuals, groups, or nation-states. By analyzing the digital evidence left behind, such as malware, network logs, or communication traces, forensic experts can piece together the tactics, techniques, and procedures (TTPs) employed by threat actors. This intelligence can be shared with relevant authorities, security organizations, or the cybersecurity community to enhance overall defense capabilities (Rogers, 2017).

3- Malware analysis: Digital forensics plays a crucial role in analyzing malware, which is often used in cyber-attacks. Forensic investigators examine the behavior, code, and impact of malicious software to understand its functionality, origins, and potential vulnerabilities it exploits. This knowledge helps in developing countermeasures, detecting similar malware variants, and improving overall cybersecurity defenses (Nelson, 2018).

4- Data breach investigations: In the event of a data breach, digital forensics helps uncover how the breach occurred, what data was compromised, and the extent of the damage. Forensic experts analyze system logs, network traffic, and compromised devices to identify the attack vector and determine whether any sensitive data was accessed, exfiltrated, or altered. This information is crucial for organizations to comply with data breach notification requirements, assess the impact on affected individuals, and implement appropriate remediation measures.

5- Legal and regulatory compliance: Digital forensics plays a crucial role in legal proceedings related to cybercrimes. The evidence collected and analyzed through digital forensic techniques can be presented in court to support legal actions against cybercriminals. Additionally, organizations may use digital forensics to demonstrate compliance with industry regulations and legal obligations related to cybersecurity, data protection, and incident response (SANS Institute, n.d).

4.2. Social media digital forensics tools and its mechanism

The process of forensic analysis of social media is a complex process and requires a lot of understanding and tracking. There are auxiliary software tools based on special software such as Python. The forensic investigation process on social media goes through several stages, the most important of which are:

- Data Collection: The process of collecting data through activity log on the digital communication platform and collecting IP addresses, social media platform APIs (e.g., Facebook Graph API, Twitter API, Instagram API) to retrieve user data, posts, comments, and other relevant information. And Implement web scraping techniques to collect information when APIs are not available or insufficient such as (Scrapy, Selenium, Apify) this platform used for web scraping or Implement new specfic web scraping tools using AI programming language.

- Data Preservation: Ensure that collected data remains unchanged and tamper-proof.

- Data Analysis: 1- Text analysis using natural language processing (NLP) to analyze text data, including sentiment analysis, topic modeling, and keyword extraction, 2- Image and video analysis Extract metadata from multimedia files, such as geolocation, timestamps, and camera information, and using Tools to verify the reliability of images or video, not fake or tampered or made with artificial intelligence. 3- User profiling: Create detailed profiles of social media users, including their connections, interests, and behavior patterns. 4- Network analysis to monitor network devices, servers, and cloud resources, there are many tools using network analysis such as (Cacti: uses SNMP to collect and display network data in graphs, Snort is an open-source intrusion detection system (IDS) and intrusion prevention system (IPS), Angry IP Scanner: Angry IP Scanner is a lightweight, cross-platform network scanner that quickly scans IP addresses and ports to discover devices on a network). 5- Analyze Hashtag the use and popularity of hashtags, and first user who create hashtag and its activity and social manner.

- Geolocation and Timestamp Analysis: Geotagging: Determine the geographical origin of posts and track the movement of users, Timestamp analysis: Establish the timeline of events based on post timestamps.

- Metadata Extraction**:** Extract metadata from images, videos, and posts to understand the context and authenticity of the content. b. Verify image authenticity by checking for digital manipulation, Identify unusual behavior patterns, such as bot accounts, fake profiles, or abnormal posting activity.

- Creating interactive visualizations information map to track a digital forensic investigation.

- Adhere to relevant legal and ethical standards in data collection and analysis, and maintain user's data privacy.

These are some of the mechanism steps for digital investigation on social media, with many tools and software used that can be obtained or developed.

4.3. The importance of digital forensics in investigating cybercrimes

Digital forensics plays a crucial role in investigating cybercrimes by providing valuable insights into the nature of the crime, identifying perpetrators, collecting evidence, and supporting legal proceedings. Here are some key points highlighting the importance of digital forensics in investigating cybercrimes (Smith, 2019):

1. Evidence Collection: Digital forensics enables the collection and preservation of digital evidence from various sources such as computers, mobile devices, networks, and cloud storage. This evidence can include log files, emails, chat conversations, deleted files, and system artifacts. By employing specialized tools and techniques, digital forensic investigators can

extract and analyze this evidence, which is vital for identifying the methods and motives of cybercriminals.

2. Attribution: Digital forensics aids in attributing cybercrimes to specific individuals, groups, or organizations. By analyzing digital evidence, investigators can trace the origin of an attack, track the activities of the perpetrators, and uncover their identities. This attribution is critical for holding cybercriminals accountable and deterring future attacks.

3. Incident Response: Digital forensics is an integral part of incident response efforts. When a cybercrime occurs, such as a data breach or network intrusion, digital forensic techniques help identify the point of entry, the actions taken by the attacker, and the extent of the compromise. This information guides the response team in containing the incident, mitigating the damage, and implementing measures to prevent similar incidents in the future.

4. Legal Proceedings: Digital forensic evidence is admissible in legal proceedings, providing solid proof of cybercrimes. It supports law enforcement agencies, prosecutors, and legal professionals in building a strong case against cybercriminals. Digital evidence, backed by forensic analysis, can establish a clear chain of custody, demonstrate intent, and prove the actions taken by the perpetrator, enhancing the chances of successful prosecution.

5. Prevention and Future Protection: Digital forensics not only investigates cybercrimes but also contributes to preventing future incidents. By analyzing the methods and vulnerabilities exploited by cybercriminals, forensic experts provide valuable insights to organizations and cybersecurity professionals. This knowledge helps in strengthening security measures, implementing effective controls, and developing proactive strategies to mitigate future threats.

4.4. Social media forensics

The development of Web 2.0 and Industry 4.0 technologies has greatly boosted social media platform acceptance, making it a main source of social interaction. Through these websites, users voluntarily exchange their information, set up accounts, and participate in social activities. As a result, hackers are presented with numerous chances to abuse user accounts (Wazid et al., 2013).

In addition, different social media applications like LinkedIn, Instagram, Facebook, and Twitter have been exposed to multiple cyber threats and malware. Attacks on social media platforms can take place outside the system/network or within the network. Outside systems attack usually include DDoS, or DoS, while attacks within the network include retrieving cookies data (Sharma et al., 2019).

Furthermore, it is known that these social media programs' databases are most susceptible to such attacks. Due to this circumstance, digital investigators are now more interested in social media forensics. Investigators can use social media posts as excellent evidence in criminal investigations because to social media forensics (See Figure 1). Social media networks, which are the best for profiling, are also an ideal source of information about possible offenders, suspects, and witnesses (Rocha, 2016).

In addition, by combining social media with digital forensics, investigators can gain access to a modern and diverse subset of sources of data, including demographic location, photographs, contact lists, geo-location, and text messages. This network data, combined with the metadata, has the potential to assist digital forensics investigations. Furthermore, the metadata can also be used to authenticate online social networking facts. Thus, it can be contended that social media forensics is a rising trend in the digital forensics' domain due to its ability to efficiently providing adequate digital evidence. The advent of social media apps on a mass of platforms has enabled these networking domains to leave digital forensic trace or artifacts that can be of a valuable asset in an investigation. For instance, research like discovered that the chat logs could be extracted from social media applications like Facebook and a huge amount of digital forensic artifacts, such as pictures, location data, friends, posts, passwords, and usernames are left behind as potential evidence. These artifacts are essential evidence, which makes social media forensics as one of the most prominent digital forensic trends (Baggili & Breitinger, 2015).

Studies like these forensically analyzed social media apps on Android, iPhone, and Blackberry devices, including MySpace, Twitter, and Facebook. According to the study, it was successful to recover digital forensic artifacts such user data in text format, timestamps, passwords, URLs, and written comments. This shows that social media forensics is a highly effective method for assessing, verifying, and obtaining digital evidence. It is also a potent tool for tracking down digital evidence dispersed over social media (Al Mutawa, 2012).

Additionally, the three functionalities that social media forensics offer are reverse search integration, tempering localization analysis, and metadata visualization and extraction (Zampoglou et al., 2016).

The first advantage of Google Image Search is that it opens a new tab in your web browser to see the results. Second, it has six separate tampering localization maps designed to locate various signs of social media manipulation. These maps were produced utilizing forensic algorithms. Thirdly, it fully supports metadata listing and shows any potential embedded thumbnails. Professional forensic investigators can go deeper into the data and retrieve pertinent evidence thanks to these characteristics. As a result, the area of digital forensics is seeing a rise in the use of social media forensics.

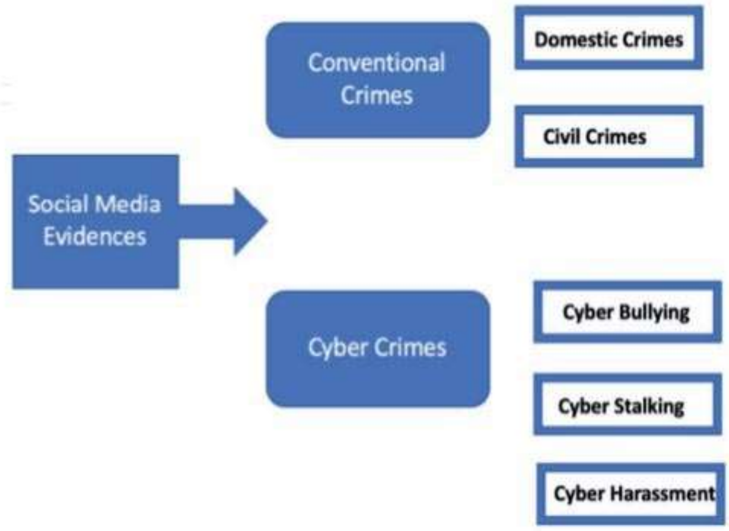

Figure 1

5. Case Studies

Russian Interference in the 2016 US Presidential Election[1]

The investigation into Russian interference in the 2016 US Presidential Election involved extensive digital forensics analysis. The investigation, headed by Special Counsel Robert S. Mueller III, aimed to uncover and document attempts by Russian entities to influence the election through social media manipulation and cyberattacks.

Digital forensic investigators utilized various techniques to identify and analyze online activities related to the Russian interference campaign. They collected and analyzed vast amounts of digital evidence, including social media posts, advertisements, email communications, and internet traffic data.

[1] United States Department of Justice (https://www.justice.gov/sco)

Through the examination of metadata, user profiles, and network connections, investigators traced the origin of deceptive social media campaigns and identified the individuals and organizations responsible for orchestrating the interference. Sophisticated forensic tools were employed to link the digital activities to specific Russian entities and track the dissemination of misinformation and propaganda.

The digital forensic investigation provided critical evidence of Russian involvement in the election interference. The findings were documented in the Mueller Report, which served as a foundation for legal and policy actions to safeguard future elections and protect against foreign influence campaigns.

Methodologies (Mueller, 2019):

1. Social Media Analytics: Investigators utilized social media analytics techniques to analyze large volumes of social media posts, advertisements, and user interactions. This involved mining data from various social media platforms and employing natural language processing and sentiment analysis to identify patterns and trends in the content shared by Russian entities.

2. Metadata Analysis: Digital forensic investigators examined metadata associated with emails, social media posts, and other digital artifacts to establish the origins, timestamps, and user identities. Metadata analysis helps in corroborating the authenticity and integrity of digital evidence.

3. Network Traffic Monitoring: Investigators monitored network traffic, including internet traffic from suspicious IP addresses and connections, to identify patterns and trace the origins of cyberattacks and intrusion attempts. Network traffic monitoring helps in understanding the techniques and infrastructure used by threat actors.

Tools:

1. Social Media Monitoring Tools: Investigators utilized specialized tools for social media monitoring and analytics, such as sentiment analysis platforms, social media listening tools, and content analysis software. These tools helped in identifying coordinated campaigns, tracking influential posts, and analyzing the reach and impact of social media content.

2. Email Forensic Tools: Investigators employed email forensic tools to analyze email headers, extract metadata, and trace the path of emails. These tools assisted in identifying suspicious

email communications and linking them to specific individuals or organizations involved in the interference campaign.

3. Network Analysis Tools: Investigators utilized network analysis tools to monitor and analyze network traffic, identify suspicious connections, and track the flow of information between various entities. These tools helped in tracing the origin of cyberattacks and mapping the infrastructure used by threat actors.

In both case studies, a combination of specialized methodologies and tools was employed to gather digital evidence, analyze data, and establish links between individuals, activities, and criminal operations. These methodologies and tools played a crucial role in the successful digital forensic investigations of social media and cybersecurity incidents

7. Conclusion

In conclusion, digital forensic investigation tools play a vital role in cases related to social media and cybersecurity incidents. These tools enable investigators to collect, analyze, and interpret digital evidence, helping uncover the truth, identify perpetrators, and support legal actions .

For social media investigations, specialized tools for social media analytics and monitoring are crucial. These tools assist in mining large volumes of social media data, detecting patterns, and identifying coordinated campaigns or malicious activities. Social media monitoring tools enable investigators to track user interactions, sentiment analysis, and content dissemination, providing insights into the motives and tactics of individuals or groups involved in social media-based crimes.

In cybersecurity investigations, digital forensic tools are essential for analyzing network traffic, identifying malicious activities, and tracing the origins of cyberattacks. Network analysis tools help investigators understand the techniques used by threat actors, map their infrastructure, and identify vulnerabilities exploited for illegal activities. Additionally, email forensic tools and metadata analysis play a significant role in tracing the origins of communications, verifying authenticity, and establishing the chain of custody for digital evidence.

Blockchain analysis tools are crucial when investigating cases involving cryptocurrencies, such as money laundering or illegal marketplaces. These tools help trace transactions, analyze blockchain data, and identify the flow of funds, assisting in linking financial activities to individuals or organizations involved in illicit operations.

Collaboration between law enforcement agencies, cybersecurity experts, and social media platforms is essential in leveraging these tools effectively. Sharing expertise, accessing specialized intelligence platforms, and collaborating with platform administrators enhances the investigation process and strengthens the evidence collected.

It is important to note that the field of digital forensics is constantly evolving, and new tools and techniques continue to emerge. Investigators must stay updated with the latest advancements and adapt their methodologies and tools accordingly to effectively tackle the ever-changing landscape of social media and cybersecurity incidents.

In conclusion, the successful utilization of digital forensic investigation tools is crucial in social media and cybersecurity cases. These tools enable investigators to navigate complex digital environments, collect evidence, and uncover the truth, ultimately contributing to the prevention and prosecution of social media-related crimes and cybersecurity incidents.

8. Results:

The study on digital forensic investigation tools for cases related to social media and cybersecurity has yielded several key results:

1. Specialized tools for social media analytics and monitoring play a crucial role in mining and analyzing large volumes of social media data, identifying patterns, and detecting coordinated campaigns or malicious activities.

2. Network analysis tools are essential in cybersecurity investigations, enabling investigators to analyze network traffic, trace the origins of cyberattacks, and map the infrastructure used by threat actors.

3. Blockchain analysis tools are valuable in cases involving cryptocurrencies, assisting in tracing transactions, analyzing blockchain data, and linking financial activities to individuals or organizations involved in illicit operations.

4. Social media plays an important role in influencing public opinion and raising social problems, which requires the presence of official or reliable bodies specialized in analyzing cyber behavior on these platforms.

9. Recommendations:

Based on the study's findings, the following recommendations are proposed:

- Investing in continuous research and development of new tools and techniques in digital forensics.

- Enabling professionals and investigators to access the most advanced and effective tools for social media and cybersecurity investigations.

- Train and develop the skills of cybersecurity professionals, enhance their investigative capabilities, and improve the overall effectiveness of social media and cybersecurity investigations.

- Strengthening mechanisms for cooperation and information exchange, enhancing the investigation process and improving the outcomes of social media and cybersecurity cases

- Educating the public about the risks associated with social media and cybersecurity incidents and providing guidance on safe online practices

10. References:

1. E. A. Gollub, (2013). “Recent trends in digital text forensics and its evaluation,” In International Conference of the Cross Language Evaluation Forum for European Languages, pp. 282-302, September.
2. A. Aminnezhad and A. Dehghantanha, (2014). “A survey on privacy issues in digital forensics,” nternational Journal of Cyber-Security and Digital Forensics (IJCSDF), vol. 3, no. 4, pp. 183-199.
3. F. Dezfouli and A. Dehghantanha, (2014). “Digital forensics trends and future,” International Journal of Cyber-Security and Digital Forensics (IJCSDF), vol. 3, no. 4, pp. 183-199.
4. B. K. Sharma, M. A. Joseph, B. Jacob and L. C. B. Miranda, (2019). “Emerging trends in Digital Forensic and Cyber security-An Overview,” In 2019 Sixth HCT Information Technology Trends (ITT), pp. 309-313, November.
5. M. Wazid, A. Katal, R. H. Goudar and S. Rao, (2013). “Hacktivism trends, digital forensic tools and challenges: A survey,” n 2013 IEEE Conference on Information & Communication Technologies, pp. 138- 144, April.
6. Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic Press.

7. Rogers, M. K., Goldman, J., & Mislan, R. (2017). Investigating digital crime. Academic Press
8. Nelson, B., Phillips, A., & Steuart, C. (2018). Guide to computer forensics and investigations. Cengage Learning.
9. SANS Institute. (n.d.). Computer Forensics, Investigation Techniques, and Incident Response. Retrieved from https://www.sans.org/reading-room/whitepapers/incident/computer-forensics-investigation-techniques-incident-response-86
10. Smith, R. (2019). The Importance of Digital Forensics in Investigating Cybercrimes. International Journal of Cybersecurity and Digital Forensics, 8(2), 45-58.
11. M. Wazid, A. Katal, R. H. Goudar and S. Rao, (2013). “Hacktivism trends, digital forensic tools and challenges: A survey,” n 2013 IEEE Conference on Information & Communication Technologies, pp. 138- 144, April.
12. A. E. A. Rocha, (2016). “Authorship attribution for social media forensics,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 1, pp. 5-33.
13. I. Baggili and F. Breitinger, (2015). “Data sources for advancing cyber forensics: what the social world has to offer.,” n 2015 AAAI Spring Symposium Series., March
14. N. Al Mutawa, I. Baggili and A. Marrington, (2012). “Forensic analysis of social networking applications on mobile devices,” Digital Investigation, vol. 9, pp. S24-S33.
15. M. Zampoglou, S. Papadopoulos, Y. Kompatsiaris, R. Bouwmeester and J. Spangenberg, (2016). “Web and social media image forensics for news professionals.,” In Tenth international AAAI conference on web and social media, April
16. United States Department of Justice (https://www.justice.gov/sco)
17. Mueller, R. S., III. (2019). Report on the investigation into Russian interference in the 2016 presidential election. United States Department of Justice. Retrieved from
18. Casey, E. (2018). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press
19. Marrington, A., & Clark, D. (2019). Digital forensics: Challenges and future research directions. Digital Investigation, 29, S88-S96

Doi: https://doi.org/10.52132/Ajrsp.e.2023.55.1