Review Paper

FORENSIC ANALYSIS OF SOCIAL MEDIA FROM OPEN-SOURCE INTELLIGENCE (OSINT)

Dhananjay Kumar[1], Amit Yadav[2], Vinny Sharma[*]

ABSTRACT

The function of social media investigation in the field of forensic science is covered in the study. A social media investigation involves searching, analysing, and compiling a person's publicly available data on social media sites such as Facebook, LinkedIn, Instagram, Snap chat, and Twitter. A range of methods and instruments are used in social media inquiry to examine data from social networks. Strategic interests and national security are among the many areas where social media has presented a serious threat. Cybercriminals now use social media as a platform to carry out their illicit actions. Cybercriminals use computers and the internet to look for victims and steal identities. A forensic process that respects people's right to privacy and conforms to legal and scientific standards must be used to collect social media evidence.

The main subjects of this review research will be the dangers and vulnerabilities in social media accounts as well as the state of evidence gathering, admissibility, and jurisdiction processes in social media forensics. It also draws attention to the actual challenges that law enforcement has in gathering, analysing, presenting, and confirming evidence from social media data.

Keywords: *Cyber Crime, Digital Forensic, Forensic, Social Media Investigation*

Authors' Affiliations:

[1] *M.Sc. Forensic Science, School of Forensic Sciences, Galgotias University, Greater Noida, Uttar Pradesh, India.*

[2]*Assistant Professor, Department of Forensic Science, T.S. Misra College of Allied and Healthcare Sciences, T.S. Mishra University, Lucknow, Uttar Pradesh, India*

[*]*Professor, School of Forensic Science, Galgotias University, Greater Noida, Uttar Pradesh, India*

Corresponding Author:

Vinny Sharma

Professor, School of Forensic Science, Galgotias University, Greater Noida, Uttar Pradesh, India

Email:

vinnysharma4n6@gmail.com

Date of Manuscript Submission	01st Review
26-12-2025	30-12-2025
02nd Review	**03rd Review**
03-01-2026	09-01-2026
Date of Acceptance	**Plagiarism (Turnitin)**
10-01-2026	5%
Conflict of Interest	**Funding**
Nil	Nil
Ethical Approval	**Paper ID**
Nil	IJFSC/DIA/01-01/003

How to cite this article
Kumar, D., et. Al, Forensic Analysis of Social Media from Open-Source Intelligence (OSINT). International Journal of Forensic Science and Criminology (IJFSC) 2026; Volume 01, Issue 01, Jan-Jun 2026

INTRODUCTION:

"Digital forensics" refers to the field of study that investigates crimes at the level of digital devices. Digital forensics' primary goal is to find, retrieve, and examine evidence from digital media in order to prepare it for the prosecution's use in court [1]. Finding and gathering evidence from the resources is crucial to the investigation of any cybercrime. The term "digital evidence" refers to any important data that is necessary to prove a crime. This data is kept and communicated digitally, and it can be utilized and accepted in court [3].

The primary areas of digital forensics are to gather data from electronic evidence, convert it into valuable evidence, and submit the verdicts for prosecution [4]. Every method uses reliable forensic methods to safeguard that the outcomes are accepted in court [5,6]. The several forms of digital forensics, including disk, network, memory, mobile, database, cloud, malware, and email forensics, are used to achieve this objective [7, 8].

Social media refers to the digital platforms and apps that facilitate "social" user networking and engagement through information sharing. The capacity to "like" and comment on postings, which fosters a two-way conversation, is an essential component of social media. A wealth of information regarding relationships and human behaviour may be found on social media sites [9,10]. Numerous studies examine this data to look at psychological patterns, business trends, and other things. Even the signs of illnesses like depression might be found using the data. Numerous research benefit from the substantial quality and variety of information found on these internet sites [11]. As a result, material found on social media sites provides insight into several facets of a legal process. Publicly available social media posts are used as tangible evidence that someone has committed a crime. Theft and homicide cases have already used social media posts as direct evidence [12, 13].

LITERATURE REVIEW:

Social Media Platforms:

1. **Facebook:** In terms of overall users and brand awareness, Facebook is the largest social media platform on the Internet. It was established on February 4th, 2004. There are 1.87 billion active Facebook users globally. Facebook is outperforming YouTube by a significant margin. 68% of users spend time on Facebook on a mobile device [14].
2. **Twitter:** There are almost 500 million users of Twitter globally. It has evolved into a platform for disseminating news, discussing concepts, and offering commentary on global events. Given the number of news, views, and information posted by both people and government sources, Twitter is an important source of health-related data [15].
3. **LinkedIn:** LinkedIn is a professional networking platform that helps users establish and grow a network of co-workers and other business associates. Owners, entrepreneurs, and business professionals may connect with one another through this network and look for relationships based on region or specialty. Through a network of reliable contacts, members may search for employment, find specialists in a certain field, or connect with other professionals [16].
4. **Telegram:** Users may communicate both individually and in groups by sharing textual and non-textual messages and

audio discussions in a number of secure methods [17].

5. **Instagram:** Instagram is presently one of the most widely used photo-sharing applications, and users may send photographs to the system in real time [18]. Instagram's popularity stems from the hashtags and symbols that are used to characterize images and videos in order to communicate with users one-on-one before sharing them. In order to improve photo sharing communication through social engagement, the program also allows users to like, comment, follow, and tag material on a chronological timeline [19].

Threats In Social Networks:

1. **Identity Theft:** This kind of crime is committed by someone who uses social media to collect the victim's personal information. Identity theft is the crime of stealing someone else's financial or personal information in order to use that person's identity to commit fraud, such as making illegal purchases or transactions. Identity theft can take many different forms, and victims typically experience damage to their credit, fortune, and reputation [20].
2. **Cyber-Stalking:** a crime where a mugger uses electronic communication, including email, instant chatting, or messages made on a website or consultation group, to harass a victim. The facelessness provided by the Internet enables a cyber-stalker to pursue their target without being discovered. Cyber stalking is the practice of harassing or threatening someone over the Internet, email, or other electronic communication means [21].
3. **Carding:** This type of credit card fraud involves charging pre-paid cards with a stolen credit card. Carding usually entails the owner of the stolen card purchasing gift cards with the store's name, which may then be sold to other people or used to purchase other items that can be sold for cash. Carders are credit card thieves who participate in this kind of fraud. It is very helpful for locating rootkits and active cyber threats. [22].
4. **Bot Networks:** is a group of compromised computers that are frequently called "zombies" because they are infected with a virus that gives muggers power over them. [23].
5. **Cyber Terrorism:** Cyber terrorism is the deliberate use of computers, computer networks, and public internet infrastructure to undermine a nation's personal goals and create public ruin. Depending on the type of terrorism and the motivation of a terrorist organization, the goals behind the spread of these types of terrorist activities through the use of information infrastructure and interconnected communication channels like the World Wide Web (WWW) may stem from political or ideological convictions [24].
6. **Defamation:** A person's reputation might be harmed by the posting of inaccurate or incorrect information about them online. The Indian judiciary offers victims legal recourse since defamation is both a civil and criminal offense [25].
7. **Fake Online Friendship:** establishing online friendships through social media with people you don't know in real life and utilizing the emotional connection to deceive you into sending money

under false pretences like a medical emergency, legal issues, difficulties abroad, etc.

8. **Sextortion:** This type of online abuse occurs when a cybercriminal uses a variety of platforms, including social media, online dating apps, SMS, instant messaging applications, and porn websites, to entice individuals into private video or audio conversations where they are forced to appear naked or provide explicit photos. Later on, the fraudsters utilize this information to harass, humiliate, threaten, take advantage of, and blackmail the victims. A combination of "sexual" and "sextortion," extortion is the act of threatening to release private, sexual content unless the victim agrees with certain requests. Cyber sextortion is a subgroup of a wider range of image-based sexual offense that involve the exploitation of photographs for malicious purposes [26].
9. **Phishing:** It is like any website that purports to operate on behalf of a third party without authorization to trick visitors into doing something they would only trust a legitimate third-party agent to do. Direct messages, emails, articles, and organic postings may include these malicious links. Clicking on these might lead to websites that need you to enter into your account or infect your device with malware [27].
10. **Cyberbullying:** Cyberbullying is the use of digital equipment such as computer, tablet, & mobile phone to bully someone. Cyberbullying may happen online via SMS, text, and programs, as well as through social media, forums, or games where users can read, engage, or share content. Cyberbullying is the act of sending, posting, or sharing nasty, damaging, or misleading information about another individual. It might entail revealing personal or sensitive information about another person, which could cause humiliation or shame [28].

Social Media Evidence and its Investigations:

1. Role of Social Media Evidence:
    - A person's mental condition is evaluated through recorded conversations.
    - Daily internet activity logs prove presence or absence at a certain location or time.
    - Cybercrimes such as cyberbullying, cyber harassment, or cyber predating can be detected through online conduct.
    - Online personas provide proof of identity theft and impersonation.
    - Potential suspects and witnesses' backgrounds are checked on social media
2. Social Media Investigation:

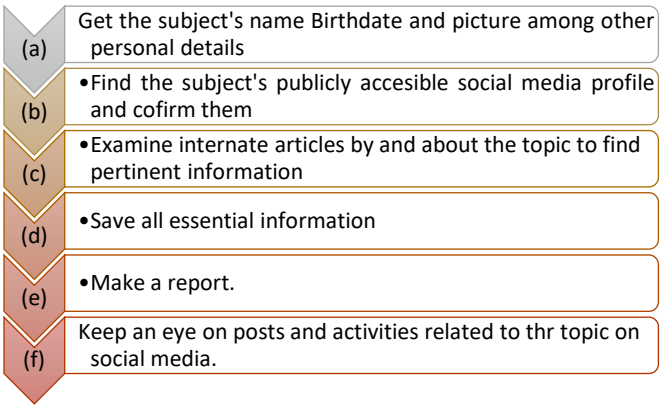

Figure 1: Steps for social media investigation

The Challenges of Performing Social Media Investigations:

1. **Lack of Experience:** For social media investigations, many businesses engage internal investigators and employees. While other company personnel might not have expertise examining and analysing web data, digital investigators usually do. A company may find it challenging to obtain the necessary results without spending a lot of money due to this lack of knowledge, particularly if the research team does not have investigative tools that may expedite the procedure [30].
2. **Identification Issues:** Appropriate topic data and social media account identification are essential for social media investigations. Without both, an investigative team may have to spend hours looking for and gathering evidence regarding the wrong individual or taking into account a time period that is not relevant. In addition to wasting time and money, this might lead to poor decision-making or a negative outcome in court [30].
3. **Platform Variation:** Social media platforms differ greatly from one another, despite the fact that there are hundreds of social media channels. These variations include layout, the style of postings, and interactive features. For internal teams looking to find, evaluate, and extract important information, each of these variants may offer a fresh learning curve [30].
4. **Data Complexity:** There are many various kinds of data on social media, including data that has to be extracted. Multimedia assets, such links, images, videos, and gifs, are examples of embedded files that are present on a webpage. Metadata, or data that comprises information on other data, such as images, documents, and videos, is also included in social media. In addition to being discoverable and admissible in court, metadata may reveal a variety of information about a file, including who owns it and the time and location of a photo or video. To handle particular types of data and provide access to the information they contain, even a seasoned social media investigator needs specialist technology [30].

Open-Source Intelligence Gathering Tool (OSINT):

It describes the information that may be obtained from legally and publicly accessible sources [31]. OSINT is intelligence generated by gathering, assessing, and analyzing material that is accessible to the public in order to address a particular intelligence query. Information that is available from a variety of sources, including:

- Public Records
- News media
- Libraries
- Social media platforms
- Images and Videos
- Websites

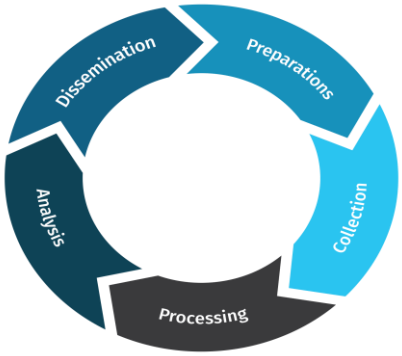

Figure 2: Stages of the Intelligence Cycle [31]

1. Preparation is the process of evaluating the needs and requirements of the request, including figuring out the task's objectives and the best sources to employ to locate the information you're searching for.
2. The first and most crucial stage in gathering data and information from as many pertinent sources as possible is collection.
3. The organization or collation of the gathered data and information is known as processing.
4. The interpretation of the data gathered to make sense of it, such as finding trends or creating a travel history timeline, is called analysis and production.
5. The presentation and transmission of open-source results, such as written reports, timelines, suggestions, etc., is known as dissemination. Respond to the stakeholders' intelligence query.

How Law Enforcement Is Using Social Media Investigation:

1. **Identifying Persons of Interest:** If the information is made public and there are no legal restrictions on accessing or keeping an eye on such a social media presence, law enforcement can actively monitor such accounts. Law enforcement investigators can discover acquaintances linked to people of interest (POIs) in adding to locating postings, Tweet, photos, or supplementary supporting evidence. This may be extremely beneficial in tracing down and dismantling organized criminal networks, such as drug traffickers and prostitution rings, which routinely promote their unlawful operations on social media sites.
2. **Determining the Position of Criminal Motion:** Social media has utilized location-based resources that are integrated into the website itself as a result of the growing popularity of global positioning systems (GPS) technology and its accessibility on mobile devices like Android and iPhones. Users may tag location-based content on a number of social media sites using geolocation. Finding patterns in criminal activities may also benefit from the use of geolocation data.
3. **Collecting Corroborated Evidence:** Corroborated evidence, sometimes known as "fruits of the crime" by legal professionals, can be vital in establishing the legitimacy of a criminal case. Social media status keep posted & images may sometimes disclose an offender's mentality and/or help hunt down a suspicious in connection with a certain crime. There are several approaches and strategies for doing this. As an example, photos can identify a suspect in a location at a specific moment in time. Images uploaded to social media platforms can also establish the existence of a fact or connect suspects to victims.
4. **Identifying Criminal conduct:** Social media is regularly used by law enforcement to find and punish illegal activity that may occur on websites such as Facebook. Instagram, Telegram, and Twitter, despite the fact that this is a wide generalization [33].

DISCUSSION:

In this review paper we have discussed about the social media investigations using open sources. It's critical to safeguard social media users against cyber-attacks and provide forensic analysis tools to find and identify offenders. To find fraudulent users on social media sites, forensic analysts may employ authorship analysis, profile matching, and user classification techniques. We are discussed about the collection and examination process of data from social media platforms and social media investigation is useful in the court of law. We are recommended some suggestions which are very helpful to protect us from all social media crimes which are done by our mistakes. In order to gather information on the culprits, social media detectives may examine traces of open-source data.

Some suggestion to the social media users to secure your account:

- Refusing to reveal needless personal data
- Managing security and privacy settings correctly
- Turning down connections from random people
- Eliminate pointless or useless friendships.
- Setting up applications for online security
- Removing third-party programs
- Reporting malicious users

CONCLUSION:

In the current situation social media crimes are increasing and the victims still don't know the reason behind the crimes. In this review paper we are discussed about the social media users and their awareness towards cybercrimes. The data has a bright future in terms of improving intelligence analysis and criminal efficacy and efficiency. There is still a great deal of awareness needed to eradicate online crime. Because it gives us insight into how we can collect data about criminality on the system. Fraudulent transactions, hacking, cyber stalking, defamation, and more. The conviction rate for these offenses is quite low, and India has effective legislation to deal with them. The area of cyber forensics is growing. It is necessary to promote the search for cyber proof. Indian laws must also be changed to comply with the IT Act in order to deter cybercrimes.

Acknowledgement:
The authors have made no acknowledgement in this article.
Conflict of Interest:
The authors declare that there is no commercial or financial links that could be construed as conflict of interests.
Source of Funding:
The author declares that there is no funding for this project.

REFERENCES:

1. L. Daniel, Digital forensics for legal professionals: understanding digital evidence from the warrant to the courtroom. Elsevier, 2011.
2. C. Hargreaves and J. Patterson, —An automated timeline reconstruction approach for digital forensic investigations, ‖ Digital Investigation, vol. 9, pp. S69–S79, 2012.
3. "USLegal-Definitions,‖http://definitions.uslegal.com/d/digitalevidence, 2019"
4. N. T. A. Recipes-A, J. McCaffrey, V. T. Patch, S. Manzuik, P. Chandra, M. Messier, J. Viega, O. D. Wiley, P. Elst, Y. T. Apress et al., —of the book author publisher

5. H. Dreger, A. Feldmann, M. Mai, V. Paxson, and R. Sommer, —Dynamic application-layer protocol analysis for network intrusion detection,‖ in 15th USENIX security symposium. USENIX Association, 2006, pp. 257–272.
6. G. Maier, R. Sommer, H. Dreger, A. Feldmann, V. Paxson, and F. Schneider, —Enriching network security analysis with time travel,‖ in ACM SIGCOMM Computer Communication Review, vol. 38, no. 4. ACM, 2008, pp. 183–194
7. Aljaedi A, Lindskog D, Zavarsky P, Ruhl R, Almari F. Comparative Analysis of Volatile Memory Forensics: Live Response vs. Memory Imaging. Proceedings of 3rd IEEE International Conference on Privacy, Security, Risk and Trust. 2011.p. 1253–8
8. M. Petraityte, A. Dehghantanha, and G. Epiphaniou, —Mobile phone forensics: an investigative framework based on user impulsivity and secure collaboration errors,‖ in Contemporary Digital Forensic Investigations of Cloud and Mobile Applications. Elsevier, 2017, pp. 79–89.
9. Akter, O., Akther, A., Uddin, M. A., & Islam, M. M. (2020). Cloud forensics: Challenges and blockchain based solutions. International Journal of Wireless and Microwave Technologies, 10(5), 1-12.
10. M. Harbawi and A. Varol, "An improved digital evidence acquisition model for the internet of things forensic i: A theoretical framework," in 2017 5th International Symposium on Digital Forensic and Security (ISDFS). IEEE, 2017, pp. 1–6
11. S. Simou, C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Cloud forensics: identifying the major issues and challenges," in International conference on advanced information systems engineering. Springer, 2014, pp. 271– 284.
12. Devendran, V.K., Shahriar, H. and Clincy, V., "A Comparative Study of Email Forensic Tools", Journal of Information Security, 6, pp- 111-117, 2015.
13. Umar, R., Riadi, I., & Muthohirin, B. F. (2019). Live forensics of tools on android devices for email forensics. TELKOMNIKA (Telecommunication Computing Electronics and Control), 17(4), 1803-1809.
14. Quan-Haase, A., Young, A.L., 2010. Uses and gratifications of social media: a comparison of facebook and instant messaging. Bull. Sci. Technol. Soc. 30 (5),350–361. http://dx.doi.org/10.1177/0270467610380009.
15. Garcia, K., & Berton, L. (2021). Topic detection and sentiment analysis in Twitter content related to COVID-19 from Brazil and the USA. Applied soft computing, 101, 107057.
16. Ali H. Al-Badi, Michelle, O. Okam, Roobaea Al Roobaea and Pam J. Mayhew (2013), Journal of Internet Social Networking & Virtual Communities, DOI: 10.5171/2013.889433
17. Anglano, C., Canonico, M., & Guazzone, M. (2017). Forensic analysis of telegram messenger on android smartphones. Digital Investigation, 23, 31-49.
18. Silva, T.H., de Melo, P.O., Almeida, J.M., Salles, J., Loureiro, A., 2013. A picture of Instagram is worth more than a thousand words: workload characterization and application. In: Paper Presented at the Distributed

Computing in Sensor Systems (DCOSS), 2013.

19. McNely, B.J., 2012. Shaping organizational image-power through images: Case histories of Instagram. In: Paper Presented at the Professional Communication Conference (IPCC), 2012 IEEE International
20. Diganth Raj Sehgal, All You Need to Know About Identity Theft in Cyberspace in India, I PLEADERS (Sep. 2019), https://blog.ipleaders.in/all-you-need-to-know-about-identity-theft-in-cyberspace-in-india/
21. Cyberstalking: A New Challenge for Law Enforcement and Industry: A Report From the Attorney General to the Vice President | Office of Justice Programs, n.d.
22. Ammar Yassir and Smitha Nayak, Cybercrime: A threat to Network Security [IJCSNS International Journal of Computer Science and Network Security], VOL.12 Issue No.2, February 2012.
23. ASSOCHAM-Mahindra SSG study on Cyber and Network Security Framework in 2015
24. Alex P. Schmidt, "Al-Qaeda's "Single Narrative" and Attempts to De .
25. Khan, N., Shaikh, A., & Singh, M. V. P. (2023). Understanding of cyber defamation and its impact: a critical analysis. Dogo Rangsang Res J, 13, 168-173.
26. O'Malley, R. L., & Holt, K. M. (2022). Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime. Journal of Interpersonal Violence, 37(1-2), 258-283.

https://doi.org/10.1177/088626052090 9186.

27. C. Whittaker, B. Ryner, and M. Nazif, "Large-scale automatic classification of phishing pages," in NDSS '10, 2010.]
28. Hinduja, S., & Patchin, J. W. (2012). Bullying and cyberbullying laws.
29. Van Der Hoeven, A. Historic urban landscapes on social media: The contributions of online narrative practices to urban heritage conservation. City Cult. Soc. 2019, 17, 61–68.
30. Wilson, K.; Desha, C. Engaging in design activism and communicating cultural significance through contemporary heritage storytelling A case study in Brisbane, Australia. J. Cult. Herit. Manag. Sustain. Dev. 2016, 6, 271–286.
31. Kaliyar, R. K., Goswami, A., & Narang, P. (2021). FakeBERT: Fake news detection in social media with a BERT-based deep learning approach. Multimedia tools and applications, 80(8), 11765-11788.
32. Michael W. McLaughlin, "Using open source intelligence software for cybersecurity intelligence," June 2012
33. An introduction to social media https://www.icaew.com/-media/corporate/files/technical/information- technology/technology/social-media.ashx