AG Publishing House

Investigative Frontiers Integration of Science Transforming Criminal Investigation

Year: 2026

Intelligence from the Open Web: OSINT and Forensic Investigation of Social Media

Ms. Amrica Mule[1]

[1]*Research Scholar Department of Forensic Science Medicaps University, Indore, Madhya Pradesh*

Abstract

Open Source Intelligence (OSINT) is a vital component in digital forensic investigations today as it allows investigators to gather and analyze information that is available in the public domain. Social media platforms have grown significantly, leaving behind huge digital traces that can be useful in cybercrime investigations, fraud detection, missing person investigations, terrorism monitoring and intelligence gathering. This review will discuss the basics of OSINT and Social Media Intelligence (SOCMINT), the major OSINT techniques used in forensic investigations, and how these techniques are used in the social media world. The paper also identifies some of the significant issues, such as protection of privacy, legal jurisdiction, authenticity of data and cross-platform investigations, especially the Indian perspective. Additionally, the authors explore new technologies that have the potential to enhance the efficiency, accuracy, and reliability of future OSINT-based forensic investigations, including artificial intelligence, machine learning, natural language processing and predictive analytics.

Keywords; Open Source Intelligence (OSINT); Social Media Forensics; Digital Forensics; Social Media Intelligence (SOCMINT); Digital Footprints

[1] ISBN No. - 978-93-7640-081-2

1 Introduction

The dynamic growth of the Internet, mobile technologies, and the Internet of Things (IOT) has created a new environment for criminal investigations that has led to the proliferation of publicly available digital information. This means that Open Source Intelligence (OSINT) is now a vital part of digital investigations and a method by which investigators can systematically gather, analyse, and interpret information found on the internet, including websites, search engines, news articles, public records, blogs, online forums and social media. Unlike classified intelligence, OSINT is based on information that is available and legal, which is a valuable tool for law enforcement, cybersecurity and digital forensic investigations and a cost effective way to do so. It has become much more than an identification tool because of its capacity to link suspects together, form relationships, recreate events and lead investigations.[2]

OSINT has become even more valuable with the proliferation of social media. Applications like Facebook, Instagram, X (previously Twitter), LinkedIn, TikTok and YouTube allow billions of people to post photos, videos, comments, location data, and social interactions every day. These activities create long-term digital trace, which reveals information about a person's actions, communications, connections and movements. In consequence, social media has become a rich source of digital evidence to help investigations related to cybercrime, fraud, missing persons, terrorist acts, and other crimes. It has been shown that social media data that is publicly available can offer useful context information to supplement traditional digital evidence and enhance forensic investigations.[3]

Social media is especially useful for digital forensics, as it holds a wealth of different digital artefacts that support investigators' ability to confirm identities, trace time lines, help to establish links between people and to corroborate evidence that can be found elsewhere on the internet. Combining OSINT practices with traditional forensic methods will enhance the thoroughness and accuracy of the digital investigation and maintain adherence to legal and ethical standards for evidence collection. Despite the privacy, authenticity and ever-evolving nature of online

[2] I. Abeysekera, “Open source tools: an evaluation for digital forensic investigations,” Front. Res. Metrics andAnalytics, pp. 1–8, 2026, doi: 10.3389/frma.2026.1790333.

[3] R. K. PANDEY and P. TRIPATHI, “The Role of Social Media in Criminal Investigation,” Int. J. LAW Manag. Humanit., vol. 9, no. 2, pp. 798–821, 2026, doi: https://doij.org/10.10000/IJLMH.1111561.

content issues, OSINT-based social media analysis is becoming a critical component of modern forensic investigations.[4]

2 Fundamentals of OSINT and Social Media Intelligence

The increasing dependence on digital technologies has created a vast array of publicly available information, making Open Source Intelligence (OSINT) a critical piece of the forensic puzzle for today's investigations. Investigators are increasingly turning to the information available online for intelligence gathering, identification, relationship building, and event reconstruction without having to breach private systems. Social Media Intelligence (SOCMINT) has also become a niche field that concentrates on extracting intelligence from social networking websites along with OSINT. It is crucial to be familiar with the basic concepts, sources, and differences between OSINT, SOCMINT, and digital forensics to carry out investigations successfully and legally.[5]

A. Definition and Principles of OSINT

Open Source Intelligence (OSINT) is the process of systematically gathering, processing, analyzing, disseminating intelligence information from publicly available and legally accessible information. The key concepts of OSINT are: Legality, Source Reliability, Information Validation, Ethical Data Collection, and Analytical Interpretation. OSINT doesn't use classified information, but uses information that's openly available, and then correlates and verifies it from several different independent sources to turn it into intelligence that can be used.[6]

B. Characteristics of Publicly Available Information

There are a number of features of publicly available information that make it useful in forensic investigations. It is available to everyone and is likely to be published by a variety of online and offline sources, updated regularly and can be readily checked. This could be personal profiles, news reports, government information, websites, discussion boards, or even anything that's been

[4] D. Tewu, D. Destine, and I. Gunawan, "Analysis of Social Media User Growth and Its Implications for Digital Marketing Strategies in Indonesia 2024," Int. J. Manag. Stud. Soc. Sci. Res., pp. 236–245, 2025, doi: https://doi.org/10.56293/IJMSSSR.2025.5623.

[5] A. Perez, "Open Source Intelligence: An Overview Of Today's Operational Challenges And Human Rights Affected As A Consequence," Rom. Intell. Stud. Rev., vol. 2023, Dec. 2023, doi: 10.66766/RISR.2023.2.01.

[6] D. Van Puyvelde and F. T. Rienzi, "The rise of open-source intelligence," Eur. J. Int. Secur., vol. 6, pp. 1–15, 2025, doi: 10.1017/eis.2024.61.

put out on the web. But it's important to consider the credibility, authenticity and timeliness of information before it can be used as evidential support.[7]

C. Types of Open-Source Data

OSINT leverages a variety of information sources, such as social media, websites, blogs, online discussion groups, public government records, geolocation data, satellite imagery, images, videos, and other forms of multimedia. When information is gathered from various sources, it will help investigators to build complete intelligence and verify investigative results by cross-referencing.

D. Importance of Digital Footprints

The term "digital footprint" refers to the traces of online activity that occur when people browse, use social media, share their location, make online purchases, or upload multimedia. The footprints are important forensic evidence for determining what people were doing, what time they were at a particular place, who was associated with what person or event and who was not. As a result, digital footprints have become one of the most important sources of intelligence during today's forensic investigations.[8]

Table 7: Difference between OSINT, SOCMINT, and Digital Forensics

Aspect	OSINT	SOCMINT	Digital Forensics
Primary focus	Publicly available information	Social media platforms	Digital evidence from electronic devices
Data sources	Websites, public records, news, blogs, forums	Facebook, X, Instagram, LinkedIn, YouTube, TikTok	Computers, smartphones, storage media, cloud services
Purpose	Intelligence gathering	Analysis of social media activities and interactions	Collection, preservation, examination, and presentation of digital evidence

[7] A. Yadav, A. Kumar, and V. Singh, Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security. Springer Netherlands, 2023. doi: https://doi.org/10.1007/s10462-023-10454-y.

[8] W. Lazarov, V. Moravec, P. Loutocky, and J. Vostoupal, “Comparative analysis of OSINT tools, techniques, and legal aspects,” Comput. Secur., vol. 168, p. 104938, 2026, doi: https://doi.org/10.1016/j.cose.2026.104938.

Nature of evidence	Open-source intelligence	Social media intelligence	Legally admissible digital evidence

3 OSINT Techniques and Digital Forensic Investigation Process

OSINT investigations have a structured approach to ensure that the information gathered from publicly available sources is accurate and consistent, and that it is legally admissible. OSINT is not a traditional intelligence collection process, but rather one that is systematic, legal, ethical, and documents data acquisition, analysis, preservation. Combined with digital forensic methods, these techniques allow investigators to piece together the events, make connections, and seek out suspects based on the information that's available to them in the public domain that can aid in a criminal investigation.[9]

- **Identification of Investigation Objectives:** The investigation process starts with setting clear goals for the investigation, such as identifying suspects, locating missing people, detecting fraud or reconstructing crimes. Clear goals define the range of data to be collected and help identify the information sources to be utilized and the data analysis methods to be applied.
- **Data Collection from Public Sources:** Information from social media sites, websites, blogs, discussion forums, search engines, public records and multimedia sharing sites is gathered as appropriate. Investigators use sophisticated search operators and specialized OSINT tools to collect available information from the public, and ensure that information is legally acquired and reproducible.
- **Profile Analysis:** The analysis of user profiles is a process of examination of publicly available user accounts to obtain personal information, social networks, behavior, shared content and online activity. By cross-referencing information on different platforms, identities can be verified, inconsistencies and fraudulent profiles identified.
- **Username and Email Correlation:** Usernames and email addresses can be used to track people in many online services. These identifiers can be correlated to identify corresponding accounts, to trace online activity, and to connect people with digital platforms.

[9] T. Babenko, K. Kolesnikova, and O. Abramkina, "Automated OSINT Techniques for Digital Asset Discovery and Cyber Risk Assessment," Computers, pp. 1–54, 2025, doi: https://doi.org/10.3390/computers14100430.

- **Metadata Extraction:** Metadata attached to digital photographs, video clips and documents can contain important context information such as timelapse, device specifications, file properties as well as where possible, geographic coordinates. This type of information helps investigators determine if digital evidence is authentic and where it came from.
- **Geolocation Analysis:** Geolocation analysis relies on location tags, location embedded in posts, image landmarks and publicly shared location information to ascertain where Activities have taken place. This data is used for suspect tracking, suspect movement analysis and crime scene reconstruction.
- **Timeline Reconstruction:** Information gathered from various public sources is organized in time sequence to show the chronological order of events. Using timeline analysis, investigators can correlate digital activities, determine the patterns of behavior, and determine a temporal relationship between the evidence and criminal events.
- **Preservation and Documentation of Digital Evidence:** Any information collected must be stored as it is found and documented in detail, with acquisition methods, time stamps, URLs of the source, screenshots and, if applicable, file hashes. Good documentation will increase transparency, repeatability and evidential integrity.
- **Chain of Custody in OSINT Investigations:** A chain of custody is established to help keep digital evidence in the investigation unchanged and unaltered. Proper documentation of evidence collection, handling, storage, and analysis creates accountability and aids in the admission of OSINT-derived evidence in legal proceedings.

4 Applications of OSINT in Social Media Forensic Investigations

Social media has become ubiquitous, and Open Source Intelligence (OSINT) has become an essential tool for forensic investigations. Social network information that is openly accessible can assist investigators in many ways to identify persons, discover behavioral patterns, reconstruct events, and aid in investigations. The integration of OSINT with digital forensic methods allows investigators to gain intelligence quickly, while minimizing investigative time and expense. Due to its versatility, OSINT has been utilized in various fields of law enforcement and cybersecurity.[10]

[10] G. P. Ramadhany, "Open-Source Intelligence (OSINT) Tools for Law Enforcement," ENDLESS Int. J. Futur. Stud., vol. 7, no. 3, pp. 21–33, 2024.

- **Cybercrime Investigations:** OSINT is a useful tool for investigating ransomware attacks, online harassment, cyberstalking, online markets, and phishing. Investigators review social media profiles, websites, forums, communications platforms, etc., to find out who may be involved in threats, who to look out for, and who may be connected to other cybercriminals and their operations.
- **Missing Person Investigations:** Social media websites may be able to help investigators find missing persons by offering recent photos, "check-ins" to the location, social interactions, and communications histories. In time-sensitive incidents, public posts and online associations can be used to determine an individual's last known activities, identify possible contacts and provide investigative leads.
- **Terrorism and Extremism Monitoring:** In recent years, many law enforcement agencies have started to use OSINT as a tool for tracking extremist content that can be accessed publicly, for spotting trends in radicalisation and for spotting online recruitment. Social media, multimedia and online communities provide investigators with analysis tools that allow them to determine potential threat, support counter-terrorism efforts and honour legal requirements.
- **Fraud and Identity Theft Investigations:** OSINT can be used to help with the detection of fraud and identity theft, financial frauds and social engineering attacks by correlating personal information that is publicly available with online profiles and transaction-based activities. By verifying digital identities across platforms, inconsistencies and fraud can be identified.
- **Misinformation and Fake Account Detection:** Social media's ability to rapidly spread misinformation and fake information has made OSINT more pertinent to the detection of fake accounts, coordinated misinformation campaigns and manipulated digital content. Different behaviors, posting patterns, network connections, and the authenticity of multimedia content are analyzed by investigators to determine whether a user is an actual person or an online impostor.
- **Law Enforcement and Intelligence Applications:** In addition to individual investigations, OSINT is used to help law enforcement and intelligence officials in crime prevention, suspect identification, threat assessment, event monitoring and situational awareness. The ability of investigators to combine information from several public sources to create actionable intelligence, provide forensics corroboration, and aid in decision-making during criminal investigations while maintaining legal and ethical standards.

5 Challenges, Ethical Issues, and Emerging Technologies

As the world increasingly adopted OSINT in forensic social media investigations, the ability of Indian law enforcement agencies to tackle cybercrime and digital offences has also improved. But the utility of OSINT comes with striking a balance between investigative efficiency and legal compliance, protection of privacy, and ethical responsibility. The digital landscape of India is growing quickly, with social media usage becoming common, and cyber incidents are on the rise, which can be both challenges and opportunities for investigators. Meanwhile, developments in AI and data analytics have made it possible to gather and analyse public data in new ways, opening up new opportunities in the digital investigation world.

A. Challenges

There are a number of operational and legal difficulties in conducting OSINT investigations in India. With the introduction of the Digital Personal Data Protection Act, 2023, the sharing of personal data has come under the microscope, with the need for responsible sharing and the protection of individual rights taking centre stage. The legal jurisdiction is still complicated as data on social media is stored in various countries, and international cooperation is required to acquire evidence. Investigators should also consider the authenticity of the data, as altered photos, deepfakes, and fake social media posts can affect the reliability of the evidence. Most of the time, evidence is lost to the web through the use of end-to-end encryption and the removal of online content. Furthermore, cross-platform investigations involve the need to gather information from many social networking platforms, and the fact that user generated data is voluminous means that information must be efficiently filtered and verified to find evidence.[11]

B. Emerging Technologies

New technologies are making OSINT investigations more efficient. Artificial Intelligence (AI) and Machine Learning (Machine Learning) help identify suspicious behaviour, fake accounts and criminal networks in vast datasets, automatically. Natural Language Processing (NLP) helps in sentiment analysis, multilingual text mining, and identifying online threats in the linguistically diverse social media landscape of India. Moreover, automated OSINT tools enable efficient and

[11] S. R. Shakya and E. Ceh-varela, "Social media analytics for investigations: A survey of recent trends, challenges and future research direction," J. Soc. Media Res., vol. 2, no. 4, pp. 297–318, 2025, doi: https://doi.org/10.29329/jsomer.57.

swift gathering, linking and visualizing of open-source data, and predictive analytics help investigators detect new cyber threats and anticipate crimes by analyzing trends in the data.[12]

C. Future Research

Future research aims to create frameworks for investigation with the help of artificial intelligence systems that are able to analyse the multilingual content of social media, while maintaining transparency and fairness. There is also a need to place more emphasis on cross-platform evidence integration to increase the evidence correlation of digital evidence gathered from various digital platforms. Additionally, developing uniform methodologies, evidence preservation protocols and legal rules that are compatible with the developing cybersecurity and data protection laws in India will improve the reliability, admissibility and utility of OSINT-driven forensic investigations.[13]

6 Conclusion

Open Source Intelligence has revolutionized digital forensic investigations by providing investigators with actionable intelligence derived from information that is publicly available and in compliance with the law and ethics. As the number of people using social media continues to rise, there are now extensive digital footprints that can help identify suspects, reconstruct events, verify online identities and gather valuable digital evidence. This review covered the basics of OSINT and SOCMINT, the systematic investigation process and the various roles of OSINT in cybercrime investigations, fraud investigations, missing persons investigations, terrorism monitoring and law enforcement. It also pointed to significant issues like privacy concerns, legal jurisdiction, authenticity of data, encrypted communications, and the processing of vast social media data, especially in India. Artificial Intelligence, Machine Learning, NLP and predictive analytics are emerging technologies that will substantially improve the capabilities of OSINT. Future research, standardized approaches and strong legal structures will be crucial to guarantee reliable, ethical and effective OSINT-based social media forensic investigations.

---

[12] N. Soni and K. Chauhan, "Social Media Forensics: Foundations, Technical Frameworks, and Emerging Challenges," Forensic Allied Sci., 2025, doi: https://doi.org/10.5281/zenodo.16811398.

[13] N. Soni and D. R. POONIA, "Enhancing Digital Forensics with AI-Driven OSINT: A Proactive Approach to Cybercrime Investigation," Res. Sq., pp. 1–14, 2025, doi: https://doi.org/10.21203/rs.3.rs-6581767/v1.

7 Reference

[1] I. Abeysekera, “Open source tools: an evaluation for digital forensic investigations,” Front. Res. Metrics andAnalytics, pp. 1–8, 2026, doi: 10.3389/frma.2026.1790333.

[2] R. K. PANDEY and P. TRIPATHI, “The Role of Social Media in Criminal Investigation,” Int. J. LAW Manag. Humanit., vol. 9, no. 2, pp. 798–821, 2026, doi: https://doij.org/10.10000/IJLMH.1111561.

[3] Tewu, D. Destine, and I. Gunawan, “Analysis of Social Media User Growth and Its Implications for Digital Marketing Strategies in Indonesia 2024,” Int. J. Manag. Stud. Soc. Sci. Res., pp. 236–245, 2025, doi: https://doi.org/10.56293/IJMSSSR.2025.5623.

[4] Perez, “Open Source Intelligence: An Overview Of Today’s Operational Challenges And Human Rights Affected As A Consequence,” Rom. Intell. Stud. Rev., vol. 2023, Dec. 2023, doi: 10.66766/RISR.2023.2.01.

[5] Van Puyvelde and F. T. Rienzi, “The rise of open-source intelligence,” Eur. J. Int. Secur., vol. 6, pp. 1–15, 2025, doi: 10.1017/eis.2024.61.

[6] Yadav, A. Kumar, and V. Singh, Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security. Springer Netherlands, 2023. doi: https://doi.org/10.1007/s10462-023-10454-y.

[7] W. Lazarov, V. Moravec, P. Loutocky, and J. Vostoupal, “Comparative analysis of OSINT tools, techniques, and legal aspects,” Comput. Secur., vol. 168, p. 104938, 2026, doi: https://doi.org/10.1016/j.cose.2026.104938.

[8] T. Babenko, K. Kolesnikova, and O. Abramkina, “Automated OSINT Techniques for Digital Asset Discovery and Cyber Risk Assessment,” Computers, pp. 1–54, 2025, doi: https://doi.org/10.3390/computers14100430.

[9] P. Ramadhany, “Open-Source Intelligence (OSINT) Tools for Law Enforcement,” ENDLESS Int. J. Futur. Stud., vol. 7, no. 3, pp. 21–33, 2024.

[10] S. R. Shakya and E. Ceh-varela, “Social media analytics for investigations: A survey of recent trends, challenges and future research direction,” J. Soc. Media Res., vol. 2, no. 4, pp. 297–318, 2025, doi: https://doi.org/10.29329/jsomer.57.

[11] N. Soni and K. Chauhan, “Social Media Forensics: Foundations, Technical Frameworks, and Emerging Challenges,” Forensic Allied Sci., 2025, doi: https://doi.org/10.5281/zenodo.16811398.

[12] N. Soni and D. R. POONIA, “Enhancing Digital Forensics with AI-Driven OSINT: A Proactive Approach to Cybercrime Investigation,” Res. Sq., pp. 1–14, 2025, doi: https://doi.org/10.21203/rs.3.rs-6581767/v1.