Multiple Case Study Validation of Online Social Networks Forensic Investigation Metamodel (OSNFIM)

Aliyu Musa Bade., Adamu Abdullahi Garba

Department of Computer Science, Yobe State University, Damaturu, Nigeria

DOI: https://doi.org/10.51244/IJRSI.2026.1306000337

Received: 22 June 2026; Accepted: 27 June 2026; Published: 10 July 2026

ABSTRACT

Digital Forensic Investigation is facing complex challenges due to the proliferation of the online social networks (OSNs). This necessitates the development of robust frameworks to guide the whole investigation process. In order to address these challenges, a structured and comprehensive framework; the Online Social Networks Forensic Investigation Metamodel (OSNFIM) was developed. Also, to evaluate the applicability, dependability, performance, and efficiency of OSNFIM across retrospective documented investigations cases, multiple case study validation technique was applied to examine three distinctive and documented cases in this study, based on the four phases of the OSNFIM; Preliminary, Acquisition/Preservation, Analysis, and Presentation. The validation process ensures that each conceptual element is addressed through each phase by following the OSNFIM framework. The validation has demonstrated the applicability of the OSNFIM framework to various OSN-related forensic investigations. By validating a metamodel that improves investigative precision in the landscape of OSNs, this research has contributed to the rising field of digital forensics.

Keyword: forensic investigation, online social networks, multiple case study, metamodel validation.

INTRODUCTION

Digital media plays a vigorous role in creating, processing, and sharing data which makes numerous organizations to extensively depend on it [1]. Incidents of cybercrimes and fraud are increasingly growing due to the rising use of digital platforms that generates significant challenges for law enforcement agencies in tackling these threats. The frequency of criminal activities related to OSNs continues to increase progressively due to the predominant acceptance and the availability of accessible application interfaces [2]. As such, Online Social Networks (OSNs) have become a main focus of forensic investigations.

Consequently, understanding and investigating crimes and attacks on these platforms is vital for averting illegitimate behavior, detecting malicious users, and supporting in criminal investigations. OSNs have presented new challenges for digital forensic investigations as they have become essential to modern communications. Therefore, ensuring the highest level of protection for OSN users is indispensable.

For conducting forensic investigations within OSNs, the Online Social Networks Forensic Investigation Metamodel (OSNFIM) was developed to provide a structured and comprehensive framework. The metamodel has theoretical value, however, its practical applicability across varied real-world documented investigations remains underexplored. Hence, this research proposes a multiple case study validation to evaluate the heftiness, adaptability, and efficiency of OSNFIM in diverse forensic contexts.

OBJECTIVE OF THE REVIEW

Model validation ensures precision, coherence, and compliance to language specifications and domain needs [3]. To ensure that any metamodel framework has fulfilled the requirements of generalization, adaptability, and extensiveness, validating the metamodel framework is crucial [4]. This process checks the metamodel's integrity and reliability, as highlighted by [5]. Validation aids to determine how well a conceptual model reflects real-world situations pertinent to its envisioned purpose or the conditions it aims to accomplish [6], [7],

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

and likewise authenticates that the fundamental values and assumptions of the metamodel are sound [8]. Furthermore, it confirms that the system is represented appropriately and practically for its designated purpose [9].

Three key techniques were used to validate the OSNFIM framework. These techniques are: comparison with existing models, frequency-based selection, and expert evaluation. To ensure the completeness through identifying gaps and aligning them with well-known standards, the comparison with existing models was utilized. Frequency-based selection highlights the significance of certain concepts and checks that the attributes utilized in creating the metamodel are forensically robust [10]. In order to improve the general integrity and applicability of the framework, expert review offers valuable perspectives on the meaning and contextual relevance [11].

A multiple case study approach is employed to further enhance the validation of the OSNFIM framework. Incorporating multiple case studies offers a practical means of assessment since the metamodel validation evaluates how effectively a conceptual model reflects real-world elements associated with its proposed functions or specified requirements. In real-world contexts, this method allows researchers to scrutinize actual/documented scenarios, improve methodologies, and apply theoretical concepts. By so doing, it fortifies the framework's applicability, ensures its robustness, and confirms that it can address varied forensic challenges across numerous online social network environment.

METHODOLOGY

The metamodel's performance in real-world documented contexts will be evaluated based on three distinct case studies ranging from cyberbullying incidents, illegal account hacking to social engineering with technical exploitation. Preliminary, acquisition/preservation, analysis and presentation phases are the four layered components of the OSNFIM that will be used to analyze each of the case.

Research Design

Multiple case study approach is adopted as the research design to evaluate the OSNFIM metamodel's applicability in diverse forensic contexts. To ensure that the framework is verified across psychological manipulation, illegal access, and hybrid exploitation scenarios, case studies were selected to reflect both human-centered and technology-centered incidents. OSNFIM was selected because of its layered structure; preliminary, evidence acquisition/preservation, analysis, and presentation which offers a methodical trail from raw data to validated insights.

Case Study Selection

Three distinct types of OSN cases were selected to assess the performance of the metamodel. These are:

- Cyberbullying incident
- Unauthorized Account Hacking
- Social Engineering with Technical Exploitation

From demonstrative manipulation to technical breaches, this multiplicity certifies that OSNFIM is verified against a wide range of forensic challenges.

Analytical Framework

The four phases of the OSNFIM will be used to examine each of the case studies. These phases are: Preliminary, Acquisition/Preservation, Analysis, and Presentation phases as presented in Figures 1, 2, 3, and 4.

Validation Criteria and Evaluation Dimensions

- Completeness: ability to show that all real-world/documented situations in the field can be correctly represented.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

- Traceability: ascertain all links, gadgets, and channels associated with a scenario are retrieved.
- Adaptability: ability of the OSNFIM to suit into the three different case studies
- Practical alignment: involves using structured, model-driven methods of the OSNFIM to map the case studies
- Evidentiary integrity: involves administering a rigorous procedure for validating the accurately of OSNFIM, and that the metamodel can be reliable to protect evidence with integrity.
- Cross-case consistency: the same phases and concepts of the OSNFIM framework were steadily used across the three case studies.

Comparison with Existing Digital Forensic Investigation Models

Due to the prevalence of non-uniform and ad hoc forensic techniques, existing DFIMs face a critical challenge [12]. In criminal contexts, these practices weaken the effectiveness of investigations and corrode the dependability and acceptability of evidence [13]. Numerous models have been developed, however, rather than the models covering a broader OSN environment, their scope often remains limited to individual platforms or specific content types [14], [15]. Some of the existing models still requires manual management [16], thus reducing the dependability and evidentiary value of discoveries in criminal proceedings [17]. As a result, OSNFIM was developed to support forensic investigations in OSNs and associated digital cases, making it particularly effective in scenarios where social engineering and psychological factors converge with digital evidence, such as cyberbullying.

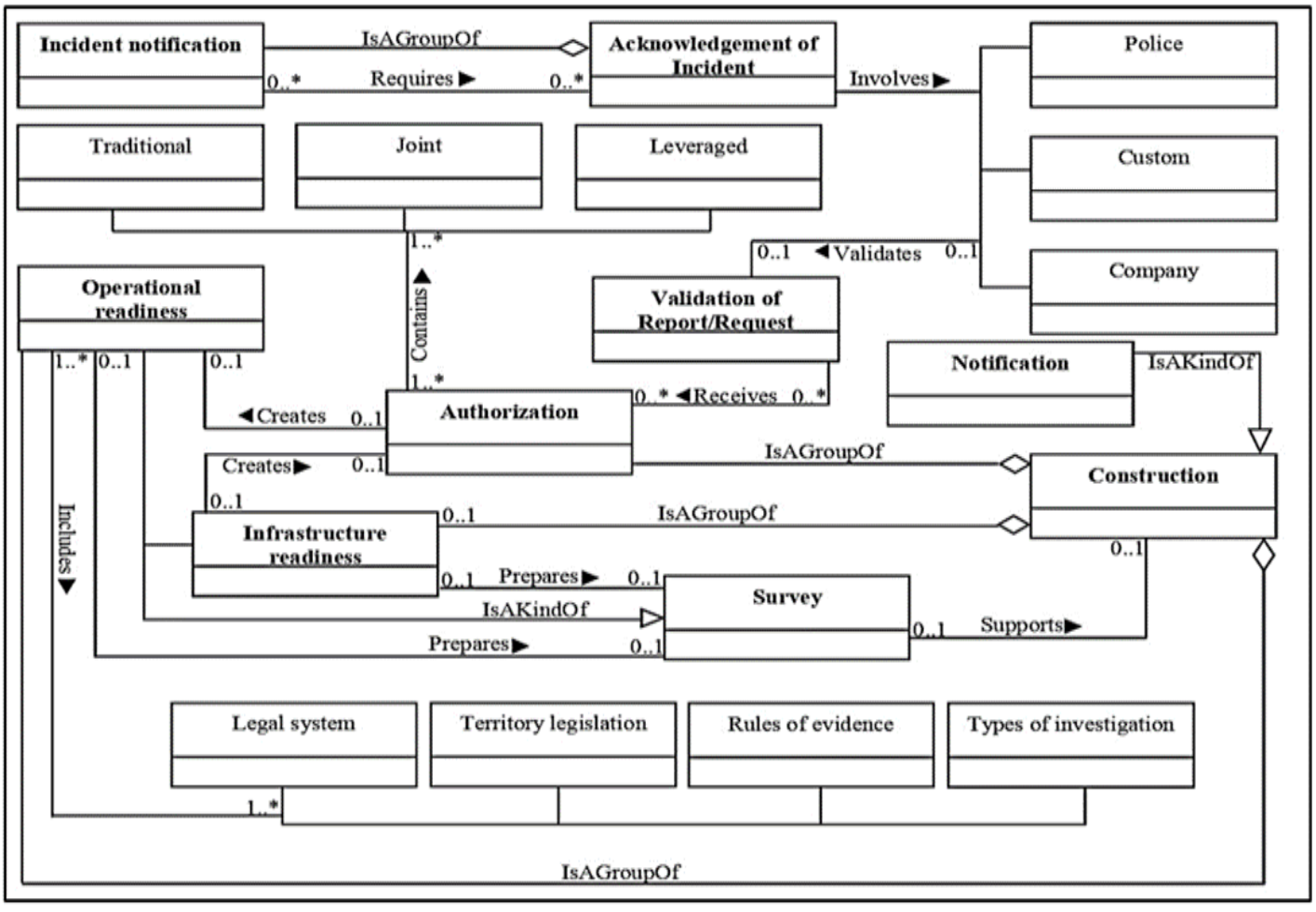

Fig. 1. Preliminary-phase

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

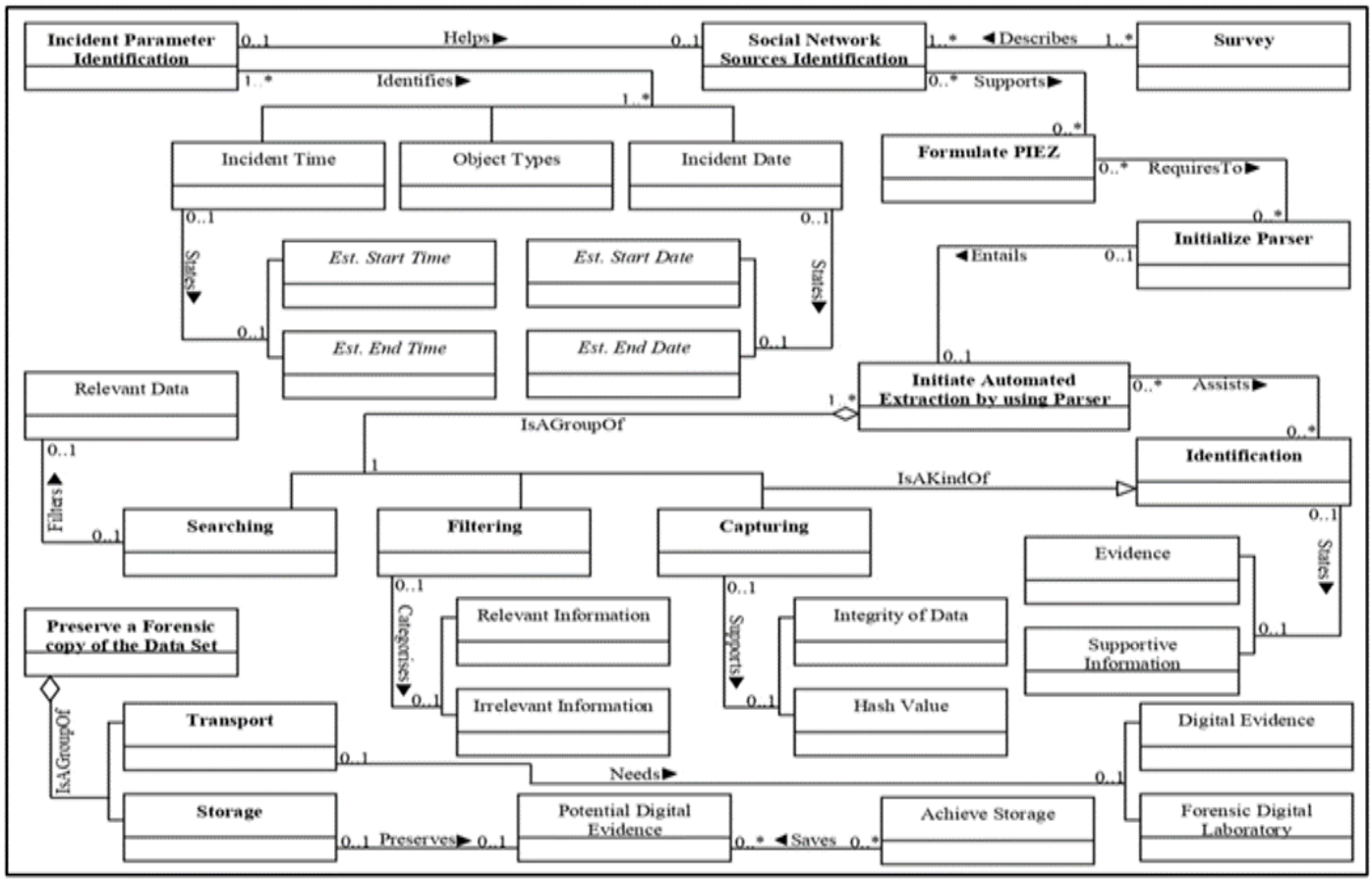

Fig. 2. Acquisition/Preservation-phase

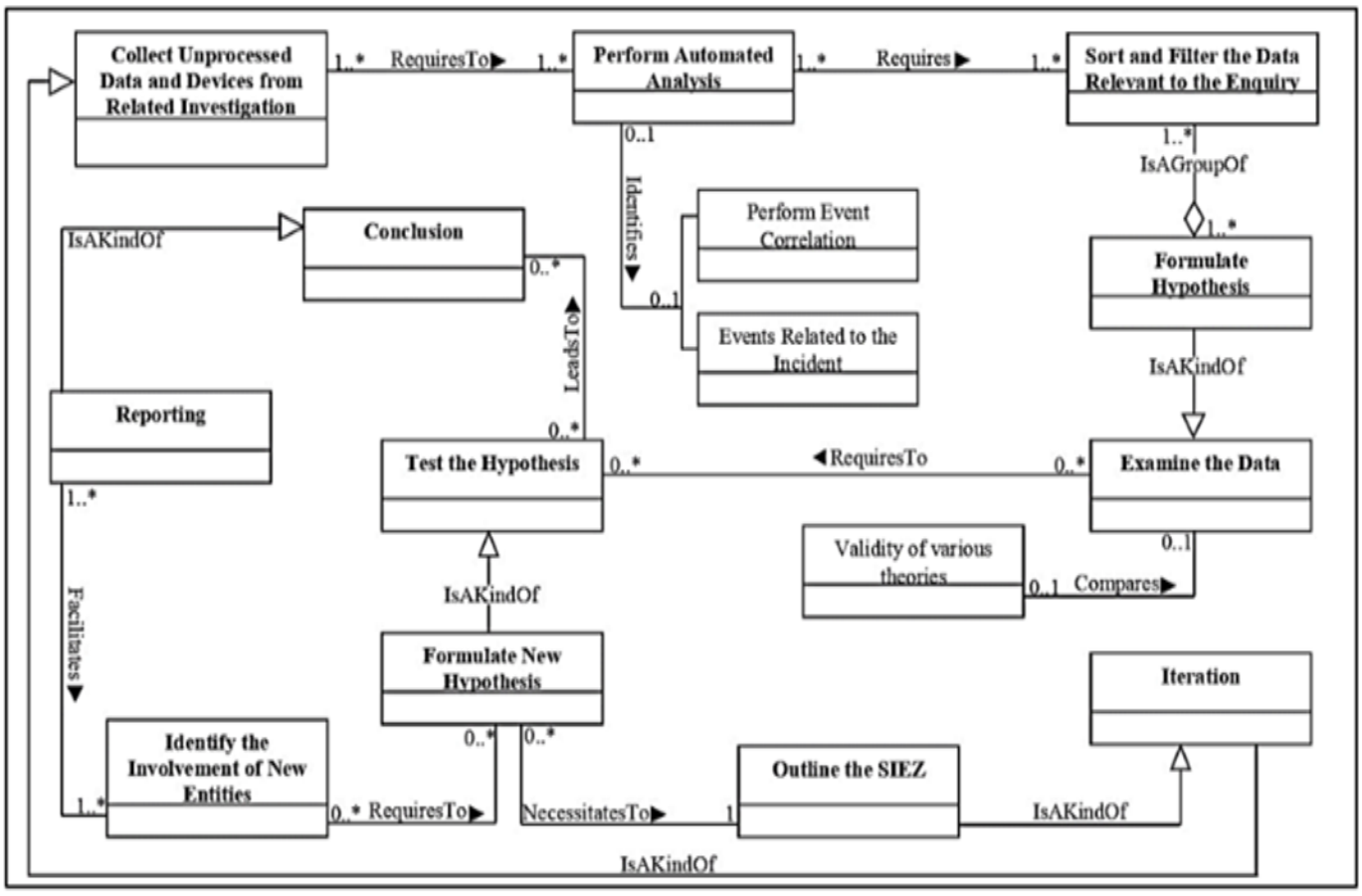

Fig. 3. Analysis-phase

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

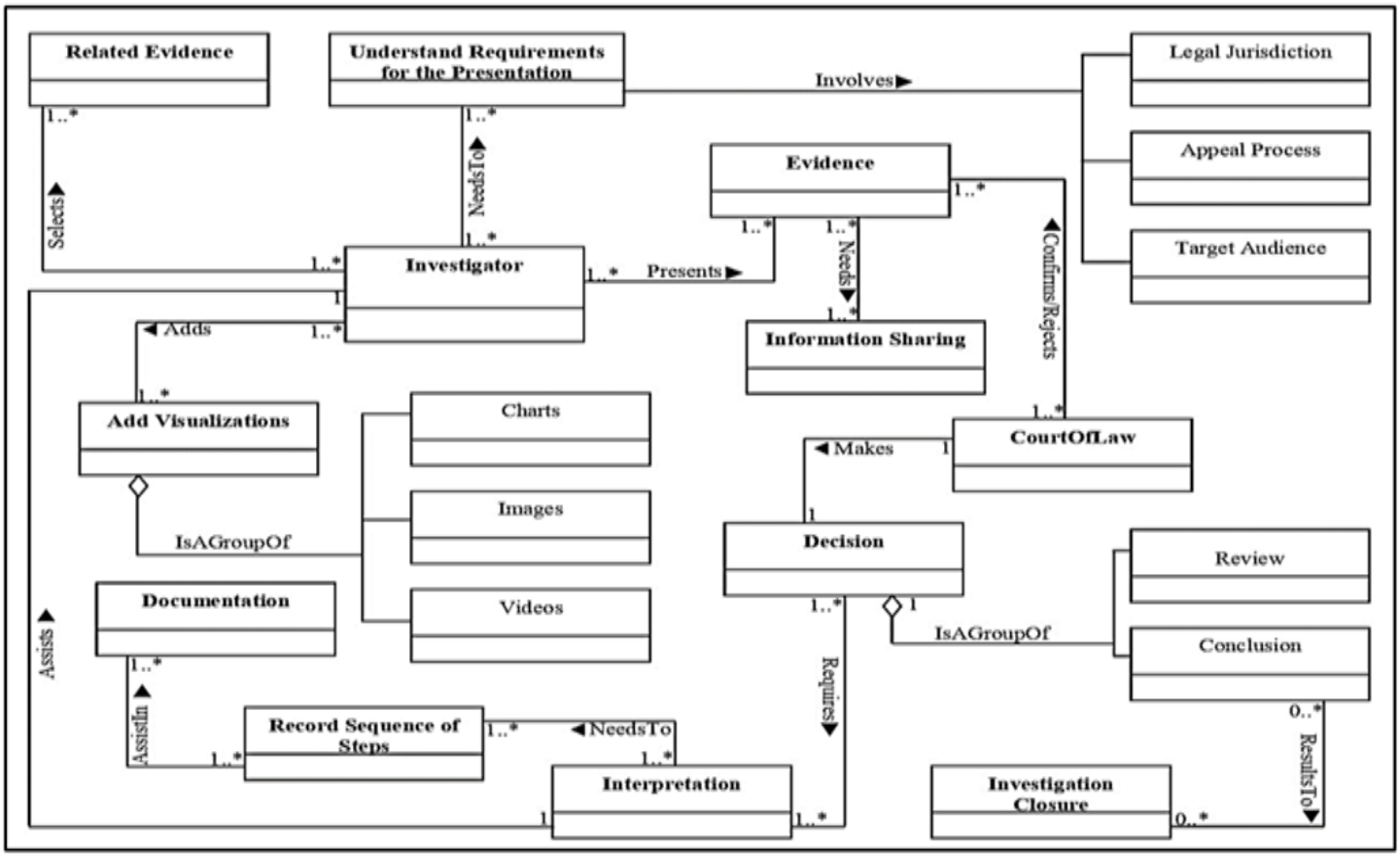

Fig. 4. Presentation-phase

Mapped Incidents to OSNFIM

- **The Megan Meier Case (2006)**

The case of Megan Meier, a 13-year-old girl in Missouri is one of the earliest and most widely recognized case of cyberbullying resulting in suicide. A neighbor, among others, created a fake social media profile under the name "Josh Evans" to emotionally manipulate and verbally attack her which at the end, she took her own life after being endangered to the online trick [18].

- **2020 Twitter Account Hijacking**

The 2020 Twitter account hijacking is another protuberant example of an unauthorized social media account hacking. It was an organized social engineering attack which was investigated and led to manifold arrest. The incident compromised some high-profile accounts, including those of Barack Obama, Joe Biden, Elon Musk, and Apple. Three individuals were charged for their roles in this incident [19].

- **The Uber Data Compromise (2022)**

The Uber data breach of 2022 signifies an important cybersecurity incident which joined social engineering with technical exploitation to break into Uber's internal network. This was ascribed to an 18-year-old hacker reportedly connected to the Lapsus$ group. The attack was distinguished for both the ease of its initial access vector and the extensive lateral movement that followed [20].

All the three cases were mapped based on the phases of the OSNFIM, and presented in table 1, 2, 3, and 4.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Table 1 Applicability of OSNFIM Preliminary-phase based on the three (3) cases

Case Studies			
Concept	***Megan Meier Case (2006)***	***2020 Twitter Account Hijacking***	***Uber Data Compromise (2022)***
Operational readiness	• A multidisciplinary investigative team was established to ensure procedures for handling sensitive cases involving minors are in place. DF tools for social media, email, and device analysis were arranged.	• Operational readiness failed because employees lacked training in recognizing social engineering attempts. This allowed attackers to trick staff into giving access credentials.	• Uber's operational readiness was weak, as employees were vulnerable to social engineering and MFA fatigue attacks, showing gaps in training and awareness.
Infrastructure readiness	• Trace the IP address associated with the "Josh Evans" account and obtaining records from MySpace	• Infrastructure readiness was weak. Privileged access controls and multi-factor authentication for internal systems were insufficient, enabling attackers to escalate privileges and compromise 130 accounts.	• The company's identity and access management systems was weak which resulted in the attackers taking advantage of it.
Incident notification	• MySpace profile	• Twitter users and the public identified the breach before Twitter formally acknowledged it.	• Uber detected the breach on September 19, 2022, and publicly acknowledged it the same day, notifying stakeholders more promptly than in past breaches.
Authorization/ Acknowledgment	• St. Charles County Sheriff's Department • St. Charles County Prosecutor's Office • Federal Bureau of Investigation (FBI)	• Twitter's security team authorized emergency measures, including locking all verified accounts temporarily.	• Uber's security team authorized emergency measures, including restricting employee access, disabling compromised accounts, and engaging external cybersecurity experts.
Construction	• A timeline was created documenting the fake "Josh Evans" profile, initial communications with Megan Meier, escalation to verbal attacks, and her final interactions before death. In parallel, digital evidence repositories, emails, chat logs, and metadata were established to preserve and organize artifacts for forensic validation	• Investigators reconstructed the attack timeline: • Initial compromise via social engineering. • Access to internal tools. • Hijacking of 130 accounts. • Execution of Bitcoin scam tweets.	• Investigators reconstructed the attack timeline, beginning with social engineering, followed by access to internal systems, and culminating in exposure of sensitive corporate information.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

	and presentation.		
Notification	• Stakeholders were notified of investigative progress (family of the victim), and updates were provided while maintaining confidentiality.	• Internally, Twitter notified law enforcement and regulators (e.g., New York Department of Financial Services); externally, Twitter issued public statements explaining the breach and mitigation steps.	• Internally, Uber notified employees and executives; externally, regulators, law enforcement, and the public were informed through official statements.
Survey	• Forensic surveys were conducted on Megan's computer, phone, and perpetrator-linked accounts/devices. Network traffic logs were examined to trace IP addresses and digital linkages. Interviews with family, friends, and neighbors provided testimonial evidence, integrated with digital artifacts to strengthen the investigation.	• Investigators surveyed compromised accounts, internal logs, and employee communications. • They confirmed 69 accounts were actively used in the scam, while 130 were accessed overall. Blockchain analysis traced Bitcoin wallets, showing attackers collected about $110,000.	• A forensic survey examined compromised accounts, cloud services, and communication channels, confirming that sensitive customer data was not stolen, though internal corporate information was accessed.
Validation of report/request	Validate all collected evidence against multiple sources: • Cross-check MySpace logs with ISP records. • Verify timestamps with device metadata. • Confirm witness statements with digital communications. • Ensure forensic integrity (no tampering, proper chain-of-custody).	• Law enforcement validated forensic findings, leading to arrests of three individuals involved. Regulators confirmed Twitter's cybersecurity weaknesses. • Validation provided accountability, legal closure, and recommendations for stronger cybersecurity practices.	• Findings were validated by law enforcement and regulators, with independent cybersecurity experts confirming Uber's claims and recommending stronger identity frameworks and employee training.

Table 2 Applicability of OSNFIM Acquisition/Preservation-phase based on the three (3) cases

Case Studies			
Concept	***Megan Meier Case (2006)***	***2020 Twitter Account Hijacking***	***Uber Data Compromise (2022)***
Identify Incident Parameters	• Platform: MySpace social networking site. • Actors: Megan Meier (victim), Lori Drew and accomplices (perpetrators using fake profile "Josh Evans").	• Incident: July 15, 2020 hijacking of 130 Twitter accounts. • Attack vector: Social engineering (phone spear-phishing of employees). • Impact: Fraudulent Bitcoin	• Identified the incident parameters as the September 2022 compromise of Uber's systems, where attackers used social engineering (MFA fatigue and phishing) to gain access to internal tools, Slack, and cloud

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

	• Nature: Harassment, deception, emotional manipulation.	scam tweets, ~$110,000 collected, reputational damage.	services.
Identify Social Network sources	• Primary source: MySpace account of Megan Meier. • Secondary sources: Fake profile "Josh Evans," communications between Lori Drew and others. • Supporting sources: Local ISP logs, metadata from MySpace servers, Megan's personal computer.	• Twitter platform logs (account activity, password resets, admin tool usage). • Blockchain records (Bitcoin wallet transactions linked to scam). • External communications (tweets, DMs, public statements).	• Identified social network sources including Uber's internal communication channels (Slack), employee accounts, cloud service logs, and external social media posts made by the attackers claiming responsibility.
Formulate PIEZ	• Preservation: Secure Megan's MySpace account data before deletion. • Identification: Recognize fake accounts and associated IP addresses. • Extraction: Retrieve chat logs, friend requests, private messages. • Zoning: Separate victim's legitimate communications from malicious ones.	• People: Twitter employees, attackers, affected account holders. • Infrastructure: Twitter's internal admin tools, authentication systems, network logs. • Events: Account takeovers, scam tweets, Bitcoin transfers. • Zones: Internal corporate environment, external Twitter ecosystem, blockchain ledger.	• People: Uber employees, attackers (linked to Lapsus$), and investigators. • Infrastructure: Uber's identity management system, cloud services, and internal tools. • Events: MFA fatigue attacks, unauthorized logins, Slack messages, and data exposure. • Zones: Corporate IT environment, cloud infrastructure, and external social networks.
Initialize Parser	• Develop forensic parser to read MySpace message formats, metadata, and timestamps. • Ensure compatibility with MySpace's database structure.	• Configure forensic parsers to process Twitter logs, JSON/CSV exports, and blockchain transaction data. • Ensure compatibility with Twitter's internal monitoring formats.	• Initialized forensic parsers capable of processing Slack logs, cloud service logs, and system authentication records in JSON/CSV formats.
Initiate Automated Extraction by using Parser	• Extract all communications between Megan and "Josh Evans." • Collect metadata (IP addresses, login times, geolocation).	• Extract login attempts, credential resets, and admin tool activity. • Extract tweet timelines from compromised accounts. • Extract blockchain transaction flows from scam wallets.	• Initiated automated extraction to collect login attempts, MFA push notifications, Slack messages, and cloud activity logs for analysis.
Identification	• Identify perpetrators by	• Identify compromised	• Identified compromised

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

	correlating IP addresses with Lori Drew's household. • Confirm fake identity creation and intent.	accounts (130 total, 45 actively tweeting scams). • Identify Bitcoin wallets used in fraudulent activity.	employee accounts, attacker-controlled IP addresses, and specific internal tools accessed during the breach.
Searching	• Search Megan's computer for cached MySpace data, saved conversations, and screenshots. • Search ISP logs for traffic related to MySpace sessions.	• Search internal logs for unauthorized access patterns. • Search blockchain for wallet addresses and transaction chains.	• Searched across Uber's system logs and Slack channels to trace unauthorized access patterns and attacker communications.
Filtering	• Filter out irrelevant communications (friends, unrelated chats). • Focus on abusive, manipulative, or deceptive messages.	• Filter legitimate account activity to isolate malicious actions. • Narrow logs by time window (July 15, 2020) and employee access anomalies.	• Filtered legitimate employee activity from malicious actions, focusing on abnormal login attempts, repeated MFA push requests, and suspicious Slack messages.
Capturing	• Capture forensic images of Megan's computer and MySpace server logs. • Ensure chain of custody is documented.	• Capture forensic images of compromised accounts' activity. • Capture blockchain transaction records tied to scam wallets.	• Captured forensic images of compromised accounts, Slack conversations, and system logs to preserve evidence of attacker activity.
Survey	• Survey Megan's social network interactions to establish behavioral changes. • Compare normal interactions vs. abusive exchanges.	• Survey compromised accounts for extent of damage. • Survey employee access points to determine insider compromise.	• Surveyed the compromised systems to assess the extent of exposure, confirming that sensitive customer data was not accessed but internal corporate information was exposed.
Transport	• Transport forensic copies securely to investigation lab. • Maintain integrity using write-blockers and cryptographic hashes.	• Securely transport forensic datasets (logs, blockchain records) to investigation repository. • Maintain chain-of-custody for admissibility in court.	• Securely transported the collected forensic datasets to the investigation repository, maintaining strict chain-of-custody protocols.
Storage	• Store datasets in secure forensic repository. • Apply encryption and access control.	• Store forensic data in encrypted repositories. • Organize by category: account logs, admin tool logs, blockchain evidence.	• Stored the forensic data in encrypted repositories, organized by category (authentication logs, Slack logs, and cloud activity records).
Preserve a forensic copy of Data	• Preserve complete forensic copy of MySpace	• Preserve immutable forensic copies of all datasets.	• Preserved immutable forensic copies of all datasets, applying hashing

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Set	communications, metadata, and victim's device. • Maintain immutability for court admissibility.	• Apply integrity checks (hashing) to ensure authenticity. • Maintain redundancy for long-term preservation.	for integrity verification and ensuring redundancy for long-term admissibility in court.

Table 3 Applicability of OSNFIM Analysis-phase based on the three (3) cases

Case Studies			
Concept	***Megan Meier Case (2006)***	***2020 Twitter Account Hijacking***	***Uber Data Compromise (2022)***
Perform automated Analysis	• Gather all digital traces from MySpace: user accounts, messages, bulletin posts, and metadata. • Identify the fake profile "Josh Evans" used to interact with Megan.	• Automated tools were used to analyze Twitter's internal logs, employee access records, and blockchain transactions to detect anomalies.	• Automated tools were used to analyze Uber's internal system logs, Slack communications, and cloud service activity to detect anomalies linked to the breach.
Sort and filter the data relevant to the inquiry	• Filter communications between Megan and "Josh Evans." • Highlight abusive messages, sudden behavioral shifts, and shared private information. • Exclude unrelated MySpace activity to focus on the cyberbullying trail.	• Suspicious login attempts, unauthorized password resets, and Bitcoin wallet activity were isolated from legitimate account activity.	• Suspicious login attempts, repeated MFA push notifications, unauthorized Slack messages, and abnormal cloud access were isolated from legitimate employee activity.
Formulate hypotheses	• Hypothesis A: Megan's suicide was triggered by cyberbullying from the "Josh Evans" account. • Hypothesis B: The account was controlled by individuals close to Megan (neighbors/classmates). • Hypothesis C: Systemic gaps in MySpace's moderation enabled prolonged abuse.	• Investigators hypothesized that attackers exploited employees through social engineering and misused internal administrative tools.	• Investigators hypothesized that attackers exploited employees through MFA fatigue and phishing, then escalated privileges to access internal tools and cloud services.
Examine the Data	• Timestamps of messages were analyze leading up to 17 October 2006. • IP logs and account registration details were validated to trace "Josh Evans" back to Lori Drew. • Megan's emotional replies as testified by family with message content were compared.	• Extract logs, tweets, and blockchain records and examine to validate the timeline and scope of compromised accounts	• Extracted logs, Slack records, and cloud activity were examined to validate the timeline of compromise and confirm the scope of accessed systems.
Test the Hypothesis	• Offensive online interactions directly led Megan's suicide was	• Employee access anomalies were correlated with the	• The hypothesis was tested by correlating employee login

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

	established as "Hypothesis A" • The fake account was created by Lori Drew, neighbor and mother of Megan's classmate, and was confirmed as "Hypothesis B" • It was partially confirmed as Hypothesis C that, the MySpace lacked effective protections against impersonation and harassment.	timing of fraudulent tweets, and blockchain wallet addresses were matched with scam transactions.	anomalies with attacker communications and matching compromised credentials with unauthorized system access.
Conclusion	• Megan Meier's death caused from targeted cyberbullying that was made possible by the aptitude for culprits to remain unidentified online. • The forensic evidence confirmed Lori Drew's involvement, notwithstanding the fact that her conviction was later dismissed.	• The attack was confirmed to have originated from spear-phishing calls to employees, leading to unauthorized use of Twitter's internal tools.	• The analysis concluded that the breach originated from social engineering attacks on employees, leading to unauthorized access of Uber's internal infrastructure.
Reporting	• Findings in a structured forensic report. • Present technical evidence (IP logs, account metadata) and social evidence (message content, witness testimony). • Recommend legal and policy reforms to address cyberbullying.	• Findings were documented in forensic reports detailing the attack sequence, compromised accounts, financial impact, and infrastructure weaknesses.	• Findings were documented in forensic reports detailing the attack sequence, compromised systems, methods used, and recommendations for stronger identity management.
Formulate new hypotheses	• Could stronger parental monitoring or platform safeguards have prevented escalation? • Would real-time detection of abusive language reduce harm?	• New hypotheses were developed regarding insider involvement and additional vulnerabilities in Twitter's systems.	• New hypotheses were developed regarding potential insider negligence and additional vulnerabilities in Uber's authentication framework.
Identify the Involvement of new Entities	• Entities: Lori Drew, Megan's classmates, MySpace as a platform, law enforcement, and later the courts.	• External Bitcoin exchanges and additional wallet addresses were identified as entities linked to laundering stolen funds.	• External entities such as the hacking group Lapsus$ and associated IP addresses were identified as being directly involved in the compromise.
Outline the Secondary Information Extraction Zone	• Secondary data: media coverage, citizen journalism, and public discourse around the case. • These sources shaped societal understanding and legal debates.	• Secondary zones such as employee communications, external social media chatter, and extended blockchain analysis were outlined for deeper investigation.	• Secondary zones such as employee communications, external social media posts by attackers, and extended cloud service logs were outlined for deeper investigation.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Iteration	• Re-examine evolving cyberbullying cases using lessons from Megan's case. • Update forensic models to incorporate social media dynamics and anonymity risks.	• Logs and blockchain flows were re-examined to uncover overlooked connections and strengthen the evidence chain.	• Logs and communications were re-examined iteratively to uncover overlooked connections and strengthen the evidence chain.
Collect unprocessed Data and Devices from related investigation	• Retrieve Megan's personal devices (computer, phone) for local message logs. • Secure MySpace server logs for forensic preservation.	• Seized computers and phones of suspects were collected and integrated into the primary forensic dataset.	• Additional unprocessed data and devices, including seized attacker-controlled accounts and external communications, were collected to integrate with the primary forensic dataset.

Table IV. Applicability Of OSNFIM Presentation-Phase Based On The Three (3) Cases

Case Studies			
Concept	***Megan Meier Case (2006)***	***2020 Twitter Account Hijacking***	***Uber Data Compromise (2022)***
Related Evidence	• MySpace account "Josh Evans" created by Lori Drew and associates. • Message logs showing abusive interactions with Megan. • Metadata (timestamps, IP addresses) linking the fake account to Drew's household. • Testimonies from Megan's parents and classmates about her emotional state.	• Compiled related evidence including Twitter internal logs, employee access records, compromised account activity, and blockchain transactions tied to the Bitcoin scam.	• Internal system logs, Slack communications, authentication records, attacker-controlled IP addresses, and external social media posts claiming responsibility were compiled.
Understand requirements for the presentation	• Evidence must be admissible in court (chain of custody, authenticity). • Present digital forensic findings in a way understandable to non-technical audiences (jury, judge). • Highlight causal link between online harassment and Megan's suicide.	• Reviewed the requirements for presenting evidence to regulators, law enforcement, and the court, ensuring compliance with admissibility standards and clarity for non-technical audiences.	• Evidence was aligned with legal admissibility standards and tailored for both technical and non-technical stakeholders.
Add Visualizations	• Timeline visualization of Megan's interactions with "Josh Evans."	• Timelines of account takeovers, flowcharts of attacker access paths, and	• Timelines of attacker activity, diagrams of MFA fatigue attacks, and

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

	• Graph showing escalation of abusive messages leading to October 17, 2006. • Network diagram mapping account ownership and connections between Lori Drew, her daughter, and Megan.	graphs of Bitcoin transaction flows were added to make the evidence more comprehensible.	flowcharts of compromised access paths were created to aid comprehension.
Record Sequence of Steps	• Account creation traced. • Message logs collected. • IP addresses matched to Drew's computer. • Evidence preserved and analyzed. • Findings reported to law enforcement.	• Recorded the sequence of investigative steps, from initial detection of anomalies to the identification of compromised accounts and wallets, ensuring transparency and reproducibility.	• The investigative steps from incident detection to evidence acquisition, analysis, and preservation were documented for transparency.
Present the Evidence	• Presented evidence showed Lori Drew's involvement. • Verified how the fake account was used to manipulate and emotionally hurt Megan. • Forensic trace from MySpace servers to Drew's household Presented.	• Presented the evidence in structured sessions to Twitter executives, regulators, and law enforcement, highlighting the attack timeline, methods used, and financial impact.	• Findings were formally presented to Uber executives, regulators, and law enforcement, highlighting the attack timeline, methods, and impact.
Decision	• Lori Drew was charged under the Computer Fraud and Abuse Act (CFAA). • Jury sentenced her of delinquencies linked to illegal computer access. • Conviction later upturned on appeal due to interpretation of CFAA.	• Based on the evidence, decisions were made to charge the perpetrators, strengthen Twitter's internal security protocols, and recommend employee training against social engineering.	• Decisions were made to pursue charges against perpetrators, strengthen internal security protocols, and implement employee training against social engineering.
Interpretation	• Case underscored gaps in cyberbullying laws. • Raised questions around if current computer crime decrees might address psychological hurt. • Caused national debate on online harassment and accountability.	• Interpreted the evidence to demonstrate that the attack was a targeted social engineering exploit of employees with privileged access and not a system-wide technical failure.	• Evidence was interpreted to show that the breach stemmed from social engineering rather than a technical system failure.
Documentation	• Forensic reports compiled by investigators. • Court transcripts documenting	• Documented all findings in a comprehensive forensic report, including evidence logs,	• A comprehensive forensic report was produced, including evidence logs,

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

	proceedings. • Media coverage providing secondary documentation of societal impact.	visualizations, interpretations, and recommendations for future prevention.	visualizations, interpretations, and recommendations for prevention.
Investigator	• Local police and FBI cybercrime units involved. • Digital forensic experts analyzed MySpace logs and Drew's computer.	• Ensure impartiality, accuracy, and adherence to forensic standards throughout the evidence collection and presentation process.	• The investigator ensured impartiality, accuracy, and adherence to forensic standards, maintaining chain-of-custody throughout.
CourtOfLaw	• Case tried in federal court in Los Angeles. • Drew's conviction overturned by Judge George Wu in 2009.	• The evidence was submitted to the court of law, where it supported charges against the identified perpetrators and demonstrated the chain-of-custody integrity.	• Evidence was submitted to the court, supporting charges and demonstrating the integrity of the forensic process.
Information sharing	• Case widely reported in media, raising awareness of cyberbullying. • Shared among legal scholars, educators, and policymakers as a landmark case.	• Information was shared with regulators such as the New York Department of Financial Services, law enforcement agencies, and Twitter's internal security team to strengthen collective cybersecurity resilience.	• Findings were shared with regulators, law enforcement, and Uber's internal security team to strengthen collective cybersecurity resilience.
Investigation closure	• Case legally closed after conviction overturned. • No further criminal liability for Lori Drew. • Case remains a reference point in cyberbullying and forensic investigation discussions.	• The investigation was formally closed after arrests were made, forensic findings validated, and recommendations implemented, ensuring accountability and lessons learned for future incidents.	• The investigation was closed after arrests were made, findings validated, and Uber implemented recommended security improvements.

RESULT AND DISCUSSION

The validation of the OSNFIM produced positive results across all the three selected case studies (cyberbullying, unauthorized account hacking, and social engineering with technical exploitation). The four phases of the framework (preliminary, evidence acquisition/preservation, analysis, and presentation) were applied to every single case as presented in table 1, 2, 3 and 4.

Psychological manipulation and digital traces were efficiently captured by OSNFIM making sure that both human-centered and technical evidence were preserved. A simplified and organized analysis of the communication patterns, user behaviors, and contextual factors, were attained based on the phases approach leading to reliable insights. In the case of unauthorized account hacking, the framework has established robust adaptability. Forensic reliability were ensured by the acquisition/preservation phase, while the intrusion vectors and verification weakness were highlighted by the analysis phase. A clear and acceptable outcomes appropriate for legal contexts were provided by the presentation phase. OSNFIM effectively assimilated human-centered

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

deception with technical exploitation evidence. The preliminary phase contextualized the manipulation approaches, while the analysis phase linked psychological tactics with digital footprints. The framework's comprehensiveness in addressing hybrid threats is confirmed based on the holistic approach.

Significantly, the OSNFIM has confirmed its completeness, traceability, adaptability, practical alignment, evidentiary integrity, and cross case consistency across various forensic contexts by completely accommodating all the three case studies. The positive results underscored numerous important contributions of OSNFIM to the field of digital forensics: Generalization and Applicability, Integrity and Reliability, Structured Investigative Trace, and Contribution to Digital Forensics. Furthermore, the results affirm that OSNFIM is a reliable, extensible, and practical framework capable of handling the complex challenges of online social network forensics. Its validation through different case studies highlights its potential as a basis in evolving digital forensic practices.

CONCLUSION AND FUTURE WORK

The multiple case studies validation of the Online Social Networks Forensic Investigation Metamodel (OSNFIM) has demonstrated its applicability to various OSN-related forensic documented investigations. The OSNFIM has reliably provided a structured and consistent framework that guides investigators through each phase of the procedure from cyberbullying to account hacking and social engineering incidents. The total of forty-six concepts across the four phases of the OSNFIM were used to assess the three cases. Its flexibility to both technical and social scopes of online delinquency confirmed its significance in real-world retrospective contexts and validates its capability to handle the complexity of online social networks. Potential area for future research could be the integration of an AI-assisted forensic analysis to the OSNFIM framework investigation process. This will assist in speeding up the investigation procedure and analyzing huge datasets from digital records such as audio and video.

REFERENCES

1. Sethurajan, M. R. and Natarajan K. A web forensic optimization framework for investigating false information on social media using the ForenOptiNet model. Discov. Comput. 2025;1–33.
2. Bade A. M. and Othman SH. Towards Adapting Metamodelling Technique for an Online Social Networks Forensic Investigation (OSNFI) Domain. Int. J. Adv. Comput. Sci. Appl. 2022;13:166–73.
3. Cibrián E, Olivert-iserte J, Díez-fenoy C, Llorens J, Álvarez-rodríguez JM. Ensuring Semantic Consistency in SysML v2 Models Through Metamodel-Driven Validation. 2025;13.
4. Celio, E., Brunner, S. H., & Grêt-regamey, A. (2012). Participatory Land Use Modeling with Bayesian Networks : a Focus on Subjective Validation Participatory Land Use Modeling with Bayesian Networks : a Focus on Subjective Validation.
5. Ali A, Abd Razak S, Othman SH, Mohammed A, Saeed F (2017) A metamodel for mobile forensics investigation domain. PLoS ONE 12(4): e0176223. doi:10.1371/journal.pone.0176223
6. IEEE. (2010). IEEE Recommended Practice for Distributed Interactive Simulation-Verification, Validation, and Accreditation.
7. Ralyté J, Koutsopoulos G, Stirna J. Verification , validation , and evaluation of modeling methods : experiences and recommendations. Softw. Syst. Model. [Internet] 2025;Available from: https://doi.org/10.1007/s10270-025-01304-2
8. Xiang, X., Kennedy, R. and Madey, G. (2005) 'Verification and Validation of Agent based Scientific Simulation Models', Agent-Directed Simulation Conference, pp. 47–55. Available at: http://www.nd.edu/~nom/Papers/ADS019_Xiang.pdf
9. Sargent, R. G. (2013) 'Verification and validation of simulation models', Journal of Simulation, 7(1), pp. 12–24. doi: 10.1057/jos.2012.20.
10. Bade, A. M. et al. (2023) 'Expert Validation of Online Social Networks Forensic Investigation Metamodel (OSNFIM)', 2023 International Conference on Data Science and Its Applications, ICoDSA 2023, pp. 500–505. doi: 10.1109/ICoDSA58501.2023.10277048.
11. Fernández-Gómez, E. et al. (2020) 'Content validation through expert judgement of an instrument on the nutritional knowledge, beliefs, and habits of pregnant women', Nutrients, 12(4). doi: 10.3390/nu12041136.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

12. Bade, A. M. and Othman, S. H. (2021) 'A Systematic Review of Published Articles, Phases and Activities in an Online Social Networks Forensic Investigation Domain', International Journal of Advanced Computer Science and Applications, 12(11), pp. 153–160. doi: 10.14569/IJACSA.2021.0121118.
13. Arshad, H., Jantan, A., & Omolara, E. (2019). Evidence collection and forensics on social networks: Research challenges and directions. Digital Investigation, 28, 126–138. https://doi.org/10.1016/j.diin.2019.02.001
14. Taylor, D. C. P. J. et al. (2019) 'Science & Justice Forensic investigation of cross platform massively multiplayer online games : Minecraft as a case study', Science & Justice, 59(3), pp. 337–348. doi: 10.1016/j.scijus.2019.01.005.
15. Arshad, H., Omlara, E., Oludare, I., & Aminu, A. (2020). Computers & Security A semi-automated forensic investigation model for online social networks. Computers & Security, 97, 101946. https://doi.org/10.1016/j.cose.2020.101946
16. Mohd Zainudin, N., Merabti, M., & Llewellyn-Jones, D. (2011). Online social networks as supporting evidence: A digital forensic investigation model and its application design. 2011 International Conference on Research and Innovation in Information Systems, ICRIIS'11. https://doi.org/10.1109/ICRIIS.2011.6125728
17. Zainudin et al. (2010) 'A Digital Forensic Investigation Model for Online Social Networking', pp. 1–6.
18. Vickery, J. (2008). The Megan Meier MySpace suicide: A case study exploring the social aspects of convergent media, citizen journalism, and online anonymity and credibility. International Symposium on Online Journalism. Retrieved from https://isoj.org/wp-content/uploads/2018/01/Jaqueline.pdf
19. United States Department of Justice. (2021, July 27). Three individuals charged for alleged roles in Twitter hack. Retrieved from https://www.justice.gov/opa/pr/three-individuals-charged-alleged-roles-twitter-hack
20. Sharma, U. and Kalekar, S. M. (2024). Dissecting the Uber security breach: Root cause analysis and mitigation strategies. International Journal of Computer Engineering and Technology, 15(4), 620–628. Retrieved December 30, 2025, from https://lib index.com/index.php/IJCET/article/view/IJCET_15_04_062