INTEGRATING NETNOGRAPHY INTO FORENSIC ACCOUNTING FOR FRAUD AND CORRUPTION ANALYSIS

Yana Mustika[1*]
Senda Yunita Leatemia[2]
Andi Octavianus[3]
Natalius Sinulingga[4]

[1,2]Universitas Pattimura Ambon, Maluku, Indonesia
[3]Sichuan University, Chengdu, China
[4] Universiti Poly-Tech Malaysia, Kuala Lumpur, Malaysia
yana.mustika@lecturer.unpatti.ac.id

Article History:
Received : May 18, 2026
Revised : October 19, 2026
Accepted : October 20, 2026

Keywords:
Digital Evidence, Forensic Accounting, Fraud Fiscourse, Netnography, Public Sector Corruption

Abstract:
Purpose - This article develops a framework for incorporating netnography into forensic accounting when public online discussion contains potentially relevant information about fraud and corruption. It addresses the practical problem of converting culturally situated claims into proportionate, verifiable investigative questions.
Method - A critical narrative review is combined with bounded analysis of official documents on Rafael Alun Trisambodo and the PT Timah proceedings involving Harvey Moeis. The source set comprises 24 scholarly, contextual, case, and guidance sources. The analysis distinguishes documented observations, interpretive inferences, and proposed procedures; no primary social media netnography was conducted.
Findings - Research suggests social media discussions about finance can generate leads, but circulation does not establish credibility. Indonesian official records highlight asset-declaration checks and the need to distinguish judicial stages and monetary categories. Four dimensions follow: lifestyle–wealth incongruity, informal disclosure, institutional trust, and narrative convergence. Each requires documentary verification and consideration of alternative explanations.
Implications - The framework sets out source evaluation, escalation decisions, a Digital Discourse Lead Register, and organizational responsibilities. Proposed measures cover corroboration, useful leads, analyst time, and harmful escalation; effectiveness remains untested.
Originality - It links contextual interpretation to forensic verification and positions netnography alongside OSINT, computational analysis, and digital forensics.
.

This is an open access article under the CC BY-SA license

How to cite this article : Mustika, Y., Leatemia, S. Y., Octavianus, A., & Sinulingga, N. (2026). Integrating netnography into forensic accounting for fraud and corruption analysis. Assets: Jurnal Ekonomi, Manajemen, dan Akuntansi, 16(2), 318–337. https://doi.org/10.24252/assets.v16i2.68136

INTRODUCTION

Forensic accounting teams increasingly face allegations that circulate publicly before the underlying records have been examined. A photograph, procurement complaint, or fragment of a document may attract attention, yet the team must decide whether it identifies a testable issue. Acting on weak material can divert resources and damage reputations; ignoring a specific disclosure can leave a control failure unexplored. The research urgency lies in this decision problem: organizations need a defensible procedure for assessing online information while financial, procurement, and asset records remain the basis of verification.

The ACFE's Occupational Fraud 2024 report examined 1,921 cases across 138 countries and territories and reported tips as the initial detection method in 43% of cases (Association of Certified Fraud Examiners, 2024). These findings support attention to information originating outside routine transaction testing. They do not establish that public social media tips are accurate or equivalent to protected reporting channels. Indonesia's historical 2024 Corruption Perceptions Index score of 37/100 and rank of 99 among 180 countries provide additional context for accountability concerns (Transparency International Indonesia, 2025). Neither measure diagnoses an individual case or validates a particular digital method.

The Rafael Alun Trisambodo and Harvey Moeis proceedings make the problem concrete. Official records concerning the former connect public attention to lifestyle with examination of asset declarations; records concerning the latter distinguish an appeal outcome from a subsequent cassation decision (Komisi Pemberantasan Korupsi, 2024a, 2024b; Mahkamah Agung Republik Indonesia, 2025; Prakoso, 2025). For an analyst, these documents raise different questions: which assets should be checked, which procedural event is being described, and whether a circulating amount concerns a fine, compensation, or broader case losses. An online narrative that merges these categories may be socially influential while remaining unsuitable for a forensic conclusion.

Existing digital investigation methods address parts of this task. OSINT helps locate public sources; computational text analysis supports classification at scale; digital forensics addresses the acquisition and examination of electronic material. A remaining interpretive task is to explain what an image, phrase, or accusation means within a particular discussion and whether participants are presenting firsthand information, repeating a report, using satire, or contesting an institutional account. Netnography contributes a disciplined examination of interaction and cultural context (Kozinets, 2002; Kozinets & Gretzel, 2024). Its potential value is greatest where meaning affects the choice of verification question.

The need for netnography is therefore conditional. When an investigator already has an authenticated invoice and a defined transaction question, documentary examination may be sufficient. When the problem concerns why an apparently ordinary document is understood as evidence of preferential treatment, the surrounding exchange may clarify an unstated procurement practice or a disputed relationship. This contextual work can improve the formulation of a lead, but its incremental value must be assessed against the time required. It should complement

the investigation's existing methods rather than become a compulsory stage for every allegation.

This article addresses two research questions. RQ1 asks how netnographic interpretation can be integrated into forensic accounting to formulate specific investigative leads from online fraud and corruption discourse. RQ2 asks which verification, ethical, and organizational safeguards should govern the assessment and escalation of those leads. The objective is to develop an operationally explicit framework grounded in published research and a limited set of official case documents. The article neither estimates detection accuracy nor claims that public attention caused a prosecution or judicial outcome.

The practical output is a record of the claim, its context, its original source, competing explanations, the required test, and the resulting decision. This can help an audit manager allocate work, a forensic accountant request relevant records, and a digital examiner understand what needs preservation. The framework also makes rejection and correction visible. Its contribution is the traceability of these decisions: readers should be able to reconstruct how an interpretive observation became a verification task and why its evidential status changed.

THEORETICAL REVIEW

This study adopts an integrative conceptual framework rather than relying on a single grand theory. Forensic accounting provides the overarching conceptual foundation, emphasizing evidence-based investigation and verification. Fraud theories serve as sensitizing concepts for identifying potential irregularities, while netnography facilitates the contextual interpretation of digital interactions. These perspectives are complemented by OSINT and digital forensics to support source assessment, authenticity, and evidentiary reliability. This integration is necessary because no single theoretical perspective adequately explains the relationship among online narratives, potential fraud indicators, and forensic verification. Accordingly, the framework connects digital signals, investigative leads, corroborated patterns, and forensic evidence within a structured analytical process.

Forensic Accounting and the Limits of Fraud Theory

Forensic accounting applies accounting, auditing, investigative, and analytical skills to questions involving suspected misconduct, disputes, asset recovery, and litigation. An anomaly becomes useful when the analyst can connect it to a transaction, control, asset, or accountable decision. Fraud research provides explanations for potentially relevant conduct, but theoretical fit does not authenticate the material used to support an explanation. A synthesis of fraud research identifies a broad field of issues concerning perpetrators, organizations, detection, and responses (Trompeter et al., 2013). The present framework concentrates on the preliminary formulation of questions within that larger field.

Free's (2015) review identifies limitations in conventional fraud frameworks and calls for closer attention to matters including rationalization, collusion, and whistleblowing. This criticism matters for online analysis because pressure, opportunity, and rationalization are often inferred after a case is already known. Retrospective interpretation can make almost any lifestyle display appear consistent with fraud. An analyst who begins with a suspect's eventual conviction may overlook lawful explanations that would have been plausible at the observation date. Fraud

concepts should guide questions without turning a public narrative into a psychological diagnosis.

Vousinas (2019) extends fraud theorization through the S.C.O.R.E. model and consideration of collusion. Capability and relationships can draw attention to access rights, authority, and coordinated conduct. However, adding explanatory categories also increases the risk of fitting ambiguous posts to an expansive checklist. Visible consumption does not measure ego, and references to several people do not establish collusion. The analytical gain depends on identifying the mechanism that a document, transaction, or access record could test. Concealment is treated here as a possible process requiring investigation, rather than an additional validated personality dimension.

Table 1 preserves the distinction between a sensitizing concept and a verification task. Its categories are not a scale, a diagnostic instrument, or an additive fraud score. A single observation may raise several questions, and a concept may remain unassigned when the available context is insufficient.

Table 1. Fraud Concepts and The Questions They Can Support

Concept	Cautious interpretive question	Documentary test and competing explanation
Pressure or stimulus	Does a specific account describe debt, targets, or status expectations?	Check relevant financial and employment records; distinguish firsthand knowledge from speculation.
Opportunity	Which approval or oversight weakness is actually alleged?	Examine permissions, procurement records, and control operation; unusual authority may still be lawful.
Rationalization	Who offers the justification and in what context?	Compare statements and organizational evidence; public commentary may not express the actor's own reasoning.
Capability	What expertise or access would the alleged conduct require?	Test role, system access, and transaction authority; seniority alone is insufficient.
Ego or perceived impunity	Why is a display interpreted as entitlement?	Verify ownership and funding before inferring relevance; assets may be borrowed or misidentified.
Collusion	Which relationship could explain coordinated action?	Link contracts, ownership, and money flows; social acquaintance alone proves little.
Possible concealment	What changed, disappeared, or became inconsistent?	Examine lawful preservation and chronology; deletion can have routine or privacy explanations.

Source: Authors' synthesis, 2026.

Netnography and Adjacent Digital Approaches

Kozinets (2002) introduced netnography as an adaptation of ethnographic research for online communities. Subsequent work emphasizes evolving contexts, procedures, researcher engagement, and ethical sensitivity (Kozinets & Gretzel, 2024), while Bartl and colleagues review its broader research development (Bartl et al., 2016). The forensic application requires a further distinction: interpreting a community's meaning-making differs from establishing the truth of a financial allegation.

Content analysis provides explicit procedures for assigning categories to material (Hsieh & Shannon, 2005). It can support reproducible comparison, including within netnographic research. Its limitation in a particular investigation arises when isolated categories remove relevant context, not from an inherent inability to consider meaning. Similarly, sentiment analysis describes opinion and affects (Pang & Lee, 2008); a negative score cannot identify the transaction or legal issue that should be examined. Method choice should follow the question and available material. No exclusive boundary is claimed between techniques that may be combined within one study.

OSINT research describes the opportunities and challenges of collecting and evaluating publicly available information (Pastor-Galindo et al., 2020). OSINT can include sophisticated contextual analysis; netnography's added emphasis is sustained attention to interaction, community conventions, and the analyst's interpretive position. Digital forensics, in turn, addresses the integrity and examination of electronic material (Horsman, 2020). These functions overlap operationally but answer different questions. Table 2 identifies the primary contribution sought from each method in the proposed workflow, without implying that any one method can establish guilt on its own.

Table 2. Contributions of adjacent methods to a forensic inquiry

Approach	Principal question in this workflow	Useful output	Main constraint
Netnography	How does this claim acquire meaning in its discussion context?	Contextual interpretation and a proposed lead	Interpretation requires reflexivity and external testing.
Content analysis	How can material be consistently categorized and compared?	Categories, coded passages, and comparisons	Unit and coding choices can remove context.
Sentiment analysis	What opinion or affect is expressed?	Estimated polarity or affect	Affect does not measure factual reliability.
Digital ethnography	How are practices experienced across digital and other settings?	Contextual accounts of practice	Access, engagement, and participant protection require explicit design.

Approach	Principal question in this workflow	Useful output	Main constraint
OSINT	Which public sources can inform the defined question?	Source assessments and information links	Public availability does not ensure independence or accuracy.
Digital forensics	What can electronic material reliably establish?	Preserved material and examination findings	Integrity alone does not establish truth or legal relevance.

Source: Authors' synthesis, 2026.

Research Questions and Conceptual Position

The framework distinguishes four claim levels. A digital signal is an observable item or pattern. An investigative lead identifies a specific actor, asset, transaction, document, control, or event that can be checked. A corroborated pattern has support from genuinely independent material relevant to the same proposition. Forensic evidence is material lawfully acquired and evaluated for authenticity, integrity, relevance, and use in the applicable proceeding. A lead may close or be corrected; admissibility remains a separate determination.

RESEARCH METHODS

Research Design and Source Boundaries

This study employs critical narrative synthesis and bounded documentary analysis to integrate theoretical and methodological perspectives on netnography in forensic accounting. Following Snyder (2019), the review prioritizes conceptual integration rather than exhaustive coverage or quantitative aggregation. Documentary analysis examines official records concerning two illustrative Indonesian proceedings, Rafael Alun and Harvey Moeis, to distinguish investigative relevance from established procedural facts. The purposively selected source set comprises 24 items: 16 scholarly publications (Bartl et al., 2016; Braun & Clarke, 2006; Dong et al., 2018; Ferrara et al., 2016; Free, 2015; Horsman, 2020; Hsieh & Shannon, 2005; Kozinets, 2002; Kozinets & Gretzel, 2024; Murthy, 2008; Pang & Lee, 2008; Pastor-Galindo et al., 2020; Snyder, 2019; Trompeter et al., 2013; Vosoughi et al., 2018; Vousinas, 2019); two contextual sources (Association of Certified Fraud Examiners, 2024; Transparency International Indonesia, 2025); four official case sources (Komisi Pemberantasan Korupsi, 2024a, 2024b; Mahkamah Agung Republik Indonesia, 2025; Prakoso, 2025); and two guidance documents (Franzke et al., 2020; Kent et al., 2006). Publication coverage spans 2002–2025, with source verification conducted on 20 October 2026. Foundational methodological publications were retained despite their earlier publication dates.

The cases were selected for their contrasting documentary contributions. Rafael Alun illustrates lifestyle scrutiny and asset declaration examination, whereas Harvey Moeis illustrates distinctions between judicial communication and cassation records. Their prominence introduces visibility and outcome biases, preventing generalization to ordinary investigations or unsuccessful allegations. The unit of analysis is a source-supported proposition drawn from scholarly publications or official documents. No

primary social media corpus, private communications, interviews, or financial transaction datasets were collected. Consequently, the study does not measure hashtag frequencies, sentiment, network centrality, or netnographic saturation. Proposed online analytical categories should not be interpreted as findings from direct platform observation.

Literature Selection and Evaluation

Sources were identified through a seed bibliography supplemented by targeted open-web searches, DOI and publisher records, institutional repositories, and official Indonesian websites. Search terms combined netnography, digital ethnography, forensic accounting, fraud, corruption, social media, digital evidence, authentication, and preservation. Case-specific searches included KPK, State Officials' Wealth Report or LHKPN, appeal, and cassation terminology. No subscription database search or systematic screening procedure was undertaken. Eligible sources required identifiable authorship or institutional provenance and substantive relevance to fraud mechanisms, online interaction, methodological comparison, information reliability, or forensic verification and ethics. Both English- and Indonesian-language publications were considered. Unsupported commentary, duplicate accounts, unverifiable claims, and methodologically irrelevant social media studies were excluded.

Source evaluation considered authority, provenance, methodological transparency, relevance, independence, temporal and procedural context, and interpretive scope. Scholarly publications informed conceptual interpretation, while official records supported only institutionally documented events or procedural outcomes. Repeated reporting was not treated as independent corroboration. These criteria are summarized in Table 3.

Table 3. Source evaluation criteria and permitted uses

Criterion	Assessment question	Consequence for synthesis
Authority and provenance	Is authorship identifiable and the original source traceable?	Exclude unsupported attribution; prefer the originating institution.
Method transparency	Is the design or basis of the reported assertion visible?	Separate empirical results from conceptual argument or commentary.
Relevance	Does the source answer a research question or define a verification task?	Retain for an explicit role rather than general topical similarity.
Independence	Does the account provide new evidence or repeat an existing source?	Do not count republication as corroboration.
Temporal and procedural fit	Which date, observation window, and legal stage does it cover?	Restrict the claim to that period and stage.
Access and interpretive scope	Was the relevant claim available in the text, abstract, or official summary?	Avoid claims requiring unavailable methods, data, or full reasoning.

Source: Authors' synthesis, 2026.

The review is purposive rather than systematic; therefore, PRISMA screening statistics and screening agreement measures are not reported. Its scope is defined by the reference list, eligibility criteria, and source-to-claim matrix.

Analytical Procedure and Operational Definitions

The synthesis adapts Braun and Clarke's iterative thematic logic (Braun & Clarke, 2006) to documentary propositions through five stages: (1) examining relevant passages and source limitations; (2) developing provisional codes concerning asset visibility, disclosure specificity, accountability, repetition, source dependence, and verification requirements; (3) comparing codes across methodological and case materials; (4) evaluating alternative explanations and contradictory evidence; and (5) translating refined categories into a proposed forensic workflow and investigative lead register. Four analytical dimensions emerged are lifestyle and wealth incongruity, informal disclosure, institutional trust, and narrative convergence. These represent conceptual categories rather than measured variables or prevalence estimates. Each potential indicator requires independent verification and consideration of competing explanations.

An evidence matrix distinguishes documented propositions, interpretive implications, and proposed forensic procedures. This separation prevents conceptual recommendations from being misrepresented as empirical investigative findings. No independently coded primary corpus or inter-coder reliability measurement was available. Future applications should assess interpretive consistency using shared contextual material and field-based validation.

Trustworthiness and Ethics

Trustworthiness was supported through source differentiation, provenance assessment, and consideration of competing explanations. Interpretations were restricted to the evidence available, recognizing that institutional records may provide incomplete contextual information. Consistent with AoIR guidance (Franzke et al., 2020), the study emphasizes lawful access, contextual sensitivity, data minimization, privacy protection, and proportionate preservation. No identifiable ordinary-user posts, screenshots, or private communications were reproduced. Publicly accessible allegations are treated solely as potential investigative leads, not as proof of misconduct or grounds for adverse legal or employment decisions.

RESULTS AND DISCUSSION

Evidence from published research

The first finding is that social information has a defensible role in fraud inquiry, but the available evidence supports different functions. ACFE's reported importance of tips (Association of Certified Fraud Examiners, 2024) concerns how surveyed occupational fraud cases were initially detected; it does not evaluate netnography. Dong et al. (2018) analyzed financial social media associated with 64 fraudulent firms and 64 matched nonfraudulent firms. Their reported framework combined textual and social features with machine learning and compared them with financial and language baselines. This supports the potential value of complementary social data within that study's setting, rather than a performance claim for the present interpretive framework. The second finding concerns the unreliability of circulation as a credibility measure. Vosoughi et al. (2018) examined approximately 126,000

stories shared by about three million people and found that false news spread farther and faster than true news in their Twitter dataset. Ferrara et al. (2016) discuss social bots and their implications for online interaction and information diffusion. Taken together, these sources justify examining origin and amplification separately. They do not provide a calibrated probability that a corruption allegation is false, nor do they establish that a particular discussion is automated.Table 4 provides the source-to-claim matrix. The published studies and official records support a limited conclusion: relevant clues and serious reliability problems can coexist. The framework's response is to require a proposition-specific test. Its four dimensions organize that task; their usefulness, relative frequency, and contribution to detection have not been empirically measured here.

Table 4. Documentary Evidence and The Limits of The Resulting Inference

Source and basis	Documented observation	Analytical implication	Unresolved issue
ACFE 2024 report (Association of Certified Fraud Examiners, 2024)	Tips were a major initial detection route in surveyed cases.	Preserve a route for assessing externally supplied information.	Public online disclosures were not separately evaluated.
Dong et al. (2018), empirical study	Financial social media informed a tested classification framework.	Social material can complement financial information.	Transfer to interpretive work and Indonesian cases is untested.
Vosoughi et al. (2018), empirical study	False news spread more extensively in the studied dataset.	Popularity cannot serve as independent verification.	No corruption-specific error rate follows.
KPK annual report (Komisi Pemberantasan Korupsi, 2024b)	Lifestyle attention was followed by asset declaration examination.	Specify ownership and declaration questions.	No independent reconstruction of platform-level causation.
KPK execution report (Komisi Pemberantasan Korupsi, 2024a)	The institution reported execution and state receipts.	Distinguish verified procedural outcomes from initial signals.	The report does not validate individual online allegations.

Source and basis	Documented observation	Analytical implication	Unresolved issue
Judicial communication (Prakoso, 2025) and register (Mahkamah Agung Republik Indonesia, 2025)	Appeal sanctions and a later cassation rejection are separately recorded.	Track stage, date, and monetary category.	No basis for attributing the outcome to online sentiment.

Source: Authors' synthesis, 2026.

Official case documents and verification questions

KPK's 2023 annual report describes attention to Mario Dandy's lifestyle and subsequent examination of Rafael Alun's LHKPN against conditions in the field (Komisi Pemberantasan Korupsi, 2024b). This is a documented institutional account connecting public visibility with an asset declaration inquiry. It supports a question about how a visible object can focus verification. It cannot establish post-level causation or reconstruct the full investigative chronology. The relevant interpretive inference is that asset visibility can help specify an inquiry when ownership and lawful funding remain open questions.

KPK's separate release of 28 August 2024 reported execution of Rafael Alun's case, a 14-year prison sentence, and approximately Rp40.5 billion deposited into the state treasury (Komisi Pemberantasan Korupsi, 2024a). That later report concerns formal enforcement and receipts. It cannot retrospectively authenticate every earlier lifestyle claim. Separating the two documents prevents hindsight from converting public suspicion into proven investigative knowledge. A valid asset inquiry would still need to identify the object, the relevant period, legal or beneficial ownership, and the documentary basis for any discrepancy.

The Supreme Court's judicial news service reported that the appeal court imposed 20 years' imprisonment on Harvey Moeis, a Rp1 billion fine, and Rp420 billion in replacement payment on 13 February 2025 (Prakoso, 2025). The latter amount is compensation or a replacement payment, not the fine. The cassation register for Decision 5009 K/Pid.Sus/2025 records rejection on 25 June 2025 (Mahkamah Agung Republik Indonesia, 2025). These records demonstrate why analysts should preserve the stage and legal category attached to a number before interpreting a circulating claim. The study uses the judicial communication and register entry; it does not claim a full analysis of the judgment's reasoning.

This second case provides evidence for documentary discipline rather than a finding about measured public trust. The records cannot establish community sentiment or an effect of online pressure on sentencing. Institutional trust is therefore retained as a proposed dimension for future netnographic inquiry. An empirical study could examine how participants interpret proportionality, but it would need

contemporaneous material, a defined sampling frame, and a chronology that separates public reaction from formal decisions.

Lifestyle and wealth incongruity

The first analytical dimension concerns how a visible object becomes an anchor for questions about wealth, public office, and disclosure. An image may be interpreted differently by participants familiar with an official's role, remuneration, or local status conventions. Netnographic interpretation can explain those contextual associations and the disagreements surrounding them. The forensic task then narrows the issue: which asset, held by whom, during which period, and compared with which declaration or financial record? A broad impression of extravagance is insufficiently specific for an asset finding.

The necessary counterinterpretations include lawful wealth, inheritance, borrowing, rental, promotional activity, incorrect dating, and misidentification. These possibilities should be written before an analyst requests verification, rather than added after the preferred explanation fails. A historical image should not be compared uncritically with a later declaration; a displayed asset should not be assigned automatically to the person appearing beside it. The practical contribution of this dimension is a more precise asset question, not a lifestyle-based proxy for criminality. A lead should close when the claimed discrepancy is resolved.

Informal disclosure and document circulation

The second-dimension concerns specific disclosures that appear outside an organization's formal reporting channels. A participant may identify a procurement package, document number, approval date, or contractor relationship. The conversational context can help distinguish a request for explanation from a claim of firsthand knowledge and reveal whether other participants correct or challenge it. An anonymous source can still supply a testable document identifier, but anonymity limits assessment of proximity and motive. A formal whistleblower relationship should never be inferred merely from the existence of a public post.

A useful lead separates the document's existence from the truth of the interpretation attached to it. An authentic contract can be misunderstood, and an apparently persuasive screenshot can omit decisive pages. Verification should seek the originating record, its version, relevant attachments, and the applicable transaction context. Analysts should avoid eliciting confidential disclosures publicly or encouraging retaliation against a presumed source. Where further contact is appropriate, the organization's authorized reporting arrangements should govern it. These controls are proposed for future application.

Institutional trust and accountability narratives

The third dimension asks how participants interpret an institution's conduct and explanation. Comments may concern the clarity of asset disclosure, consistency of enforcement, access to reporting channels, or perceived proportionality of sanctions. These concerns can matter operationally because an investigation may depend on cooperation and access to relevant information. However, distrust does not establish a financial irregularity, and supportive commentary does not rebut one. The analysis should identify the issue being contested and separate evidence about misconduct from perceptions of institutional legitimacy.

For organizations, the appropriate response may include clearer process explanations, a protected reporting route, or correction of a misleading financial figure. These are governance responses that can be considered even where no transaction allegation is substantiated. They should remain separate from decisions about culpability. Criticism should receive contextual assessment before either a communication or an investigative response. Public reporting should explain verified process facts without disclosing sensitive personal material or promising outcomes before examination is complete.

Narrative convergence and source independence

The fourth-dimension concerns recurrence across platforms, periods, and types of account. Repetition can identify a persistent issue deserving contextual analysis, but apparent convergence may result from copying one post or one institutional announcement. Analysts should trace the origin of each factual proposition and distinguish a new observation from a new presentation of existing material. Ten articles drawing on the same release do not constitute ten independent confirmations. Likewise, agreement among participants may reveal a shared interpretive frame without adding evidence about the underlying transaction.

A practical source map should record the original claim, subsequent citations or reposts, newly supplied documents, and corrections. Cross-platform variation may be analytically informative: satire, professional discussion, and news commentary can assign different meanings to the same event. Such differences justify interpretive attention without implying a measured network structure. This article uses narrative anchor to describe the object or claim organizing discussion. It does not use centrality, reach, coordinated behavior, or sentiment intensity as measured findings because the required platform data and analysis are absent.

Signal to verification framework

Table 5 translates the four dimensions into a proposed workflow. The sequence is iterative. Verification may change an interpretation, a new source may reveal dependence, and a negative case may close the lead. The analyst records revisions and closures. Escalation concerns the next justified investigative action; it is not a declaration that the allegation is true.

Table 5. Proposed workflow and decisions required at each stage

Stage	Required analytical output	Decision	Review control
Define scope and capture	Mandate, source, date, context, and minimal relevant material	Is collection necessary and authorized?	Record access basis and exclude irrelevant identifiers.
Interpret and classify	Contextual meaning and tentative analytical dimension	What specific proposition is being advanced?	Record ambiguity, satire, and alternative readings.

Stage	Required analytical output	Decision	Review control
Test specificity	Identified asset, transaction, document, control, or event	Can a lawful and proportionate test be specified?	Close vague claims or retain only a justified monitoring note.
Assess provenance	Origin, dependence, contradictions, and time sequence	Does further examination have a defensible basis?	A second reviewer checks source dependence and counterevidence.
Verify and preserve	Results of documentary tests and preservation details	Is the claim supported, unresolved, or contradicted?	Apply access, integrity, and custody procedures as relevant.
Report and review	Current status, reasons, owner, and next action	Close, correct, seek more records, or refer?	Separate analytical conclusions from legal determinations.

Source: Authors' synthesis, 2026

Priority should be determined through a reasoned decision, not an unvalidated fraud score. A specific procurement identifier with a relevant contradiction may justify limited record retrieval even if it receives little attention. A widely repeated allegation without an identifiable proposition may justify no further investigative action. Preservation urgency can warrant prompt action when relevant material may disappear, but it does not itself increase the claim's credibility. The manager should record the scope, likely cost, and expected value of the next test so that resource allocation remains reviewable.

Electronic material requires appropriate handling at the point of collection and whenever it is transferred. NIST SP 800-86 provides an established account of integrating forensic techniques into incident response, with an IT rather than a universal law-enforcement scope (Kent et al., 2006). Horsman's discussion of digital evidence principles likewise emphasizes the importance of scrutinizing evidential practice (Horsman, 2020). The organizational adaptation proposed here records collection method, time zone, tool, integrity checks where applicable, access, transformations, and transfers. A hash can support integrity assessment; it cannot prove that the original content was truthful or that an account belonged to a particular person.

Digital Discourse Lead Register

The Digital Discourse Lead Register is the framework's operational output. Table 6 groups its fields by function to keep the instrument readable. In use, each lead has a unique identifier and links to authorized supporting records. The register records reasons and controlled references to supporting material. Access to a lead register does not confer access to the underlying bank, tax, personnel, or platform records; those permissions require separate authorization.

Table 6. Required fields in the proposed lead register

Field group	Minimum information	Purpose
Observation and provenance	Lead ID, source location, observation time and time zone, originating source, access basis	Reconstruct what was available at the decision date.
Interpretation	Claim, conversational context, analytical dimension, ambiguity	Separate observed material from the analyst's inference.
Verification question	Specific asset, document, transaction, event, and relevant period	Define what the next test could establish.
Challenge and corroboration	Alternative explanation, contradictory material, source dependence, independent support	Prevent repetition or theoretical fit from becoming confirmation.
Decision and accountability	Status, reason, analyst, reviewer, responsible unit, review date	Make escalation, correction, and closure reviewable.
Preservation and protection	Supporting record reference, collection method, integrity and transfer records, access and retention limits	Support controlled handling and later examination.

Source: Authors' synthesis, 2026

For example, a hypothetical entry H-01 could record a public claim that a vehicle was omitted from an official's declaration. The test concerns registration, beneficial ownership, the declaration period, and lawful funding. Borrowing or incorrect dating are competing explanations. Until the relevant records are checked, the entry remains an unverified lead. If registration and contextual records resolve the apparent discrepancy, the reason for closure is recorded. This example describes no actual person and should not be confused with a coded observation from the two proceedings.

Theoretical and professional implications

The theoretical contribution is to distinguish the social construction of suspicion from verification of the alleged conduct. Fraud theory helps identify a possible mechanism; netnographic interpretation explains why participants regard a claim as meaningful; forensic accounting specifies the evidence needed to evaluate the mechanism. These operations can inform one another without becoming equivalent. The distinction also clarifies the framework's unit of contribution: a better-specified question and an accountable decision about how to test it.

This integration addresses a weakness in applying fraud theories to visible behavior. If an analyst labels luxury consumption as arrogance and then treats arrogance as proof of fraud, the reasoning becomes circular. Requiring an ownership, funding, or control test interrupts that circle. Similarly, a discourse about collusion should lead to a relationship and transaction question rather than a presumed network. Critical use of theory thus includes deciding when a concept adds no explanatory value. A blank or uncertain classification can be more informative than a complete checklist built from weak material.

The framework also changes what should count as a useful result of preliminary analysis. A rejected allegation, a corrected amount, or a finding that several sources have one origin can reduce wasted work. Counting only escalations would reward overinterpretation. Professional value should instead be assessed through the relevance of new information, the quality of documentary tests, the clarity of decisions, and the avoidance of unsupported adverse action. These criteria require testing.

For public institutions, the framework can connect public concerns with existing asset disclosure, complaint handling, and internal control processes. An asset question may belong with a competent disclosure unit, a procurement question with an audit team, and an authenticity question with a digital examiner. Referral should follow the issue and the unit's competence. Defined referral responsibilities can preserve continuity while avoiding the circulation of unnecessary personal information across departments.

For companies and audit practices, the contribution concerns engagement planning and inquiry design. A contextual lead might identify a related-party question, a recurring supplier complaint, or an unexplained change in an approval process. Its place in an engagement depends on mandate, materiality, lawful access, and the client's or investigating authority's procedures. The framework does not expand an accountant's legal powers. It supplies a reasoned basis for requesting an authorized examination and documenting why a particular source was considered relevant.

The implications for accountability extend beyond identifying misconduct. Institutions can learn where public explanations repeatedly confuse financial or procedural categories and where formal reporting routes appear inaccessible. However, the information should not be used to equate dissent with risk or to monitor individuals without a defined purpose. The same interpretive sensitivity that helps explain a complaint should constrain collection and reporting. An organization's ability to justify its own investigative decisions is part of the framework's professional value.

Organizational implementation and responsibilities

Implementation should begin with a limited pilot linked to an existing investigative mandate. The organization defines the types of issue covered, public sources permitted, collection limits, retention rules, and referral authority. An initial pilot could focus on document-specific procurement complaints rather than open-ended monitoring of employees. Restricting the question allows managers to compare the information gained with analyst time and privacy exposure. Expansion should

follow evidence of useful, proportionate results rather than the volume of material collected.

Responsibility must remain explicit. A contextual analyst documents meaning and provenance; a forensic accountant formulates and conducts financial tests; a digital examiner handles acquisition questions requiring specialist expertise. Legal and privacy staff assess access and disclosure issues, while a case owner approves the next investigative step. The audit committee or an equivalent independent body should receive material concerns when operational managers have a conflict. Smaller teams may combine roles while retaining independent review.

Competence is a practical constraint. Accounting expertise does not automatically provide knowledge of platform conventions, sarcasm, local language, or subcultural meaning. Conversely, skill in interpreting online discussion does not establish competence to trace assets or evaluate a financial loss. Training should use ambiguous and disconfirming examples, require analysts to distinguish copies from independent sources, and examine how their professional expectations influence interpretation. Specialist consultation is appropriate when a contextual conclusion depends on unfamiliar language or community practice.

Technology should support a defined inquiry. An approved repository can record source references, collection events, permissions, and decisions, while access controls limit exposure of sensitive supporting material. Integration with case management should preserve version history and distinguish leads from evidence records. Automatic collection or classification may reduce handling effort, but each tool introduces assumptions about access, completeness, and meaning. The organization should assess those assumptions before relying on outputs. Dashboard labels must express a claim's current status accurately.

Implementation challenges and responses

Organizational resistance can arise when a lead concerns senior decision-makers, a valuable supplier, or the unit responsible for handling complaints. Without independent review, contextual analysis can be suppressed or used selectively against less powerful actors. The proposed response is a documented referral route, conflict declarations, and review of both closed and escalated leads. Senior support should protect the process while leaving substantive conclusions open to challenge. Table 7 summarizes other constraints and the operational responses proposed by this study.

Table 7. Implementation constraints and proposed organizational responses

Constraint	Consequence for inquiry	Proposed response and review focus
Skills and language gaps	Satire, status conventions, or technical claims are misread.	Use contextual expertise and supervised training; review ambiguous interpretations.
Limited time and resources	Viral issues displace specific, lower-visibility leads.	Limit scope and time; examine usefulness per analyst hour.

Constraint	Consequence for inquiry	Proposed response and review focus
Fragmented records and access	Leads cannot be matched to authorized financial records.	Assign an owner and lawful request route; record unresolved access barriers.
Hierarchy and conflicts	Sensitive leads are suppressed or selectively escalated.	Provide independent referral and conflict review; sample closure decisions.
Privacy and retaliation	Collection exposes ordinary users or suspected informants.	Minimize identifiers and restrict access; assess disclosure and retaliation risks.
Manipulation and source dependence	Copied or fabricated material appears corroborated.	Trace origins and examine contradictory records before escalation.
Deletion and platform change	Context and provenance become incomplete.	Use proportionate preservation and record collection gaps explicitly.

Source: Authors' synthesis, 2026.

Resource constraints require more than a general call for training or technology. Each lead should have a bounded initial test and a review point. If the relevant document cannot be obtained lawfully or the factual claim remains too vague, the case owner records that limit and decides whether further work is justified. This prevents an indefinite monitoring burden. Smaller organizations may need external specialist support for selected tasks, but they still require an internal owner accountable for purpose, access, and the final decision.

Protection of complainants and ordinary users must also affect workflow design. Removing a handle may not sufficiently anonymize a distinctive quotation that can be searched online. Reports should paraphrase nonessential wording, omit irrelevant personal detail, and restrict links to original material where identification would create avoidable harm. At the same time, authorized underlying records must preserve enough context for review. Differentiated access should protect both provenance and confidentiality.

Platform changes create an additional implementation problem. Search results can be personalized; posts can be edited; account names and visibility can change; and a screenshot can omit surrounding replies. Collection records should state the conditions under which material was seen and what could not be retrieved. Missing content should remain missing rather than being reconstructed as fact from repeated descriptions. Where authenticity is material to a formal inquiry, the case should be referred for appropriate acquisition and examination within the applicable authority.

Evaluation and future empirical research

A future field study should test whether contextual interpretation improves investigative planning compared with existing practice. One design would compare conventional OSINT and documentary triage with the same process supplemented by

netnographic interpretation, using matched tasks and a predefined time budget. Reviewers assessing the resulting leads should be unaware of the method used where feasible. Including low-visibility complaints and cases closed without findings would reduce success bias.

The protocol should define a lead, independent corroboration, a useful new item, and an unsupported escalation before analysis begins. Relevant measures include the proportion of tested leads corroborated, the number of nonduplicate actionable leads, analyst time, time to a justified decision, and the number of corrections or harmful disclosures. A corroboration rate must identify its denominator and distinguish unresolved cases from disproved claims. These measures could reveal whether contextual interpretation adds information, merely repackages existing sources, or increases workload without a corresponding benefit.

Chronology is essential to any early-warning claim. Researchers should retain the date a digital signal was available, the date analysts first recorded it, and the dates of formal investigative milestones. Analysis based only on posts selected after an official announcement cannot establish advance warning. A prospective study could assess whether a specific lead preceded an authorized investigation and whether it supplied information not already available internally. Even temporal precedence would not, by itself, establish that netnography caused improved detection.

For the netnographic component, future researchers should define platforms, community boundaries, observation periods, engagement level, and sampling rules. They should retain contextual fieldnotes and examine negative cases and researcher positioning. Independent analyst comparison can identify disputed readings and improve an operational codebook, while reflexive discussion explains why differences arose. A numerical agreement statistic, if used, should match the coding task and should not be presented as a substitute for contextual depth or evidential validity.

Study limitations and scope of transfer

The source set is purposive, the case-document sample is small, and several scholarly claims are assessed through accessible publisher or institutional summaries rather than reanalysis of original data. The study cannot estimate detection performance, establish the prevalence of the four dimensions, or infer what particular online communities believed. Official records are used for their stated content and procedural role, not as comprehensive accounts of every event. Platform-level meaning remains untested.

Transfer to another organization requires attention to its reporting arrangements, record access, language, platform use, and legal setting. Benefits cannot be presumed from these prominent examples. The article's defensible contribution is a transparent integration procedure with an explicit evaluation agenda. Future empirical work should be able to revise, narrow, or reject its components when the costs, error patterns, or organizational consequences do not justify their use.

CONCLUSION

The main contribution of this study is a traceable procedure for translating contextual interpretation of online claims into specific forensic verification tasks. For RQ1, the synthesis identifies four analytical dimensions and explains their different

uses: lifestyle and wealth questions, specific informal disclosures, institutional accountability concerns, and recurring narratives. Published studies establish the potential relevance and reliability problems of social information, while the official case documents demonstrate the importance of asset examination, procedural chronology, and accurate financial categories. The framework combines those insights without treating the proposed dimensions as validated detection variables.

For RQ2, the workflow requires a lawful purpose, a specific proposition, source provenance, competing explanations, appropriate documentary tests, and recorded review decisions. The Digital Discourse Lead Register makes these requirements operational. Organizational application depends on competence, independent oversight, access to verification records, proportionate preservation, and protection against unnecessary disclosure. Useful outcomes include well-founded escalation, correction, and justified closure.

The article advances method integration by making the transition between interpretation and verification explicit and reviewable. It does not demonstrate that netnography improves detection accuracy or investigative speed. That question requires prospective comparison with existing practice, attention to source independence and chronology, and reporting of unsuccessful as well as successful leads. The framework provides a defined basis for that evaluation and a practical specification that organizations can test within an authorized pilot.

REFERENCES

Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf

Bartl, M., Kannan, V. K., & Stockinger, H. (2016). A review and analysis of literature on netnography research. *International Journal of Technology Marketing, 11*(2), 165–196. https://doi.org/10.1504/IJTMKT.2016.075687

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Dong, W., Liao, S., & Zhang, Z. (2018). Leveraging financial social media data for corporate fraud detection. *Journal of Management Information Systems, 35*(2), 461–487. https://doi.org/10.1080/07421222.2018.1451954

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. *Communications of the ACM, 59*(7), 96–104. https://doi.org/10.1145/2818717

Franzke, A. S., Bechmann, A., Zimmer, M., Ess, C. M., & Association of Internet Researchers. (2020). *Internet research: Ethical guidelines 3.0*. https://aoir.org/reports/ethics3.pdf

Free, C. (2015). Looking through the fraud triangle: A review and call for new directions. *Meditari Accountancy Research, 23*(2), 175–196. https://doi.org/10.1108/MEDAR-02-2015-0009

Horsman, G. (2020). ACPO principles for digital evidence: Time for an update? *Forensic Science International: Reports, 2*, Article 100076. https://doi.org/10.1016/j.fsir.2020.100076

Hsieh, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research, 15*(9), 1277–1288. https://doi.org/10.1177/1049732305276687

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response* (NIST Special Publication 800-86). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86

Komisi Pemberantasan Korupsi. (2024a, August 28). *Eksekusi perkara Rafael Alun, KPK setorkan Rp40 miliar ke kas negara*. https://www.kpk.go.id/id/ruang-informasi/berita/eksekusi-perkara-rafael-alun-kpk-setorkan-rp-40-miliar-ke-kas-negara-2

Komisi Pemberantasan Korupsi. (2024b). *Laporan tahunan KPK 2023*. https://cms.kpk.go.id/storage/4200/Laporan-Tahunan-KPK-2023.pdf

Kozinets, R. V. (2002). The field behind the screen: Using netnography for marketing research in online communities. *Journal of Marketing Research, 39*(1), 61–72. https://doi.org/10.1509/jmkr.39.1.61.18935

Kozinets, R. V., & Gretzel, U. (2024). Netnography evolved: New contexts, scope, procedures and sensibilities. *Annals of Tourism Research, 104*, Article 103693. https://doi.org/10.1016/j.annals.2023.103693

Mahkamah Agung Republik Indonesia. (2025, June 25). *Putusan Mahkamah Agung Nomor 5009 K/Pid.Sus/2025* [Decision register]. https://putusan3.mahkamahagung.go.id/direktori/putusan/zaf0937ad1a3239ea2b7313130303136.html

Murthy, D. (2008). Digital ethnography: An examination of the use of new technologies for social research. *Sociology, 42*(5), 837–855. https://doi.org/10.1177/0038038508094565

Pang, B., & Lee, L. (2008). Opinion mining and sentiment analysis. *Foundations and Trends in Information Retrieval, 2*(1–2), 1–135. https://doi.org/10.1561/1500000011

Pastor-Galindo, J., Nespoli, P., Mármol, F. G., & Pérez, G. M. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *IEEE Access, 8*, 10282–10304. https://doi.org/10.1109/ACCESS.2020.2965257

Prakoso, A. (2025, February 13). *Tok, Majelis Hakim Banding PT Jakarta perberat hukuman Harvey Moeis*. MARINews, Mahkamah Agung Republik Indonesia. https://marinews.mahkamahagung.go.id/berita/pt-jakarta-perberat-hukuman-harvey-moeis-0bt

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Transparency International Indonesia. (2025, February 11). *Indeks persepsi korupsi 2024: Korupsi, demokrasi dan krisis lingkungan*. https://ti.or.id/indeks-persepsi-korupsi-2024-korupsi-demokrasi-dan-krisis-lingkungan-2/

Trompeter, G., Carpenter, T., Desai, N., Jones, K., & Riley, R. (2013). A synthesis of fraud-related research. *Auditing: A Journal of Practice & Theory, 32*(Supplement 1), 287–321. https://doi.org/10.2308/ajpt-50360

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science, 359*(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

Vousinas, G. L. (2019). Advancing theory of fraud: The S.C.O.R.E. model. *Journal of Financial Crime, 26*(1), 372–381. https://doi.org/10.1108/JFC-12-2017-0128