MOBILE AND FORENSICS
Vol. 8, No. 2, 2026, pp. 127-142 | DOI: 10.12928/mf.v8i2.15926
ISSN: 2714-6685 (Online)
ISSN: 2656-6257 (Print)

Artefact-to-Legal Element Mapping in iOS-Based Web Gambling Cases: A Cross-Source Correlation Framework under KUHP and ITE Law

Sudirman [a,1,*], **Yudi Prayudi** [a,2]

[a] Universitas Islam Indonesia, Yogyakarta, Indonesia
[1] sudirmankamaruddin.07@gmail.com*; [2] prayudi@uii.ac.id

* Corresponding Author

ARTICLE INFO

ARTICLE HISTORY

Received: Mar 02, 2026
Revised: Jul 12, 2026
Accepted: Jul 19, 2026

KEYWORDS

Digital Forensics, Online Gambling, iOS Artefacts, Magnet AXIOM, Law

ABSTRACT

The widespread use of web-based online gambling through mobile browsers and instant messaging applications has made digital traces increasingly difficult to interpret as legally admissible evidence. Previous forensic research primarily concentrated on artefact recovery from dedicated gambling applications, leaving limited attention to systematic approaches for associating web-based traces with legal elements. This study examined the identification, classification, and legal mapping of web-based gambling artefacts using the proposed Artefact-to-Legal Element Mapping Framework (ALMF). A real-case evidence set acquired from an Apple iPhone XR was analysed with Magnet AXIOM Process v9.4.0.44917, generating Quick Image and Decrypted evidence for extraction and correlation. The analysis identified four major artefact categories, including web browsing traces, credential and persistence artefacts, WhatsApp communication records, and visual media files. Browser artefacts reflected intentional discovery and access to gambling websites, whereas credential artefacts indicated recurring or sustained access. WhatsApp conversations provided the strongest evidence of promotional activities through shared links, invitations, and dissemination patterns. Visual artefacts further strengthened the gambling context by revealing website interfaces and financial indicators. Cross-source correlation differentiated player activities from promoter or distributor behaviour. The mapped evidence supported KUHP Article 303 and UU ITE Article 27(2). The findings demonstrated that contextual interpretation across multiple artefact sources produced stronger evidential value than analysing individual artefacts separately.

1. INTRODUCTION

Digital technology has gradually but decisively reshaped the landscape of crime: actions that once required physical space have increasingly taken place discreetly through mobile screens, moved rapidly, and left traces that were not always straightforward to interpret. Gambling has been a crime that has undergone a clear shift in modus operandi, from conventional practices to network-based activities that often “disguise” themselves behind digital game mechanics that appear ordinary to casual users. In web-based gambling games, gambling elements were frequently embedded through

features such as betting, slot-style gameplay, or economically valued reward systems, making the activity resemble a typical game while, in fact, involving wagering that met the characteristics of gambling [1], [2], [3]. This condition meant that proof could not rely on mere suspicion; it required a structured way to explain what happened, what traces remained, and how those traces related to the construction of the offence [4].

In Indonesia, the prohibition of gambling has been regulated explicitly through Article 303 of the Criminal Code (KUHP), while its digital dimension has been reinforced through Article 27(2) of the ITE Law, which targets the distribution/transmission of gambling content through electronic systems [5], [6], [7], [8]. However, in enforcement practice, the persistent challenge often lay not in the absence of legal norms, but in the "bridge" connecting those norms to digital reality: investigators needed to demonstrate a concrete chain of conduct ranging from intent, access, and involvement to the offender's role through relevant digital artefacts. This difficulty became especially visible in website-based cases, because most activity occurred at the browser layer (search, history, tab sessions, cookies/tokens), while the expansion of access frequently shifted to instant communication platforms such as WhatsApp, where link sharing and persuasive invitations became a central part of the criminal conduct pattern [9], [10], [11]. At this point, artefacts were no longer merely "residual data", but fragments of events that had to be arranged into a coherent evidentiary narrative [6], [12], [13].

Accordingly, legal admissibility became a key issue. The ITE Law provided a foundation for electronic information/documents to function as lawful evidence, yet admissibility still depended on requirements such as accessibility, presentability, integrity assurance, and the ability to validate the evidence [14]. This meant that digital forensic processes needed to demonstrate that evidence was collected and analysed without compromising its integrity, using documented, measurable steps aligned with recognised standards. Recent reproducible workflows have highlighted the value of integrity-preserving acquisition and processing, e.g., generating cryptographic hashes and maintaining transparent pipelines to strengthen evidentiary defensibility in practice [15]. In this context, international standards such as ISO/IEC 27037:2012 (handling and preservation of digital evidence) and NIST SP 800-86 (a digital forensic investigation framework from collection to reporting) served as foundations to ensure that evidence moved from device to report without losing authenticity or context [5], [16], [17]. Such integration was essential because, in online gambling cases, the artefacts required for proof were often distributed across sources: some existed in browser artefacts, while others appeared in communication applications, visual media, and stored credentials.

This study emerged from that need: to develop a systematic perspective that linked the characteristics of digital artefacts to the elements of the offence, so that technical (forensic) interpretation did not run separately from juridical interpretation (legal construction). Beyond technical extraction, recent work on LLM-assisted forensics has argued that investigative outputs must be guided by a disciplined reasoning framework, so that conclusions remain structured, reviewable, and legally accountable [18]. Operationally, the study employed a real-case digital forensic investigation scenario involving a web-based online gambling game, with evidence in the form of an iOS device image (Apple iPhone XR) processed using Magnet AXIOM Process version 9.4.0.44917, including the "Apple iPhone XR Quick Image" and "Apple iPhone XR Quick Image – Decrypted" files as the basis for artefact tracing [16]. Therefore, the focus went beyond "artefact findings" alone: the artefacts were classified, interpreted as an activity sequence, and then mapped to offence elements under KUHP Article 303 and ITE Law Article 27(2) to assess their evidentiary relevance in an investigative context [19].

The main contribution of this study was to offer a framework that enabled digital artefacts to "speak" in the language of proof. For web-based online gambling cases, the study treated artefacts as an integrated evidence package: search and history could indicate intent and access [20]; tab sessions and browser traces could strengthen indications of involvement; visual media (e.g., gameplay screenshots) could clarify context; and communication artefacts particularly WhatsApp messages could demonstrate link distribution and invitations that were legally relevant to the construction of the offence [9], [16], [21], [22]. When such a package was assembled in sequence, the relationship among conduct, role (player versus promoter), and statutory elements became clearer, and the forensic report could be read not merely as technical output but as a stronger evidentiary document.

Existing studies on digital forensics in online gambling cases have identified key investigative challenges, particularly in the extraction and presentation of relevant digital evidence under

Indonesian criminal law [23]. However, prior work has predominantly focused on individual extraction procedures or isolated artefact types, without providing a structured framework that systematically maps artefact categories to specific statutory elements for legal admissibility purposes. Furthermore, the role-based differentiation between a player's personal access behavior and a promoter's distribution conduct a distinction that is critical to the construction of offences under both KUHP Article 303 and ITE Law Article 27(2) remains underdressed in the existing forensic literature. This study addresses that gap by proposing the Artefact-to-Legal Element Mapping Framework (ALMF), which bridges forensic artefact categories (browser traces, credential artefacts, WhatsApp communication, and visual media) with the specific statutory elements of the relevant criminal provisions, including explicit role-based interpretation. Unlike prior approaches that treat artefact extraction as an end in itself, ALMF functions as a bridge between technical forensic outputs and juridical reasoning, enabling investigators to construct an evidence package that speaks directly to the elements of the offence rather than presenting data in isolation.

This study addressed the following research questions: 1) How can relevant digital artefacts of web-based online gambling activity be identified and classified from iOS mobile evidence? 2) How can the extracted artefacts be mapped to the statutory elements under KUHP Article 303 and ITE Law Article 27(2) to support role-based interpretation (player vs promoter)?

This paper makes three contributions, 1) It proposes an Artefact-to-Legal Element Mapping Framework (ALMF) that links artefact categories (browser, credentials/persistence, WhatsApp communication, and visual media) to offence elements under KUHP Article 303 and ITE Law Article 27(2), including explicit separation of player vs promoter roles; 2) It formalizes cross-source correlation rules that connect WhatsApp link sharing to corresponding browser access traces and visual confirmation of gambling context, enabling an evidence package rather than isolated findings; 3) It reports an iOS case-study pattern showing that WhatsApp and visual artefacts tend to provide the most explicit indicators for promotion and gambling-object context, while browser traces primarily anchor intent and initial access, offering transferable insights for similar website-based gambling investigations.

2. METHOD

This study adopted a case-study approach centered on web-based online gambling activity accessed through a mobile device. The approach was selected because website-driven gambling typically leaves traces scattered across multiple sources: browser artefacts, authentication residues, instant-messaging exchanges, and visual media that only become meaningful when read as a connected sequence of actions rather than isolated data fragments. With this design, the analysis pursued two primary outcomes: (1) identifying and classifying the digital artefacts most relevant to online gambling behaviour, and (2) mapping those artefacts to the constituent elements of criminal liability under the Indonesian Criminal Code (KUHP) and the ITE Law.

2.1. Study Design

Fig. 1 summarized the study workflow, moving from defining the case scenario and processing the digital evidence to extracting and classifying artefacts, and ultimately mapping them to the relevant statutory elements. The workflow was deliberately kept linear and well-documented so readers could locate each artefact within the broader process and see how technical findings were carried forward into legally meaningful interpretations.

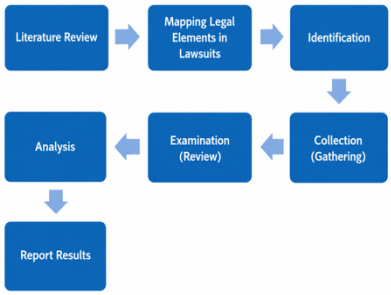

Fig. 1. Research flow chart

2.2. Case Scenario and Digital Evidence

The case scenario reflected a typical user-facing pathway of web-based online gambling. Operationally, player activity could be understood as a sequence of stages account registration → deposit → gameplay → withdrawal with minor variations depending on the order of steps or the communication channel involved. This flow mattered because each stage tended to generate different traces: search and browsing history commonly appeared during initial access, authentication/persistence artefacts emerged during registration and login, while communication and visual media often strengthened context during promotion, transactions, or activity documentation.

The digital evidence analyzed in this study originated from an iOS mobile device (Apple iPhone XR) and consisted of two evidence items: a device image (quick image) and a decrypted image (decrypted). All evidence was processed using Magnet AXIOM Process v9.4.0.44917 in a mobile forensics context.

2.3. Evidence Acquisition and Integrity Verification

The integrity of the evidence item was verified through cryptographic hashing prior to examination. The recorded hash values are as follows: MD5 (Quick Image) and SHA-256 (Quick Image). The evidence was received in sealed condition and processed within a controlled forensic workstation environment without any modification to the source image. All examinations were conducted using parsed outputs generated by AXIOM, thereby preserving the integrity of the original source throughout the analysis process as show in Fig. 2.

Fig. 2. Sequential flow of player activities in a web-based online gambling game, from link discovery and website access to registration/login, deposit, gameplay, and withdrawal.

As shown in Fig. 2, that player activity did not unfold as a single, discrete act, but rather as a chain of interconnected stages. Each stage tended to produce a different kind of trace: link discovery and site access were typically reflected in search artefacts and browser history, registration and login were associated with authentication or access-persistence artefacts such as tokens and stored credentials, while gameplay and withdrawal were often reinforced by visual media artefacts (e.g., screenshots) or repeated access-session traces. This activity-flow framework was then used to guide the subsequent artefact classification strategy and the mapping of artefacts to statutory elements.

2.4. Digital Forensic Procedure (NIST-aligned)

The digital forensic procedure in this study was aligned with the NIST SP 800-86 framework, which structured forensic investigations into four primary phases: Collection, Examination, Analysis, and Reporting. This framework was used to preserve evidence integrity, ensure process traceability, and reduce interpretive bias by clearly separating artefact extraction from contextual interpretation. The implementation of each phase in this study was described as follows:

first, the Collection phase. This phase focused on preparing the data source in the form of a forensic image as the basis for analysis. The evidence was handled in a way that enabled examination without modifying the source data, thereby preserving integrity from the outset.

Second, Examination. At this stage, the evidence was processed using Magnet AXIOM to perform parsing, indexing, and artefact extraction. The extracted outputs were then filtered to keep the examination focused on artefacts most relevant to web-based online gambling activity, particularly access/search traces, authentication or access-persistence artefacts, communication artefacts, and

visual media. Artefacts were retained if they met at least one of the following criteria: (1) a direct keyword or URL association with known gambling platforms; (2) temporal proximity to identified gambling access events; or (3) content explicitly referencing gambling mechanisms, monetary transactions, or platform invitations.

Third, Analysis. The analysis phase was conducted by correlating artefacts across sources based on context, including artefact type, content, timestamps where available, and linkages between artefacts (for example, the relationship between a link shared in a conversation and corresponding access traces in the browser, or visual media that reinforced the gambling context). This correlation was essential to ensure that the findings were not interpreted as isolated data fragments, but as a coherent sequence of activity consistent with the player flow.

Fourth, Reporting. The reporting phase presented the findings through narrative description, results tables, and verifiable visual evidence. Rather than treating artefacts as mere technical outputs, the reporting framed them in terms of conduct and evidentiary function, so they could serve as a basis for mapping statutory elements under the KUHP and the ITE Law.

As shown in Fig. 3, the study's results were not taken directly from tool outputs; they were derived through two critical steps filtering during the examination phase and cross-source correlation during the analysis phase so that the discussed artefacts remained relevant to the conduct scenario and defensible methodologically.

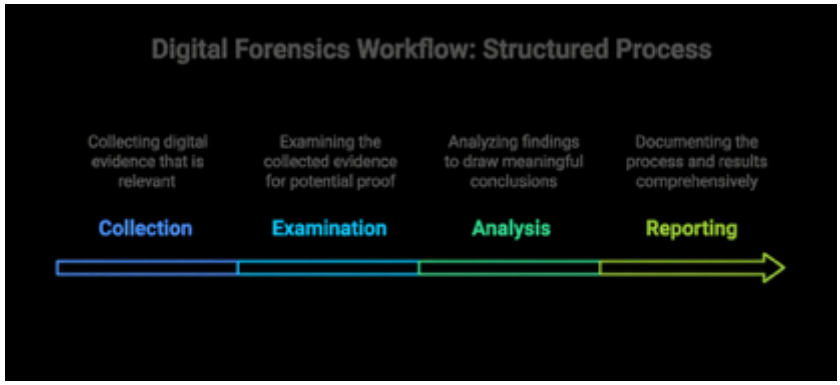

Fig. 3. Digital Forensic Workflow

2.5. Proposed Framework (ALMF)

While the NIST SP 800-86 phases ensured a traceable and integrity-preserving forensic procedure, this study additionally applied an Artefact-to-Legal Element Mapping Framework (ALMF) to turn extracted artefacts into legally interpretable evidence. ALMF structured the workflow from artefact categorization and cross-source correlation to role inference (player vs promoter) and statutory element mapping under KUHP Article 303 and ITE Law Article 27(2), so that the results were presented as an evidence package rather than isolated tool outputs.

As illustrated in Fig. 4, ALMF started from the set of artefacts extracted by AXIOM and organised them into four operational categories: browser traces (search/history/session indicators), credentials or access-persistence artefacts (tokens, passwords, keychain entries), messaging artefacts (WhatsApp chats/messages/contacts), and visual media (screenshots and related metadata). The framework then applied cross-source correlation to connect artefacts describing the same event chain, most notably by matching URLs and keywords across sources and, where timestamps were available, aligning records temporally to link a shared message to subsequent browser access and visual confirmation. Based on the correlated package, ALMF performed role inference by distinguishing patterns consistent with personal participation (player) versus promotion or access enabling (promoter), for example when link-sharing and call-to-action instructions appeared in conversations and were reinforced by corresponding access traces. Finally, the correlated and role-tagged artefacts were mapped to the relevant statutory elements under KUHP Article 303 and ITE Law Article 27(2), producing three concrete outputs: an evidence package, a filled element-mapping table, and a role-based comparison that supported legal interpretation.

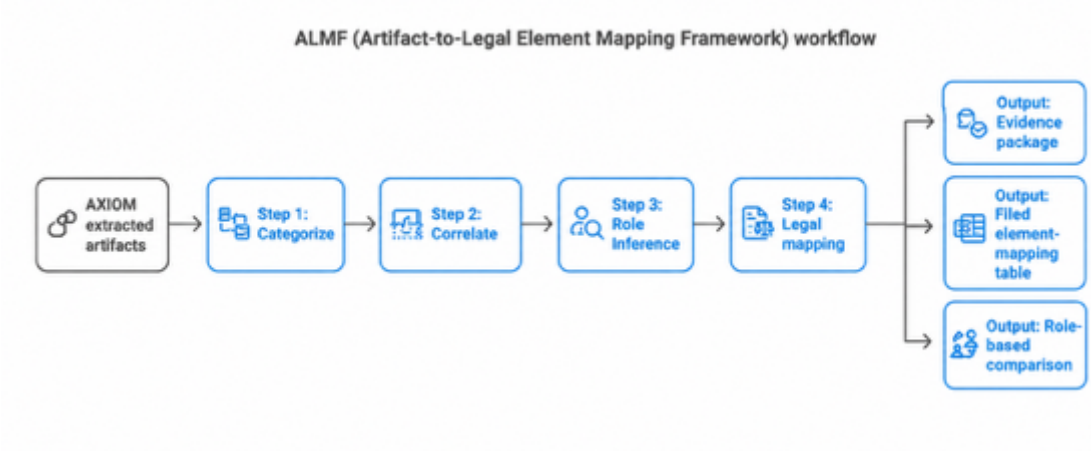

Fig. 4. Proposed Framework (ALMF)

The ALMF workflow can be formalised as follows. Starting from the raw artefact set extracted using Magnet AXIOM, each artefact was initially assigned to one of four categories Browser, Credential, Messaging, or Visual with its type, content, timestamp, and source recorded as core attributes. Cross-source correlation was subsequently performed by identifying artefact pairs that shared common domain names, brand keywords, or URL fragments, and grouping these matches into a correlation set. Where timestamps were available, the temporal sequence of the correlated artefacts was validated to confirm the logical ordering of events and to flag any inconsistencies for manual review.

Following correlation, role inference was conducted based on the resulting artefact set. Artefacts containing outbound links and call-to-action phrases within messaging channels were classified under the promoter role within the scope of UU ITE Article 27(2), whereas artefacts reflecting only personal access and gameplay activities were classified under the player role within the scope of KUHP Article 303. Finally, each correlated and role-tagged artefact package was mapped against the relevant statutory elements' intent, conduct, object, and purpose, thereby producing three principal outputs: an evidence package summary, a completed element-mapping table, and a role-based comparison to support legal interpretation.

2.6. Artifact Extraction and Classification

Artefacts were extracted through Magnet AXIOM processing and then classified according to their relevance to web-based online gambling activity. The classification was used to keep the analysis focused on artefacts that contributed to the reconstruction of the underlying conduct, including access/search traces (browser), authentication or access-persistence traces (tokens/credentials), communication and link-distribution traces (WhatsApp), and visual context traces (media). The resulting classification was presented in the Results and Discussion section as an artefact summary and category-based analysis.

2.7. Legal Mapping

The legal mapping was carried out by linking the extracted artefacts to the relevant offence elements under the KUHP and the ITE Law. The mapping was developed by interpreting the conduct context (grounded in the player flow) and correlating artefacts across sources to assess element fulfilment, particularly with respect to intent, conduct, object, and purpose. The mapping results were presented in the Results and Discussion section as a completed element-mapping table, alongside a role-based discussion distinguishing player and promoter behavior.

3. RESULTS AND DISCUSSION

This section presented the digital artefacts extracted from the mobile evidence using Magnet AXIOM and discussed them as activity traces that reflected two key dimensions in web-based online gambling cases: (1) access and involvement as a player, and (2) link distribution and persuasive invitations that indicated a promotion/access-enabling role. With this focus, the discussion did not emphasise the sheer volume of collected artefacts; instead, it centred on which artefacts “spoke” most clearly in explaining the nature of online gambling activity and its relevance to the legal construction under the KUHP and the ITE Law.

3.1. Digital Artefact Findings from AXIOM Forensics

AXIOM processing showed that traces of online gambling activity on the iOS device emerged as a combined set of browser artefacts, credential/access-persistence artefacts, WhatsApp communication artefacts, and visual media. This distribution was important because web-based gambling typically did not leave artefacts resembling a dedicated "gambling application" as seen in native apps; instead, the activity was embedded in web usage (Safari) and often migrated into instant messaging for link promotion and circulation.

Fig. 5, provided concise context for the AXIOM outputs and served as an entry point for reading the findings as an evidentiary landscape. Rather than treating the tool output as an end in itself, the analysis in this paper focused on the artefact categories most informative for reconstructing web-based online gambling activity, namely search/access traces, visual-context evidence, and conversations indicating link distribution.

Fig. 5. AXIOM evidence overview– excerpt from report

Table 1 summarized the extracted artefacts quantitatively and revealed a distinctive pattern: purely "history-based" browser traces contributed only a small share of the total, whereas visual media and WhatsApp communication dominated. Visual artefacts (Pictures, Photos Media Information, and Videos) accounted for 62.65% of the records, while WhatsApp-related artefacts contributed 32.09%, indicating that the richest contextual evidence was carried by screenshots and messaging traces rather than extended browsing histories. This distribution was consistent with website-based gambling behaviour, where access could occur quickly and may not generate long history trails, while promotional exchanges and visual documentation often preserved the clearest context for evidentiary interpretation.

Table 1. Distribution of relevant AXIOM-extracted artefacts from the examined evidence

Artefact type (AXIOM)	Count	%
Pictures	812	59.36
WhatsApp Messages (iOS)	435	31.80
Photos Media Information	44	3.22
Google Searches	36	2.63
Passwords and Tokens	25	1.83
Apple Keychain Internet Passwords	4	0.29
User Accounts	3	0.22
Safari History	2	0.15
Safari Suspended State Tabs	2	0.15
WhatsApp Chats (iOS)	2	0.15
WhatsApp Accounts Information (iOS)	1	0.07
WhatsApp Contacts (iOS)	1	0.07
Videos	1	0.07

3.2. Browser Traces: Google Search

The Google Searches artefact (36 records) served as an important marker because it showed an active effort to obtain access, whether through keyword queries, specific terms, or searches that led to relevant websites/links. The value of this finding lay not in the number of records, but in the direction of the searches that signalled intent, namely queries directly associated with target sites or commonly used terms for reaching online gambling services.

Fig. 6 shows that search artefacts preserved sufficient context to build a narrative of "how access began", because they contained the search terms used, resulting links, and time-related information. In the context of this paper, browser artefacts served as a chronological anchor, connecting the early stages of activity (link discovery and site access) to more explicit forms of evidence, particularly visual artefacts and WhatsApp conversations. The relatively limited browser trace footprint identified in this case is consistent with the inherent data retention behaviour of iOS Safari, which may evict session data under storage pressure, exclude persistent history entries generated during private browsing sessions, and aggressively regulate cache storage. Consequently, browser artefacts on iOS devices should be interpreted as indicative rather than exhaustive records of user access in gambling-related investigations. The absence of an extensive browsing history should therefore not be construed as evidence of non-access; rather, it reflects the platform's storage architecture. Accordingly, cross-source corroboration, particularly from messaging and visual artefacts, becomes methodologically indispensable in establishing reliable forensic conclusions.

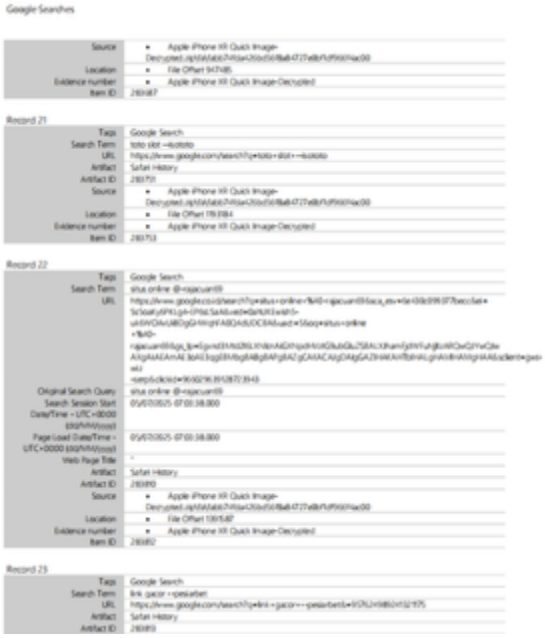

Fig. 6. Google search artifacts extracted by AXIOM (query + timestamp + URL)

3.3. Visual Artifacts: Images Indicative of a Suspected Online Gambling Website

The presence of Pictures (812 records) and Photos Media Information (44 records) indicated that the device retained a rich set of visual artefacts. In online gambling cases, visual artefacts especially screenshots were particularly consequential because they could present context directly, including website appearance, game menus, balance information, and the identity of the accessed service. In this paper, visual artefacts were treated as contextual reinforcement that prevented the interpretation of browser and communication artefacts from becoming speculative.

Fig. 7 effectively "locked in" the object under examination by demonstrating that the accessed content was not a generic website, but a platform featuring gameplay elements and economic indicators (e.g., balance/jackpot). Visual artefacts of this kind were particularly effective in distinguishing a gambling context from ordinary web activity and in strengthening the "object" element when the findings were mapped to the relevant statutory provisions.

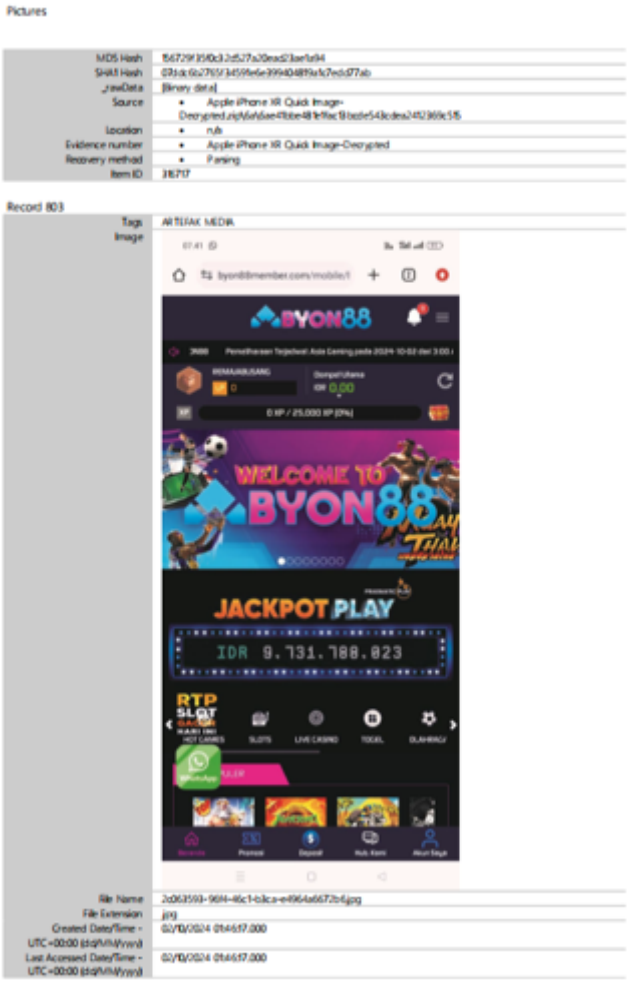

Fig. 7. Screenshot artefact showing the suspected gambling website interface (e.g., BYON88), extracted as media evidence

3.4. WhatsApp Artifacts: Promotion and Link Distribution as a Strong Finding

The strongest evidence in this paper emerged from WhatsApp artefacts, particularly WhatsApp Messages (435 records). The predominance of message records indicated early on that communication was not incidental, but rather a primary channel accompanying online gambling activity, especially in the form of promotion, invitations, and link distribution. What made WhatsApp artefacts especially valuable was not only the message content itself, but the conversational context that reflected active conduct: directing, persuading, and encouraging others to access specific links. The dominance of WhatsApp artefacts (435 messages, representing 32.09% of the total evidence) compared to browser history traces indicates a behavioural pattern consistent with social-network-driven online gambling recruitment. In such cases, users are more likely to receive links to gambling platforms from trusted messaging contacts than to discover them independently via search engines. This recruitment-first behaviour shifts the evidentiary centre of gravity from browser traces to messaging channels. From an investigative standpoint, this pattern suggests that WhatsApp extraction should be prioritised early in the forensic workflow whenever web-based gambling activity is suspected.

Fig. 8 illustrated a distinctive pattern: the message not only provided a direct access link (rebrand.ly/Daftargajian123) but coupled it with an explicit win incentive and a dissemination condition "gue kasih lu menang tapi setelah lu menang lu sharre ke temen temen lu ya situs gue" demonstrating a structured recruitment approach that went beyond passive link sharing. From a role-based perspective, these artefacts differentiated user activity as a “player” (personal access) from activity as a “promoter/access enabler” (access intended for others). This distinction formed the core

contribution of the paper: communication artefacts could provide the clearest indicator for the statutory element of "distributing/making accessible" gambling content.

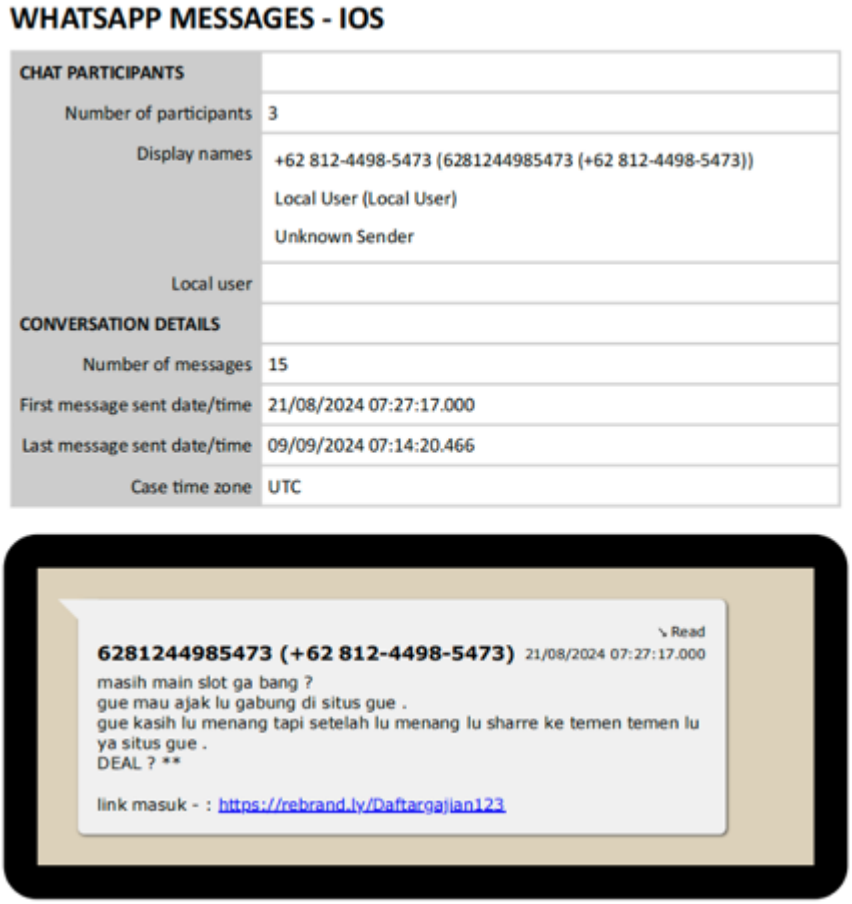

Fig. 8. WhatsApp Messages (iOS) artefact extracted by AXIOM showing a group promotion conversation (3 participants, 15 messages, 21/08/2024–09/09/2024): the sender invites the recipient to join a gambling site, offers a win incentive contingent on further dissemination, and provides a gambling access link (rebrand.ly/Daftargajian123), demonstrating call-to-action behaviour relevant to UU ITE Article 27(2)

In addition, WhatsApp chats/contacts/account artefacts although fewer in number still served as contextual scaffolding by linking messages to account identity and conversation structure, ensuring that the evidence did not stand merely as disconnected screenshots. The AXIOM-extracted metadata, including participant count (3), message volume (15), and timestamped conversation window (21 August to 9 September 2024), further supported the integrity of this artefact as a documented communication chain rather than an isolated screenshot, strengthening its admissibility as digital evidence.

3.5. Discussion: What These Artifacts Mean for the Paper Focus

When the extracted artefacts were read against the player activity flow (link discovery → site access → registration/login → deposit → gameplay → withdrawal), browser artefacts most commonly supported the early stages of "finding a link/accessing a site", while credential artefacts (tokens/keychain) reinforced access persistence traces that typically appeared when authentication occurred or access was stored. However, the two categories that most effectively captured the nature of web-based online gambling in this study were visual media artefacts (which directly showed the gambling object/context) and WhatsApp artefacts (which revealed access distribution and promotion).

In other words, the paper's focus was not built on a single type of evidence, but on a mutually reinforcing "artefact package":

- The browser provided signals of intent and initial access.
- Visual media established the context of the gambling object.

- Social media/instant messaging provided evidence of distribution and persuasive invitations that enabled access.

This framework then served as the basis for the element mapping presented as results (rather than a design template), because the subsequent tables contained element-by-element analysis grounded in extracted artefacts. Cross-source correlation was established primarily through domain/brand and keyword matching across WhatsApp and browser-related artefacts, and reinforced by visual confirmation from screenshots showing the same gambling service context. Table 2 summarizes representative correlation chains linking WhatsApp-based promotion to browser/search indicators and BYON88 visual artefacts, demonstrating how the findings form a coherent evidence package rather than isolated traces.

Table 2. Cross-source correlation examples linking WhatsApp promotion, browser/search traces, and BYON88 visual confirmation

Correlation ID	WhatsApp evidence (message/link indicator)	Browser/Search evidence (trace)	Visual evidence (context lock)	Correlation basis	Role
C1	Link sharing to **BYON88** accompanied by an invitation to click/access the site	Google Searches trace containing **BYON88** or gambling-related access keywords leading to the same service	Screenshot showing the **BYON88** site/interface (e.g., home/menu display)	Domain/brand match + visual confirmation	Promoter
C2	Instructional message encouraging others to **click the BYON88 link** and share it further	Safari-related trace consistent with site access (e.g., history/tab trace pointing to the same BYON88 service)	Screenshot showing **BYON88** gambling context (e.g., balance/jackpot/menu indicative of wagering)	Keyword match + consistent access narrative + visual confirmation	Promoter
C3	Message reflecting **personal participation** (e.g., discussing play/results) in the same promoted service	Search/access indicator consistent with personal access to the gambling site	Gameplay-related screenshot consistent with **BYON88** activity	Context match (participation narrative + object shown)	Player

3.6. Legal Element Mapping (Results-Based)

Table 3 underscores the paper's main contribution: in web-based online gambling cases, WhatsApp artefacts often provided the most explicit basis for distinguishing a promotional/access-enabling role from personal participation, while visual artefacts functioned as a contextual "anchor" that confirmed the gambling object being accessed and promoted. In contrast to app-based gambling investigations, in which dedicated application artefacts such as APK installation traces, in-app databases, and application-specific cache files commonly constitute the primary sources of evidence, web-based gambling cases, as demonstrated in this study, depend primarily on artefacts derived from browser and messaging layers. This structural distinction has significant practical implications: app-based investigations benefit from predictable and schema-driven artefact locations, whereas web-based investigations necessitate cross-source correlation across heterogeneous artefact types to compensate for the absence of dedicated application-level evidence. This distinction further underscores the value of ALMF as a correlation-first forensic framework, particularly in cases involving browser-accessed gambling services.

Table 3. Legal element mapping based on extracted artifacts [KUHP Pasal 303; UU ITE Pasal 27(2)

Violated Legal Provisions (Articles):
KUHP Pasal 303 (gambling)
UU ITE Pasal 27 ayat (2) (gambling content; distribution/enabling access)
Case: Web-based online gambling activity on a mobile device, including website access and the distribution of promotional links via WhatsApp.

Aspect	Element	Case Analysis and Evidence (Conduct)	Required Evidence (from AXIOM)
Fault	**Intent**	Search and access did not appear as random occurrences; patterns pointed to gambling-related sites/terms, supported by conversations containing invitations and access instructions.	Google Searches; WhatsApp Messages (invitations/links); contextual timestamps.
Unlawfulness	**Gambling content / gambling activity**	Visual artefacts displayed a platform/interface containing gambling elements (game/slot/balance/jackpot).	Screenshot/media of gambling website (Pictures/Photos Media); related URLs.
Act	**Gambling access/participation (KUHP) and distribution/enabling access (UU ITE)**	Access was supported by search/history traces; access distribution was clearly indicated by WhatsApp messages sharing links and encouraging others to access them.	Safari/Google artefacts; WhatsApp Messages; promotional screenshots; stored links.
Object	**Gambling-content website/service**	Media artefacts showed that the accessed object was an online gambling service rather than a general website.	Website screenshots (e.g., BYON88); media metadata.
Purpose	**Gain/participation & access expansion**	Promotional conversations indicated a purpose to expand access (inviting/instructing/asking others to share), while visual evidence reflected an economic orientation (balance/jackpot).	WhatsApp Messages (invitations + share prompts); screenshots showing balance/jackpot/relevant menus.

3.7. Limitations and Threats to Validity

This study is an exploratory case analysis of a single iOS device (iPhone XR) to demonstrate how the proposed Artefact-to-Legal Element Mapping Framework (ALMF) can structure an evidence package for web-based online gambling, including role-based interpretation (player vs. promoter) in the BYON88 context. Accordingly, the contribution is methodological transferability to categorizing, correlating, and mapping artefacts to legal elements, rather than statistical generalization across devices, platforms, or jurisdictions.

All findings were derived through Magnet AXIOM processing, meaning the observable artefacts depend on AXIOM's parsing support and the acquisition conditions. Web traces may be absent or sparse due to iOS/Safari storage behavior (e.g., private browsing, cache eviction, session-only data), while messaging or media artefacts may be incomplete if content was deleted or is not fully recoverable. To reduce interpretive bias, the study relied on cross-source support when forming event chains and role inference, prioritizing matches across URLs/keywords, consistent visual context, and corroborating communication patterns rather than single-artefact claims.

- Scope limitation: single-device, single-case setting; results support methodological transferability, not population-level generalisation.

- Tool/extraction limitation: artefact visibility depends on Magnet AXIOM and iOS/Safari data retention behaviour; some traces may be missing or underrepresented.
- Validity constraints: attribution and timing may be imperfect (who operated the device; incomplete timestamps), so conclusions prioritise cross-source corroboration for event chaining and role inference.

4. CONCLUSION

Addressing RQ1, this study identified and classified four dominant digital artefact categories from iOS evidence: (1) web search and browser access traces, (2) credential and access-persistence artefacts, (3) WhatsApp communication artefacts, and (4) visual media artefacts. Each category corresponded to a distinct phase of the player activity flow, from initial link discovery to active gameplay. Addressing RQ2, the ALMF successfully mapped these categories to the statutory elements of KUHP Article 303 and ITE Law Article 27(2), enabling explicit role-based differentiation: browser and visual artefacts primarily supported player-role attribution, while messaging artefacts provided the most direct basis for promoter/distributor-role inference under UU ITE Article 27(2). This study showed that the characteristic digital artefacts in web-based online gambling cases tended to appear as a combined set of web-access traces, authentication persistence, promotional communication, and visual context, such that evidentiary interpretation was unlikely to be effective if it relied on a single artefact type. Based on Magnet AXIOM analysis, the most relevant artefacts for explaining online gambling activity were identified and classified into four main groups: (1) access and search artefacts (e.g., Google Searches and available session/history traces), (2) account and access-persistence artefacts (e.g., passwords and tokens, and keychain entries), (3) communication and link-distribution artefacts (particularly WhatsApp messages containing invitations and links), and (4) visual media artefacts (images/screenshots showing website interfaces, gameplay elements, and economic indicators such as balance or jackpot). This classification helped position each finding within the appropriate conduct context, from initial discovery and site access to the dissemination of information through instant communication.

The findings further indicated that the extracted artefacts could be linked more systematically to offence elements under KUHP Pasal 303 and UU ITE Pasal 27 ayat (2). Under the KUHP Pasal 303 framework, access traces and visual artefacts strengthened the inference that the device was used to access and interact with gambling-content services, allowing the conduct and object elements to be supported through a combination of search/access traces and website-interface evidence. Under the UU ITE Pasal 27 ayat (2) framework, WhatsApp artefacts, especially messages containing links, invitations, and dissemination patterns, provided the most explicit basis for explaining the act of "distributing or making accessible" gambling content through an electronic system. This contrast reinforced a role-based reading: when an offender acted as a player, the key artefacts tended to centre on access traces and visual context; when acting as a promoter/distributor, the evidentiary centre shifted to communication traces and link circulation. Accordingly, the study concluded that, in web-based online gambling cases, the strongest evidentiary value emerged from a cross-source "artefact package" interpreted contextually and mapped directly to the relevant statutory elements.

For investigators and law enforcement, these findings suggest that effective evidence collection in web-based online gambling cases should prioritise the extraction of communication channels, particularly WhatsApp, alongside the preservation of visual media, as these two categories yielded the most legally actionable artefacts. This structured approach can be operationalised as an investigative checklist: (1) secure browser history and search artefacts as intent indicators; (2) extract credential/token artefacts to evidence access persistence; (3) conduct full messaging application extraction to capture promotion/distribution evidence; and (4) document all visual media for gambling-object confirmation. Future research should: (1) extend ALMF to multi-device scenarios to trace promotion networks across multiple suspects' devices; (2) apply comparative analysis on Android platforms, where artefact retention behaviour and file system structure differ significantly from iOS; (3) investigate partial automation of the ALMF correlation step using rule-based pattern matching or machine-learning-assisted classification to increase investigative throughput; and (4) examine the cross-jurisdictional applicability of the framework beyond the Indonesian legal context, including countries with comparable digital gambling laws.

REFERENCES

[1] A. E. Saragih, N. Christian, and P. Khoirunisa, "Analisis Penggunaan Barang Bukti Digital di Dalam Sistem Hukum di Indonesia (Studi Kasus Putusan Nomor 3 K/PID.SUS/2019)," *Media Hukum Indonesia (MHI)*, vol. 2, no. 2, Jun. 2024, doi: 10.5281/zenodo.12082755.

[2] S. Marsela, A. Syifa, F. D. Pratama, and R. A. Muqfi, "Persoalan Penjudi dan Judi Online dalam Analisa Teori Etika Utilitarianisme," *Das Sollen: Jurnal Kajian Kontemporer Hukum Dan Masyarakat*, vol. 1, no. 2, 2023.

[3] Y. Gao, H. Wang, L. Li, X. Luo, G. Xu, and X. Liu, "Demystifying Illegal Mobile Gambling Apps," in *Proceedings of the Web Conference 2021*, Ljubljana Slovenia: ACM, Apr. 2021, pp. 1447–1458. doi: 10.1145/3442381.3449932.

[4] T. A. Maryam, M. A. Maharani, T. A. Fahrezi, and A. A. Nugroho, "Peran Digital Forensik Dalam Pengumpulan Bukti Pada Kasus Judi Online di Kabupaten Demak," *KONSENSUS : Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi*, vol. 1, no. 3, Jun. 2024.

[5] A. Sitanggang, B. P. Sari, E. D. Sidabutar, Halimah, M. Cahya, and R. Y. Nababan, "Penegakan Undang-Undang ITE Terhadap Kasus Judi Online," *MJOL*, vol. 2, no. 4, pp. 16–22, Dec. 2023, doi: 10.51178/mjol.v2i4.1620.

[6] A. T. Sowakil, S. Paparang, and H. A. Mau, "Rekonstruksi Pembuktian Tindak Pidana Perjudian Media Online dalam Sistem Peradilan Pidana Indonesia," *Inovasi Global Jurnal*, vol. 2, no. 9, pp. 1278–1291, Sep. 2024, doi: 10.58344/jig.v2i9.171.

[7] Wijaya and T. Oktavia, "Factors Influencing Online Gambling Discontinuance Intentions: An SOR Analysis," *ICIC Express Letters*, vol. 19, no. 11, 2025, doi: 10.24507/icicel.19.11.1191.

[8] N. Parmar and N. Chaudhary, "Exploring the Future of Drone Forensics: A Systematic Study of Methods and Applications," in *Information Security, Privacy and Digital Forensics*, vol. 1456, N. K. Chaudhary, S. S. Iyengar, C. Modi, and S. J. Patel, Eds., in Lecture Notes in Electrical Engineering, vol. 1456. , Singapore: Springer Nature Singapore, 2026, pp. 95–137. doi: 10.1007/978-981-95-2196-8_7.

[9] P. D. Nigroho and Mu. N. Al-Azhar, "IT : Digital Forensic," *1*, vol. 5, no. 1, Jun. 2017, doi: 10.58217/ipsikom.v5i1.31.

[10] A. FFaizal and A. Luthfi, "Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as A Framework for Digital Forensic Evidence Analysis," *journalisi*, vol. 6, no. 2, pp. 701–718, Jun. 2024, doi: 10.51519/journalisi.v6i2.717.

[11] I. K. Kawi Arta and I. G. A. Wira Sena, "Perbedaan Makna Frasa Kata Judi online dengan Game Online dari Perspektif peraturan Perundang-undangan.," *KW*, vol. 13, no. 1, pp. 49–69, Aug. 2025, doi: 10.37637/kw.v13i1.2496.

[12] N. Maryani and U. Sastradipraja, "Peranan Audit Investigatif dalam menjadikan Bukti Audit sebagai Bukti Hukum untuk Pembuktian Tindak Pidana Korupsi," *1*, vol. 17, no. 2, pp. 116–147, 2020, doi: 10.26874/portofolio.v17i2.199.

[13] A. A. Shetty and P. Trevorrow, "Digital Forensic Investigation of Wearable Android Fitness Applications," *Journal of Applied Security Research*, vol. 21, no. 1, pp. 35–59, Jan. 2026, doi: 10.1080/19361610.2025.2562398.

[14] K. Schmid, K. Bayreuther, and F. Freiling, "Limits to the Forensic Analysis of Container Applications in Cloud Environments," *Digital Threats*, vol. 6, no. 4, pp. 1–20, Dec. 2025, doi: 10.1145/3765629.

[15] M. Y. Halim, F. W. Giffary, Y. Prayudi, M. F. Ramadhan, and I. V. Paputungan, "Cryptanalysis of Encrypted Drone Device Manager Log Extracted From Android Using Static Method," in *2025 10th International Conference on Information Technology and Digital Application (ICITDA)*, Yogyakarta, Indonesia: IEEE, Nov. 2025, pp. 1–7. doi: 10.1109/ICITDA68167.2025.11332242.

[16] Novianti, "Pemberantasan Konten Judi Online dalam Perspektif Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)," 2022.

[17] A. Ahmadi, T. Akbar, and H. M. Putra, "Perbandingan Hasil Tool Forensik Pada File Image Smartphone Android Menggunakan Metode NIST," *JIKO*, vol. 4, no. 2, pp. 92–97, Aug. 2021, doi: 10.33387/jiko.v4i2.2812.

[18] M. F. Ramadhan, Y. Prayudi, E. Ramadhani, and M. Y. Halim, "Design of an Alexiou Principle Guided Large Language Model Framework for Digital Forensic Investigation," in *2025 10th International Conference on Information Technology and Digital Application (ICITDA)*, Yogyakarta, Indonesia: IEEE, Nov. 2025, pp. 1–6. doi: 10.1109/ICITDA68167.2025.11332241.

[19] G. Waney, "Kajian Hukum terhadap Tindak Pidana Perjudian (Penerapan Pasal 303, 303 BIS KUHP)," *Lex Crimen*, vol. 5, no. 3, 2016.

[20] R. R. Chand, N. A. Sharma, and M. A. Kabir, "Advancing Web Browser Forensics: Critical Evaluation of Emerging Tools and Techniques," *SN COMPUT. SCI.*, vol. 6, no. 4, p. 355, Apr. 2025, doi: 10.1007/s42979-025-03921-6.

[21] S. Pirzada, N. H. Ab Rahman, N. D. W. Cahyani, and M. F. Othman, "A Framework of Forensic Analysis and Visualization: Using WhatsApp Chat Data as a Case Study," *JOIV : Int. J. Inform. Visualization*, vol. 8, no. 3–2, p. 1834, Nov. 2024, doi: 10.62527/joiv.8.3-2.2868.

[22] M. F. M. Nahdli, M. K. Biddinika, and I. Riadi, "Forensic Analysis of the WhatsApp Application Using the National Institute of Justice Framework," *International Journal of Advances in Data and Information Systems*, vol. 5, no. 2, Sep. 2024, doi: 10.59395/ijadis.v5i2.1328.

[23] Z. R. Likumahua, N. D. W. Cahyani, and E. M. Jadied, "Digital Forensics and Its Challenges in Investigating Online Gambling Cases," in *2024 12th International Conference on Information and Communication Technology (ICoICT)*, Bandung, Indonesia: IEEE, Aug. 2024, pp. 108–114. doi: 10.1109/ICoICT61617.2024.10698693.

AUTHOR BIOGRAPHY

Sudirman received the S.Kom degree in Computer Science from Institut Teknologi Dirgantara Adisutjipto, Yogyakarta, Indonesia. He is currently pursuing the M.Kom. degree in Informatics with a specialization in Digital Forensics at Universitas Islam Indonesia (UII), Yogyakarta, Indonesia. He is the founder and Chief Executive Officer (CEO) of an information technology consulting company, where he leads software development, IT consulting, digital transformation, and cybersecurity projects for public and private organizations. His professional interests focus on digital forensics, cybersecurity, information security, digital evidence management, and enterprise information systems. His current research focuses on the application of digital forensic methodologies and artificial intelligence to support digital investigations.

Yudi Prayudi received the B.Sc. degree in Computer Science from Universitas Gadjah Mada (UGM), Indonesia, the M.Kom. degree from Institut Teknologi Sepuluh Nopember (ITS), Surabaya, Indonesia, and the Ph.D. degree in Computer Science from Universitas Gadjah Mada in 2020. He is currently an Associate Professor with the Department of Informatics, Universitas Islam Indonesia (UII), Yogyakarta, Indonesia, and Director of the Center for Digital Forensics Studies (PUSFID/CDFS). His research interests include digital forensics, digital evidence, chain of custody, cyberlaw, computer security, steganography, watermarking, cloud forensics, and mobile forensics. He has authored numerous publications in digital forensics and information security and actively serves as an editor, reviewer, consultant, and expert witness in cybercrime investigations.