International Journal of Technology and Education Research

https://e-journal.citakonsultindo.or.id/index.php/IJETER

E-ISSN: 2986-0733

Evidence Traceable Capability Alignment Of Digital Forensic Frameworks For Data Breach Investigation

Alih R Hamda[1], Bisyron Wahyudi[2]

[1] Cyber Defense Engineering, Faculty of Defense Engineering and Technology, Indonesian Defense University, Bogor, Indonesia

[2] Lecturer in Cyber Defense Engineering, Faculty of Defense Engineering and Technology, Indonesian Defense University, Bogor, Indonesia

Corresponding Author: arhmda4@gmail.com

Abstract

Digital forensic frameworks vary in scope, procedural depth, evidence organization, and incident specificity, making framework selection difficult for data-breach investigations. This study develops an Evidence-Traceable Capability Alignment Index (ET-CAI) and applies it to five framework archetypes: IDFPM, SRDFIM, CFFTPM, D4I, and KARAFFE. Reproducible discovery used seven Scopus Advanced Search blocks. F1 returned 160 records, F2 returned 84, and the five named-verification searches returned nine. After six duplicate records were removed, 247 unique publications remained. Rule-based title-abstract mapping identified 134 records without a framework/process-model title signal, 49 without explicit proposal language, and 64 candidate publications requiring manual or primary-source verification. A purposive maximum-variation sample was then selected to represent integrated process, systematic investigation, field triage, artifact-centered reconstruction, and data-breach-specific designs. Six binary capabilities were scored using traceable evidence and exact locators where available. KARAFFE achieved 100% documented alignment, D4I 50.0%, SRDFIM and CFFTPM 33.3%, and IDFPM 16.7%. Sensitivity tests preserved the ordering. The 100% score denotes alignment with the selected documented capabilities, not perfect operational effectiveness, legal admissibility, or organizational readiness.

Keyword: digital forensics, data breach, capability alignment, framework selection, incident response.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Technology and Education Research

https://e-journal.citakonsultindo.or.id/index.php/IJETER

E-ISSN: 2986-0733

INTRODUCTION

Data-breach investigation requires more than confirming unauthorized access. Investigators must preserve potentially relevant evidence, reconstruct the sequence of events, identify affected systems and information, determine who acted and where the activity occurred, explain the causal conditions, and document how data moved outside organizational control. These tasks connect evidence handling, incident response, governance, and reporting. NIST SP 800-86 integrates collection, examination, analysis, and reporting with incident response, while ISO/IEC 27037 emphasizes the identification, collection, acquisition, and preservation of digital evidence. The NIST Cybersecurity Framework 2.0 also places adverse-event analysis and incident analysis within the Detect and Respond functions (Kent et al., 2006; International Organization for Standardization, 2012; National Institute of Standards and Technology, 2024).

Digital forensic process models are intended to reduce inconsistency by structuring investigative activities and clarifying the relationship between evidence and findings. However, process models vary substantially in purpose and granularity. Some harmonize general forensic activities, some emphasize rapid field triage, and others focus on artifact analysis or a specific class of incident. This diversity is valuable, but it also creates a selection problem: a framework can be conceptually sound and still provide insufficient operational detail for a particular data-breach scenario (Casey, 2011; Horsman & Sunde, 2022).

The selection problem is increasingly important because enterprise investigations now involve endpoints, network devices, identity systems, cloud services, security platforms, and large heterogeneous log sets. Reviews of digital forensic research continue to identify fragmented procedures, evidence-acquisition complexity, limited standardization, and difficulties translating technical findings into defensible investigative conclusions (Casino et al., 2022; Breitinger et al., 2024). At the organizational level, forensic readiness also depends on people, policy, technology, legal authority, and evidence availability rather than on a process model alone (Reddy & Venter, 2013; Ariffin & Ahmad, 2021; Bankole et al., 2022).

Five frameworks provide a useful maximum-variation sample. The Integrated Digital Forensic Process Model (IDFPM) consolidates activities from earlier models into an integrated process (Kohn et al., 2013). The Systematic Digital Forensic Investigation Model (SRDFIM) structures cybercrime and computer-fraud investigation in sequential stages (Agarwal et al., 2011). The Computer Forensics Field Triage Process Model (CFFTPM) supports rapid on-site identification, analysis, and interpretation of evidence (Rogers et al., 2006). D4I strengthens examination and analysis by categorizing artifacts and mapping them to attack phases

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

(Dimitriadis et al., 2020). KARAFFE is designed specifically for data-breach investigation using Data Breach Breakdown phases, categorized evidence, artifact relationships, timeline analysis, attack-flow analysis, and explicit 5WH reporting (Hakim et al., 2023).

A prior dissertation comparison represented six characteristics as present or absent and explicitly recommended the development of a metric or index that could guide practitioners in selecting a framework for a particular incident (Hakim, 2025). Converting check marks into a percentage without a reproducible identification log or evidence trail, however, would create a false impression of precision. Unlike the earlier descriptive matrix, the present study adds a Scopus-based candidate map, explicit screening decisions, source locators, sensitivity analysis, and a contextual selection guide. No new claim is made about the empirical effectiveness of the compared frameworks.

This study addresses that methodological gap through an Evidence-Traceable Capability Alignment Index (ET-CAI). The term capability alignment is deliberately narrower than operational readiness. It refers only to the proportion of selected investigation capabilities that are explicitly documented in a framework publication. ET-CAI does not assess organizational maturity, investigator competence, tool reliability, legal admissibility, or effectiveness in live incidents.

Two research questions guide the analysis. RQ1 asks: To what extent do the selected frameworks explicitly document the capabilities required for data-breach investigation? RQ2 asks: How stable are the resulting comparisons when incident-specific criteria are separated from core workflow criteria or when individual criteria are removed? The study contributes (1) a reproducible framework-identification log, (2) an auditable coding protocol and source-linked score matrix, (3) preliminary validity evidence through theoretical mapping and sensitivity analysis, and (4) a contextual selection and professional-training guide.

METHOD

Research design and source selection

The study used structured comparative document analysis following the principle that coding categories must be defined before claims are counted (Krippendorff, 2018). The unit of analysis was the documented framework, not an organization, software product, investigator, or incident outcome. The search stage mapped the broader literature, whereas the scoring stage used a purposive maximum-variation sample representing five distinct design objectives. Accordingly, the analytical sample is not presented as an exhaustive census or a systematic ranking of every digital forensic framework.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Technology and Education Research

https://e-journal.citakonsultindo.or.id/index.php/IJETER

E-ISSN: 2986-0733

Reproducible discovery was completed on 29 July 2026 using seven Scopus Advanced Search blocks. F1, the broad framework query, returned 160 records. F2, the revised data-breach recall query without a year-only filter, returned 84. Five named-verification queries returned F3A=1, F3B=2, F3C=2, F3D=2, and F3E=2 records. The raw set therefore contained 253 records. Deduplication by EID, DOI, and normalized title removed six duplicate records, leaving 247 unique publications. A reproducible title-abstract mapping rule separated 134 records without a framework/process-model title signal and 49 records whose title or abstract did not explicitly propose, introduce, present, or materially extend a framework/model. The remaining candidate map contained 57 explicit original/material-extension candidates and seven mixed review, comparative, or proposal papers requiring manual or primary-source verification. IDFPM and KARAFFE were verified directly in Scopus. The named searches did not retrieve the foundational SRDFIM, CFFTPM, or D4I publications, so those three primary sources were verified through publisher or institutional repositories. Supplementary File S1 records the exact queries, deduplicated publications, mapping decisions, analytical-sample rationale, and criterion-level score evidence.

Table 1. Source selection and document-audit protocol

Protocol element	Operational decision
Primary discovery source	Scopus Advanced Document Search.
Search date and coverage	29 July 2026; all publication years available through the search date; no year-only filter.
Query blocks and yields	F1=160; F2=84; F3A=1; F3B=2; F3C=2; F3D=2; F3E=2; raw total=253.
Deduplication	EID, DOI, then normalized title; six duplicate records removed; n=247 unique publications.
Candidate-mapping rule	Title identifies a framework/process model and title/abstract explicitly proposes, introduces, presents, or materially extends it.
Mapping outcome	134 without title signal; 49 without proposal language; 57 explicit original/material-extension candidates; 7 mixed review/comparative/proposal candidates.
Analytical inclusion	Primary source, identifiable process structure, adequate documentation for C1-C6, and non-redundant contribution to one design archetype.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Technology and Education Research

https://e-journal.citakonsultindo.or.id/index.php/IJETER

E-ISSN: 2986-0733

Protocol element	Operational decision
Non-retention grounds	No proposal evidence, secondary-only role, specialized scope outside the five archetypes, design redundancy, or inadequate comparability.
Supplemental verification	Publisher and institutional repositories were used to verify foundational SRDFIM, CFFTPM, and D4I sources not retrieved by named Scopus searches.
Analytical design	Purposive maximum-variation sample of five archetypes; not an exhaustive census or universal ranking.
Audit material	Supplementary File S1 includes query strings, 247-record log, 64-record candidate map, scoring codebook, and source-linked evidence matrix.

Table 2. Scopus framework-identification and candidate-mapping log

Stage	Count(s)	Operational rule	Outcome
Query retrieval	F1=160; F2=84; F3A-E=9; total=253	Seven predefined Scopus Advanced Search blocks.	Raw discovery set.
Deduplication	6 removed; 247 unique	Match EID, DOI, then normalized title.	Unique mapping set.
Framework-title signal	134 without title signal	No framework/process-model indicator in the title.	Excluded from candidate map.
Proposal-language screen	49 without proposal language	No explicit propose, introduce, present, develop, or material-extension statement.	Excluded from candidate map.
Candidate map	57 explicit + 7 mixed-format = 64	Retain candidate publications for manual or primary-source verification.	Candidate-verification pool.
Named verification	IDFPM and KARAFFE retrieved	Check exact framework names and robust title/keyword combinations.	Two target primary sources verified in Scopus.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Technology and Education Research

https://e-journal.citakonsultindo.or.id/index.php/IJETER

E-ISSN: 2986-0733

Protocol element	Operational decision		
Supplemental primary-source verification	SRDFIM, CFFTPM, D4I	Use publisher/institutional repositories when named Scopus searches do not retrieve the target primary source.	Complete the five-archetype primary-source set.
Analytical sample	5 frameworks	Maximum variation, source adequacy, and non-redundant design objective.	Five-framework ET-CAI comparison.

F1 functioned as the main discovery query. F2 substantially improved recall by retrieving 84 publications across 2012-2026, including the KARAFFE primary article. The five named searches were diagnostic rather than assumed to be complete: F3A retrieved IDFPM, and F3E retrieved KARAFFE and a later adaptation, whereas F3B, F3C, and F3D did not retrieve the foundational SRDFIM, CFFTPM, and D4I publications. This under-retrieval is reported transparently and was addressed through targeted primary-source verification, not by altering the Scopus counts.



Figure 1. Evidence-traceable comparative analysis and index-development workflow

Capability construction and theoretical mapping

The six criteria were retained because they jointly capture incident specificity, investigative completeness, evidence structure, procedural usability, empirical demonstration, and output traceability. C1 and C2 represent data-breach-specific requirements: the exfiltration-oriented incident structure and complete 5WH reporting. C3-C6 represent core investigation-workflow requirements that can be applied across incident types. The distinction permits both a full data-breach alignment index and a core-workflow sub-index.

Construct relevance was supported by mapping the criteria to established forensic functions. Evidence categorization and examination-analysis detail correspond to the collection, examination, and analysis functions in NIST SP 800-86 and to evidence-handling principles in ISO/IEC 27037. Case application distinguishes demonstrated use from conceptual assertion.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

Stage-level outputs test whether evidence can be traced to intermediate and final findings. The 5WH criterion reflects the investigative goal of producing a complete explanatory account, while incident specificity prevents a general model from being treated as a data-breach playbook without supplementation. These links provide theoretical mapping, not external construct validation.

Table 3. Capability definitions and conservative scoring anchors

Code	Capability	Score 1: explicit documented support	Score 0: not explicit
C1	Data-breach or exfiltration specificity	The framework is designed around data-breach/exfiltration characteristics.	The framework is general or targets another incident type.
C2	5WH mapping	Evidence or findings are explicitly mapped to What, Who, When, Where, Why, and How.	No explicit 5WH mapping is provided.
C3	Evidence categorization	A categorized evidence/artifact model guides subsequent examination or analysis.	Evidence is mentioned without an operationalized categorization scheme.
C4	Examination and analysis detail	The publication provides procedural guidance beyond high-level phase labels.	Only high-level stages are listed without usable examination/analysis detail.
C5	Demonstrated application	A case, implementation, or formal evaluation demonstrates use of the framework.	No demonstrated application is reported.
C6	Stage-level outputs	Relevant stages produce identifiable outputs that link evidence to findings.	Outputs are absent, implicit, or not traceable by stage.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Technology and Education Research

https://e-journal.citakonsultindo.or.id/index.php/IJETER

E-ISSN: 2986-0733

Coding, traceability, and index calculation

A conservative binary rule was adopted to reduce ambiguity. A criterion received 1 only when explicit support was identifiable in the source. Partial or inferential support was coded 0 and discussed qualitatively. Each decision was recorded with a source location and short rationale. Coding was completed in two passes: the first pass assigned provisional values; the second pass rechecked every positive score against the operational definition and the original publication. The dissertation table was then used as a consistency audit. This is an intradocument audit, not independent inter-rater validation.

The equal-weight ET-CAI is the percentage of criteria with explicit documented support. Let xi be the binary score for criterion i and wi its weight. The general form is shown below. Equal weighting uses wi = 1 for all six criteria.

$$\text{ET-CAI} = (\Sigma\, w_i x_i \,/\, \Sigma\, w_i) \times 100$$

The score is an alignment percentage, not a performance probability. A value of 100% means that all selected capabilities are explicitly documented. It does not mean that investigations are always complete, accurate, fast, legally admissible, or effective across all organizations.

Preliminary validity evidence and robustness checks

Three forms of preliminary validity evidence were assembled. First, theoretical relevance was supported through the standards mapping described above. Second, evidential adequacy was strengthened through criterion-level traceability to primary publications and a consistency audit against the dissertation comparison. Third, robustness was examined using three sensitivity tests. These checks support transparency and internal coherence; they do not establish expert content validity, inter-rater reliability, predictive validity, or operational effectiveness.

The first sensitivity test calculated a core-workflow sub-index using C3-C6 only, thereby removing the two criteria most likely to favor a data-breach-specific framework. The second assigned double weight to C1 and C2 to represent a data-breach-priority context. The third recalculated the index six times while removing one criterion at a time. Stable ordering across these scenarios provides a transparent robustness check and preliminary evidence that the results are not driven by a single criterion. Expert content-validity ratings, inter-rater reliability, and empirical outcome validation remain future requirements.

Data and audit availability. Supplementary File S1 provides the complete Scopus search

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

strategies, query yields, deduplicated publication records, candidate-screening decisions, analytical-sample rationale, coding protocol, and criterion-level ET-CAI evidence with traceable source locators.

RESULTS AND DISCUSSION

Evidence traceability

Tables 4 and 5 expose the evidence behind every score. A zero does not indicate that a framework is invalid; it indicates that the specific capability was not explicitly operationalized in the publication under the conservative rule. The source-linked matrix also makes disagreements auditable. A future coder can revisit a decision without reconstructing the entire analysis.

Table 4. Traceability of incident-specific and evidence-organization criteria

Framework	C1: incident specificity	C2: 5WH mapping	C3: evidence categorization
IDFPM	0 - General integrated process model; no breach/exfiltration scope (Kohn et al., 2013, pp. 103-115).	0 - No explicit 5WH mapping (Kohn et al., 2013).	0 - No incident-specific evidence taxonomy is operationalized (Kohn et al., 2013).
SRDFIM	0 - General cybercrime and computer-fraud scope (Agarwal et al., 2011, pp. 118-131).	0 - No explicit 5WH mapping (Agarwal et al., 2011).	1 - Evidence handling is explicitly structured across the model stages (Agarwal et al., 2011).
CFFTPM	0 - Field-triage scope rather than data-breach reconstruction (Rogers et al., 2006, pp. 19-38).	0 - No explicit 5WH mapping (Rogers et al., 2006).	0 - Evidence prioritization is central, but a reusable categorized evidence model is not sufficiently operationalized under the criterion (Rogers et al., 2006).
D4I	0 - General cyber-attack investigation scope (Dimitriadis et al., 2020, Sections 3-5).	0 - Attack-phase mapping is provided, but no explicit 5WH mapping (Dimitriadis et al., 2020).	1 - Artifacts are categorized and mapped to attack phases (Dimitriadis et al., 2020).

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

Framework	C1: incident specificity	C2: 5WH mapping	C3: evidence categorization
KARAFFE	1 - Explicitly designed for data-breach and exfiltration characteristics (Hakim et al., 2023, pp. 42644-42659).	1 - Findings are explicitly mapped to 5WH questions (Hakim et al., 2023).	1 - Host, network-device, and security-device evidence is categorized and linked to analysis (Hakim et al., 2023).

Table 5. Traceability of workflow depth, demonstration, and outputs

Framework	C4: examination/analysis detail	C5: demonstrated application	C6: stage-level outputs
IDFPM	1 - Integrated phases and process interactions are described beyond a simple list (Kohn et al., 2013).	0 - No data-breach or worked investigative application is reported in the framework article.	0 - Stage outputs are not specified in an incident-traceable form.
SRDFIM	1 - The model provides a systematic multi-stage investigative procedure (Agarwal et al., 2011).	0 - No worked data-breach case or formal implementation is reported.	0 - Stage-level outputs are not explicitly linked to final findings.
CFFTPM	1 - The model provides a time-constrained field process for identifying and interpreting evidence (Rogers et al., 2006).	1 - The approach was formally evaluated and illustrated through field-oriented use (Rogers et al., 2006).	0 - Comprehensive stage-level outputs for full reconstruction are not specified.
D4I	1 - Sequential examination and analysis instructions are a central contribution (Dimitriadis et al., 2020).	1 - The publication demonstrates the framework through an applied cyber-attack investigation (Dimitriadis et al., 2020).	0 - Outputs are not consistently defined for every relevant stage under this criterion.
KARAFFE	1 - Content analysis, chain of artifacts, timeline, attack flow, and 5WH mapping are procedurally described (Hakim et al., 2023).	1 - A complete data-breach case study is presented (Hakim et al., 2023).	1 - Each analytical stage produces identifiable findings that contribute to the final 5WH account (Hakim et al., 2023; Hakim, 2025).

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Technology and Education Research

https://e-journal.citakonsultindo.or.id/index.php/IJETER

E-ISSN: 2986-0733

Capability alignment results

The full index reproduces the pattern of the dissertation comparison while replacing check marks with an auditable percentage. KARAFFE documents all six selected capabilities and therefore obtains 100% alignment. D4I documents three capabilities, SRDFIM and CFFTPM two each, and IDFPM one. The 100% value is bounded: it signifies complete documented alignment within this six-criterion construct, not perfect operational effectiveness.

Table 6. Evidence-Traceable Capability Alignment Index

Framework	C1	C2	C3	C4	C5	C6	ET-CAI (%)
IDFPM	0	0	0	1	0	0	16.7
SRDFIM	0	0	1	1	0	0	33.3
CFFTPM	0	0	0	1	1	0	33.3
D4I	0	0	1	1	1	0	50.0
KARAFFE	1	1	1	1	1	1	100.0

Note. ET-CAI is the percentage of selected capabilities explicitly documented in the source set. It is not an organizational readiness score, accuracy rate, legal-admissibility score, or universal ranking.

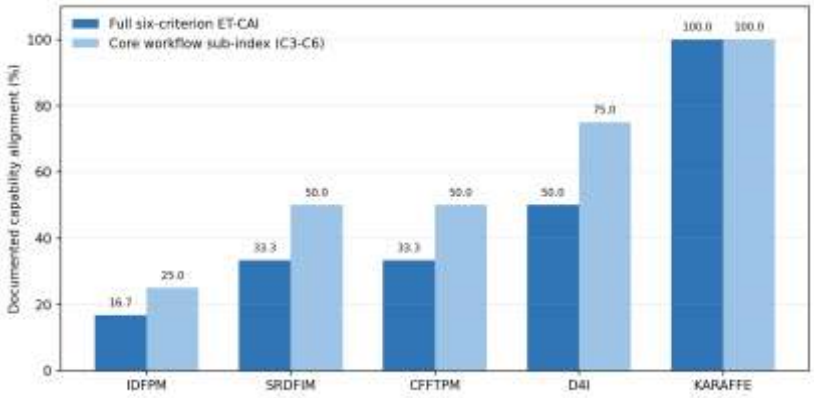


Figure 2. Full ET-CAI and the core-workflow sub-index

Robustness analysis and preliminary validity evidence

The core-workflow sub-index removes C1 and C2, the criteria most closely associated

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

with the design objectives of KARAFFE. Under this test, KARAFFE remains at 100%, but D4I rises to 75%, while SRDFIM and CFFTPM reach 50%. The smaller gap shows that D4I is comparatively strong when the question is general examination and analysis rather than data-breach-specific reconstruction.

The data-breach-weighted scenario assigns weight 2 to C1 and C2 and weight 1 to the remaining criteria. This scenario increases the influence of incident specificity and 5WH completeness. KARAFFE remains at 100%, while D4I falls to 37.5%. The result is expected because D4I was not designed as a data-breach framework. The scenario should therefore be chosen based on the investigation objective rather than used as a universal ranking.

Leave-one-criterion-out analysis produced the same ordering in all six recalculations: KARAFFE first, D4I second, SRDFIM and CFFTPM jointly next, and IDFPM last. This stability indicates that no single criterion determines the ordering. It does not constitute external index validation, but it provides a transparent internal robustness check.

Table 7. Sensitivity and robustness results

Framework	Full ET-CAI	Core workflow C3-C6	Data-breach weighted	Leave-one-out range
IDFPM	16.7%	25.0%	12.5%	0-20%
SRDFIM	33.3%	50.0%	25.0%	20-40%
CFFTPM	33.3%	50.0%	25.0%	20-40%
D4I	50.0%	75.0%	37.5%	40-60%
KARAFFE	100.0%	100.0%	100.0%	100%

Interpretation by framework

IDFPM is most useful as a harmonizing process architecture. Its integrated structure can support policy development and common terminology, but the publication does not operationalize data-breach evidence categories, 5WH reporting, case outputs, or a breach-specific playbook. Its low ET-CAI therefore reflects scope and granularity, not conceptual weakness.

SRDFIM offers a systematic multi-stage process and explicit evidence-handling structure. It can support broad cybercrime reconstruction and education on investigation sequencing. Its limitations for the present purpose are the absence of data-breach specificity, explicit 5WH

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

mapping, a worked breach case, and stage-linked outputs.

CFFTPM addresses a different operational need: rapid on-site analysis during the first hours of an investigation. Its demonstrated field orientation is valuable when speed and prioritization are critical. However, triage is not equivalent to complete reconstruction, and CFFTPM requires a fuller process for comprehensive reporting and long-form evidence traceability.

D4I is the strongest general cyber-attack framework in the comparison. Its artifact categorization, attack-phase mapping, sequential examination and analysis instructions, and applied demonstration produce a 75% core-workflow score. D4I's lower full ET-CAI results from the deliberate absence of data-breach specificity and explicit 5WH mapping rather than from weak forensic procedure.

KARAFFE obtains complete alignment because the six criteria correspond closely to its stated design: data-breach-specific phases, 5WH reporting, categorized evidence, detailed analytical steps, a case study, and stage-level findings. This close fit also creates a risk of criterion-selection bias. The core-workflow and leave-one-out tests reduce that concern but do not eliminate it. Independent experts should assess whether the six capabilities are sufficient, whether additional legal and cloud-forensic dimensions are needed, and whether weights should vary across contexts.

Framework selection and professional education implications

ET-CAI should be used as a profile rather than a league table. The relevant question is not which framework is universally best, but which documented capabilities match the task, evidence environment, reporting obligation, and investigator competence. Table 8 converts the results into a contextual guide.

Table 8. Contextual framework selection and training use

Investigation or learning objective	Suggested framework	Rationale	Required supplementation
Data-breach or exfiltration reconstruction with complete 5WH reporting	KARAFFE	Incident-specific phases, categorized evidence, analytical outputs, and 5WH mapping.	Validate across additional architectures, cloud environments, and jurisdictions.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

Investigation or learning objective	Suggested framework	Rationale	Required supplementation
General cyber-attack reconstruction with detailed artifact analysis	D4I	Strong artifact categorization, attack-phase mapping, and examination-analysis instructions.	Add breach-specific questions, notification outputs, and cross-platform artifacts where required.
Rapid field triage and immediate prioritization	CFFTPM	Time-sensitive on-site evidence identification and interpretation.	Follow with a complete forensic process, preservation controls, and comprehensive reporting.
Broad cybercrime or computer-fraud process instruction	SRDFIM	Systematic sequencing of investigation and evidence handling.	Add incident-specific taxonomy, worked scenarios, and stage-output templates.
Organization-wide process harmonization	IDFPM	Integrated high-level process and common investigative structure.	Add operational procedures, evidence categories, incident playbooks, and evaluation exercises.

The index also has educational value for university courses, professional certification, and CSIRT tabletop exercises. Learners can code a new framework against the criteria, defend each decision with source evidence, compare full and core-workflow scores, and then select a framework for a scenario. This approach teaches that framework selection is an evidence-based design decision rather than memorization of process stages. It also exposes the difference between a documented framework, an organization's readiness, and the competence required to apply the framework.

Limitations and future validation

This study has five limitations. First, it evaluates publications rather than live deployments. Implementation quality may differ from documented capability. Second, the

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

sample contains only five frameworks and is purposive rather than exhaustive. Third, the six criteria originated partly from a data-breach framework comparison, so additional criteria may alter the results. Fourth, the audit was not performed by independent human coders; inter-rater reliability therefore cannot be claimed. Fifth, no empirical relationship has yet been established between ET-CAI and investigation duration, completeness, reproducibility, legal acceptance, or analyst confidence.

Future validation should proceed in stages. A panel of digital forensic investigators, CSIRT practitioners, academics, and legal specialists should rate item relevance to calculate a content-validity index. At least two independent coders should score the source documents and report agreement using Cohen's kappa or Krippendorff's alpha. Expert-derived weighting can then be developed through Delphi, analytic hierarchy process, or best-worst methods. Finally, the index should be tested in multiple controlled cases using outcome measures such as unresolved 5WH questions, evidence-to-finding traceability, completion time, reporting quality, and cross-investigator consistency.

CONCLUSION

This study developed ET-CAI as an evidence-traceable method for comparing the documented capabilities of digital forensic frameworks in data-breach investigation. The analysis answers RQ1 by showing clear differences in scope and workflow support: KARAFFE explicitly documents all six selected capabilities, D4I documents three, SRDFIM and CFFTPM two, and IDFPM one. These values describe publication-level alignment only.

RQ2 is answered through sensitivity analysis. KARAFFE remained first and D4I second when incident-specific criteria were removed, when data-breach criteria were weighted more heavily, and when each criterion was omitted in turn. The core-workflow result is particularly important because it shows D4I's strength without conflating general cyber-attack investigation with data-breach-specific reporting.

The principal contribution is not the 100% score, but the traceable relationship between criteria, evidence, scoring decisions, and contextual interpretation. ET-CAI can support framework selection, gap analysis, curriculum design, and incident-response exercises. It should not be used as a certification, procurement, maturity, or legal-admissibility standard until independent expert validation and multi-case empirical testing have been completed.

REFERENCE

Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

model. International Journal of Computer Science and Security, 5(1), 118-131.

Ariffin, K. A. Z., & Ahmad, F. H. (2021). Indicators for maturity and readiness for digital forensic investigation in the era of Industrial Revolution 4.0. Computers & Security, 105, 102237. https://doi.org/10.1016/j.cose.2021.102237

Bankole, F. O., Taiwo, A. A., & Claims, I. P. (2022). An extended digital forensic readiness and maturity model. Forensic Science International: Digital Investigation, 40, 301348. https://doi.org/10.1016/j.fsidi.2022.301348

Breitinger, F., Hilgert, J.-N., Hargreaves, C., Sheppard, J., Overdorf, R., & Scanlon, M. (2024). DFRWS EU 10-year review and future directions in digital forensic research. Forensic Science International: Digital Investigation, 48, 301685. https://doi.org/10.1016/j.fsidi.2023.301685

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet (3rd ed.). Academic Press.

Casino, F., Dasaklis, T. K., Spathoulas, G., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. IEEE Access, 10, 25464-25493. https://doi.org/10.1109/ACCESS.2022.3154059

Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I - Digital forensics framework for reviewing and investigating cyber attacks. Array, 5, 100015. https://doi.org/10.1016/j.array.2019.100015

Hakim, A. R. (2025). Pengembangan kerangka kerja forensik digital dan metode baru berbasis machine learning untuk investigasi insiden kebocoran data [Doctoral dissertation, Universitas Indonesia].

Hakim, A. R., Ramli, K., Gunawan, T. S., & Windarta, S. (2023). A novel digital forensic framework for data breach investigation. IEEE Access, 11, 42644-42659. https://doi.org/10.1109/ACCESS.2023.3270619

Horsman, G., & Sunde, N. (2022). Unboxing the digital forensic investigation process. Science & Justice, 62(2), 171-180. https://doi.org/10.1016/j.scijus.2022.01.002

International Organization for Standardization. (2012). ISO/IEC 27037:2012: Guidelines for identification, collection, acquisition and preservation of digital evidence. ISO.

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.

Kohn, M. D., Eloff, M. M., & Eloff, J. H. P. (2013). Integrated digital forensic process model.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

Computers & Security, 38, 103-115. https://doi.org/10.1016/j.cose.2013.05.001

Krippendorff, K. (2018). Content analysis: An introduction to its methodology (4th ed.). SAGE Publications.

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Reddy, K., & Venter, H. S. (2013). The architecture of a digital forensic readiness management system. Computers & Security, 32, 73-89. https://doi.org/10.1016/j.cose.2012.09.008

Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. Journal of Digital Forensics, Security and Law, 1(2), 19-38. https://doi.org/10.15394/jdfsl.2006.1004

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.