

# The FACT Attribution Framework v1.0

A Legal and Attribution-Centered Model for  
Digital Forensics and Incident Response

Brett Shavers

Version 1.0 – December 2025

© 2025 Brett Shavers All Rights Reserved.

DOI: <https://doi.org/10.5281/zenodo.17745959>

## **Legal Disclaimer**

This framework is provided for educational and analytical purposes only and does not constitute legal advice. Application of FACT requires adherence to all applicable laws, regulations, organizational policies, and jurisdictional requirements. Practitioners should consult qualified counsel when acting under statutory, constitutional, contractual, or regulatory authority. All third-party marks referenced in this work are the property of their respective owners, and their inclusion does not imply endorsement. Commercial use, derivative works, and incorporation into paid training programs require prior written permission from the author.

## Abstract

Digital forensics has become highly effective at answering **what happened**, **on which device**, **how it happened**, and **when it happened**. Examiners can extract artifacts, reconstruct timelines, and demonstrate that specific content once existed or that particular actions occurred. What has been far less developed is a structured, legally grounded way to answer the next question:

*Which specific person, among the realistic candidates, is most likely responsible for those actions, and how confident are we in that conclusion?*

The FACT Attribution Framework™ (FACT) is proposed as a jurisprudence-centered attribution methodology for digital forensics and incident response that explicitly separates **identification** ("what acted?") from **attribution** ("who acted?"). FACT does not replace existing incident response or evidence-handling models. Instead, it overlays them with a structured, legally informed approach to person-level attribution built on four stages:

- **F – Forensic Authority & Compliance**
- **A – Analyze Evidence**
- **C – Correlate & Sequence**
- **T – Testify & Transfer**

The framework is intentionally conservative. When the requirements for person-level attribution are not met, FACT directs the practitioner to reach and document a non-attribution conclusion. FACT is designed for practitioners, investigators, and experts who must **tie the act to actor** in real-world cases, and who may later need to defend those conclusions before courts, regulators, or internal tribunals.

### Use FACT When:

Insider threat, shared devices/accounts, cloud credential misuse, HR investigations, disciplinary / firing decisions, litigation-arb-bound cases, any case where "who did it" will matter in court, arbitration, or employment law.

### Do Not Use FACT When:

Pure triage, commodity malware, volume alert-handling, where you will never name a specific human or take action against them.

### What FACT Is:

- An attribution framework-
- A legal reasoning model-
- A defensibility structure for investigative conclusions-

### What FACT Is Not:

- A threat model-
- An IR workflow-
- A forensic acquisition standard-

---

## Keywords

Attribution framework; digital forensics; incident response; investigative reasoning; identity layers; evidence convergence; falsification; legal authority; actor attribution; device–actor distinction.

---

## **1. Introduction: The Attribution Gap in Digital Forensics**

Digital forensics (DF) has traditionally focused on artifacts and timelines such as recovering deleted files, reconstructing user activity, and mapping events across devices and logs. In routine practice, however, examiners and investigators still lack a transparent, inspectable method for moving from device- or account-level findings to person-level conclusions.

Recent work underscores this gap. Spichiger (2025) distinguishes among person, account, and device and highlights the “person–account/device gap” that must be bridged before identity claims are defensible. Shamsi et al. (2016) describe three levels of cyber attribution, “weapon, origin, attacker,” and observe that true attacker-level attribution is rarely achieved. Rid and Buchanan (2015) emphasize how difficult it is to attribute complex operations in strategic or intelligence contexts. Thompson (2011) and others have examined how investigative facts interact with scientific evidence in legal decision-making.

The result in practice is a patchwork of habits: some investigators implicitly treat devices and accounts as if they were persons; others avoid attribution altogether out of fear of overstepping. Courts and internal tribunals see both overconfident claims and timid reports that fail to address the central attribution question. FACT is intended to fill this gap by giving practitioners a structured, inspectable way to move from *act* to *actor* or to say honestly that it cannot be done.

## **2. Conceptual Foundations and Definitions**

### 2.1 Digital Forensics as Forensic Jurisprudence

In this framework, the “**digital forensics**” term is used in its strict forensic sense: work conducted in a manner such that its results may reasonably be relied upon in legal, regulatory, disciplinary, or other adjudicative decision-making.

Where there is genuinely no realistic prospect that findings will inform any such decision, the activity is more accurately described as **technical analysis** or **incident response**, not digital forensics in the forensic-science sense. Typical examples include transient triage during live incident handling or exploratory lab work performed solely for tool testing.

In practice, investigators rarely know at the outset whether a matter will later become the subject of litigation, arbitration, regulatory review, or employment disputes. FACT therefore proceeds on a conservative assumption: Any attribution-related work may ultimately be scrutinized under forensic standards.

Accordingly, when FACT is applied, digital-forensic activity is treated as a **forensic jurisprudence** function whose purpose is to generate and interpret evidence in ways that:

- satisfy evidentiary reliability and admissibility standards,
- withstand adversarial or independent scrutiny, and
- support fair, reviewable adjudication or other formal decision-making.

Incident response (IR) properly prioritizes speed and business continuity. Attribution-focused digital forensics (DF), as governed by FACT, must instead prioritize legality, rigor, and defensibility.

DF practitioners are therefore required to:

- establish lawful authority and scope before substantive analysis,
- document how authority, scope, and proportionality were determined,
- treat digital evidence as one evidentiary stream among several (physical, testimonial, contextual), and

- express conclusions in terms compatible with forensic evidence evaluation, rather than as bare tool outputs or configuration states.

This orientation places attribution squarely within forensic science and legal reasoning, even when the immediate audience is an internal decision-maker rather than a court.

## 2.2 Identification vs Attribution

FACT draws a strict distinction between **identification** and **attribution**:

- **Identification answers what acted:** which artifact, device, account, or system user is involved (for example, a specific log entry, endpoint, virtual machine, user profile, or credential).
- **Attribution answers who acted:** assigning responsibility to a specific person or persons through converging evidence and explicit reasoning.

Identification is a necessary but never sufficient condition for attribution. Under FACT, DF practitioners must clearly distinguish between:

- statements about what the observable data show (**identification**), and
- statements about who is most likely responsible, given all available evidence and alternatives (**attribution**).

This distinction is not merely semantic. Many recurring errors in digital investigations, such as treating “activity on Alice’s laptop” as equivalent to “Alice did it,” arise from silently collapsing identification into attribution. FACT treats that collapse as a methodological failure.

## 2.3 Identity Layers and Attribution Categories

Digital actions typically map to intermediate identity constructs rather than directly to persons. FACT formalizes this by defining a set of **identity layers**:

- **Artifact identification:** log entries, files, registry keys, database records, metadata, timestamps, protocol traces, and similar technical objects.
- **Device identification:** physical or virtual systems (endpoints, servers, mobile devices, virtual machines, cloud instances).
- **Account identity:** credentials, tokens, or identity objects used for authentication or authorization (usernames, SSO identities, API keys, service accounts).
- **User identity:** the system-level login or interactive session context active when the action occurred.
- **Person identification:** a real-world human actor.

Building on this ontology, FACT distinguishes three categories of attribution:

- **Technical attribution:** associating observed activity with specific artifacts, devices, accounts, or other technical identities. This is within the core expertise of both digital-forensic examiners and practitioners. It does *not* by itself establish who, as a person, acted.
- **Investigative attribution:** integrating digital and non-digital evidence (physical, testimonial, contextual, behavioral, organizational) to identify the most plausible person and to exclude or appropriately limit reasonable alternatives. This is primarily an investigative function, including when performed by someone who also serves as an examiner.
- **Legal attribution:** formal assignment of responsibility by a court, tribunal, regulator, or internal adjudicative body under the applicable burden of proof.

A central FACT principle is that **linking layers**, for example, from device to person, or from account to person, must be justified with explicit evidence and articulated reasoning. Habit, convenience, role expectations, or organizational pressure do not constitute justification. The identity-layer structure is used throughout the FACT lifecycle to prevent devices, accounts, or sessions from being silently treated as human identities.

## 2.4 Propositions and Competing Hypotheses

FACT adopts a **proposition-based** structure consistent with established practice in forensic interpretation. For a given digital action (or class of actions), the primary propositions are:

- $H_p$ : The named person  $P$  performed the relevant digital action. E.g. “Alice sent the email.”
- $H_a$ : Someone other than  $P$  performed the action. E.g. “An unknown person accessed Alice’s workstation and sent the email.”

In many cases,  $H_a$  will be further specified into concrete alternatives, such as:

- another household member, coworker, or administrator,
- an unknown external intruder,
- an automated process or scheduled task,
- an AI system or synthetic agent acting under configured rules or learned behavior.

Under FACT, the goal is **not** to “prove”  $H_p$  in isolation. The question is how strongly the totality of the evidence supports  $H_p$  **relative to**  $H_a$  and any specified alternative propositions.

FACT treats such failures as departures from proper attribution practice. The requirement to formulate and address competing propositions is carried forward into the evidence-convergence, falsification, and reporting stages of the framework.

## 2.5 Roles and Attribution Boundaries: Examiner, Investigator, Practitioner

In practice, the same person may perform technical analysis, investigative reasoning, and case presentation at different times. FACT therefore defines **roles** in functional terms rather than job titles and assigns different attribution boundaries to each role.

### **Examiner / Analyst**

An **examiner** (or technical analyst) performs **isolated technical analysis** of digital artifacts, devices, accounts, and systems. Examiners focus on **identification and technical attribution**, ie, what happened, on which system, under which account or identity object, without drawing conclusions about which person acted.

In this role, the examiner/analyst:

- acquires and analyzes artifacts,
- describes the presence, absence, and characteristics of digital traces, and
- states which devices, accounts, or sessions are associated with digital actions.

Examiners may be aware of non-technical case facts needed to scope and prioritize their work (for example, which custodians are relevant, which date ranges matter), but under FACT they **must not** allow allegations, interviews, or contextual narratives to stretch or reinterpret what the artifacts themselves support. In reports and testimony, examiners remain in the lane of:

*“This device, this account, this action, at this time, with these uncertainties,” and do not state that a particular person “did it.”*

Once a digital examiner begins to collect, review, or rely on evidence beyond the imaged device and its derivative artifacts, such as interviews, CCTV, financial records, physical evidence, HR files, or witness statements, they are no longer acting solely as an examiner. Functionally, they have stepped into the practitioner-investigator role and assume the investigative responsibilities and risks that go with it.

#### Note on Forensic Scientists:

When a digital forensics scientist operates strictly within the technical boundaries of artifact analysis, without integrating contextual evidence, drawing conclusions about real-world actors, or forming case-level hypotheses, they are functionally performing in the **examiner role** under the FACT framework. This applies regardless of title, expertise, or seniority.

The examiner role is defined by **scope of function**, not credentials. A scientist engaged solely in interpreting digital traces (e.g., timestamps, file system behavior, log activity) without extending into investigative synthesis is subject to the same attribution constraints as any other examiner: attribution must stop at the identity-object or account level and must not extend to person-level conclusions.

#### Investigator

An investigator is the reasoning role responsible for formulating and comparing propositions ( $H_p$  vs  $H_a$ ), integrating digital and non-digital evidence, and deciding whether person-level attribution is defensible or whether the correct outcome is non-attribution. Investigators operate primarily at the level of investigative attribution:

*"Given all available evidence and tested alternatives, [Person X] is the most likely actor for [Action Y] at [Date/Time], subject to the stated uncertainties."*

Investigators may or may not perform hands-on technical work, but within FACT their distinctive function is to reason **across** identity layers and evidence streams, not to solely forensically process media. Their conclusions must explicitly account for alternative actors, limitations, and uncertainty.

#### Practitioner (Umbrella Term)

A practitioner is any DF/IR professional who performs one or more of these roles over the course of a case or career. Many practitioners act as both examiner and investigator at different times. FACT uses **practitioner** as the umbrella term and then distinguishes what the practitioner is doing in a given step:

- when they are carving data, parsing logs, etc., they are acting as an **examiner**;
- when they are weighing hypotheses about who acted, integrating interviews, physical access records, and digital traces, or considering other evidence streams as part of their examination, they are acting as an **investigator**.

Practitioners are at risk of accidental attribution when drifting into investigative conclusions without formally changing roles or applying convergence standards. FACT requires strict boundary discipline to avoid attribution by assumption.

#### Mixed Roles and Documentation Requirements

FACT does not require strict organizational separation between examiner and investigator roles, but it treats mixed-role situations as a specific risk that must be managed. When a single practitioner occupies both roles in the same matter, FACT requires:

- **Explicit role labeling** in notes and reports (for example, sections titled "Technical Analysis (Examiner Role)" versus "Attribution Reasoning (Investigator Role)",

- **Mindset transitions**, moving deliberately from “describe what the data show” to “evaluate who most likely acted,” strive to blind themselves to contextual bias, and
- **Attribution boundaries**, ensuring that even when one person fills both roles, technical findings and attribution conclusions are clearly separated and that legal attribution remains reserved for the appropriate adjudicative body.

This functional role model allows FACT to be applied in small teams, solo-practitioner environments, and large organizations while preserving the distinction between what the artifacts show and what can be said, defensibly, about who acted.

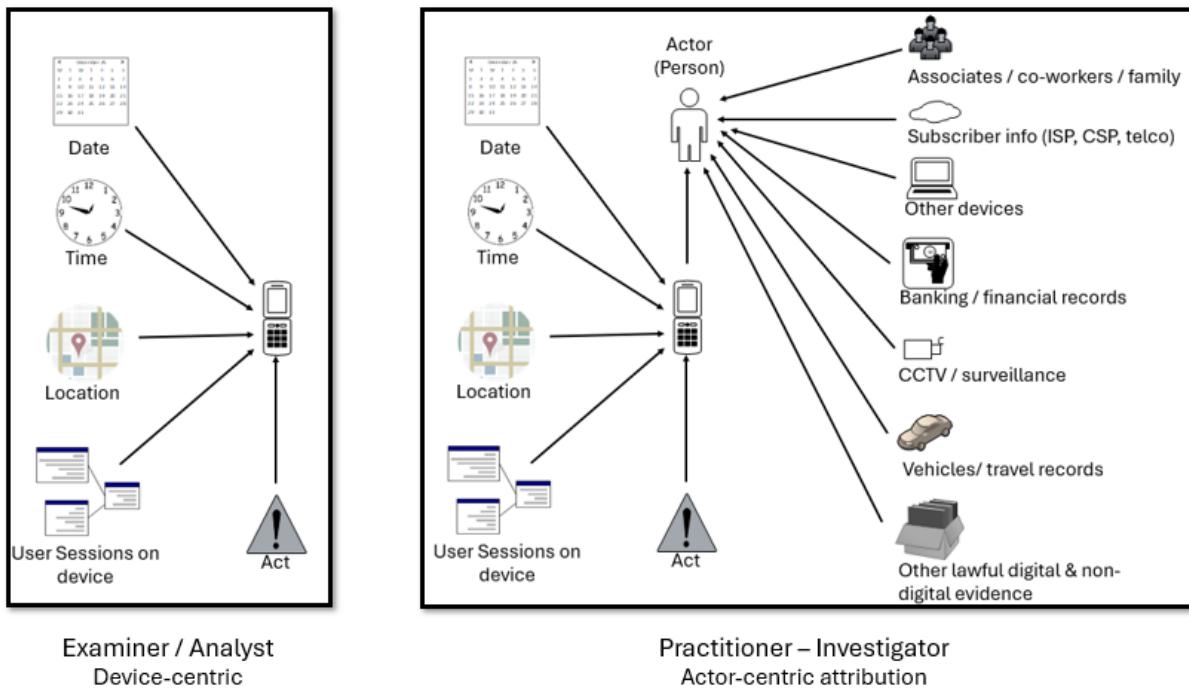


Figure 1 Roles in digital forensics

### Role separation in practice

Figure 1 contrasts DF roles. On the left, the examiner is bounded by the device: date, time, location, and accounts or user sessions on that device converge on the Act. Attribution at this stage is **technical attribution** only as the examiner can say what happened, when, where, and under which account on the device, but not who the real-world actor is.

The right panel shows the practitioner–investigator extending beyond that boundary. The same device-level findings become one stream among many: associates and family, subscriber records, other devices and systems, banking and financial records, CCTV and access logs, surveillance, vehicles and travel records, and other lawful digital and non-digital evidence.

These streams converge on the Actor (Person) to support or refute competing hypotheses about which candidate is most likely responsible for the act.

At this stage, the practitioner–investigator reaches a person-level attribution conclusion: given all realistic candidates, they identify which specific individual is best supported by the converged evidence, which alternatives were considered and ruled out, and what uncertainty remains.

When testifying **as a fact witness**, they describe that outcome in terms of investigative steps and focus, for example:

*"Based on the evidence we collected and reviewed, our investigation focused on [Name] as the primary suspect, and I forwarded that case for charging,"*

without offering comparative probability opinions between candidates.

When qualified **as an expert witness**, they may go further and give a structured attribution opinion at the actor level, for example:

*"In my opinion, based on my training and experience and my review of the digital, documentary, and testimonial evidence, [Name] is more likely than the other realistic candidates to have performed the acts in question; I considered [A, B, C] as alternatives and ruled them out for the following reasons, and these are the uncertainties that remain."*

In both roles, they are not making a legal finding of fact as that remains the court's function. They provide the trier of fact with a transparent, evidence-based explanation of how specific acts were tied to a specific individual.

### 3. The FACT Attribution Framework

#### 3.1 Overview and Purpose

FACT (see Figure 1) is a lifecycle framework for attribution that integrates legal authority, structured analysis, convergence of multi-stream evidence, and transparent reporting. Rather than treating attribution as a vague, end-of-report statement, FACT makes it an explicit process: starting with authority and scope, moving through evidence analysis and convergence, and ending with clearly framed attribution or non-attribution conclusions.

Each stage is designed to force practitioners to separate what the artifacts show from who they say acted, to test alternative actors, and to express uncertainty instead of hiding it.

It is designed to complement and not replace existing DFIR and incident response models, including NIST SP 800-86 and 800-61, ISO/IEC 27037 and 27043, MITRE ATT&CK, the EDRM model, SWGDE guidance, and the SOLVE-IT knowledge base. Those models address preparation, detection, response workflows, evidence handling, and adversary behavior; FACT sits above them and adds the missing attribution-specific structure where they remain silent.

In practice, organizations can keep their existing IR and evidence-handling runbooks, while using FACT whenever digital findings will be used to answer the question of who performed the act and whether that conclusion is defensible.

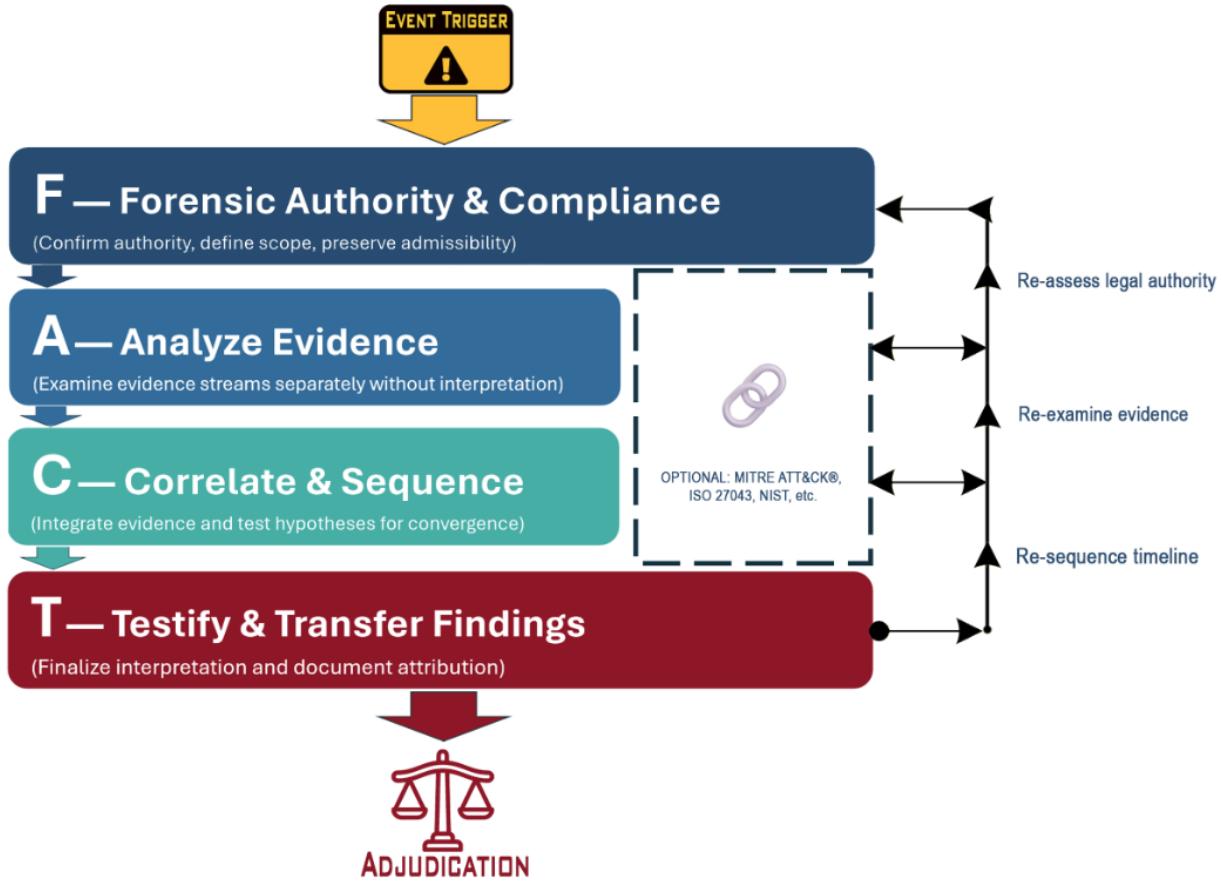


Figure 2 FACT visual illustrates this lifecycle.

At the front end, FACT constrains authority, scope, and identity assumptions so that collection and analysis are grounded in lawful, proportionate, and role-appropriate action. In the middle, it forces practitioners to articulate and test alternative actors, specify convergence thresholds, and separate technical attribution (device/account) from investigative attribution (person).

At the back end, FACT structures how any person-level attribution can be framed in reporting and testimony so that it survives legal scrutiny and does not overstate what the evidence can actually support. This overlay allows organizations to continue using their preferred operational frameworks while adding an explicit, inspectable path from “this device did X” to “this person is, or is not, responsibly tied to X.”

As FACT can overlay other frameworks (Figure 3), it provides the missing analytical and jurisprudential layer required when digital evidence will be used to attribute actions to persons. FACT, in effect, provides legal bookends to frameworks that are intended as response or evidentiary models.

It does not replace models such as ISO incident lifecycles, NIST-style IR playbooks, or EDRM-style evidence handling; instead, it sits across them and governs when and how their outputs may be used to support person-level attribution.

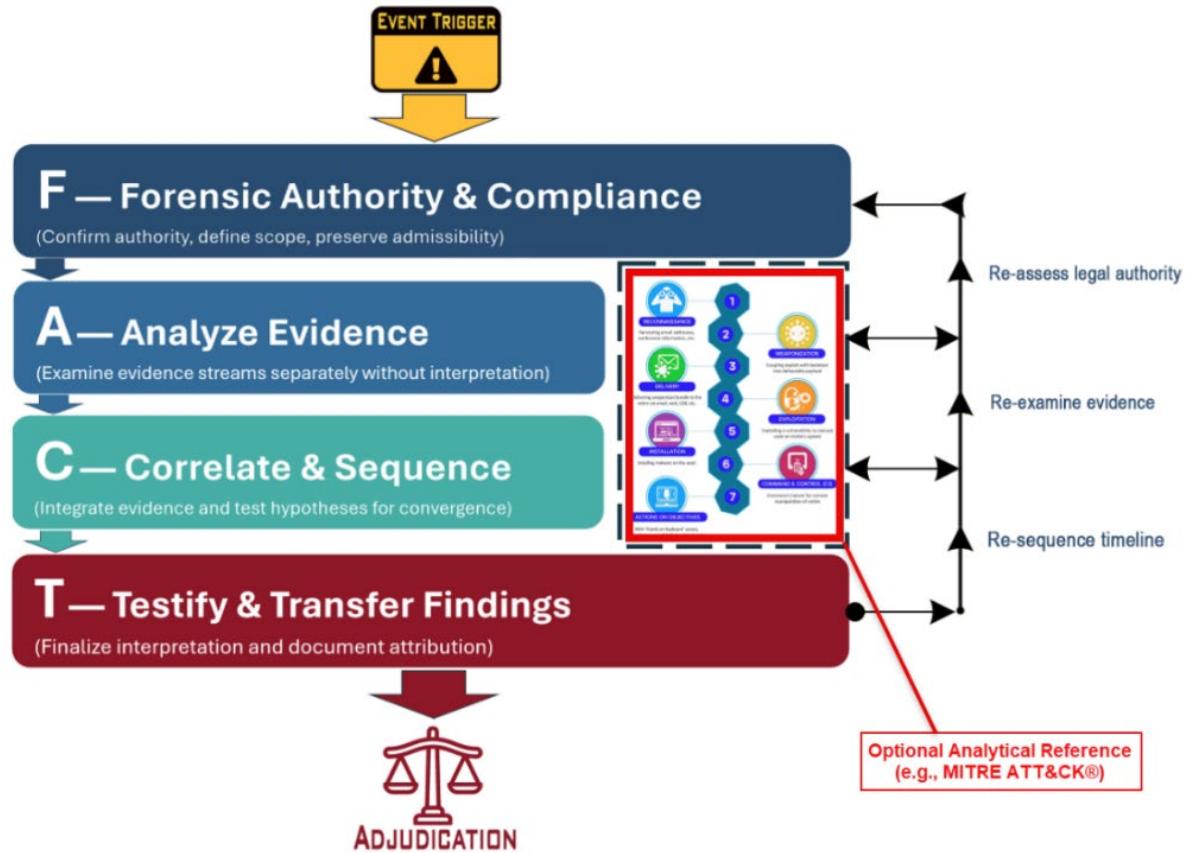


Figure 3 FACT with ATT&CK overlay (© MITRE, CC BY 4.0 license; no endorsement implied)

### 3.2 FACT Lifecycle (F → A → C → T)

The framework is organized into four stages.

Although described in a nominal F → A → C → T order, FACT is intentionally **iterative**, not strictly linear. New evidence or scope changes may require revisiting authority in F, and convergence work in C often exposes gaps that send the case back to A for further analysis. T reflects the current state of attribution being expressed and transferred, with the understanding that new evidence can move the matter back into earlier stages.

In practice, investigators often iterate A↔C several times before T is even contemplated:

#### **1. F – Forensic Authority & Compliance**

- Document legal or organizational authority (warrant, consent, statute, contract, employment policy).
- Define scope, jurisdiction, proportionality, and retention constraints.
- Establish preservation, integrity, and chain-of-custody requirements and prevent premature identity assumptions.

#### **2. A – Analyze Evidence**

- Identify the specific digital action(s) to be examined (e.g., file export, command execution, login event).
- Acquire and examine digital and non-digital evidence.

- Evaluate artifact reliability (completeness, timestamp accuracy, potential manipulation).
- Generate an initial set of candidate actors and alternative explanations (shared accounts, automation, remote compromise, malware).

### **3. C – Correlate & Converge**

- Correlate evidence across identity layers: artifact → device → account → user → person.
- Integrate and evaluate digital, physical, contextual, and testimonial evidence.
- Evaluate multi-stream convergence and test each alternative hypothesis.
- Determine whether a convergence threshold for person-level attribution is met, or whether only non-attribution is defensible.

### **4. T – Testify & Transfer Findings**

- Finalize attribution conclusions and express them with explicit uncertainty.
- Prepare reports and testimony that explain the reasoning pathway, the handling of alternatives, and the framework's limits.
- Support adjudicators or decision-makers in understanding both what is known and what must remain unresolved.

#### **3.3 Core Principles**

FACT's core contributions can be summarized as:

- Identity ≠ attribution; devices and accounts are not people.
- Digital evidence alone is insufficient for person-level attribution.
- Attribution requires multi-stream evidence convergence from independent sources.
- FACT adopts falsification as a methodological duty, consistent with forensic science best practice.
- Role separation (examiner vs investigator) must be documented, even when one person fills both roles.
- Attribution statements must be legally and ethically bounded; Practitioners should conclude and document non-attribution when conditions are not met.

### **4. Analytical Structure: Convergence, Alternatives, and Uncertainty**

#### **4.1 Evidence Convergence**

FACT recommends attribution as justified when evidence from multiple, independent streams converges on the same person while substantially weakening reasonable alternatives.

Streams may include:

- Device and system logs,
- Network and cloud telemetry,
- Physical access and surveillance data,
- Behavioral and workflow patterns,
- Testimonial and contextual evidence.

Independence is critical. Two artifacts derived from the same logging mechanism are one stream, not two. Convergence demands that:

- Streams consistently support  $H_p$ ,
- The same streams undermine or fail to support  $H_a$ , and
- Layer transitions (device → account → person) do not introduce unresolved contradictions.

As a conservative best practice, FACT expects at least two independent evidence streams before making person-level attribution. Organizational policies may dictate lower thresholds for internal actions and **exceptions can exist needing only one evidence stream, which requires explicit justification.**

#### 4.2 Falsification of Alternative Actors

FACT treats falsification as a methodological duty consistent with forensic science best practice.

Investigators must:

- Enumerate plausible alternative actors and mechanisms (other users with access, administrators, remote intruders, automated processes, AI agents).
- Ask what evidence would support each alternative and what would contradict it.
- Actively search for that evidence, rather than assuming alternatives away.

The absence of evidence about an alternative is not proof against it. If a reasonable alternative remains plausible after analysis, person-level attribution is not supportable under FACT; the correct conclusion is non-attribution.

#### 4.3 Uncertainty and Likelihood Reasoning

Digital investigations lack robust empirical error rates for many artifact types; formal Bayesian likelihood ratios are currently feasible only in a small minority of routine cases. FACT therefore uses qualitative likelihood reasoning, aligned with other forensic disciplines:

- Weak support for  $H_p$ ,
- Moderate support,
- Strong support,
- Very strong support,
- Support for  $H_a$ ,
- Inconclusive.

Every attribution conclusion must:

- Identify the specific action being attributed,
- State which person is attributed,
- Describe evidence streams and how they support  $H_p$  vs  $H_a$ ,
- Disclose uncertainties, assumptions, and conditions that could change the conclusion.

### **5. Legal and Ethical Guardrails**

#### 5.1 Legal Nexus and Global Principles

Across jurisdictions, decision-makers look for a nexus between a person and the relevant digital environment: dominion and control, access and opportunity at the relevant time, knowledge or foreseeability, and exclusion of alternative actors.

FACT models these requirements via:

- Identity-layer reasoning (device, account, user, person),
- Explicit documentation of authority, scope, and proportionality (Stage F),
- Reporting that ties attribution to evidentiary sufficiency rather than to organizational preference.

FACT is jurisdiction-agnostic: it does not bake in “beyond a reasonable doubt” or “balance of probabilities,” but produces reasoning that can be evaluated under whichever burden applies.

## 5.2 Ethical Obligations

Attribution is a high-consequence act. Misattribution can lead to wrongful conviction or termination, misplaced sanctions, damaged reputations, and loss of trust in digital forensics. FACT therefore embeds ethical constraints:

- Duty of truthfulness and transparency: clearly distinguish fact from inference, disclose limitations.
- Duty to avoid harm: refuse to overstate evidence, resist pressure to “name someone” when evidence is insufficient.
- Duty to falsify, not merely confirm: actively test whether one’s conclusion could be wrong.
- Duty to remain within scope and authority: technical capability does not authorize overreach.
- Duty to acknowledge when attribution fails: non-attribution is a correct outcome when conditions are not met.

## 5.3 AI, Automation, and Synthetic Activity

AI and automation increase the number of plausible actors and introduce synthetic artifacts (deepfakes, fabricated logs, AI-generated content). Under FACT:

- AI tools may assist with triage and organization but cannot perform person-level attribution.
- Automation and AI must be treated as explicit alternative actors when plausible.
- Synthetic or easily fabricated evidence raises the corroboration threshold and authentication requirements.
- Material use of AI in analysis must be disclosed and its outputs independently validated against source evidence.

## **6. Application Pattern: Example (Insider Database Access)**

A condensed example illustrates how FACT structures attribution. Consider an insider database-export case displayed in swim lanes:

Digital Evidence	Context / Physical Evidence	Attribution Analysis
Database audit log shows customer_export.csv created at 23:18:07.	Office access control shows only one employee (S) badged into the building between 22:00–00:00.	Only S had physical presence and the ability to operate a workstation inside the secure zone at the relevant time.
Workstation S-14 (assigned to S) shows interactive login from 23:05–23:40 using S’s credentials (password + biometric).	CCTV confirms S entering their cubicle at 23:06 and no one else in the area until after midnight.	Login and physical presence align with the exact time the export was generated.
Browser artifacts show navigation to “Export → CSV → Bulk Download” menu at 23:17.	S is one of three employees with permission to run bulk exports. The other two were off-site (VPN logs absent; no home logins).	S had role-based access, and no other authorized user was authenticated or present.
File customer_export.csv uploaded to personal Gmail via Chrome at 23:21, confirmed by upload logs.	Gmail’s IP logs match the company public IP, meaning upload occurred from inside the building, not remotely.	Upload originated from the same workstation used by S, at the same time S was present.

*Table 1: Swim lane example*

Under FACT:

- **F:** Authority to examine corporate systems and logs is documented under employer policy and applicable law.
- **A:** The contested actions (bulk export and upload) are defined; relevant artifacts and logs are forensically collected and vetted.
- **C:** Digital, physical, and contextual streams converge on Employee S as the only person with presence, access, capability, and opportunity at the critical time; alternative actors (other employees, remote intruders, automation) are investigated and reasonably excluded.
- **T:** The final attribution report states that the evidence provides strong support for the proposition that Employee S performed the export and exfiltration, compared with alternative actors, and explains the basis for that assessment and remaining uncertainties.

The same **F – A – C - T** pattern generalizes beyond insider export cases. It can be applied to shared-device households, cloud credential misuse against storage or database services, insider sabotage of production systems by administrators, business email compromise involving shared mailboxes, and ransomware deployments where local execution, remote access, and automation are all plausible.

In each of these, FACT requires the same discipline: define the digital action, separate device/account identity from person identity, correlate independent evidence streams, and either reach a defensible person-level attribution or explicitly report non-attribution.

## 7. Limitations and Failure Conditions

FACT is intentionally conservative. It defines conditions under which person-level attribution is not supportable:

- **Technical limitations:** missing or overwritten logs; opaque cloud or SaaS logging; encrypted or locked platforms that prevent execution-trace recovery; anonymizing networks (TOR, chained VPNs, proxies) that sever defensible links to individuals.
- **Investigative limitations:** shared or hot-desk environments without independent differentiation; credential sharing or theft; unresolved contradictions among witnesses or systems; insufficient scope or authority to obtain critical evidence.
- **Analytical limitations:** lack of independent corroboration; unresolved alternative actors; temporal ambiguity due to unsynchronized clocks or missing time anchors.
- **Legal and ethical limitations:** defective authority; chain-of-custody failures; methods that fail reliability standards; pressure-driven attribution.

When such conditions apply and cannot be remedied, FACT directs the practitioner to issue an explicit non-attribution finding, e.g.: “Based on the available evidence and applying the FACT Framework, a person-level attribution for Action Y cannot be made. Several reasonable alternative explanations remain, and device or account association alone is insufficient.”

## 8. Validation and Practitioner Feedback

FACT v1.0 is presented as a **practitioner-oriented framework**, not a finalized academic theory.

A pre-release review by 36 of 45 invited experienced practitioners and stakeholders (law-enforcement, corporate DFIR, private consultants, academics, and attorneys) confirmed that existing frameworks do not offer a structured, defensible approach to person-level attribution and that FACT directly and effectively addresses this gap. Reviewers overwhelmingly rated the four-stage model as clear and well-communicated, agreed that FACT adds significant value beyond current standards, especially in legal and

evidentiary rigor that strengthens courtroom defensibility, and stated they are likely to adopt elements of the framework for reports, expert testimony, and training.

Criticisms focused less on conceptual flaws and more on practical concerns: perceived complexity, documentation overhead, and the need for worked examples, templates, and organizational buy-in.

## 9. Discussion and Conclusion

Attribution has long been digital forensics' weakest, **least formalized component**. Existing models focus on evidence handling, adversary behavior, or incident workflows, but rarely treat *who performed the act* as the central forensic question. FACT addresses this by:

- Framing digital forensics as a forensic jurisprudence discipline in legal matters.
- Separating identification from attribution and making identity layers explicit.
- Requiring that attribution be built on competing propositions, multi-stream convergence, and falsification of alternatives.
- Embedding legal and ethical guardrails, including authority, proportionality, and non-maleficence.
- Providing reporting requirements that make reasoning transparent, reproducible, and suitable for adversarial and inquisitorial systems.

Importantly, FACT is clear about its limits. It does not claim that attribution is always possible. In environments dominated by shared access, missing logs, anonymization, opaque cloud systems, or unresolved automation and AI alternatives, FACT directs the practitioner to reach a non-attribution conclusion. A framework that cannot refuse attribution cannot be trusted when it asserts attribution.

FACT is intended as a foundation rather than an endpoint. Future work includes deeper empirical studies... more detailed mappings to other models such as ISO/IEC 27043 (International Organization for Standardization, 2015), CASE/UCO (Casey et al., 2018), and SOLVE-IT (Hargreaves et al., 2025).

In an era of remote access, synthetic media, autonomous systems, and fragmented cloud telemetry, digital forensics cannot rely on intuition, single-stream artifacts, or tool-centric narratives to answer the most consequential question: **Who did it?**

FACT offers a principled, globally compatible method for answering that question and, just as importantly, for recognizing when it cannot yet be answered responsibly.

In practice, FACT is intended to be used alongside existing IR and DF workflows: as a checklist when planning authority and scope, as a reasoning scaffold when weighing candidate actors, and as a reporting structure for attribution conclusions and non-attribution findings.

## References

- Spichiger, H. (2025). Please mind the gap: A taxonomy for addressing the issue of linking person, account and device. *Science & Justice*, 65(5), 101314. <https://doi.org/10.1016/j.scijus.2025.101314>
- Shamsi, J. A., Zeadally, S., Sheikh, F., & Flowers, A. (2016). Attribution in cyberspace: Techniques and legal implications. *Security and Communication Networks*, 9(15), 2886–2900.  
<https://doi.org/10.1002/sec.1485>
- Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 38(1–2), 4–37.  
<https://doi.org/10.1080/01402390.2014.977382>
- Thompson, W. C. (2011). What role should investigative facts play in the evaluation of scientific evidence? *Australian Journal of Forensic Sciences*, 43(2–3), 123–134.  
<https://doi.org/10.1080/00450618.2010.541499>
- 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>
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide* (NIST Special Publication 800-61, Rev. 2). National Institute of Standards and Technology.
- International Organization for Standardization. (2012). *ISO/IEC 27037:2012—Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence*.
- International Organization for Standardization. (2015). *ISO/IEC 27043:2015—Information technology—Security techniques—Incident investigation principles and processes*.
- Scientific Working Group on Digital Evidence. (2018). *SWGDE best practices for digital evidence collection* (Version 1.0). <https://www.swgde.org>
- MITRE Corporation. (n.d.). *MITRE ATT&CK®: Adversarial tactics and techniques knowledge base*. Retrieved December 8, 2025, from <https://attack.mitre.org>
- EDRM. (n.d.). *EDRM model*. Electronic Discovery Reference Model. Retrieved December 8, 2025, from <https://edrm.net>
- Hargreaves, C., van Beek, H., & Casey, E. (2025). SOLVE-IT: A proposed digital forensic knowledge base inspired by MITRE ATT&CK. *Forensic Science International: Digital Investigation*, 52, 301864.  
<https://doi.org/10.1016/j.fsidi.2025.301864>
- Casey, E., Barnum, S., Griffith, R., Snyder, J., van Beek, H., & Nelson, A. (2018). The evolution of expressing and exchanging cyber-investigation information in a standardized form. In M. A. Biasiotti, J. Mifsud Bonnici, J. Cannataci, & F. Turchi (Eds.), *Handling and exchanging electronic evidence across Europe* (pp. 43–58). Springer. [https://doi.org/10.1007/978-3-319-74872-6\\_4](https://doi.org/10.1007/978-3-319-74872-6_4)
- All third-party marks are the property of their respective owners. Their use here does not imply endorsement.

## **Author**

Brett Shavers is an independent researcher, practitioner, author, and trainer in digital forensics and incident response. He is the founder of the *Placing the Suspect Behind the Keyboard*® initiative and the PSBK™ Training System.

---

The FACT Attribution Framework™ v1.0, including all text, figures, terminology, diagrams, and visualizations, is © 2025 Brett Shavers. All rights reserved.

Non-commercial use is freely permitted for the following purposes only, provided full attribution to the author and this document is retained and the framework is not rebranded or modified:

- personal professional practice,
- internal government, law-enforcement, or corporate investigations and training,
- academic teaching, research, theses, and non-commercial publications,
- inclusion and reference in reporting and testifying.

Any use in paid or for-profit training courses, workshops, certifications, conferences, consulting offerings, or any other commercial product or service — including merely teaching or presenting the FACT framework (in whole or in part) to paying attendees — is strictly prohibited without prior written permission from the author.

Critique, comparison, or citation of FACT in commercial publications or presentations is allowed only if the framework itself is not taught or distributed as part of the paid offering.