

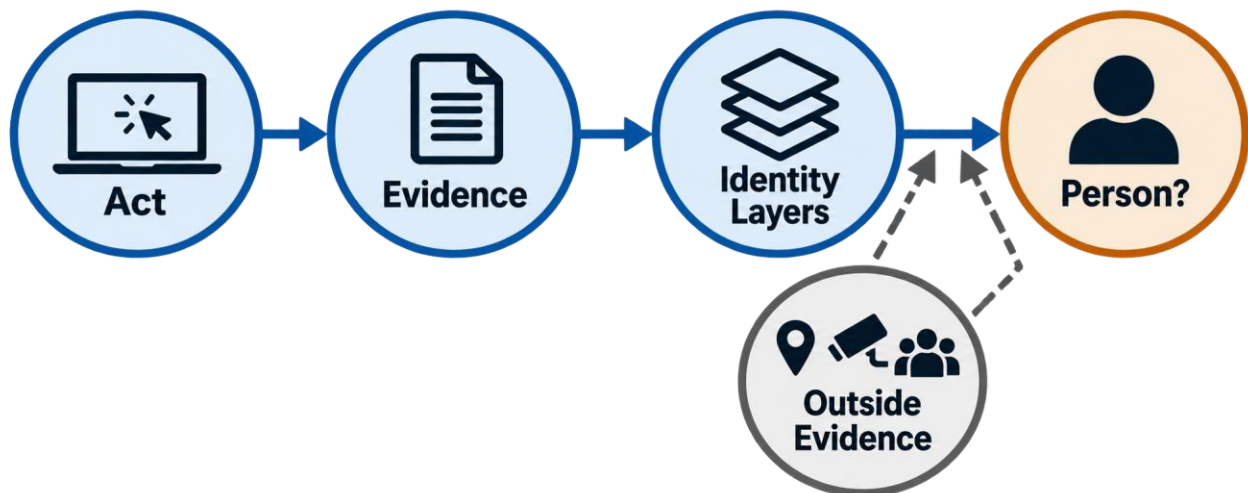
THE ATTRIBUTION STRESS TEST

Identifying digital activity does not establish who performed it.

The **Attribution Stress Test** is a short, practical reference designed to challenge assumptions before reaching a conclusion. Its six questions help investigators examine what the evidence supports, identify gaps, test alternative explanations, and determine whether person-level attribution is justified.

Based on the [FACT Attribution Framework](#), this guide helps investigators separate what the evidence establishes from what they assume, test competing explanations, and recognize when attribution cannot be supported.

The purpose of person-level attribution is to determine whether the evidence supports connecting a specific person to a specific act. Don't mistake technical identification for human attribution.



BEFORE YOU NAME THE ACTOR

You may have identified the device, account, session, and digital activity. You may even have a likely suspect. But how much of that conclusion is supported by evidence, and how much depends on assumptions?

Attribution requires more than finding evidence that points toward someone. It requires testing the connections, considering other possible explanations, and recognizing what remains unknown.

Before concluding who performed the act, put your evidence through these six questions.

THE SIX QUESTIONS



1. STATE THE ACT (NOT THE PERSON)

What specific action does the evidence establish?

Start with legal authority to access the evidence. Separate what was observed from what is inferred. Identify the action, date, time, and relevant system or device. Do not assume that activity associated with an account or device identifies the person who performed it.

2. IDENTIFY THE SOURCE

What evidence supports your finding, and how reliable is it?



Identify the original artifacts, logs, records, or other evidence supporting the action. Consider completeness, timestamp accuracy, possible manipulation, and alternative interpretations.

3. MAP THE IDENTITY LAYERS

What evidence connects the digital act to a specific person?"



Examine the relationships among the artifact, device, account or credential, session context, and possible human actor. Identify which connections are supported, inferred, or unresolved. Do not treat device ownership, account assignment, or an authenticated session as proof of human activity.

4. TEST ACCESS AND CONTROL

Who else could have performed the act?



Consider physical access, shared devices, compromised credentials, remote access, delegated authority, and automated processes. Examine independent evidence such as surveillance, witness statements, access records, and other information that may connect or exclude possible actors.

5. CHALLENGE CORROBORATION

Does your evidence provide independent support, or are you counting the same source more than once?



Multiple artifacts do not necessarily mean multiple independent sources. Determine whether findings have distinct causal origins or merely repeat information from the same event or system. Evaluate whether digital + non-digital evidence converge on the same actor.

6. TRY TO DISPROVE YOUR CONCLUSION

What evidence could show that your proposed attribution is wrong?



Identify reasonable alternative actors and explanations. Look for evidence that supports or contradicts each possibility. Consider missing evidence, incomplete records, conflicting timelines, and investigative gaps.

THE STOP RULE

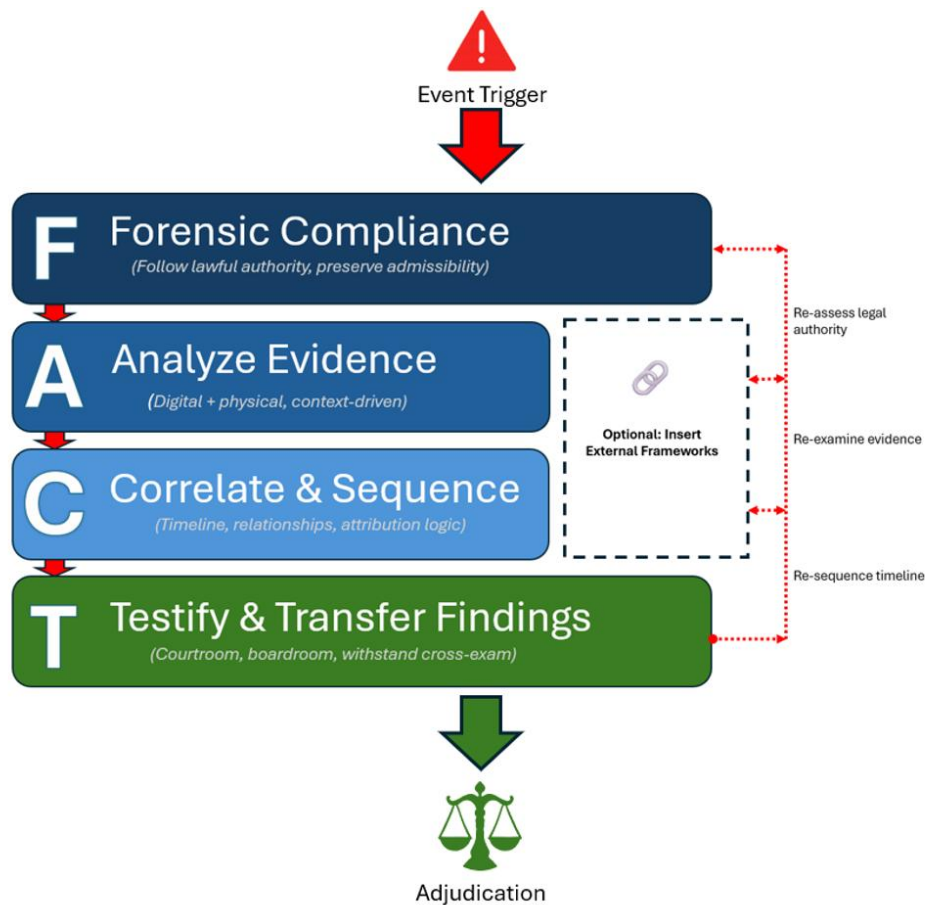
If the evidence does not establish who performed the act, limit your attribution conclusion to what the evidence supports (that doesn't mean to stop investigating!).



Report the supported findings, explain what remains unresolved, and document when person-level attribution cannot be made.

An account is not a person. Access is not proof of operation. Suspicion is not attribution.

The purpose is not to avoid attribution. It is to make sure the evidence supports it.



*Based on the FACT Attribution Framework v1.1 - Brett Shavers (2025).

<https://zenodo.org/records/18005597>