

Four Kinds of Investigation, Four Bars of Proof

Wed, Sep 2, 10:00 AM EDT · <https://scottslab.io/posts/investigation-types-and-evidence-standards>



TL;DR

The kind of investigation you're in sets how strong your evidence has to be: operational (fix the tech, no legal exposure, low bar), criminal (government-led, "beyond a reasonable doubt"), civil ("preponderance of the evidence"), and regulatory (borrows whichever standard the underlying case turns out to be). There's a lesser-known third standard, "clear and convincing evidence," that sits between the other two. Two ideas govern all four regardless of label: Locard's exchange principle, the actual reason there's evidence to collect, and the interview/interrogation line, which is yours to stay on the right side of.

Before you collect a single log, know which kind of investigation you're in, because it sets how rigorous everything downstream has to be. Four types pull cybersecurity people in, and they don't share a bar.

An operational investigation resolves a technical infrastructure problem: an outage, a misconfiguration, a service that fell over. There's no legal action at the end, so the evidence bar is low; you're solving a problem, not building a case. A criminal investigation is government-led and carries the highest standard of proof there is, "beyond a reasonable doubt," because someone's liberty is on the line. A civil investigation is a dispute between parties, and its standard is lower: "preponderance of the evidence," essentially more-likely-than-not, just over half, no more precision

than that. A regulatory investigation can be civil or criminal in nature, so its standard simply matches whichever kind of case it turns out to be.



Four Kinds of Investigation, Four Bars of Proof

The standard nobody mentions

Most people stop at two standards and call it done. There's a third, sitting between them: **clear and convincing evidence**. In *Colorado v. New Mexico* (1984) the Supreme Court described it as requiring an "abiding conviction" that the factual contentions are "highly probable". That's a real step up from more-likely-than-not, but short of eliminating reasonable doubt.

You'll run into it in certain civil claims (fraud is the textbook example) and in some administrative and regulatory proceedings, professional license revocations among them. Which proceedings use it and which default to preponderance varies by jurisdiction and by statute, so don't assume; check the rule that governs the specific forum you're in. The reason to know this standard exists at all is that a regulatory investigation isn't automatically "the easy one" just because nobody's going to prison. You might be building a case against a middle standard you didn't know you had to clear.

Why any of this works at all

Underneath all four types is one idea from a French criminologist a century before any of this was digital: **Locard's exchange principle**: every contact leaves a trace. Edmond Locard's observation was about physical crime scenes, but it's the entire premise of digital forensics too. An intruder who touches a system leaves something behind: a log entry, a timestamp, a process that shouldn't exist, a file that got read. The job of any investigation, at any evidence bar, is finding that trace and proving it means what you think it means. If nothing were ever exchanged, there'd be nothing to investigate. The principle is why the discipline exists, not just a fact about it.

Interviews, not interrogations

One working note matters regardless of type: know your lane on people. As a security professional you conduct **interviews**: voluntary conversations to gather information. **Interrogations** are adversarial, rights-bound, and aimed at a confession, and they're a law-enforcement function, not yours.

The legal reason this line exists is worth knowing precisely, because it's not just etiquette. *Miranda v. Arizona*, 384 U.S. 436 (1966), requires warnings before **custodial interrogation by police**. It's a constraint on state action. A private employer running an internal investigation isn't bound by it; nobody has to Mirandize an employee. That doesn't mean coercive tactics are free of consequence. Pressure someone into a statement and you're exposed to claims of false imprisonment, defamation, or wrongful termination that have nothing to do with criminal procedure and everything to do with how you conducted yourself. Blur the interview/interrogation line and you don't just risk tainting a case; you create a second one, against you.

Even the low-bar operational investigation demands root-cause analysis, not symptom resolution. Restarting the service that crashed isn't an investigation, it's a reset. Finding *why* it crashed is the investigation. It's still evidence, even with no court in sight.

The test that applies no matter which type you're in

RFC 3227, the IETF's guidelines for evidence collection, sets out a five-property test for computer evidence that's a useful closer here because it doesn't care which of the four types you're running: evidence has to be **admissible** (conforms to the legal rules of the forum), **authentic** (positively tied to the incident), **complete** (tells the whole story, not one angle of it), **reliable** (nothing about its handling casts doubt on it), and **believable** (a court can actually follow it).

That's the throughline. The investigation type tells you how high the bar is. These five properties tell you what clearing it actually looks like, and they're the same five whether you're closing out a misconfigured firewall or handing a case to a prosecutor.