

Evidence That Actually Holds Up: Types and Admissibility

Wed, Sep 2, 6:00 PM EDT · <https://scottslab.io/posts/evidence-types-and-admissibility>



TL;DR

Three kinds of evidence: real (tangible objects), documentary (written or digital records: logs, contracts), and testimonial (what a witness saw, or what an expert concludes). Documentary evidence has to be authenticated under Federal Rule of Evidence 901. Or, since a 2017 amendment, it can self-authenticate by hash value under FRE 902(14), which is exactly why forensics hashes everything. Logs get into evidence as business records under FRE 803(6), unless the other side shows they weren't trustworthy. And expert testimony (the thing that lets an analyst say "this pattern indicates an intrusion" rather than just "here are some logs") has to clear a reliability test that traces back to a Supreme Court case about a morning-sickness drug.

Collecting evidence is easy; collecting evidence that survives a courtroom is the actual skill. It comes in three types. Real evidence is tangible: the actual seized hard drive or laptop. Documentary evidence is written or digital records: logs, contracts, emails. Testimonial evidence is a person: either direct observation ("I saw X") or an expert's opinion.

Real
tangible objects (the actual hardware)

Documentary
written / digital records (logs, contracts)

Testimonial
witness observation or expert opinion

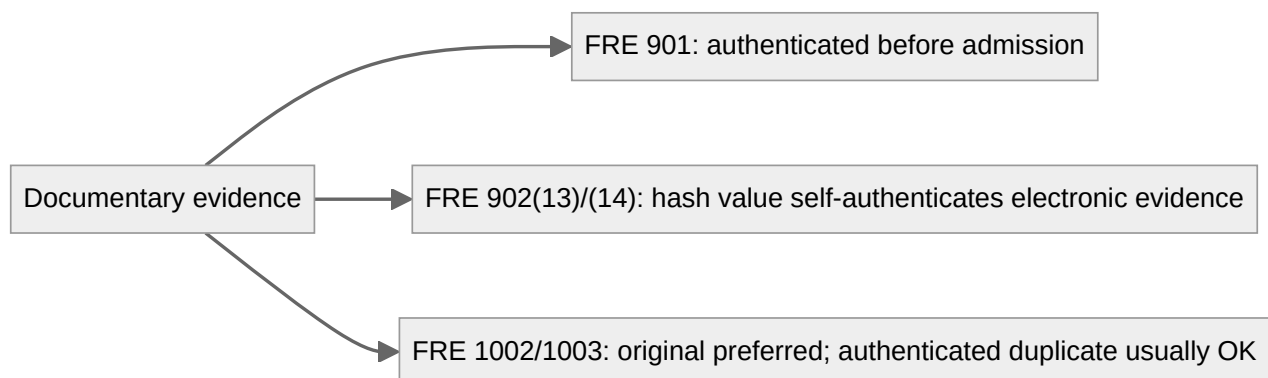
Getting documentary evidence in the door

Documentary evidence (the category most of our logs fall into) carries the rules worth memorizing, and they're specific enough to cite by number.

Authentication comes first. FRE 901 requires "evidence sufficient to support a finding that the item is what the proponent claims it is." Someone has to establish that this log really is what you say it is, from where you say it came. FRE 902 then lists categories that are **self-authenticating**, meaning no witness has to say so out loud: certified domestic public records, certified business records under 902(11), and (added by a 2017 amendment specifically for this world) 902(13) and 902(14), which let a party authenticate electronic evidence and data copied from a device or storage medium by **hash value** alone, via written certification, instead of dragging a witness into court. The rule committee's own note is blunt about why: producing a live authentication witness is often unnecessary expense when a hash proves the point just as well. This is the actual legal payoff of the hashing discipline in forensics. It isn't just good hygiene. It's what lets a disk image self-authenticate.

The best evidence rule generally requires the original to prove contents (FRE 1002), though a duplicate is admissible to the same extent as the original unless a genuine question is raised about the original's authenticity or admitting the copy would be unfair (FRE 1003). That's exactly why forensics hashes an image back to the source: the hash match is what turns "a copy" into "an authenticated duplicate."

The parol evidence rule is a different animal. It's contract doctrine, not a rule of evidence, and it says a written contract can't be modified by a verbal side-agreement. Worth knowing, easy to conflate with the rules above, genuinely a separate body of law.



Getting documentary evidence in the door

Why your log is (usually) admissible at all

A security log is hearsay by the textbook definition: an out-of-court statement offered to prove the thing it asserts (FRE 801). It gets in anyway, almost every time, through the **business records exception**, FRE 803(6): a record of an event made at or near the time by someone (or something) with knowledge, kept in the course of a regularly conducted activity, where making the record is that activity's regular practice, shown by a custodian's testimony or a 902(11)/(13) certification.

The trap is in the rule's own escape hatch: it doesn't apply if "the source of information or the method or circumstances of preparation indicate a lack of trustworthiness." That's the actual failure mode. A log nobody reviews, a system with no defined logging practice, a pipeline that drops or reorders events: none of that is a hearsay problem on paper, but it's exactly the kind of thing opposing counsel uses to argue the exception shouldn't apply. Reliable logging isn't just an operations best practice; it's the thing standing between your evidence and a successful objection.

The expert-witness exception, and where its standard comes from

A regular witness under FRE 701 can only testify to what they directly perceived. FRE 702 carves out the exception that makes forensic analysis useful at all: an expert may testify in the form of an opinion (draw a conclusion, not just report a fact) if the court finds it more likely than not that the testimony rests on sufficient facts, reliable principles and methods, and a reliable application of those methods to the case. (That "more likely than not" framing is recent: a 2023 amendment tightened the rule to make the reliability gate an actual finding the court has to make, not a box to check.)

That reliability standard traces back to *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993). It held that the Federal Rules, not the older "general acceptance" test from *Frye v. United States* (1923), govern admissibility of expert scientific testimony in federal court. Some state courts still apply *Frye*; it hasn't disappeared, it's just not the federal rule anymore. Either way, the expert exception is the whole reason a forensic analyst can look at a pile of logs and testify "this pattern indicates an intrusion" instead of reciting timestamps and hoping the jury connects the dots. That inference is the value we add, and it's admissible precisely because a court found the method behind it reliable, not because the analyst has a good reputation.

The throughline: finding the evidence is half the job. Authenticating it, fitting it through a hearsay exception, and (if you're the one drawing conclusions from it) meeting the reliability bar for expert testimony, is the other half. Evidence that can't clear all three is the same as no evidence at all.