FOR LEGAL PROFESSIONALS / INVESTIGATION METHODS

Evaluate AI-assisted material in a crypto investigation

Ask how AI was used, which claims were checked and what source material supports an investigative output.

01 Identify the role AI played

Identify the AI task, inputs and human review. Automation can organise records and surface leads. For example, an investigator checks a suggested service connection against sources and alternatives before recommending an enquiry. Validation makes the suggestion useful.

02 Treat convincing presentation as a separate question from authenticity

Preserve original messages or media and their context when authenticity is in issue. Convincing presentation does not establish identity. Do not assume an inconsistency proves AI use or treat an automated detector as conclusive.

03 Verify the claims that could affect the case

Check material dates, addresses, amounts and citations against retained sources. Ask what evidence supports a suggested link and what a confidence score actually means. Record corrections that affect the conclusion; fluency and numerical precision do not establish reliability.

04 Document use without exposing the case unnecessarily

Document the relevant tool, task, review and limitations. Establish permitted handling, retention and access before sharing case material with external AI services. The final expert conclusion should be explainable and supported independently of an impressive software demonstration.

Example. In a fictional draft, an AI summary cites a court decision for a proposition about wallet ownership. The review task is to locate the actual decision and check the proposition, rather than accepting the citation because its format looks correct.

Review checklist

- ☐ I can describe the specific task performed by AI.
- ☐ I have checked material claims against retained sources.
- ☐ I have recorded relevant limitations and human review.
- ☐ I have confirmed appropriate handling of confidential inputs.

General educational framework; assess legal steps and expert requirements in the relevant jurisdiction. Example is fictional.

References: FBI: generative AI and financial fraud / NIST: Generative AI Risk Management Profile