Detecting AI-Generated, Deepfake, or Digitally Manipulated Evidence in a Military Case

Published August 24, 2026

Executive Summary

Detecting AI-Generated, Deepfake, or Digitally Manipulated Evidence in a Military Case requires a defense investigation that is organized around verifiable sources, not labels or assumptions. The central task is testing provenance, source files, metadata, generation history, and contextual corroboration before accepting or rejecting synthetic-media claims.

The investigator should preserve original material, document collection methods, identify what each source can and cannot establish, and keep unresolved questions visible for counsel. This publication provides a practical framework for doing that work without substituting investigative judgment for legal advice.

Why This Article Exists

DI-097 addresses a recurring defense problem: a concise allegation or government conclusion may conceal separate questions of source, timing, attribution, completeness, and reliability. If those questions are not assigned and documented early, important records may disappear and unsupported language may be repeated as fact.

The purpose is not to manufacture doubt. It is to give counsel an evidence-based record that distinguishes confirmed facts, disputed facts, reasonable inferences, and unknowns.

The Fundamental Difference

An investigative lead is not evidence, and evidence is not automatically proof of the proposition for which it is offered. A record may be authentic but incomplete. A witness may be sincere but mistaken. A scientific result may be reliable within a narrow scope but overstated in a summary.

The defense investigator therefore traces each important conclusion backward: conclusion, supporting fact, original source, collection method, and limitation. When that chain breaks, the break becomes a specific follow-up task rather than a generalized suspicion.

Discussion

Define the Question Before Collecting Material

Counsel should identify the factual proposition being tested and the legal or strategic purpose of the work. The investigator can then collect relevant material without sweeping in unrelated private information or creating an unfocused file that obscures the issue.

Build a Source and Custodian Map

For each potential source, record who controls it, the relevant date range, retention risk, lawful access route, collection status, and next responsible person. Separate records known to exist from records merely believed to exist.

Preserve Originals and Record Method

Preserve originals whenever possible. Record the device, account, location, custodian, date, tool or process, file names, and any transformations. Working copies, excerpts, demonstratives, and translations should remain traceable to the source from which they were made.

Test Completeness, Attribution, and Timing

Ask whether the source is complete, whether the person or device is correctly attributed, whether clocks and time zones align, and whether missing material changes meaning. A timeline should cite its source and show conflicts rather than silently choosing one version.

Report Limits as Clearly as Findings

A useful report explains what was confirmed, what was contradicted, what remains unknown, what could not be obtained, and why. It avoids absolute language when the underlying evidence supports only a narrower statement.

Evidence the Defense Should Inventory

- The earliest available file and acquisition path.
- Encoding, metadata, edits, hashes, and platform recompression.
- Voice, face, lighting, timing, and environmental consistency.
- Independent records that corroborate the depicted event.
- The original source supporting every material summary or conclusion.
- Unsuccessful requests, missing items, access restrictions, and follow-up deadlines.

Practical Case Example

A short audio clip is alleged to be synthetic. The defense obtains the original file, longer recording, device history, and surrounding communications before consulting an expert. The inquiry avoids treating either an online detector score or a visual impression as a final conclusion.

Investigative Lesson

The example demonstrates that the defense gains the most value by narrowing the disputed proposition, locating the best independent source, and documenting limitations before drawing conclusions. The investigator should neither minimize unfavorable evidence nor exaggerate a gap. Both must be described accurately.

Source

Manual for Courts-Martial, United States (2024 ed.), M.R.E. 702 and 901.

National Institute of Standards and Technology, AI Risk Management Framework 1.0 (2023).

10 U.S.C. § 846 (Article 46, UCMJ).

Joint Service Committee on Military Justice, Current Publications and Updates (current page reviewed August 24, 2026), identifying the 2024 Manual for Courts-Martial and subsequent amendments.

From the Investigator's Desk

The best investigative question is usually not “Which side does this help?” It is “What exactly does this source establish, how do we know, and what would allow another reviewer to verify it?” That discipline protects counsel from surprises and makes favorable evidence more persuasive because its limits have already been tested.

A defensible work product is organized so that counsel can move from a conclusion to the underlying evidence without guessing. Dates, identifiers, custodians, collection history, and unresolved issues should be visible at a glance.

Investigator's Guidance

- Confirm scope, priorities, deadlines, and contact restrictions with counsel before acting.
- Create a dated evidence map showing source, custodian, relevant period, retention risk, status, and next step.
- Preserve originals and maintain a clear distinction between evidence, working copies, summaries, and demonstratives.
- Interview witnesses separately and document the witness’s own words before introducing other accounts.
- Use source-labeled timelines and record conflicts, gaps, clock issues, and attribution limits.
- Ask qualified experts to address defined questions; do not use expertise as a substitute for missing facts.
- Report unsuccessful efforts and unavailable evidence as carefully as successful collection.

Bottom Line

Detecting AI-Generated, Deepfake, or Digitally Manipulated Evidence in a Military Case is strongest when the defense can show the path from question to source, from source to verified fact, and from verified fact to a carefully limited conclusion.

The objective is a clean record that helps counsel decide what to investigate next, what legal process may be required, and what the available evidence actually permits anyone to say.

KEY POINT

Trace every important conclusion to an original source, document its limits, and leave unresolved questions visible.

Important Information

This Authority Publication is provided for educational and informational purposes and is intended to help readers better understand military defense investigations and the investigative process. It is based upon professional investigative experience and provides practical investigative insight rather than legal advice.

Every military case is unique. Investigative strategies, factual issues, and legal considerations applicable to one case may not apply to another. Readers should consult a qualified attorney regarding legal rights, legal strategy, and decisions involving individual circumstances.

Nothing in this publication creates an attorney-client or investigator-client relationship. UCMJ Investigations is independent and does not represent the Department of Defense, any military service, or any government agency.