

THE FORENSIC INVESTIGATOR'S PLAYBOOK

AUTHENTICATING ONLINE VIDEO & MANAGING DIGITAL EVIDENCE



THE THREAT LANDSCAPE

SOURCE: GLOBAL DATA ANALYTICS

VER: 2.4.1

3.5 BILLION

MONTHLY GLOBAL VIEWERS (2026)

SOURCE: GLOBAL DATA ANALYTICS

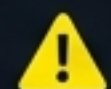
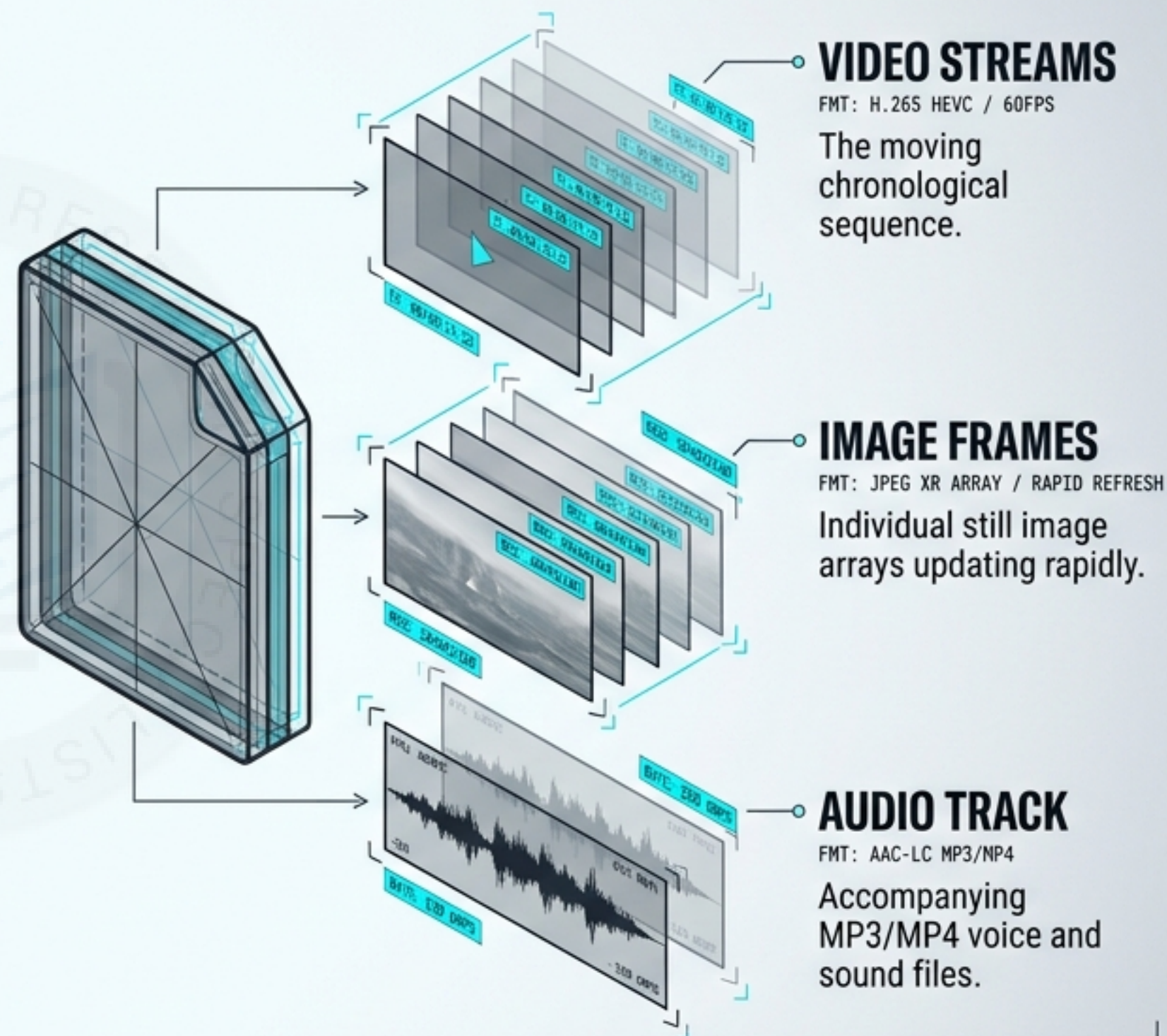
VER: 2.4.1

- Short-form video dominates global consumption.
- AI-generated video uploads are scaling exponentially.
- Historical trust in visual evidence is fundamentally compromised.

SOURCE: GLOBAL DATA ANALYTICS

VER: 2.4.1

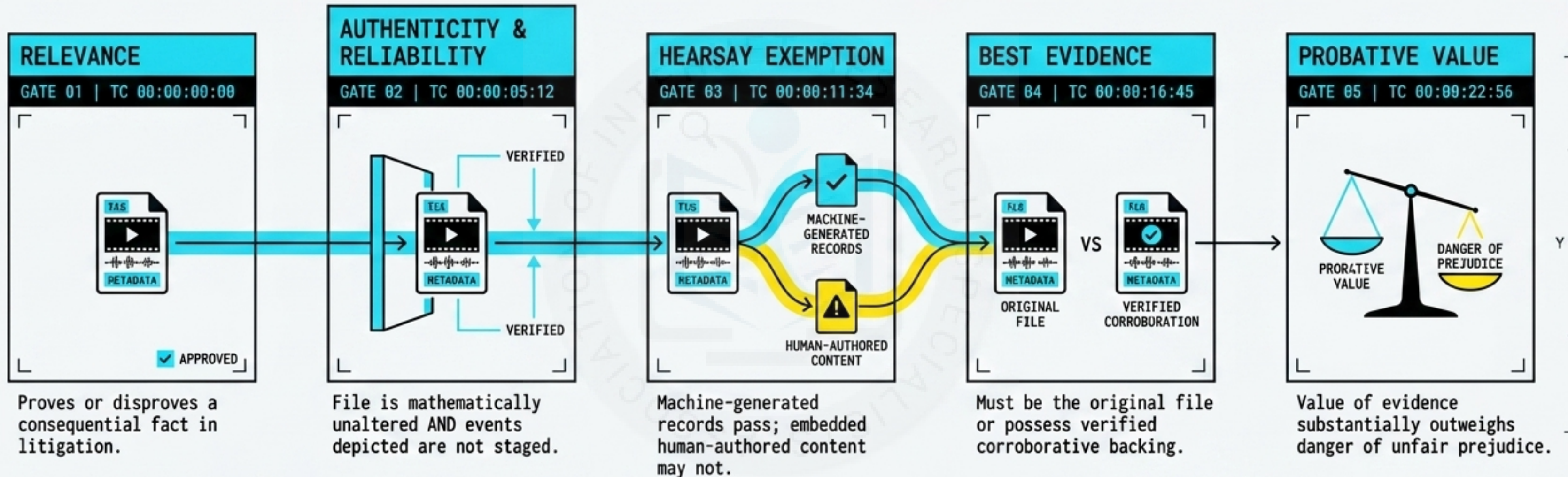
ANATOMY OF THE TARGET



INVESTIGATOR'S AXIOM: Authentication is not a single check. You are verifying three separate multimedia formats hidden inside a single file.

THE ADMISSIBILITY GATES

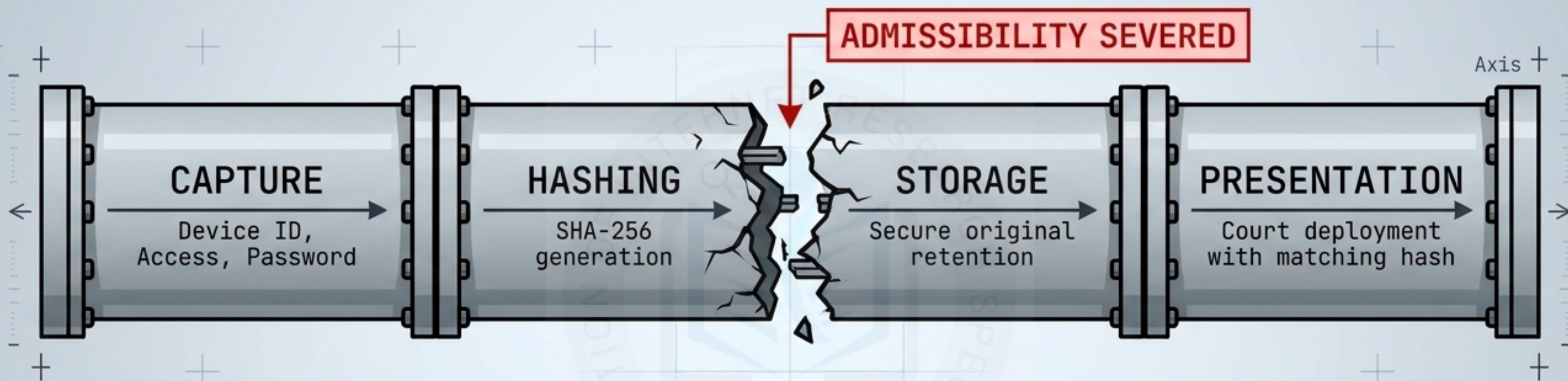
SOURCE: LEGAL FORENSICS FRAMEWORK
VER: 2.5.1



INVESTIGATOR'S AXIOM:

A video can be mathematically authentic, but factually unreliable.

THE FRAGILE PIPELINE: CHAIN OF CUSTODY



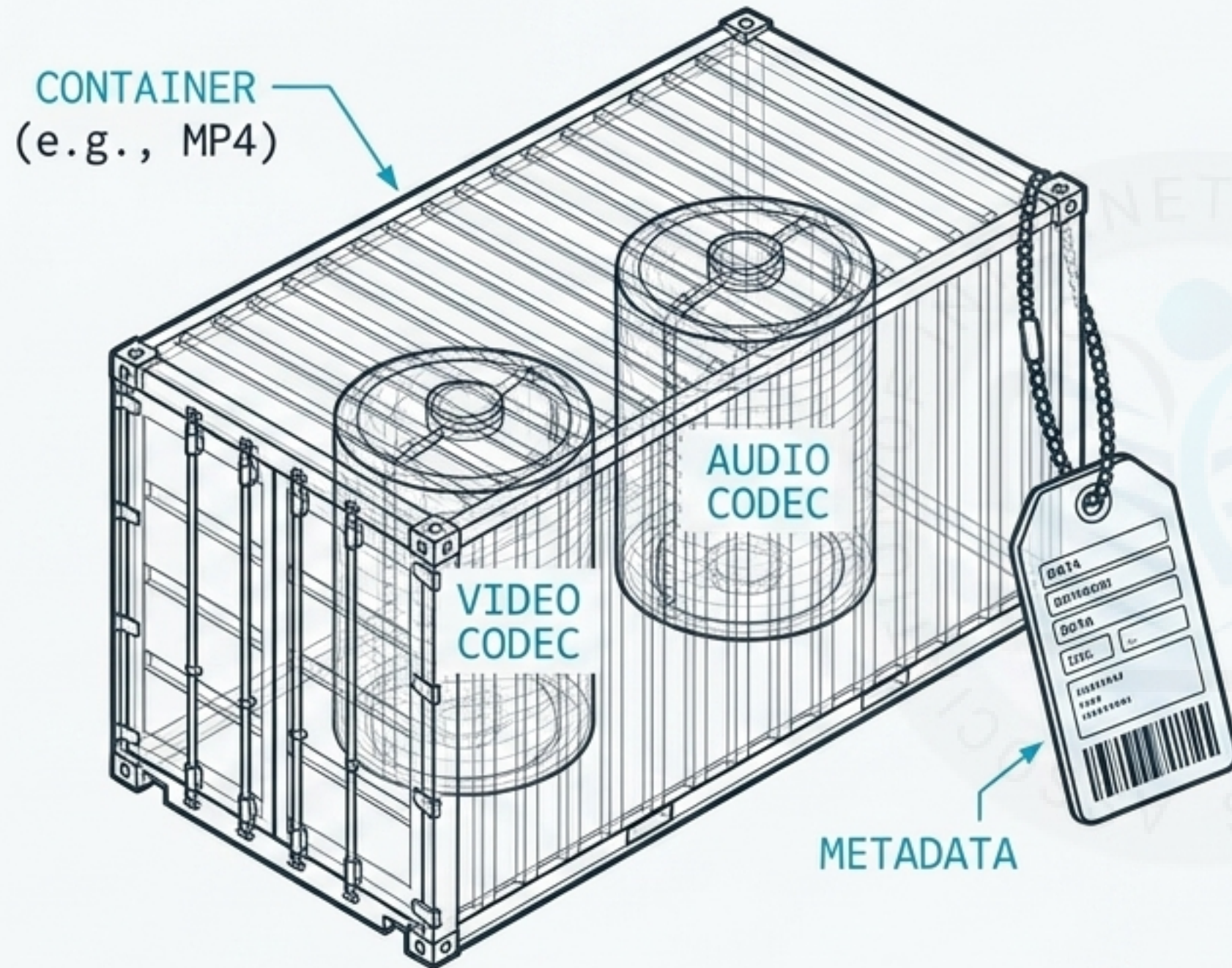
REQUIRED LOG REGISTRY

- ☐ User Identity
- ☐ IP Address
- ☐ SHA-256 Fingerprint
- ☐ Exact Timestamp

KEY INSIGHT

The source file must have a documented trail showing exact handling from creation to presentation, without any transcoding or compression.

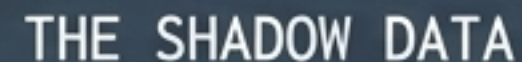
VIDEO ARCHITECTURE: CONTAINERS & CODECS



A video codec compresses/decompresses data. The container bundles the media and metadata together.

COMMON FORMATS	
	AVI Microsoft long-running standard.
	MOV Apple QuickTime format; wide codec support.
	AVCHD Panasonic/Sony high-definition camcorder standard.
	MP4 The modern universal standard; excellent compression.

VER: 2.5.3
SOURCE: LEGAL FORENSICS FRAMEWORK

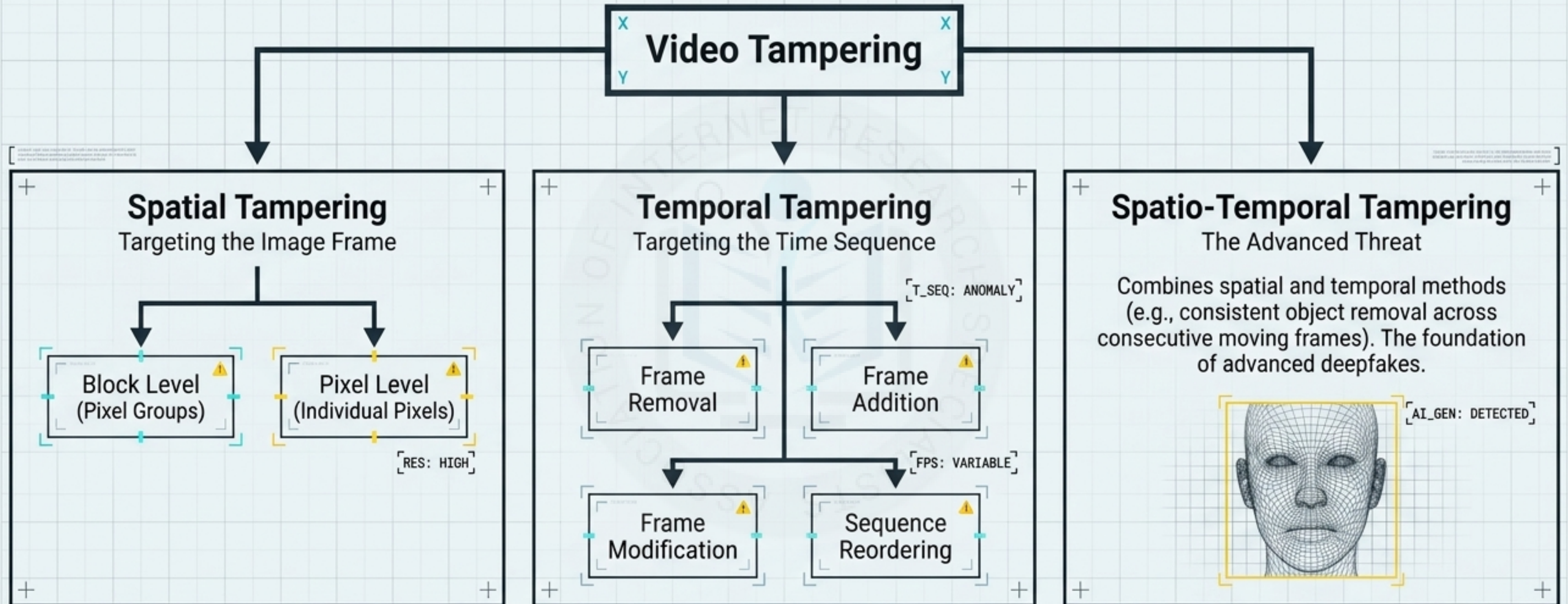


- ## THE FORENSIC COUNTERMEASURE

Original timestamps are read-only in standard software. ExifTool is the 2026 industry standard to extract hidden timestamps, verify GPS, and expose edit history.

INVESTIGATOR'S AXIOM: The visual data might be flawless, but the shadow rarely lies.

Taxonomy of Forgery

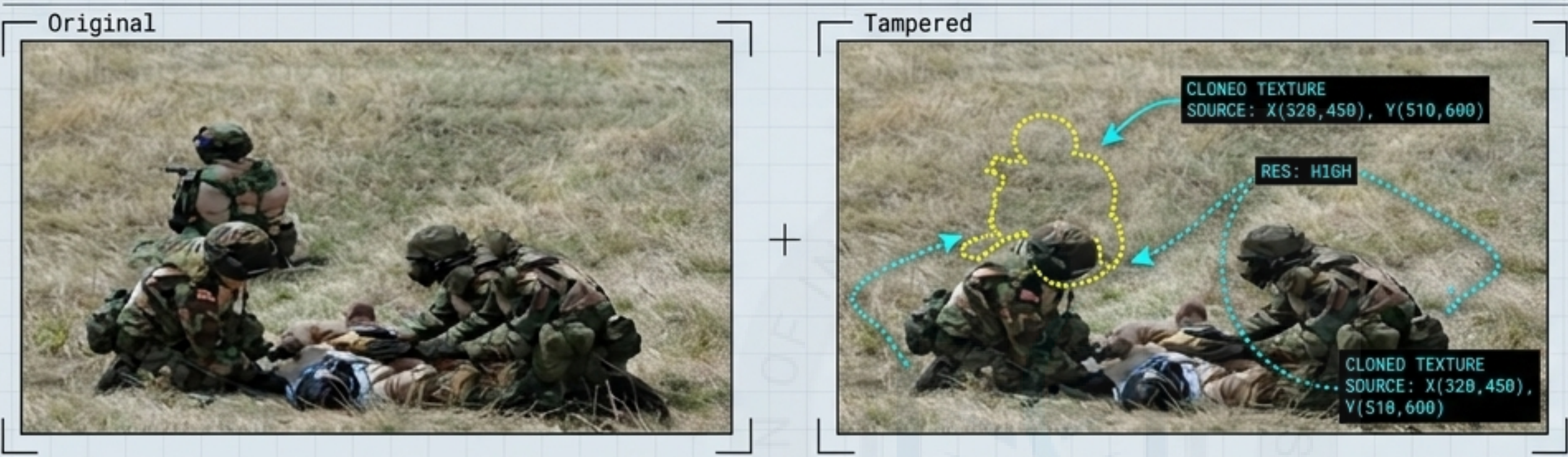


DIAGNOSTIC RULE: Knowing what type of attack is present determines which forensic detection method to deploy.

Case File 01: Spatial Forgery (Object Removal)

Panel 1 - The Soldier

VER: 2.5.3 | SOURCE: LEGAL FORENSICS FRAMEWORK



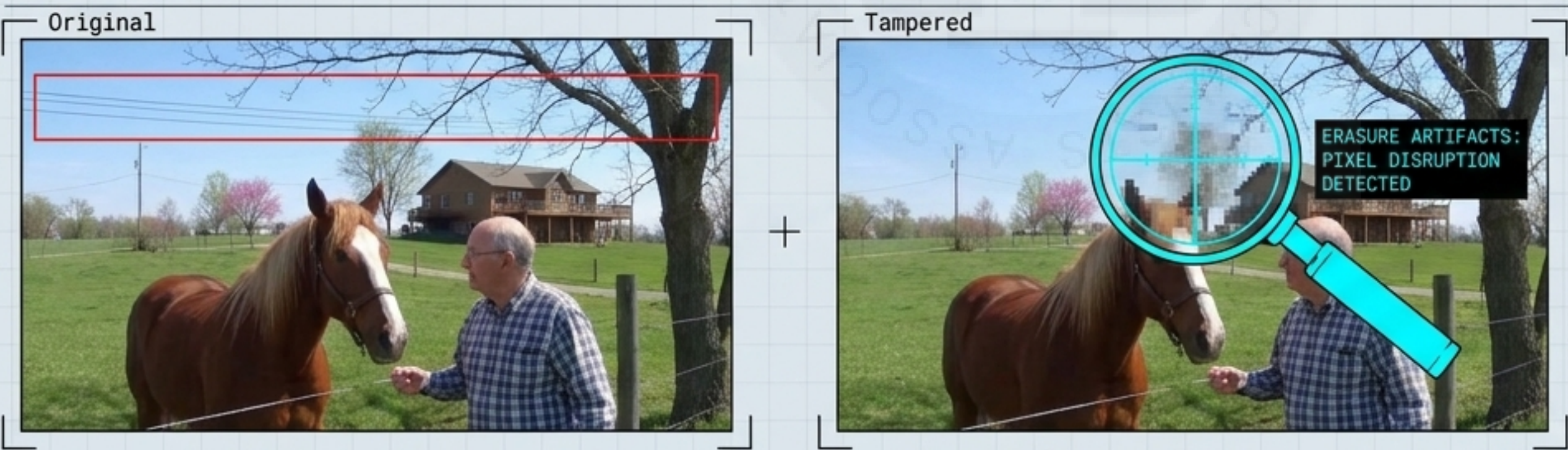
ATTACK PROFILE

Object Removal

MECHANISM: Used primarily to hide an individual's or object's presence in a specific sequence of frames.

Panel 2 - The Wires

FPS: VARIABLE | AI_GEN: DETECTED



DIAGNOSTIC RULE: Knowing what type of attack is present determines which forensic detection method to deploy.

Case File 02: Spatial Forgery (Copy-Move & Modification)

The Copy-Move Attack



+



ATTACK PROFILE:

Copy-Move & Object Modification

MECHANISM: Conceals manipulation by resizing, blending, or altering specific attributes within an existing scene, fabricating new realities.

The Modification Attack

Original Video Frames



Frame49

Frame50

Frame51

+

Tampered Video Frames



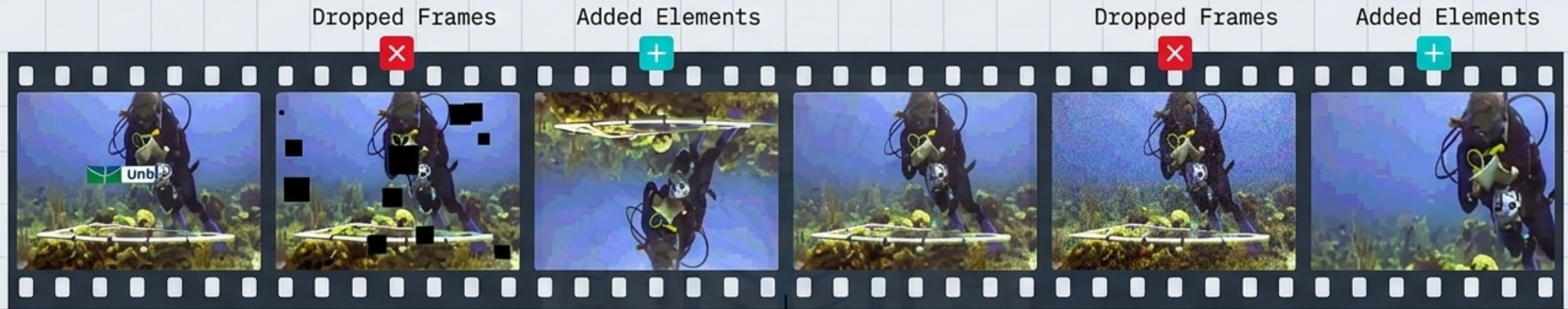
Frame49

Frame50

Frame51

MANIPULATION: FACE SWAP INJECTED. FRAMES 49-51. RES: HIGH.

Case File 03: Spatio-Temporal Manipulation



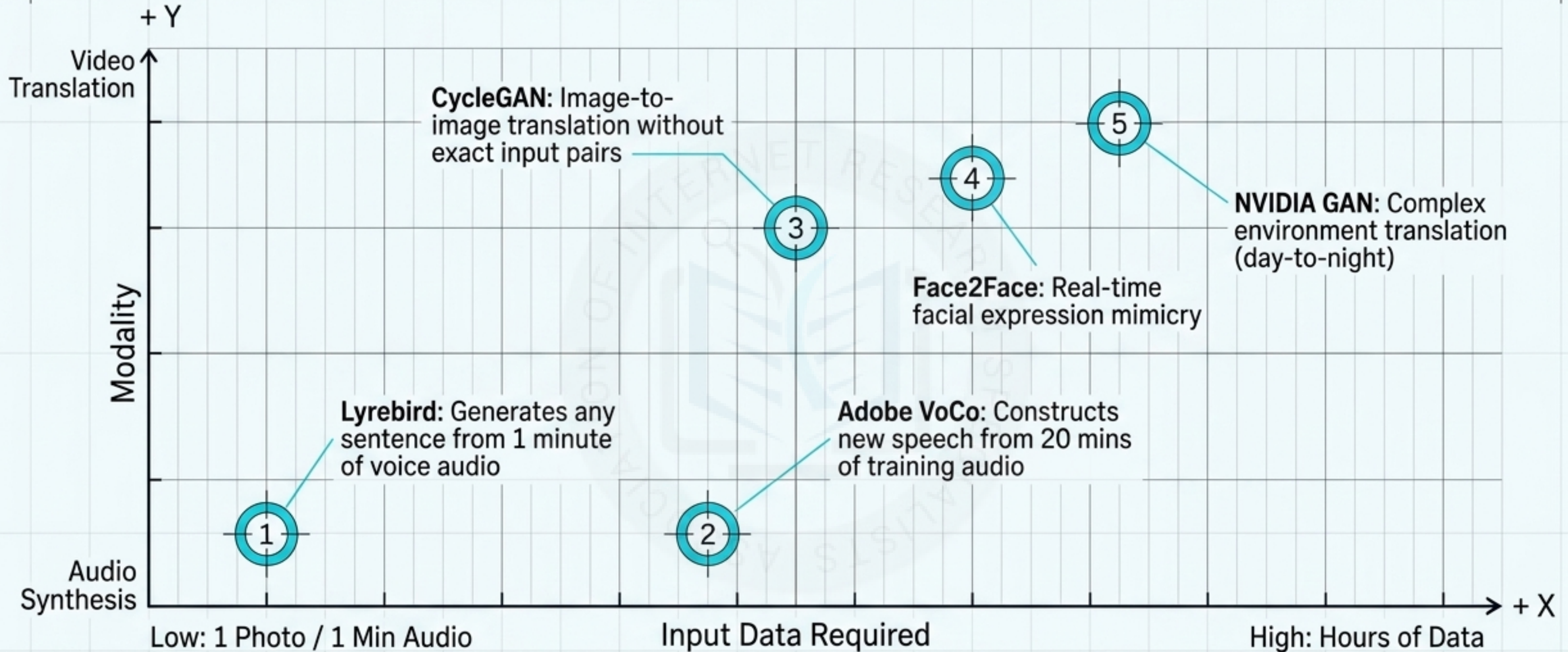
Frame Removal	Frame Addition	Sequence Modification
Erasing specific actions from the timeline.	Fabricating sequential events.	Reordering chronology to misrepresent causation.

THE DEEPPFAKE LINK: Spatio-Temporal tampering is the foundation of advanced deepfakes. It requires consistent spatial manipulation sustained dynamically across multiple moving frames over time.

Diagnostic Table: The Tampering Matrix

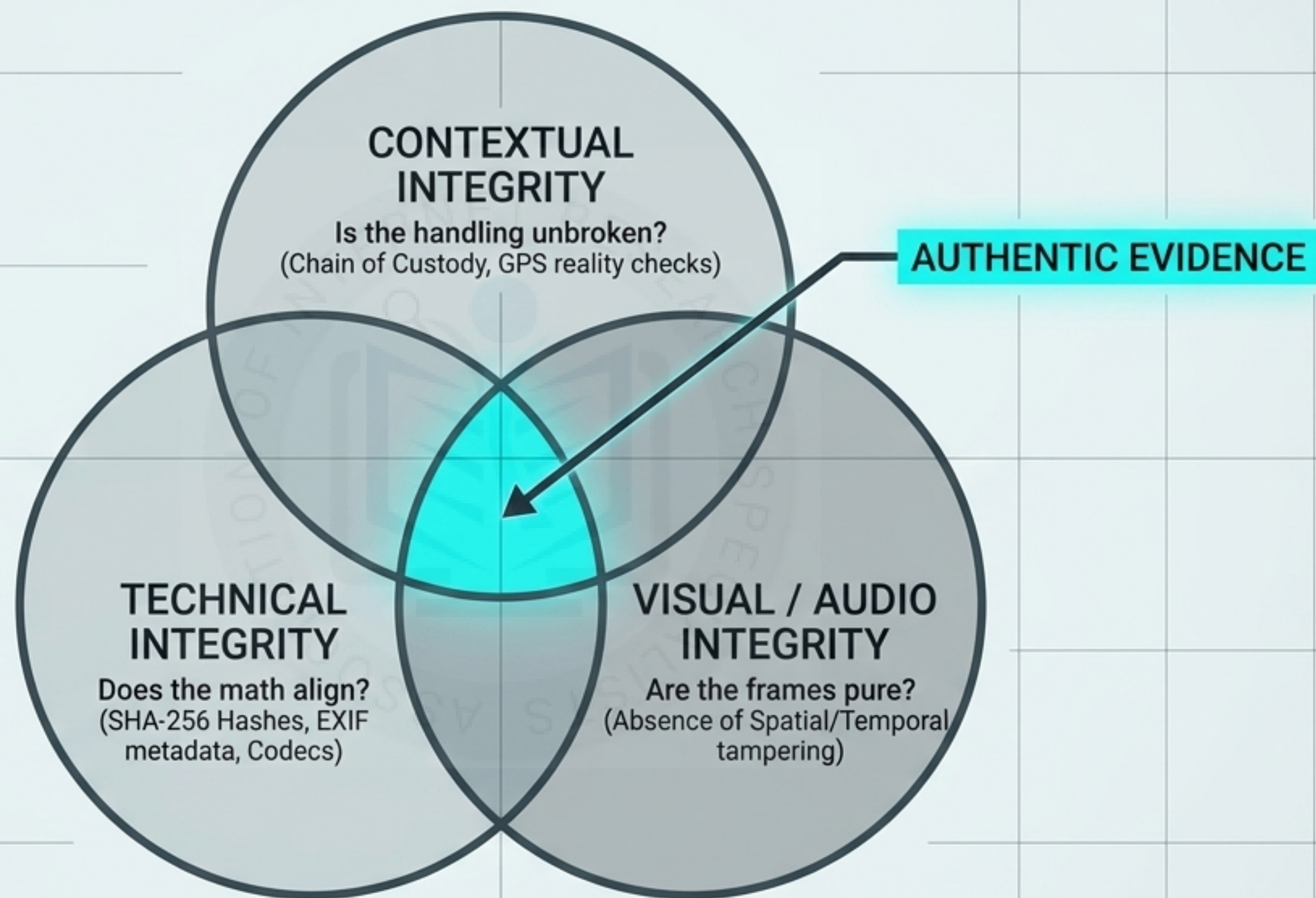
TAMPERING TYPE	TARGET DOMAIN	SUB-ATTACKS	FORENSIC DIFFICULTY	PRIMARY VISUAL MARKERS
Spatial	Pixels	Removal, Copy-Move, Pixel-Level	Low / Medium	Blending errors, repeated texture blocks, edge anomalies.
Temporal	Time	Frame Drop, Sequence Reorder, Insert	Medium	Sudden motion jumps, audio desynchronization, timestamp gaps.
Spatio-Temporal	Pixels + Time	Deepfakes, Dynamic Tracking Manipulation	High	Micro-flickering, unnatural edge rendering during movement, inconsistent lighting.

The AI Forgery Threat Landscape



KEY INSIGHT: The barrier to entry for photorealistic CGI and flawless audio cloning has dropped to consumer-level accessibility.

The CIRS Triangulation Model



INVESTIGATOR'S AXIOM: Relying on a single vector leaves you vulnerable to advanced forgery. A video is only verified when context, data, and pixels seamlessly align.