Metadata Manipulation

Artifact Authentication (KA-MOD-016)

The process of verifying the integrity and origin of digital evidence by examining surrounding data.

Metadata: The Data About Data

Definition & Importance

Metadata is **structural information** embedded within a digital file, describing its characteristics, origin, and history, but not its content.

It establishes the **who, what, when, where, and how of a digital artifact, making it critical for forensic timelines and attribution.**

Key Types of Metadata

- **System Metadata:** File creation, last modified, last accessed times (MAC times).
- **Content Metadata:** Author, application used (e.g., Word version), revision history.
- **Exif Data (Media):** Geolocation (GPS), device make/model, camera settings, date/time stamp.

Risks: Common Manipulation Tactics

MAC Time Alteration

Using specialized utilities (like 'touch' or forensic tools) to change the **Modified, Accessed, and Created** timestamps of files to obscure activity.

Exif Stripping/Editing

Removing or falsifying the embedded data in photos and videos (e.g., erasing **GPS coordinates** or changing the capture date) to mask origin.

File Header Forgery

Modifying the bytes at the start of a file to change its perceived type (e.g., disguising an executable file as a benign JPEG).

Defense: Artifact Authentication Methods

Cryptographic Hashing (The Seal)

Generating a unique, fixed-length digital fingerprint (e.g., **SHA-256**) of the file's contents. If the hash changes, the file has been tampered with.

Cross-Artifact Corroboration

Validating the metadata from one source (e.g., file MAC times) against independent sources (e.g., firewall logs, email headers, backup records).

Internal Consistency Checks

Analyzing inherent inconsistencies (e.g., Exif data showing a camera model that didn't exist at the file's 'creation' date) to expose manipulation.