MEDEX

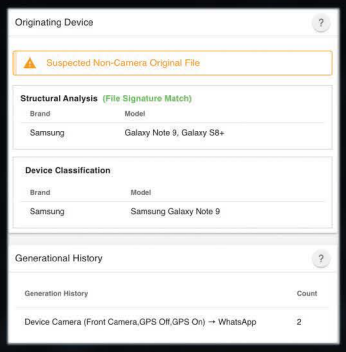
PATENT PENDING

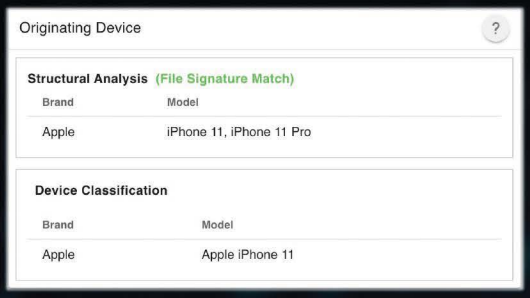
Product Overview

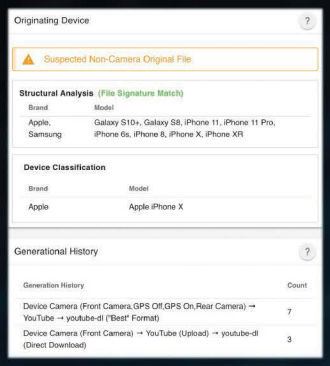
Medex uses a novel, patent-pending approach to examine video files that provides never before seen insight into digital video.

SOURCE AND GENERATION ANALYSIS

Medex uses a unique combination of file structure analysis and data classification to identify the device that originally recorded a video file as well as any means of transmission of the file and/or other software it has passed through.

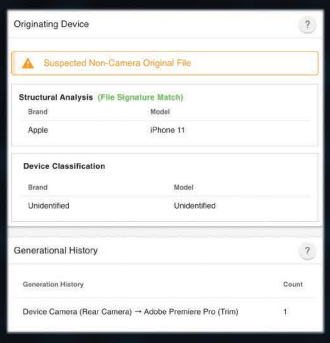


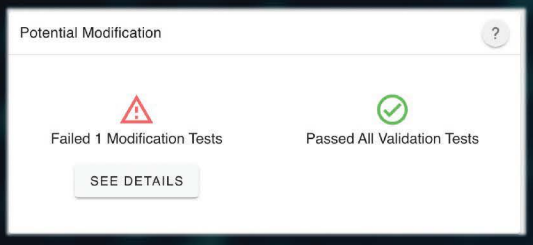


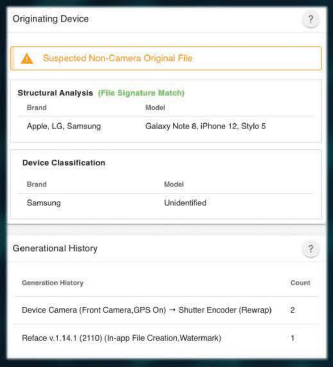


VIDEO MANIPULATION

Medex can identify manipulation by detecting the presence of editing software in a video's history. Each file is also run through a set of format-specific logical tests to determine if a file has been modified or potentially modified at a binary level.

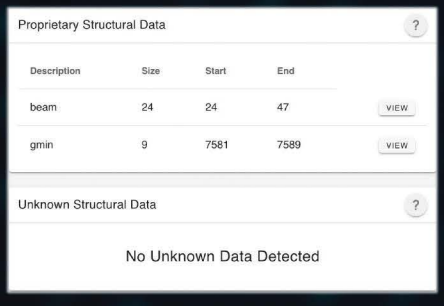


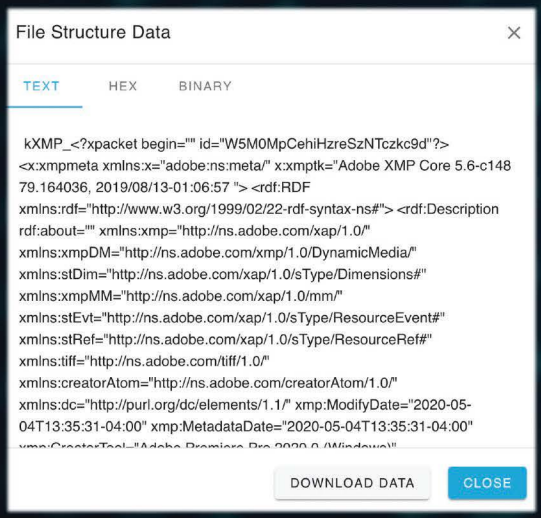




METADATA ANALYSIS

Using custom designed parsers for forensic use, Medex will report all metadata in a file, including the presence of proprietary or non-decipherable metadata elements.





www.medexforensics.com

MEDEX

PATENT PENDING

Data Security

Medex is a SaaS platform hosted on AWS GovCloud, which complies with the FedRAMP High baseline; the DOJ's Criminal Justice Information Systems (CJIS) Security Policy. This is the same platform on which the vast majority of law enforcement data in the cloud is stored.

SECURE FILE HANDLING

Medex does not store video files that it analyzes. All submitted files are analyzed by the Medex custom parser and then immediately deleted. Each file spends an average of 180 seconds on the Medex AWS GovCloud server. Only the results of the Medex examination are stored on the server, no submitted video files are retained or viewed during the process. An activity log, including the length of time that Medex had access to any submitted files, is stored within the Medex project database and is available for review and/or inclusion in reports.

KEY SECURITY FEATURES

- End to end encrytption.
- All data transfer forced to HTTPS
- Role-based access control
- AWS Web Application Firewall Implemented
- DNS and DDoS protection
- Port security hardened and limited
- Event logging
- SQL injection protection protocols
- CORS policies hardened

LOCAL PROCESSING CLIENT

The Medex Processing Client is a small Windows-only software package that can be installed on a local computer to process files prior to submission to the Medex Platform. Your original video evidence is parsed by the client on the local computer while a ZIP folder containing metadata-only processing results is sent to the Medex Platform's secure cloud for analysis. When using the local processing client your video files never leave your local computer. ZIP files generated from the Medex Local Processing Client may also be significantly smaller in size compared to the original video, reducing network traffic during the project submission process.

video file source and history identification

video manipulation detection

deepfake video detection

forensic video metadata analysis

www.medexforensics.com