jamf

Jamf Mobile Forensics

Defend mobile devices against advanced cyber attacks.

High-risk users — government officials, business executives, political figures and more — **face threats that demand actionable defense strategies**. Advanced Persistent Threats (APTs), mercenary spyware, Nation State attacks and zero-click exploits require security teams to continuously analyze device integrity and surface Indicators of Compromise (IOCs), without disrupting users, deploying invasive agents, or exposing Personally Identifiable Information (PII).

Jamf Mobile Forensics adds an advanced layer to mobile threat defense, helping security teams detect and investigate threats that traditional tools might miss.

Key Benefits

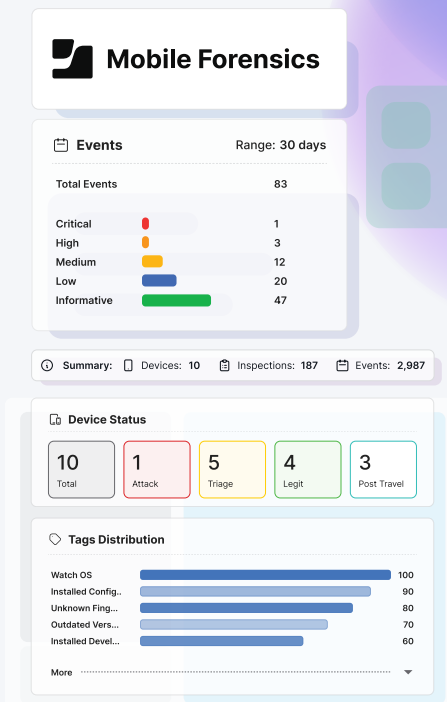
- Detect targeted attacks and zero-days before they enter the network
- Analyze deep system, crash, kernel and app logs without rooting or jailbreaking the device
- Simplify forensic analysis and reduce manual research
- Protect privacy and ensure device confidence of high-profile users

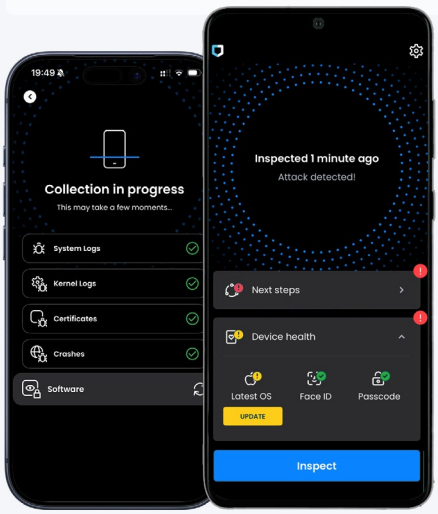
Mobile Exploitation Chain

How the mobile exploitation chain progresses from initial access to post-exploitation:

Malicious Attachment / WebKit Exploit → Initial Access → Code Execution (WebContent process compromise) → Privilege Escalation → Stealth / Evasion → Post-Exploitation Activity (data collection, mic/camera access, etc.) → C2 Communication → Cleanup / Anti-Forensics

Analysis of threats and the exploit chain help security teams understand what happened and how to respond. Jamf Mobile Forensics gives you that visibility.





Reduce mobile forensic analysis from weeks to minutes.

Remote Digital Forensics and Incident Response

Reduce downtime and keep critical users productive

- Proprietary behavioral analytics detects anomalous device behaviors, zero days and IOCs for Pegasus, Predator and other spyware
- Prevent extended exposure by exploring device level telemetry
- Instant analysis enables security teams to understand the steps required and immediately respond to advanced attacks

Proactive Threat Hunting

Translate complex security data into actionable intelligence

- Simplify investigation workflows by grouping event timelines, types and severity ratings into unified incidents
- Automate event timelines to directly inspect how and when a device was compromised
- Detect unknown IOCs by analyzing files, apps, process, crash logs and more

Human-led, AI-enhanced Analysis

AI Analysis acts as a forensic research assistant

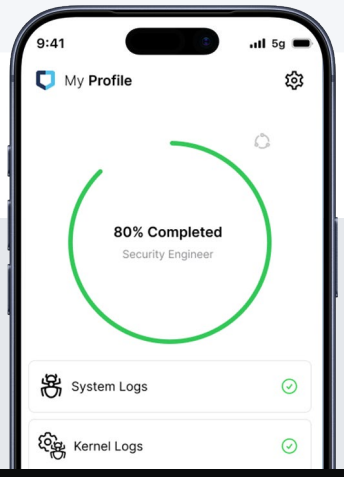
- Reduces manual research required to analyze device crashes and anomalies
- Summarizes incidents and recommends remediation next steps
- AI Analysis is turned off by default, allowing organizations to remain in control over AI usage

**AI Analysis is a cloud-only feature.*

Privacy-by-Design Forensics

Protect users across all privacy and device integrity concerns

- No PII taken. Analysis does not require access to passwords, photos, videos, messages, contacts, call history, browser history, two-factor authentication tokens or app data
- Remote DFIR app performs silent scans at organizational-set intervals and provides users with device security information



Jamf Mobile Forensics is backed by **Jamf Threat Labs**, our team of security researchers, analysts and engineers who publish research on mobile malware and spyware and drive continuous improvements to the Jamf Mobile Forensics engines.

jamf

www.jamf.com

© 2026 Jamf, LLC. All rights reserved.

To learn more, reach out to your Jamf representative.
Or request a trial.