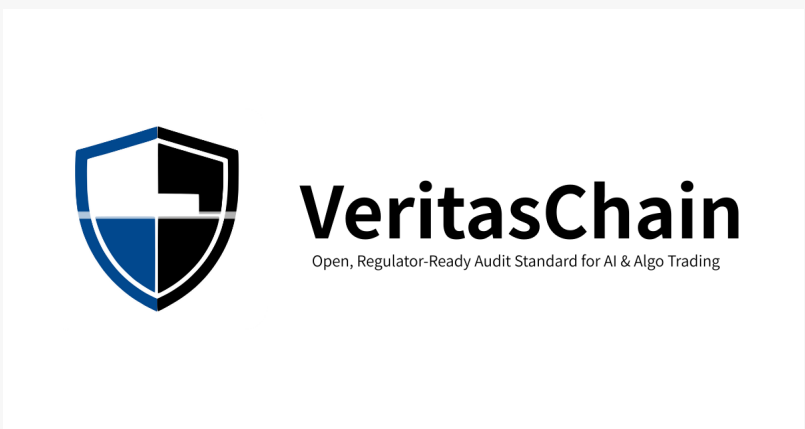
VeraSnap v1.5 Launches: World's First Multi-Sensor Fraud Detection & Software Screen Recapture Detection for Smartphones

Cryptographic evidence capture app now available on Android with barometric attestation, tremor analysis, NTP verification, and tri-modal screen detection

TOKYO, SHIBUYA, JAPAN, February 11, 2026 /EINPresswire.com/ -- VeraSnap v1.5 Now Available Globally with Android Release

VeritasChain Co., Ltd. today announced the release of VeraSnap v1.5, a cryptographic evidence capture application, alongside the global launch of VeraSnap for Android on Google Play Store.
The app is now available at:



Logo of the VeritasChain Standards Organization (VSO), a neutral standards body developing cryptographic audit and provenance frameworks for AI systems.

> In the deepfake era, proving authenticity at capture is more reliable than detecting fakes after creation. VeraSnap democratizes cryptographic provenance for everyone with a smartphone."
>
> *Tokachi Kamimura, CEO, VeritasChain Co., Ltd.*

iOS: https://apps.apple.com/app/id6757994770
Android: https://play.google.com/store/apps/details?id=org.veritaschain.verasnap

 Addressing the Deepfake Crisis with Cryptographic Provenance
As AI-generated content becomes increasingly sophisticated, the threat of deepfakes has escalated dramatically. Deepfake videos increased over 550% in 2024 alone, contributing to election interference, fraud, and non-consensual intimate imagery worldwide. Projections estimate AI-generated content fraud damages will reach

$40 billion in the United States alone by 2027.
Existing deepfake detection technologies remain locked in an arms race with AI generators. VeraSnap takes a fundamentally different approach: rather than attempting to detect fakes after creation, it cryptographically proves authenticity at the moment of capture.

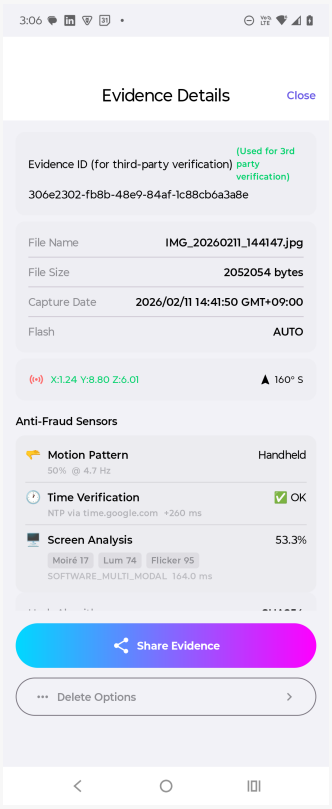
 World-First Multi-Sensor Fraud Detection System
VeraSnap v1.5 introduces four integrated fraud detection sensors, representing the first consumer smartphone application to combine these technologies with RFC 3161 cryptographic timestamping and the open Content Provenance Protocol (CPP):

1. Barometric Pressure Attestation
Utilizes the Bosch BMP390 barometer (±0.03 hPa precision, ~10cm altitude resolution) found in iPhone 6 and later devices. Captures absolute pressure, relative altitude, and environmental stability data that can be independently cross-validated against meteorological records from agencies like NOAA and JMA.

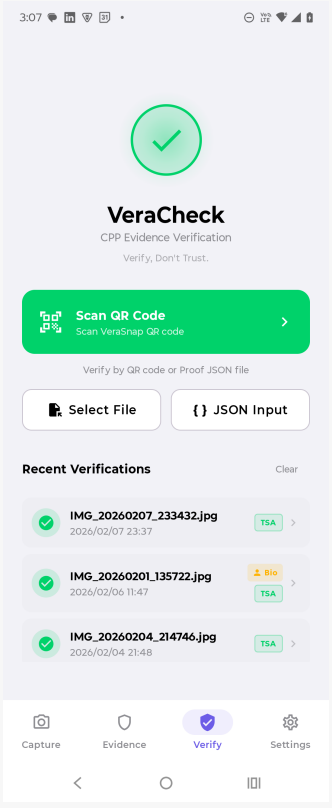
2. Physiological Tremor Analysis
Human hands exhibit involuntary physiological tremor at 8-12Hz that cannot be replicated by tripods, robots, or mechanical devices. VeraSnap samples 6-axis IMU data at 100Hz over 500ms during capture, performing Fast Fourier Transform (FFT) analysis using Apple's Accelerate.framework. Academic research demonstrates 95-97% accuracy in distinguishing human handheld from mechanical capture.

3. NTP-Based Time Consistency Verification
Combats device clock manipulation by comparing system time against NTP servers (time.apple.com, ntp.nict.jp, pool.ntp.org) at capture. Offsets exceeding ±5,000ms are flagged as inconsistent. Combined with RFC 3161 timestamps, this provides evidentiary-grade time attestation meeting Federal Rules of Evidence 901(b)(9) requirements for electronic record authentication.

4. Software-Based Screen Recapture Detection Engine
A breakthrough tri-modal fusion system enables screen detection on all devices, not just LiDAR-equipped models:



VeraSnap for Android



VeraCheck for Android

Moiré Pattern Analysis (35% weight): 2D FFT detects interference patterns between display pixel grids and camera sensors
Luminance Distribution Analysis (30% weight): Quantifies histogram entropy, local contrast uniformity, and edge sharpness differences between displays and natural

scenes
Rolling Shutter Flicker Detection (25% weight): Identifies banding artifacts from display refresh rate interaction with CMOS sensor scan lines

The system achieves 96%+ detection accuracy with <5% false positive rate, processing in 10-50ms entirely on-device using Apple Accelerate.framework.

 Expanded Global Language Support
Version 1.5 expands localization from 10 to 14 languages, adding:

Arabic (420 million speakers, MENA legal evidence demand)
Hindi (600 million speakers, growing Indian smartphone market)
Indonesian (270 million population, advancing digital evidence law)
Russian (260 million speakers, forensic demand across CIS)

Complete language support: English, Japanese, Korean, Spanish, French, German, Portuguese, Simplified Chinese, Traditional Chinese, Arabic, Hindi, Indonesian, Italian, Russian. All UI strings, sensor labels, legal disclaimers, and fraud detection status displays are fully translated, with RTL (right-to-left) support for Arabic.

 Technical Foundation: Content Provenance Protocol (CPP) v1.5
VeraSnap implements CPP v1.5, published as IETF Internet-Draft draft-vso-cpp-core. The protocol combines:

Apple Secure Enclave hardware signatures
RFC 3161 cryptographic timestamps
Biometric authentication binding
XOR Completeness Invariant for deletion detection
Multi-modal sensor attestation

This represents the first comprehensive digital evidence platform for consumers integrating these capabilities.

 Design Philosophy: Provenance ≠ Truth
VeraSnap operates on a critical principle: it cryptographically proves when, where, how, and by whom content was captured—but does not claim to verify content truthfulness. This distinction is essential for legal accuracy and regulatory compliance. The system provides forensic-grade provenance documentation while maintaining appropriate epistemic humility about content veracity.

 Free Core Features, Privacy-by-Design Architecture
All cryptographic evidence capture capabilities, including fraud detection sensors and screen detection, are available free of charge. Biometric data is processed locally without storage, and

all cryptographic operations occur on-device. No images or personal data are transmitted externally. Pro features focus on convenience (unlimited cloud storage, multiple TSA providers) rather than restricting core functionality.

 Democratizing Cryptographic Evidence
VeraSnap aims to democratize access to cryptographic provenance tools. In the deepfake era, the ability to create verifiable evidence should not be limited to experts or large enterprises. By providing professional-grade cryptographic attestation through an intuitive camera interface, VeraSnap empowers anyone with a smartphone to generate legally defensible digital evidence.

The open Content Provenance Protocol is published on GitHub, enabling anyone to verify or implement the standard. This transparency forms the foundation of trust in an age where distinguishing authentic content from AI-generated fakes has become increasingly critical.

 About VeritasChain Co., Ltd.
VeritasChain Co., Ltd., headquartered in Shibuya, Tokyo, develops cryptographic evidence capture solutions addressing digital content authenticity challenges. The company publishes the Content Provenance Protocol (CPP) as an IETF Internet-Draft and maintains the VeritasChain AI Provenance (VAP) framework for domain-specific provenance standards.

 Availability
VeraSnap is available for free download on the App Store and Google Play Store:

iOS: https://apps.apple.com/app/id6757994770
Android: https://play.google.com/store/apps/details?id=org.veritaschain.verasnap
CPP Specification: https://github.com/veritaschain/cpp-spec

 Media Contact
VeritasChain Co., Ltd.
Public Relations
Email: press@veritaschain.org
Web: https://veritaschain.org
D-U-N-S: 698368529

*"World's first" refers to consumer smartphone applications integrating barometric environmental attestation, IMU tremor pattern analysis, NTP time consistency verification, and software-based multi-modal screen recapture detection (moiré + flicker + luminance tri-modal fusion) with RFC 3161 cryptographic timestamps and an open protocol standard (CPP). As of February 11, 2026, according to company research.
**Detection accuracy figures represent theoretical expectations based on academic research; real-world performance varies by device, capture conditions, and target display characteristics.

TOKACHI KAMIMURA

VeritasChain Co., Ltd.
kamimura@veritaschain.org
Visit us on social media:
LinkedIn
Bluesky
Facebook
YouTube
X
Other
