

FORENSICS

Social Media Forensics and OSINT Investigation Platform for Law Enforcement

Comprehensive OSINT and social media investigation platform for capturing, preserving, and analysing online evidence from major social networks, forums, and open-source intelligence sources — with court-ready export and full chain of custody.



[Social Media Forensics](#)

[Official Brochure](#)

SOLUTION SNAPSHOT

<p>SUPPORTED PLATFORMS</p> <p>Facebook / X / Instagram / TikTok / YouTube + 20 more</p>	<p>DATA CAPTURE</p> <p>Posts / profiles / comments / metadata</p>	<p>PRESERVATION FORMAT</p> <p>Hash-verified, timestamped archive</p>
<p>ANALYSIS TOOLS</p> <p>Link analysis / timeline / network graph</p>	<p>EXPORT FORMAT</p> <p>PDF court report / CSV / JSON</p>	

Built for Real Operations

01

The platform automates the evidence-preservation process, capturing posts, images, videos, profile metadata, and engagement data in a forensically sound, timestamped format before content is deleted or modified. Advanced link-analysis tools map relationships between accounts, content, and events, helping investigators build actionable intelligence pictures from publicly available data.

APPLICATIONS

Where This Product Fits

03

Criminal Investigation

Preserves social media evidence in a court-admissible format before suspects delete incriminating posts or accounts.

Counter-Terrorism & Extremism Monitoring

Maps networks of extremist accounts, tracks radicalisation content, and generates intelligence reports for law enforcement agencies.

Corporate Due Diligence & HR Investigations

Audits publicly available social profiles for policy violations, reputational risk, and background verification purposes.

SPECIFICATION

Technical Details

05

Supported Platforms	Facebook / X / Instagram / TikTok / YouTube + 20 more
Data Capture	Posts / profiles / comments / metadata
Preservation Format	Hash-verified, timestamped archive
Analysis Tools	Link analysis / timeline / network graph
Export Format	PDF court report / CSV / JSON
Collection Speed	Bulk capture via API + scraping
Storage	Encrypted case files, cloud or on-premise
Access Control	Case-level role-based permissions
Audit Trail	Full investigator activity log
Warranty	Annual licence with SLA

Case Studies & Client Feedback

06

"Evidence that would have taken our team three weeks to gather manually was collected, preserved, and ready for the prosecutor within 48 hours."

Lead Digital Investigator

Cybercrime Division, National Police

RESOURCES

Media & Questions

07

Q. Is the collected evidence admissible in court?

A. Yes. The platform produces a hash-verified, timestamped archive with a full audit log of investigator actions, meeting the evidence standards of most jurisdictions. We recommend consulting local legal counsel for specific requirements.

Q. How is investigator data kept separate between cases?

A. Each case is stored in an isolated, encrypted container. Role-based access ensures investigators only see cases they are assigned to.

Q. Can it monitor accounts continuously?

A. Yes. Keyword and account monitoring modes run on a scheduled basis, alerting investigators when new relevant content is posted.

Ready to deploy Social Media Forensics?

Talk to Nirikhon for product consultation, installation planning, integration support, and enterprise deployment.

Hotline: 01712345678 | Website: www.nirikhon.com