NIRIKHON

SECURITY & DEFENCE TECHNOLOGY

PRODUCT BROCHURE

FORENSICS

Professional Cyber Forensics Platform for Digital Evidence Acquisition and Analysis

Professional digital forensics platform for endpoint triage, disk imaging, mobile device extraction, and artefact analysis. Produces case-ready reports with full chain of custody for law enforcement, corporate investigations, and incident response.

Cyber Forensics | Official Brochure

SOLUTION SNAPSHOT

ACQUISITION TARGETS **HDD / SSD / USB / mobile / cloud**	IMAGING SPEED **Up to 8 GB/min (SATA SSD)**	HASH VERIFICATION **MD5 / SHA-1 / SHA-256 dual-hash**
MOBILE SUPPORT **iOS 9+ / Android 4+ physical + logical**	ARTEFACT PARSING **700+ artefact types auto-parsed**	

OVERVIEW

Built for Real Operations 01

Combines physical and logical acquisition modules for Windows, macOS, Linux, iOS, and Android devices with an integrated artefact analysis engine that automatically parses browser history, email, chat applications, deleted files, and registry artefacts. Case management tools organise evidence, track investigator actions, and generate court-ready HTML or PDF reports at the click of a button.

APPLICATIONS

Where This Product Fits 03

Law Enforcement Digital Investigations

Extracts and analyses digital evidence from seized devices for prosecution of cybercrime, fraud, and other criminal offences.

Corporate Incident Response

Triages compromised endpoints rapidly during active security incidents, identifying attacker tools, persistence mechanisms, and data exfiltration evidence.

eDiscovery & Legal Proceedings

Provides defensible, attorney-ready digital evidence packages for civil litigation, employment disputes, and regulatory investigations.

SPECIFICATION

Technical Details 05

Acquisition Targets	HDD / SSD / USB / mobile / cloud
Imaging Speed	Up to 8 GB/min (SATA SSD)
Hash Verification	MD5 / SHA-1 / SHA-256 dual-hash
Mobile Support	iOS 9+ / Android 4+ physical + logical
Artefact Parsing	700+ artefact types auto-parsed
Report Formats	HTML / PDF / XML / CSV
Case Storage	Encrypted local + cloud backup
OS Support	Windows (investigator workstation)
Licence	Node-locked + dongle options
Warranty	Annual licence with priority support

PROOF

Case Studies & Client Feedback 06

> *"We acquired and analysed a 2 TB drive in under four hours. The auto-parsed artefacts highlighted the suspect's activity timeline immediately — no manual searching required."*
>
> **Senior Digital Forensics Examiner**
> Financial Crimes Investigation Unit

RESOURCES

Media & Questions 07

Q. Can it acquire data from encrypted drives?

A. Yes. The platform supports BitLocker, FileVault, and VeraCrypt decryption with the correct credentials or recovery key. Live acquisition from running systems can also capture decrypted memory.

Q. How are case files protected?

A. All case containers are AES-256 encrypted. Access is controlled by individual investigator credentials, and every action is logged in a tamper-evident audit trail.

Q. Is training available for investigators?

A. Yes. We offer a 5-day certified digital forensics course and a 3-day mobile forensics course, both available on-site or at our training centre.

Ready to deploy Cyber Forensics?

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

Hotline: 01712345678 | Website: www.nirikhon.com