

RECON

ITR

SUMURI



The Leading macOS Imaging, Triage, and Reporting Solution

RECON ITR v26.0 has been completely rebuilt from the ground up in 100% native Swift. This is not an update — it's a new application that acquires and processes Intel and Apple Silicon Macs like no other tool on the market. Built natively on macOS using Apple's own APIs, **RECON ITR** delivers more accurate data with zero reverse engineering.

RECON ITR now includes **557 triage plugins** (101 Mac + 456 iOS via iLEAPP 2.3.0), **12 imaging formats**, and supports every Apple Silicon processor from **M1 through M5** and the new **MacBook Neo**. Global Search, Global Timeline, and Global Report let examiners find answers and generate court-ready documentation on-site in minutes.

Every image **RECON ITR** produces uses Apple-native or open standard formats — DMG, E01, DD, SparselImage, ASIF, and more. Every image is **independently validatable with just a Mac**. No proprietary black box. No vendor lock-in. Evidence belongs to the agency.

SUMURI has designed **RECON ITR** with the customer in mind, ensuring examiners have the most versatile and powerful Mac forensic tool available — at a significantly lower price than competitors.



12 Damaging Formats

DMG, SparselImage, ASIF, E01/EX01, DD, SMART, Logical Folder — suited for any case (LIVE and Bootable)



M1 Through M5 + MacBook Neo

Full Apple Silicon support including every Pro, Max, and Ultra variant, plus Intel and T2 Macs



557 Triage Plugins

101 Mac + 456 iOS (iLEAPP 2.3.0) — the only true triage solution for live and Target Disk Mode Macs



Full Reporting Suite

Global Search, Global Timeline, and Global Report with Sequential Processing of proper macOS timestamps



Apple Extended Metadata

Correctly preserves Apple Extended Attributes, Spotlight metadata, and resource forks using native macOS libraries



Volatile Data Collection

Collects volatile artifacts through triage plugins — parsed, structured results, not raw dumps



Boot Camp & iOS Backups

Triage Boot Camp partitions and iOS backups with full plugin support



Includes PALADIN PRO v9

Bootable forensic Linux for imaging Windows, Linux, servers, and RAIDs — included at no extra cost



Independent Validation

Every format verifiable with just a Mac — no proprietary tools required to defend evidence in court

RECON



12 IMAGING FORMATS FOR EVERY SCENARIO

RECON ITR v26.0 offers 12 imaging format options across **RECON ITR** and **PALADIN PRO**: DMG, Logical DMG, FS Block Copy (DMG & SparseImage), Raw Output DMG, SparseImage, ASIF (new for macOS Sequoia), Logical SparseImage, E01/EX01, DD, SMART, and Logical Folder. Every format is an open standard or Apple-native — readable by any forensic tool.

Dual destination imaging writes to two drives simultaneously. Network share imaging supports SMB and NFS. Five-layer hashing (SHA-256, Source, Destination, Destination Image, Process Snapshots) ensures complete chain of custody.

Every purchase of **RECON ITR** includes two state-of-the-art Samsung drives:

- Samsung external SSD with Live and bootable versions of **RECON ITR** for live triage, imaging, and reporting, with both physical and logical imaging options
- Samsung USB with **PALADIN PRO** for Windows, Linux, and server imaging

SUPPORT FOR M1 THROUGH M5 + MACBOOK

RECON ITR v26.0 supports every Apple Silicon processor: M1, M1 Pro/Max/Ultra, M2 family, M3 family, M4 Pro/Max, M5, and the new MacBook Neo with its mobile SoC. Plus full Intel and T2 Mac support. Because **RECON ITR** is built natively on Apple's APIs, new hardware support arrives faster than any non-native tool.

THE ONLY TRUE macOS TRIAGE SOLUTION

RECON ITR is the only solution providing true artifact triage for live Macs and Macs in Target Disk Mode. 101 Mac plugins across 13 categories parse SQLite, plists, and app data — returning structured results in seconds. Plus 456 iOS plugins via iLEAPP 2.3.0. Other tools offer file browsing and call it “triage” — **RECON ITR** delivers parsed artifacts you can act on immediately.

INDEPENDENT IMAGE VALIDATION

Every image **RECON ITR** produces can be independently verified using just a Mac. No proprietary software required. No black box. When opposing counsel asks how you verified the image, the answer is simple: “Open it on any Mac. Verify it yourself.” This is a courtroom advantage.

FULL REPORT CAPABILITIES

RECON ITR has built-in reporting features to produce professional reports in seconds. Build comprehensive reports using Global Search and Global Timeline to locate and bookmark critical data. Sequential Processing of proper macOS timestamps ensures accurate chronological evidence. Global Report generates court-ready documentation on-site.

CORRECT USE OF APPLE EXTENDED METADATA

RECON ITR was built from the ground up on macOS to correctly support proprietary metadata in the Mac environment. Being native to macOS ensures our tool correctly identifies and preserves Apple Extended Metadata that other tools do not properly integrate.

ABILITY TO TRIAGE BOOT CAMP AND iOS BACKUPS

Like **RECON LAB**, **RECON ITR** supports more than just Mac data. **RECON ITR** has robust support for triaging Boot Camp partitions and iOS Backups.

INCLUDES PALADIN PRO v9 FOR WINDOWS AND LINUX

PALADIN PRO v9, with over 150 forensic tools, is included with every **RECON ITR** license. Image Windows PCs, Linux, servers, and RAIDs in a forensically sound bootable environment. Forensic Mode auto write protects all devices — no write-blocker required. BitLocker decryption, Autopsy integration, network imaging (SMB/NFS), multi-ISO boot, and NIST-tested reliability — all included.

VOLATILE DATA COLLECTION

RECON ITR's triage plugins automatically collect volatile artifacts active processes, network connections, system state, KnowledgeC as structured, parsed results. Not raw data dumps that require separate tools to interpret.

NATIVE SUPPORT FOR TIME MACHINE LOCAL SNAPSHOT

RECON ITR provides native support for Time Machine Local Snapshots, allowing examiners to access and triage point-in-time snapshots of the file system that macOS maintains automatically.

ABOUT SUMURI

SUMURI is a leading worldwide provider of solutions for digital evidence and computer forensic Training, Hardware, Software, and Services. **SUMURI** is also the developer of the industry standard **PALADIN** Forensic Suite, **RECON ITR**, **RECON LAB**, and **TALINO** Forensic Workstations.

sales@sumuri.com
+1 302.570.0015

Our Mailing Address:
P.O. Box 121 Magnolia,
DE 19962, USA