



A portable, digital forensics and cyber **platform** that brings evidence acquisition, media preparation, triage, case context, and operational records into one dedicated system.



DIGITAL TOOLKIT

- A multi-interface **ecosystem** - Touchscreen and computer-tablet dashboard
- A **suite** of collection and forensic tools ready to go
- **Quick-select** tool execution.
- Reporting dashboards and **metrics**.
- Field to lab workflow: Track drives from the **point of collection**.
- Choose your engine: Choose from **new native tools** or reliable open-source on the fly
- Extend the reach of technical experts: Configure repeatable **tool profiles**



Evidence acquisition

- Physical-drive imaging
- Logical file extraction
- Acquisition and standalone hashing
- Post-acquisition verification options
- Multi-destination spillover and drive-swap

Investigation and analysis

- Drive, partition, and file hashing
- Reference-set hash comparison
- Keyword and regular-expression search
- File-activity timeline views
- BitLocker and LUKS where supported
- File carving and file recovery
- Local AI Filename translation



Media preparation

- Configurable software-overwrite / wiping
- USB-aware device-assisted sanitization where supported
- Drive formatting
- Drive cloning, migration, and conversion
- Destination-media health and readiness information

Case and team control

- Case records and assignments
- Per-user authentication
- Organizations, roles, and permissions
- Case-linked evidence and execution records
- Reusable tool profiles
- Durable operation history
- Sync accounts and cases between units

Reporting and export

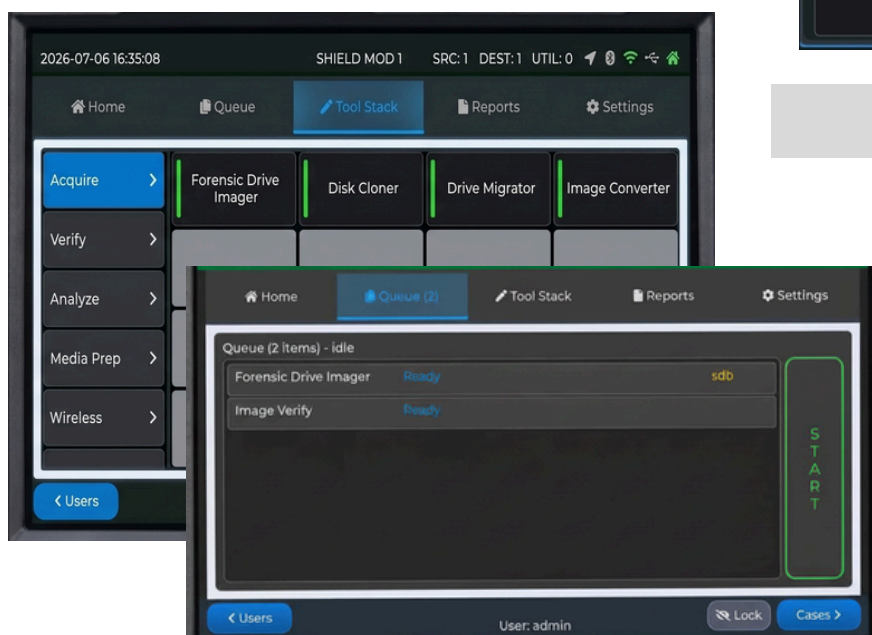
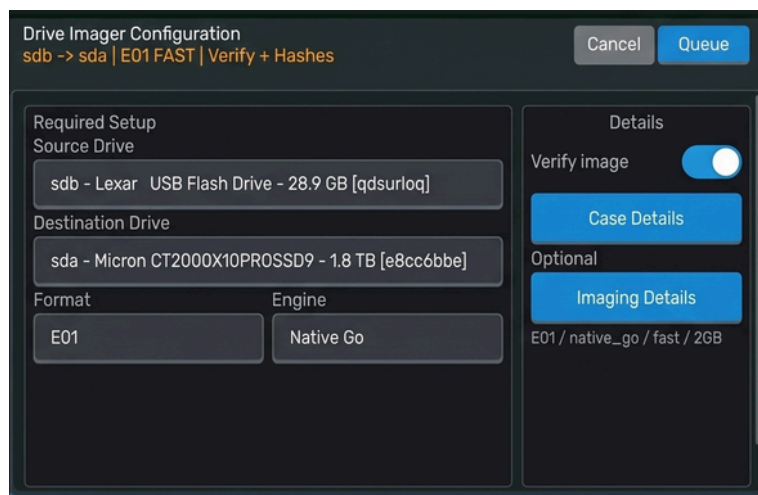
- Case Summary and Tool Execution reports
- HTML, PDF, CSV, and JSON outputs where supported
- Workflow-specific result exports
- Tool and task history with metrics





Choose your engine

- Supported capabilities allow users to select their tool of choice to perform a task.
- Imager: Select the new native Go imager, raw/DD, or ewfacquire.



Unified tool execution system

- Run imaging, verification, extraction, hashing, search, cloning, migration, sanitization, formatting, and conversion through a common queue.
- Track each task with progress monitoring, status updates, automatic order of operation, and execution history.
- Individual or team stats.

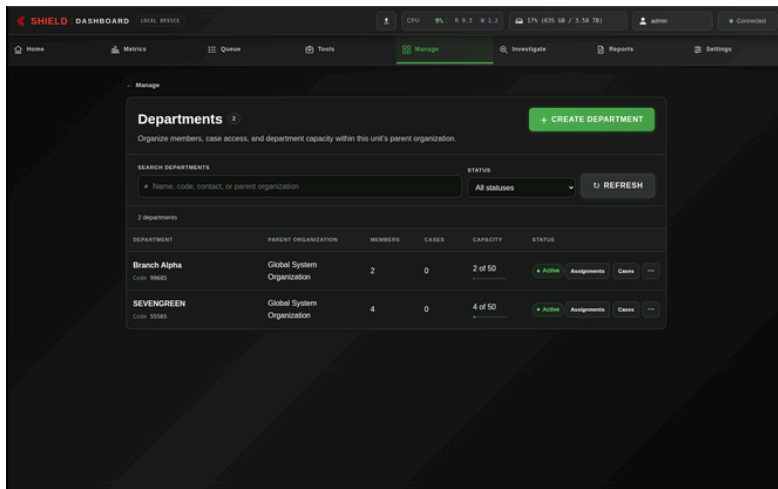
Connect and Operate

- QR codes make connecting quick and easy.
- Connect directly without a local network via USB or direct WiFi pairing.
- Access dashboard from computer, tablet, or phone.

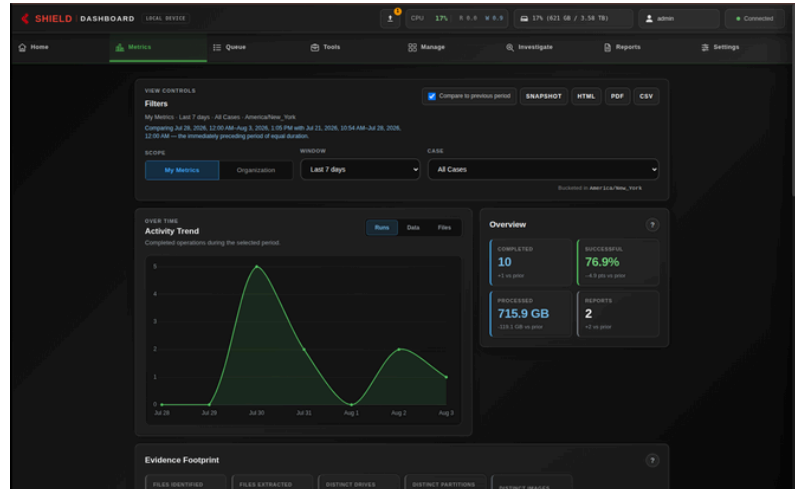


Details Details





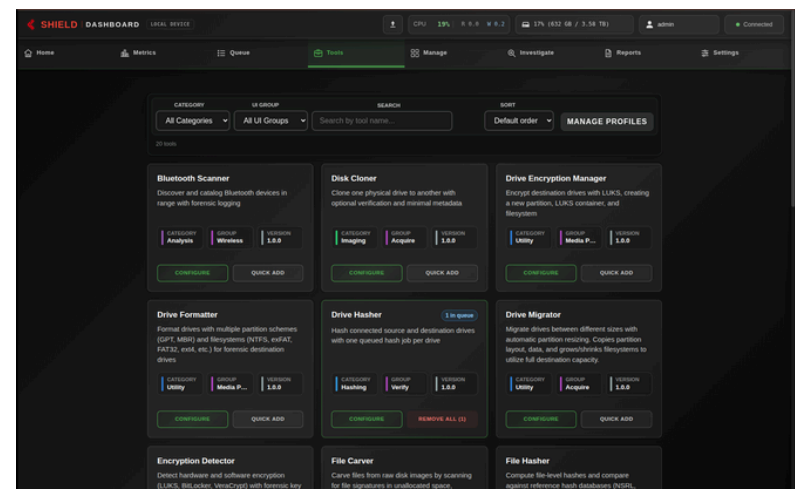
Team Assignment



Team and User Metrics

The screenshot shows the 'Tools' section of the SHIELD Dashboard, specifically the 'Keyword Search' results. The table has columns: FILE NAME, KEYWORD, HITS, CONFIDENCE, and SOURCE. It displays search results for the keyword 'Job 446d9340'. The table is paginated, showing 1-20 of 13,142 results.

Search and File View



Tool Stack and Edit

The screenshot shows the 'Investigate' section of the SHIELD Dashboard, specifically the 'Disk Layout Analysis' results. It displays a detailed table of drive data with columns: REGION, CLASSIFICATION, DESCRIPTION, START, END, and SIZE. The table is paginated, showing 1-20 of 13,142 results.

Detailed Drive Data

The screenshot shows the 'Settings' section of the SHIELD Dashboard, specifically the 'Encrypted Media & Credential Vault' configuration. It includes sections for 'OPERATOR WORKSPACE', 'ADMINISTRATIVE WORKSPACE', and 'Credential Vault'. The 'Credential Vault' section shows a table of credentials with columns: Role, Drive, Device, Type, Status, Identity, and Actions.

LUKS and Bitlocker

