Ciferware

Distributed Password Recovery & Digital Forensics Platform

Product brochure (English) · ciferware.com

Tagline

Recover secrets. Preserve evidence. Scale across your lab.

Ciferware combines **distributed password recovery** with **practical digital forensics workflows** in a single operator console—built for investigators, incident responders, and forensic labs who need Passware-class coverage without sacrificing control over their own infrastructure.

Executive summary

Ciferware is a **client–server platform** for lawful password recovery and encrypted-data analysis:

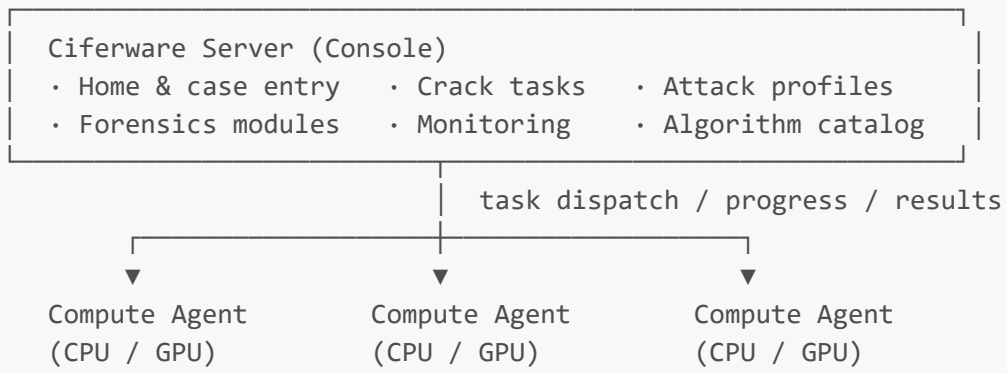
Pillar	What you get
Distributed cracking	A central **Server** coordinates **Compute nodes (Agents)** across CPUs and GPUs on your network.
Format intelligence	Automatic file-type detection, algorithm mapping, and an **Algorithm catalog** for reference and drill-down.
Forensics adjacency	Encrypted-file scanning, **memory capture & analysis**, **disk image inspection**, credential and network artifact tools, and optional **Volatility3** integration—so recovery sits inside a broader examination workflow.
Operational clarity	Live monitoring, run logs, batch jobs, attack profiles, and hardware **benchmarks** to size your cluster.

> **Intended use:** Ciferware is designed for **authorized** digital forensics, incident response, security research, and password recovery on data you own or are legally permitted to examine. Unauthorized access to systems or data is prohibited.

Who Ciferware is for

- **Digital forensic laboratories** processing cases with mixed encrypted containers, office documents, archives, and mobile backups.
- **Corporate IR teams** needing internal cluster capacity instead of cloud-only cracking services.
- **Consultants** who want one console for “open file → identify format → queue attack → document result.”
- **Training environments** comparing attack strategies, dictionaries, and node performance under controlled samples.

Architecture at a glance



- **Server:** Operator UI, task orchestration, parsing, logging, and forensic tooling that belongs in the control plane.
- **Agents:** Execute attack workloads; report speed and status back to the Server.
- **Discovery:** Agents can locate the Server on the local network (configurable listen port in **Server settings**).

Core capabilities

1. Password recovery (Cracking center)

- **Home entry:** Drag-and-drop or **Browse for file** sends encrypted material straight to **Crack tasks**.
- **Crack tasks:** Queue jobs, watch node assignment, and review outcomes.
- **Attack profiles:** Configure dictionaries, rules, masks, and related attack parameters.
- **Batch jobs:** Process many files with consistent attack settings.
- **Benchmark:** Measure per-node throughput to plan capacity and regression-test builds.

Attack types include dictionary and wordlist attacks, rules/mutations, and mask/brute-force patterns where the format allows—aligned to each file's native verification logic (not a generic hashcat-only subset).

2. Encrypted file scan

Scan filesystem locations for **encrypted files and containers**, classify them with the same detection engine used for manual tasks, and push findings into the cracking pipeline or the algorithm catalog.

3. Full-disk encryption (FDE)

Two complementary views:

Module	Role
Disk imaging	Open forensic images (E01, DD/RAW, VMDK, VHD/VHDX, QCOW2, …), parse **MBR/GPT**, flag **BitLocker, VeraCrypt, LUKS, FileVault 2**, and similar volumes, extract **crypto headers** for cracking, and optionally tie in **memory-derived keys**.

Module	Role
Decrypt disk	Operator workflows for volume-level decryption attempts once keys or passwords are known or recovered.

Import images from **EnCase, dd, VMware, Hyper-V**, or lab workflows; Ciferware focuses on **analysis and recovery**, not replacing your write-blocked acquisition hardware.

4. Memory forensics stack

- **Memory capture:** Acquire hibernation files, pagefile, SAM-related artifacts, process dumps, and **physical RAM** (via supported external capture tools such as WinPmem when deployed).
- **Memory forensics:** Search dumps for **keys, passwords, and artifacts** relevant to encrypted volumes and applications.
- **Volatility3:** Run common plugins (processes, LSA/NTLM-oriented workflows where configured) from the same console.

Captured dumps can **auto-fill** downstream analysis paths (e.g., Volatility and memory forensics tabs).

5. Credentials & network artifacts

- **Credential forensics:** Windows **SAM/SYSTEM**, domain hash extraction and cracking paths.
- **Network artifacts:** Wi-Fi profiles, browser-stored credentials, and related stored secrets.

6. Mobile forensics (workbench modules)

- **iPhone:** Encrypted backups, pairing records, and checkm8-oriented workflows where applicable.
- **Android:** PIN/pattern/gesture analysis, ADB backup inspection, and related mobile formats.

(Dedicated iOS tooling may exist outside this suite; the Server provides integrated entry points for common mobile encrypted stores.)

7. One-click forensics workflow

From **Home**, launch a guided pipeline: **scan encrypted files → memory acquisition (optional) → network credential extraction → reporting**, with staged logging suitable for case notes. Disk image analysis can participate in broader automated runs when enabled in workflow configuration.

8. Algorithm catalog

Browse supported algorithms and format families, cross-linked from scanner results and detection hints—useful for training, report writing, and verifying that a sample maps to the expected recovery module.

Format coverage (representative)

Ciferware targets **broad Passware-class coverage** across categories such as:

Category	Examples
Archives	ZIP, RAR, 7-Zip, …

Category	Examples
Documents	Microsoft Office, PDF, …
Password managers & vaults	KeePass, 1Password, LastPass, Bitwarden, Dashlane, …
Disk & volume encryption	VeraCrypt, BitLocker, LUKS, FileVault 2, …
Databases	SQLCipher, MySQL, PostgreSQL, MongoDB, …
System & enterprise auth	NTLM, Kerberos, Linux shadow, GRUB, Cisco, SSH, PGP, WPA/PMKID, …
Messengers & apps	Telegram, Firefox stores, …

The in-product footer references **50+ format families** with continuous expansion toward a large internal algorithm library. **Exact support** depends on release build and module maturity—use the **Algorithm catalog** and test samples for ground truth in your deployment.

Dictionaries: Built-in and custom **UTF-8 wordlists**; optional integration with Passware-style dictionary folders for migration from existing labs.

User experience highlights

- **Dark / light themes** with replaceable PNG icon sets (`dark/` and `light/` asset folders).
- **Multilingual UI** (English source strings; additional locales via Qt translations).
- **Recent crack jobs** on Home for fast reopening of case files.
- **Live monitoring** dashboard for cluster health and throughput.
- **Run log** export for audit trails and case documentation.

Typical workflows

Workflow A — Single encrypted file

1. Start the **Server** and connect **Agents**.
2. On **Home**, browse or drop the file → **Crack tasks** opens with path filled.
3. Confirm detected format; choose **Attack profile** / dictionary.
4. Submit task; monitor progress on **Live monitoring** or task table.
5. Record password and export **Run log** if required by policy.

Workflow B — Lab image with FDE

1. Obtain a forensic **E01/DD** image (external acquisition).
2. Open in **Disk imaging** → review partitions and encrypted volumes.
3. Extract headers or queue volumes to **Crack tasks**.
4. Optionally run **Memory forensics** on a related `.dmp`/RAM capture for key material.
5. Use **Decrypt disk** when keys are recovered.

Workflow C — Triage before crack

1. Run **Encrypted file scan** on suspect directories.

2. Double-click or submit hits to **Crack tasks** or **Algorithm catalog**.
3. Batch high-value types via **Batch jobs**.

Deployment notes

Component	Role
Ciferware Server	Windows operator station (administrator privileges recommended for some forensic acquisitions).
Ciferware Client / Agent	Worker nodes; install on machines with CPU/GPU resources you want in the pool.
Network	Server listen port configurable; ensure firewall rules allow Agent ↔ Server traffic on your lab VLAN.
Optional tools	Volatility3, WinPmem (or equivalent) for RAM capture—deploy under documented `tools/` paths when using those features.

Performance scales with **node count and hardware**; use **Benchmark** before large cases to set expectations.

Differentiators (honest positioning)

Strength	Notes
Unified console	Cracking + adjacent forensics modules without switching unrelated products for every stage.
Your infrastructure	Tasks stay on **your** network—not a mandatory cloud crack farm.
Detection-first	Parsers and `FileDetector` drive the correct verifier instead of forcing one hash mode.
Passware migration path	Dictionary import and regression matrices aligned with Passware tutorial samples (lab validation).

Known evolution areas (varies by release): GPU kernel depth, every Passware instant-decrypt RAM path (e.g., some VeraCrypt+memory combinations), and edge formats may lag flagship commercial suites—validate against your **V1 test matrix** before casework commitments.

Compliance & ethics

- Use only under **valid legal authority** (warrant, consent, organizational policy, or equivalent).
- Maintain **chain of custody** for originals; prefer forensic images for disk work.
- Document tools and versions (build number, dictionary lists) in case reports.
- Ciferware outputs are **aids to examination**; human review and jurisdictional rules apply.

About

Ciferware is developed for professional password recovery and digital forensics workflows.

Product	Ciferware Server & Compute Agents
Web	ciferware.com
Organization	Digivetus (software publisher)

Document info

Field	Value
Document	Product brochure
Language	English
Format	Markdown
Audience	Investigators, lab managers, procurement, technical evaluators

Specifications and module availability may change between releases. Evaluate your build against shipped release notes and internal test matrices before production casework.

Quick reference — Server modules

Section	Modules
Overview	Home, Live monitoring, Compute nodes, Run log
Cracking	Crack tasks, Attack profiles, Batch jobs, Benchmark
Forensics	Encrypted file scan, Memory capture, Memory forensics, Volatility3, Disk imaging, Decrypt disk
Credentials & network	Credential forensics, Network artifacts
Mobile	iPhone forensics, Android forensics
Help & reference	Algorithm catalog

© Digivetus. Ciferware™ names and logos are used for product identification. Third-party marks (Passware, Volatility, EnCase, VMware, etc.) belong to their respective owners.