GovCracker

Forensic Password Recovery & Cracking Software

DATASHEET

Version 7.1.0

Forensic password cracking - locally and across the cluster.

GovCracker is a high-performance forensic password recovery software designed for law enforcement agencies, universities and forensic laboratories. At its core, GovCore serves as the high-performance cracking engine, while GovCluster provides distributed cracking across local and remote Windows and Linux systems for scalable GPU-powered password recovery. All processing remains under the organisation's control, with full data sovereignty, comprehensive audit logging and centralised job management.

5	30+	10	100%
ATTACK MODES	Password hash extractors	Interface languages	Local data sovereignty

FORENSIC CORE PRINCIPLES

- **Self-contained data storage**
  Application data, configuration and logs remain within the GovCracker application environment.
- **Server starts on demand only**
  The GovCluster server never starts automatically, only when required.
- **Audit logging & reporting**
  Relevant actions, job events and results are recorded to support reproducible, court-ready reporting
- **Full stream analysis**
  The entire GovCore output is always checked for errors and warnings.

FOR FORENSIC TEAMS

- **Agencies & investigators**
  Distributed cracking across any number of local and remote agents.
- **Forensic labs**
  Deployed worldwide in forensic operations.
- **IT security teams**
  Central job dashboard with live status, progress and devices.
- **Case management**
  Cases, archive and structured job history for the chain of custody.

Cracking Capabilities (1 / 2)

Attack modes and distributed cracking with GovCluster

ATTACK MODES

- **Dictionary attack (Wordlist)**
  Wordlists with optional rules for targeted candidate variations.
- **Mask attack (Mask)**
  Brute-force across freely definable character masks and charsets.
- **Combinator attack (Combinator)**
  Combines two wordlists into new candidate passwords.
- **Hybrid attack**
  Merges wordlists with masks for prefix/suffix patterns.
- **Automatic attack**
  Automated multi-stage attack strategy combining appropriate attack methods and candidate sources.

GOVCLUSTER - DISTRIBUTED CRACKING

- **Integrated cluster server**
  Integrated cluster service for controlled communication with local and remote GovAgents.
- **Intelligent chunking**
  Dynamic keyspace splitting based on benchmark and agent performance.
- **Benchmark-driven**
  Adaptive chunk sizing per agent, hash mode and configured processing window.
- **Live agent tracking**
  Heartbeat with progress, speed and status of all agents in real time.
- **GovBrain mode**
  Brain client/server coordination helps prevent redundant candidate computations across participating systems.

Cracking Capabilities (2 / 2)

Job management, monitoring and hash processing

JOB MANAGEMENT & MONITORING

- **Unified job model**
  Local and cluster cracking in one shared dashboard.
- **Live progress**
  Progress, speed, ETA and device utilisation per job in real time.
- **Warning & error detection**
  GovCore output is continuously analysed and relevant warnings and errors are surfaced directly in the GovCracker UI.
- **Job lifecycle**
  Start, pause, resume, stop, complete and archive per job.
- **Cracked passwords**
  Results with timestamp and attribution to the delivering agent.

HASH PROCESSING & INTEGRATION

- **Hash extraction**
  30+ integrated extractors prepare password hashes and cracking material from supported files, containers and encrypted formats.
- **VeraCrypt, crypto wallets, BitLocker & more**
  Supports hash extraction from VeraCrypt, BitLocker, cryptocurrency wallets and numerous other encrypted sources.
- **7z, RAR, ZIP, Office & more**
  Extracts cracking material from supported archives and password-protected Office documents.
- **Potfile integration**
  Automatic matching of already cracked hashes from the potfile.
- **E-mail notification**
  Optional SMTP notifications for relevant job events, completions and results.

Benchmarks & Cost Comparison

GovCracker vs. Passware Kit Forensic - same GPU, same hash type

CRACKING SPEED (NVIDIA RTX 4090)

HASH TYPE	GOVCRACKER	PASSWARE KIT	DELTA
MS Office 2013+ (AES-256)	65.361 H/s	48.581 H/s	+35 %
RAR 5.x (AES-256)	263.581 H/s	201.723 H/s	+31 %
FileVault2 / APFS	428.985 H/s	117.395 H/s	+265 %
BitLocker	9.565 H/s	7.312 H/s	+31 %

Reference: single NVIDIA RTX 4090. GovCore/hashcat figures based on the official v7.0.0 community benchmark; Passware figures from the Passware Kit Ultimate datasheet. Results may vary depending on software version, hash parameters, drivers and system configuration.

ANNUAL LICENSE - SAME SCALE

GovCracker GOV Edition

$799 / year

Full feature set, one cluster agent, free updates. Add-on: GovAgent+ ($579/year) adds unlimited agents.

Passware Kit Forensic

$1,380 / year

10 agents included; each additional 10 agents +$1,380/year. Updates included for one year only.

1.3x
Higher cracking speed in shown benchmarks

3.7x
Higher cracking speed on FileVault2

≈50%
lower annual license cost

Technical Specifications

Architecture, compatibility and deployment

SYSTEM & ARCHITECTURE

GovCracker Platform	**Windows 10 / 11 (64-bit)**
GovAgent Platform	**Linux & Windows**
Cracking engine	**GovCore (modified hashcat build)**
Cluster	**GovCluster - integrated distributed processing architecture**
Data storage	**SQLite**
Data sovereignty	**Local processing; no case data transmitted**
Languages	**10 languages**

LICENSE EDITIONS

LITE

Local cracking with basic hash type (MD5). Dictionary & mask attacks.

GOV

Agency edition:
Complete LITE scope, 30+ hash extractors, 450+ algorithms, plus priority support & rollout assistance.

Request a live demonstration

office@decrypta-technologies.com - www.decrypta-technologies.com