DEFGET by CyberHorses AG

Defender Grand Extraction Tool

DEFGET – Advanced Forensics, Integrated at Scale

Transforming DFIR Through Seamless EDR Integration

DEFGET revolutionizes Digital Forensics and Incident Response (DFIR) by embedding advanced forensic capabilities directly into your Endpoint Detection and Response (EDR) platform. With zero-code deployment, fleet-wide scalability, and automated artifact processing, DEFGET accelerates investigations while eliminating the overhead of additional tools or physical access.

Why DEFGET

- Zero-Code Deployment – Deploy instantly, no coding or maintenance.
- Continuously Updated – Always aligned with the latest forensic methods.
- Elastic Scalability – Capture from one device or thousands simultaneously.
- Automated Enrichment – Super-timelines generated instantly from raw data.

Integrate and Consume

- Standards-compliant output - delivered in DFIR formats like PLASO timelines.
- Seamless API Integration – connects easily to your SOC, SIEM, and SOAR platforms.

Collect at scale

- Distributed Architecture - efficient for both single targets and enterprise fleets.
- Resilient by Design – adapts to target environments with built-in error recovery.

Deploy with Ease

- Preconfigured templates - start immediately.
- Adaptive collection – customer-defined collection use cases.
- Effortless setup – deployed in minutes.

Forensics without friction. From endpoint to fleet

www.cyberhorses.io