



KAPE TRIAGE AUTOMATION SUITE

Client-Facing Forensic Triage Documentation • Version 1.3

Portable • Repeatable • Defensible • Designed for Digital Investigations

This document has been prepared for clients and stakeholders to explain the purpose, scope, and assurance model of the KAPE Triage Automation Suite. It is written in clear language, while still reflecting the standards expected of professional forensic engagements.

1. Executive Summary

The KAPE Triage Automation Suite is a portable forensic triage toolset built around the industry-recognised KAPE (Kroll Artifact Parser and Extractor) framework. It enables incident responders and digital forensic analysts to rapidly acquire triage artefacts from a target system with minimal disruption to business operations. The process is standardised, logged, and designed to support legal and regulatory scrutiny.

The solution is typically deployed on encrypted removable media and executed under administrative authority. Once started, the tool silently schedules and runs a SYSTEM-level KAPE execution, storing all collected data, metadata, and logs back onto the removable media. This approach reduces the risk of human error and ensures that each execution follows a consistent, defensible pattern.

Key Benefits:

- Standardised triage workflow across all investigations.
- Portable deployment: no installation required on target systems.
- Minimal user impact: triage runs in the background under SYSTEM.
- Detailed logging to support chain-of-custody and audit trails.
- Alignment with leading digital forensics and security standards.

2. Scope and Intended Use

This document is intended for legal counsel, risk owners, CISOs, investigation leads, and other stakeholders who require assurance that triage activities are performed in a controlled and compliant manner. It is not a technical runbook; instead, it explains the safeguards, standards alignment, and evidence handling approach.

Technical operators (such as DFIR analysts) may use this document alongside internal standard operating procedures (SOPs) to brief clients or management on the methodology and limitations of the tooling.

3. High-Level Architecture

At a high level, the KAPE Triage Automation Suite follows the architecture below. This is intentionally abstracted for clarity and focuses on the flow of control and evidence rather than low-level implementation details.

Removable Media (USB) Triage Executable Environment & Permission Checks SYSTEM
Scheduled Task KAPE Execution Case Folder Creation Logs & Metadata Return Media
to Analyst

All artefacts are written to a dedicated case folder on the removable media. The target system is not used as a long-term storage location, which helps reduce contamination risk and supports a clean evidential workflow.

4. Workflow Overview

1. Authorised responder inserts approved forensic USB media.
2. Responder runs the provided executable with administrative rights.
3. The tool validates environment, locates KAPE, and prepares a case output directory.
4. A one-time scheduled task is created to execute KAPE under the SYSTEM account.
5. KAPE collects triage artefacts as configured (e.g., SANS triage profile).
6. Logs (text and JSON) are generated, documenting key metadata and timestamps.
7. Responder safely removes the media and transfers it to the analysis environment.

5. Standards and Compliance Alignment

The triage process is designed to complement, not replace, formal governance and policy frameworks. The following standards and guidance are particularly relevant:

Standard / Framework	Relevance to Triage Workflow
ISO/IEC 27001 (Annex A)	Supports A.12.4 (Logging), A.12.5 (Operational software control), A.16 (Incident man
ISO/IEC 27037	Provides guidance on identification, collection, and preservation of digital evidence.
ISO/IEC 27043	Describes investigative principles and processes for digital incidents.
NIST SP 800-61 & 800-86	Guidance on incident handling and integration of forensic techniques.
GDPR / UK DPA 2018	Requires lawful basis, minimisation, and accountability for processing personal data c

6. Output Structure and Evidence Handling

Each execution of the triage tool creates a dedicated case directory on the removable media. A typical structure is as follows:

```
CASE-YYYYMMDD-HHMM-HOSTNAME/  
  runlog.txt  
  runlog.json  
  KAPE_Task_Wrapper.ps1  
  [KAPE output folders]  
  [Optional VHDX image]
```

The JSON log is particularly important from a chain-of-custody perspective. It records key metadata such as case identifier, operator details (where available), timestamps, device identifiers, and host system name. These details should be incorporated into the broader investigative record maintained by the organisation or service provider.

7. Legal, Privacy, and Acceptable Use

Use of this tool must always be justified, proportionate, and authorised. In particular:

- It should only be deployed under a lawful mandate (e.g., corporate policy, legal instruction, or contractual right).
- Its use must be consistent with privacy and data protection obligations in relevant jurisdictions.
- Employees and affected parties should be treated fairly, and, where applicable, appropriate notices or policies must be in place.
- Data collected should be minimised to what is necessary for the specific investigation.

Greaton Forensics cannot take responsibility for how the tool is used in practice. The organisation owning or controlling the investigation is responsible for ensuring that legal advice is sought where necessary and that all triage activities fall within the agreed scope of engagement.

8. Attribution and Credits

This documentation and supporting automation were prepared by Greaton Forensics as part of its digital forensics and incident response capability.

The underlying triage engine, KAPE (Kroll Artifact Parser and Extractor), was created by Eric Zimmerman and is maintained and distributed by Kroll. All credit for KAPE and its capabilities belongs to Eric Zimmerman and Kroll. This automation merely orchestrates and logs the execution of KAPE in a controlled manner.

This document may be shared with clients, legal representatives, and relevant stakeholders as part of formal incident response or investigative reporting.