GREATON FORENSICS

SUITE DE AUTOMATIZACIÓN KAPE TRIAGE

Documentación de Triage Forense Orientada al Cliente • Versión 1.3

Portátil · Repetible · Defendible · Diseñada para Investigaciones Digitales

Este documento ha sido preparado para clientes y partes interesadas con el fin de explicar el propósito, el alcance y el modelo de aseguramiento de la Suite de Automatización KAPE Triage. Está redactado en un lenguaje claro, manteniendo al mismo tiempo el nivel de rigor esperado en compromisos forenses profesionales.

1. Resumen Ejecutivo

La Suite de Automatizaci ó n KAPE Triage es un conjunto de herramientas de triage forense port á til, construido sobre el marco KAPE (Kroll Artifact Parser and Extractor), ampliamente reconocido en la industria. Permite a los equipos de respuesta a incidentes y analistas forenses adquirir artefactos de triage de forma r á pida, estructurada y con un impacto m í nimo sobre las operaciones del negocio.

Normalmente, la soluci ó n se despliega en un medio extra í ble cifrado y se ejecuta bajo credenciales administrativas. Una vez iniciada, la herramienta programa y ejecuta silenciosamente una ejecuci ó n de KAPE con privilegios de SYSTEM, almacenando todos los datos recopilados, metadatos y registros directamente en el propio medio extra í ble. Este enfoque reduce el riesgo de error humano y garantiza que cada ejecuci ó n siga un patr ó n consistente y defendible.

Beneficios clave:

- Flujo de triage estandarizado en todas las investigaciones.
- Despliegue port á til: no requiere instalaci ó n en el sistema objetivo.
- Impacto m í nimo para el usuario: el triage se ejecuta en segundo plano como SYSTEM.
- Registro detallado para soportar la cadena de custodia y la trazabilidad.
- Alineaci ó n con las principales normas de forense digital y seguridad.

2. Alcance y Uso Previsto

Este documento est á destinado a asesores legales, responsables de riesgo, CISOs, responsables de investigaci ó n y otras partes interesadas que necesitan garant í as de que las actividades de triage se realizan de forma controlada y conforme a las normas. No es un manual t é cnico, sino una explicaci ó n de las salvaguardas, la alineaci ó n con est á ndares y el enfoque de manejo de evidencias.

Los operadores t é cnicos (como analistas DFIR) pueden utilizar este documento junto con procedimientos operativos est á ndar internos (SOP) para informar a clientes o a la direcci ó n sobre la metodolog í a y las limitaciones de la herramienta.

3. Arquitectura de Alto Nivel

A alto nivel, la Suite de Automatizaci ó n KAPE Triage sigue la arquitectura que se describe a continuaci ó n. Se presenta de forma simplificada para facilitar su comprensi ó n y se centra en el flujo de control y evidencias.

Soporte Extra í ble (USB) → Ejecutable de Triage → Verificaci ó n de Entorno y Permisos → Tarea Programada con SYSTEM → Ejecuci ó n de KAPE → Creaci ó n de Carpeta de Caso → Registros y Metadatos → Retorno del Medio al Analista

Todos los artefactos se escriben en una carpeta de caso dedicada en el medio extra í ble. El sistema objetivo no se utiliza como ubicaci ó n de almacenamiento permanente, lo que ayuda a reducir el riesgo de contaminaci ó n y respalda un flujo de evidencias limpio.

4. Flujo de Trabajo

1. El respondedor autorizado inserta el medio forense USB aprobado.
2. El respondedor ejecuta el fichero EXE con privilegios de administrador.
3. La herramienta valida el entorno, localiza KAPE y prepara el directorio de salida del caso.
4. Se crea una tarea programada de una sola ejecuci ó n para lanzar KAPE como SYSTEM.
5. KAPE recoge los artefactos de triage seg ú n la configuraci ó n (por ejemplo, perfil SANS).
6. Se generan registros (texto y JSON) con metadatos y marcas de tiempo.
7. El respondedor retira el medio de forma segura y lo traslada al entorno de an á lisis.

5. Alineaci ó n con Normas y Cumplimiento

El proceso de triage est á dise ñ ado para complementar, no sustituir, los marcos de gobierno y pol í tica existentes. Las siguientes normas y gu í as son especialmente relevantes:

Norma / Marco	Relevancia para el flujo de triage
ISO/IEC 27001 (Anexo A)	Soporta A.12.4 (Registro), A.12.5 (Control de software en operación), A.16 (Gestión
ISO/IEC 27037	Guía para la identificación, recopilación y preservación de evidencias digitales.
ISO/IEC 27043	Principios y procesos de investigación de incidentes digitales.
NIST SP 800-61 y 800-86	Guías de gestión de incidentes e integración de técnicas forenses.
GDPR / Ley de Protección de Datos de Reino Unido 2018	Requiere base jurídica, minimización y responsabilidad en el tratamiento de datos pe

6. Estructura de Salida y Manejo de Evidencias

Cada ejecuci ó n de la herramienta de triage crea un directorio de caso dedicado en el medio extra í ble. Una estructura t í pica es la siguiente:

```
CASE-YYYYMMDD-HHMM-HOSTNAME/
  runlog.txt
  runlog.json
  KAPE_Task_Wrapper.ps1
  [Carpetas de salida de KAPE]
  [Imagen VHDX opcional]
```

El registro JSON es especialmente importante desde una perspectiva de cadena de custodia. Registra metadatos clave, como el identificador de caso, detalles del operador (cuando se dispone de ellos), marcas de tiempo, identificadores del dispositivo y el nombre del sistema anfitri ó n. Estos detalles deben integrarse en el registro investigativo m á s amplio mantenido por la organizaci ó n o el proveedor de servicios.

7. Aspectos Legales, Privacidad y Uso Aceptable

El uso de esta herramienta debe ser siempre justificado, proporcionado y autorizado. En particular:

- Solo debe desplegarse bajo un mandato legal v á lido (por ejemplo, pol í tica corporativa, instrucci ó n legal o derecho contractual).
- Su uso debe ser coherente con las obligaciones de privacidad y protecci ó n de datos en las jurisdicciones relevantes.
- Los empleados y las personas afectadas deben ser tratados de forma justa y, cuando proceda, deben existir avisos o pol í ticas adecuadas.
- Los datos recopilados deben limitarse a lo necesario para la investigaci ó n concreta.

Greaton Forensics no puede asumir responsabilidad por la forma en que se utilice la herramienta en la pr á ctica. La organizaci ó n que dirige o controla la investigaci ó n es responsable de asegurarse de que se obtenga asesoramiento legal cuando sea necesario y de que todas las actividades de triage se mantengan dentro del alcance acordado del compromiso.

8. Atribución y Créditos

Esta documentación y la automatización asociada han sido preparadas por Greaton Forensics como parte de su capacidad de respuesta ante incidentes y forense digital.

El motor de triage subyacente, KAPE (Kroll Artifact Parser and Extractor), fue creado por Eric Zimmerman y es mantenido y distribuido por Kroll. Todo el crédito por KAPE y sus capacidades corresponde a Eric Zimmerman y Kroll. Esta automatización únicamente orquesta y registra la ejecución de KAPE de forma controlada.

Este documento puede compartirse con clientes, representantes legales y otras partes interesadas como parte de la documentación formal en investigaciones o respuestas a incidentes.