# KAPE

**KAPE Notes**

**Task 1: Learning Objectives**

* Understand what **KAPE** is and how it works in DFIR.
* Learn about **Targets** (what to collect) and **Modules** (how to process/analyze collected data).
* Use both **GUI** and **CLI** for investigations.
* Perform a **hands-on forensic collection challenge**.

**Task 2: Introduction to KAPE**

* **KAPE** = Kroll Artifact Parser and Extractor.
* A **triage tool** that quickly collects important forensic artifacts from a live or mounted system.
* Works in **two phases**:
  1. **Target collection** → gathers forensic artifacts (e.g., registry, event logs, browser data).
  2. **Module execution** → processes data using forensic tools/scripts (e.g., parse registry hives, extract browser history).
* Commonly run from a **USB drive** for portability.

**Task 3: Target Options**

* **Targets** = predefined sets of artifacts to collect.
* Examples:
  + Registry hives
  + Event logs
  + Browser history
  + Prefetch files
* Can create **custom targets** for specific cases.
* Output stored in a chosen directory (often on an external USB).

**Task 4: Module Options**

* **Modules** = scripts/programs run on collected data.
* Examples:
  + Parse registry → RegRipper
  + Parse event logs → EvtxECmd
  + Extract browser history → BrowsingHistoryView
* Automates analysis → saves time vs manual parsing.
* Can chain multiple modules for **bulk analysis**.

**Task 5: KAPE GUI**

* Easy-to-use graphical interface.
* Allows selection of:
  + **Targets** (what to collect)
  + **Modules** (how to process data)
  + Output location
* Useful for beginners and quick collections.

**Task 6: KAPE CLI**

* Command-line interface (faster, scriptable, remote execution).
* Common syntax:
* kape.exe --tsource C: --tdest D:\Output --target !BasicCollection --mdest D:\Modules --module !SANS\_Triage
* Options:
  + --tsource → source drive/directory
  + --tdest → target output directory
  + --target → select target(s)
  + --mdest → where module results are stored
  + --module → select module(s)

**Task 7: Hands-on Challenge**

* Run KAPE in a real scenario:
  1. Select **targets** (e.g., system & user artifacts).
  2. Save to **USB** or designated folder.
  3. Run **modules** to parse evidence.
  4. Review output in text/CSV/HTML reports.
* Goal: simulate a **real forensic acquisition and triage**.

**Task 8: Conclusion**

* **KAPE = powerful triage tool** for rapid collection & processing.
* Supports both **GUI** and **CLI** modes.
* Targets = define what to collect, Modules = define how to process it.
* Saves time for DFIR analysts by automating repetitive evidence extraction tasks.

