


Евразийский национальный университет имени Л.Н. Гумилева
Национальная инженерная академия РК
Казахский национальный педагогический университет имени Абая, Казахстан
Институт математики и математического моделирования КН МВНО, Казахстан
Институт информационных и вычислительных технологий КН МВНО, Казахстан
Международный математический центр ИМ им. С.Л. Соболева СО РАН, Россия
Российский национальный комитет по индустриальной и прикладной математике, Россия
ОФ «Международный фонд обратных задач», Казахстан
Математическое Общество Тюркского Мира.

ЕУРАЗИЯЛЫҚ ХАЛЫҚАРАЛЫҚ ҒЫЛЫМИ КОНФЕРЕНЦИЯ
ЕВРАЗИЙСКАЯ МЕЖДУНАРОДНАЯ НАУЧНАЯ КОНФЕРЕНЦИЯ

«ҒЫЛЫМДАҒЫ, ТЕХНИКА МЕН ИНДУСТРИЯДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕКТ ЖӘНЕ КЕРІ ЕСЕПТЕР»

«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ОБРАТНЫЕЗАДАЧИ В НАУКЕ, ТЕХНИКЕ И ИНДУСТРИИ»

«ARTIFICIAL INTELLIGENCE AND INVERSE PROBLEMS IN SCIENCE, TECHNOLOGY AND INDUSTRY»

ЕҢБЕКТЕРІ ТРУДЫ PROCEEDINGS

Астана
14-16 апреля 2025 г.

УДК 004.896:001(082)

Еуразиялық халықаралық ғылыми конференция
«Ғылымдағы, техника мен индустриядағы жасанды интеллект және кері есептер»
Евразийская международная научная конференция
“Искусственный интеллект и обратные задачи в науке, технике и индустрии”
Eurasian internationalscientific conference
«Artificial intelligence and inverse problems in science, technology and industry»

ISBN 978-601-385-052-8

Еуразиялық халықаралық ғылыми конференция «Ғылымдағы, техника мен индустриядағы жасанды интеллект және кері есептер» баяндамалар жинағы. 14-16 сәуір 2025 жыл.

Сб. докл. Евразийской международной научной конференций «Искусственный интеллект и обратные задачи в науке, технике и индустрии» 14-16 апрель 2025 год.

Collection of reports the Eurasian internationalscientific conference «Artificial intelligence and inverse problems in science, technology and industry»

– Астана: Л.Н. Гумилев атын. Еуразия ұлттық университеті, 2025. – 451 б. – қазақша, орысша, ағылшынша.

1 СЕКЦИЯ . «КЕРІ ЕСЕПТЕРДІ ШЕШУДЕ ЖАСАНДЫ ИНТЕЛЛЕКТ»

СЕКЦИЯ 1. «ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В РЕШЕНИИ ОБРАТНЫХ ЗАДАЧ»

SECTION 1. «ARTIFICIAL INTELLIGENCE IN SOLVING INVERSE PROBLEMS»

2 СЕКЦИЯ «КЕРІ ЖӘНЕ ДҰРЫС ҚОЙЫЛМАҒАН ЕСЕПТЕРДІҢ ТЕОРИЯЛЫҚ ЖӘНЕ ЕСЕПТЕУ АСПЕКТІЛЕРІ»

СЕКЦИЯ 2 «ТЕОРЕТИЧЕСКИЕ И ВЫЧИСЛИТЕЛЬНЫЕ АСПЕКТЫ ОБРАТНЫХ И НЕКОРРЕКТНЫХ ЗАДАЧ»

SECTION 2 «THEORETICAL AND COMPUTATIONAL ASPECTS OF INVERSE AND ILL-POSITIONED PROBLEMS»

3 СЕКЦИЯ «АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР ЖӘНЕ ЕСЕПТЕУ ИНТЕЛЛЕКТІСІ

3 СЕКЦИЯ «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ВЫЧИСЛИТЕЛЬНЫЙ ИНТЕЛЛЕКТ»

SECTION 3 «INFORMATION TECHNOLOGY AND COMPUTATIONAL INTELLIGENCE»

4 СЕКЦИЯ «КРИПТОГРАФИЯДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕК ЖӘНЕ КИБЕРҚАУІПСІЗДІК»

4 СЕКЦИЯ «ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КРИПТОГРАФИИ И КИБЕРБЕЗОПАСНОСТИ»

SECTION 4 "ARTIFICIAL INTELLIGENCE IN CRYPTOGRAPHY AND CYBERSECURITY"

UDC 004.056.b.

Meiramkhan E.A. – master's student (Astana, L.N. Gumilyov ENU)

METHODS OF INTEGRATING KAPE WITH OTHER DIGITAL FORENSICS TOOLS

Abstract: KAPE (Kroll Artifact Parser and Extractor) is a digital forensics tool developed by Eric Zimmerman to streamline the rapid collection and processing of forensic artifacts in Windows environments. Unlike traditional forensic tools, KAPE is highly customizable, allowing investigators to define what data is collected, how it is gathered, and whether additional processing is applied.

KAPE overcomes common triage limitations, such as metadata loss, locked file restrictions, and rigid data collection parameters. By acting as a high-speed forensic engine, it enables investigators to acquire actionable intelligence in under 90 minutes. This paper examines KAPE's key functionalities, integration with other forensic tools, and its role in enhancing the efficiency of digital forensic investigations.

Keywords: Digital forensics, KAPE, triage imaging, artifact collection, windows forensic analysis, incident response, volume shadow copies, chain of custody, forensic automation, data integrity

I. Introduction

KAPE is a triage tool designed to rapidly identify and extract the most relevant forensic artifacts from a target system. Its high-speed processing allows investigators to prioritize critical systems in their case, expediting forensic analysis. Additionally, KAPE can collect essential artifacts at the beginning of a traditional imaging process, enabling analysts to review extracted data for leads, build timelines, and accelerate investigations while imaging completes. KAPE serves two primary functions: collecting files and processing them using external forensic tools. Instead of executing these tasks independently, KAPE relies on configuration files that define which artifacts to collect and how to process them. This modular design makes KAPE highly customizable without requiring software modifications[1-2].

At a technical level, KAPE operates by adding file masks to a queue, directing the collection of targeted files from a source location. If files are locked by the operating system, KAPE performs a secondary pass to bypass restrictions. The collected files and metadata are then preserved in a designated directory. Additionally, KAPE can process extracted data using third-party forensic tools, categorizing results into structured groups such as EvidenceOfExecution, BrowserHistory, and AccountUsage. This method simplifies analysis by organizing artifacts based on their forensic significance rather than requiring expertise in individual artifacts(Figure 1).

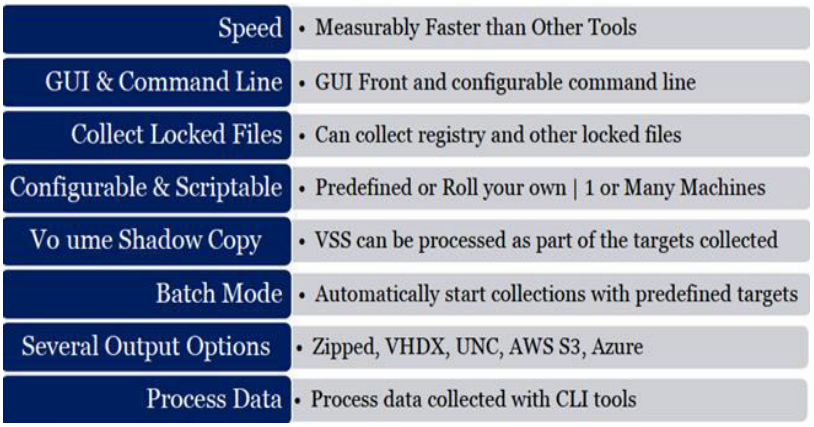

Figure 1. Key features of KAPE

KAPE is available in two licensing models: Solo and Enterprise. The Solo edition is free for government agencies, educational institutions, and internal corporate investigations, while the Enterprise edition is required for third-party engagements or commercial use.

II. KAPE Configuration and Customization

KAPE operates using a system of targets and modules, both defined using YAML configurations. This structured approach ensures flexibility and ease of use, allowing forensic investigators to efficiently customize data collection and processing. KAPE includes numerous preconfigured targets and modules that can be used as-is or modified to meet specific forensic requirements. These configurations have been rigorously tested for accuracy and reliability. By modifying the provided YAML files, users can extend KAPE's functionality for various investigative scenarios(Figure 2).

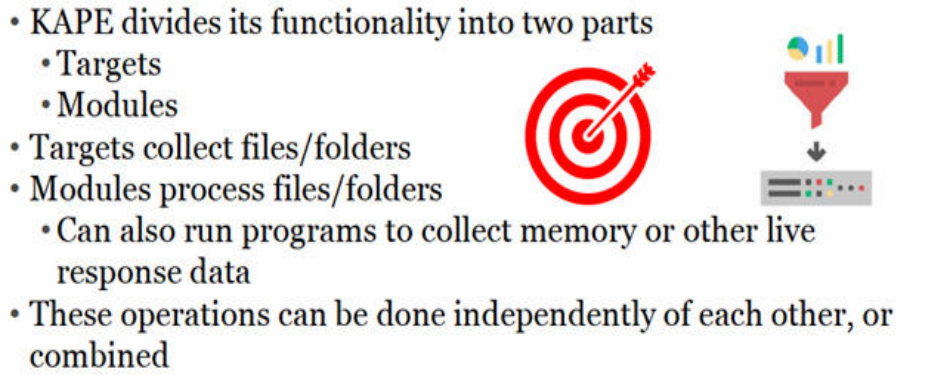

Figure 2. KAPE Targets & Modules

Targets

Target configurations specify file masks used to locate different types of artifacts on a storage device. These masks allow KAPE to collect files based on full name, extension, or even an entire directory structure. Recursive searching can be enabled to capture nested files, ensuring comprehensive artifact collection. This method provides investigators with an efficient way to acquire critical forensic evidence.

Modules

Modules process the files collected by KAPE, executing commands using external forensic tools. Each module configuration defines parameters such as command-line arguments, export formats, and processing options. Modules enable automated execution against live systems or previously acquired forensic data. This modular design allows seamless integration with CLI-based forensic tools, optimizing digital forensic workflows. By combining targets and modules, KAPE provides a powerful, adaptable solution for forensic investigations, enabling precise data acquisition and automated artifact analysis.[3] This structured workflow significantly enhances efficiency in digital forensics and incident response(Figure 3).

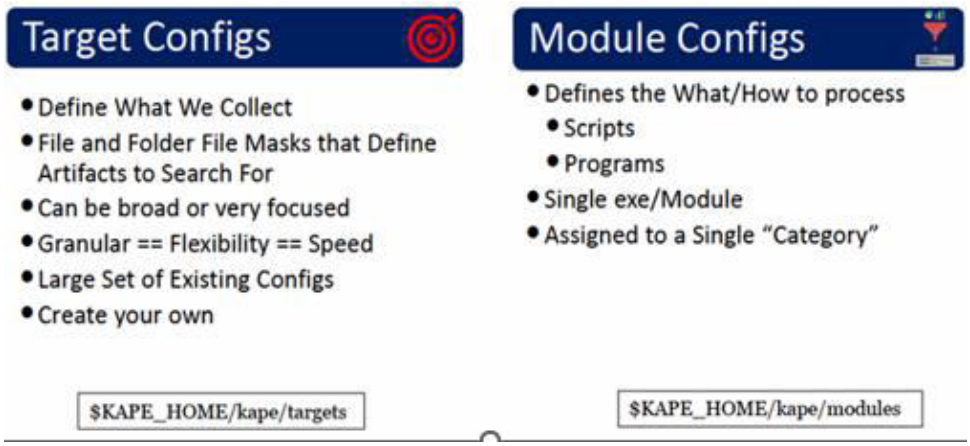

Figure 3. KAPE configuration files

III. Optimizing forensic analysis with KAPE Targets and Modules

Targets in KAPE define file and directory specifications used to identify and extract forensic artifacts. KAPE processes these specifications, compiles a list of relevant files, and copies them to a destination directory.

For locked files, KAPE employs a two-step approach: accessible files are copied first, while locked files are added to a secondary queue and extracted using raw disk reads. This ensures the preservation of in-use files without system interference. All copied files retain their original timestamps, and metadata is logged in text and CSV formats.

Targets should focus on specific artifacts, such as Jump Lists or LNK files, keeping collections granular for flexibility. Modular targets can be combined as needed, except for cases like NTFS file system data, where elements like $MFT, $LogFile, and $J are typically used together. This structured approach optimizes forensic investigations by maintaining accuracy and adaptability[4].

Like targets, KAPE modules are defined using YAML properties and are designed to execute forensic tools on collected data or live systems. Modules allow investigators to automate the processing of artifacts, such as using JLECmd to extract Jump List contents or RECmd to analyze Windows registry files. Additionally, live response commands, such as netstat.exe or ipconfig /dnscache, can be executed through modules for real-time system analysis.

Each module references a single executable but can be configured to export data in multiple formats, including CSV, HTML, and JSON. This enables integration with big data platforms like SOF-ELK or Splunk, as well as forensic tools like Timeline Explorer for in-depth analysis.

Modules are categorized based on their function, such as Evidence of Execution, File and Folder Opening, or Browser History. Maintaining standardized categories ensures consistency in forensic workflows, making data analysis more structured and efficient(Figure 4).

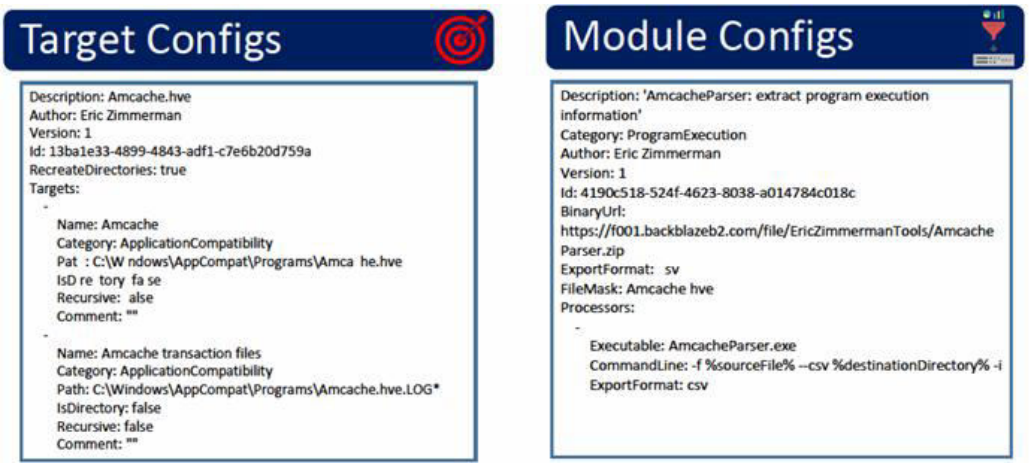

Figure 4. KAPE configuration file examples

KAPE includes a variety of predefined targets, including those from the SANS Forensics Analysis poster, covering browser history, file system metadata, LNK files, Jump Lists, Outlook data, and event logs. Users can utilize these targets or create custom ones to fit specific forensic needs.

Similarly, KAPE provides built-in modules for processing collected data, which can also be customized. The KAPE manual offers detailed documentation on configuring targets and modules, with additional examples available in the installation directory. Full documentation is accessible online[5].

The GUI version of KAPE simplifies forensic data collection by allowing analysts to select artifacts for triage with a simple checkbox system. The left panel of the interface represents the Target selection, while the right panel (partially shown in the interface) corresponds to the Module processing side(Figure 5).

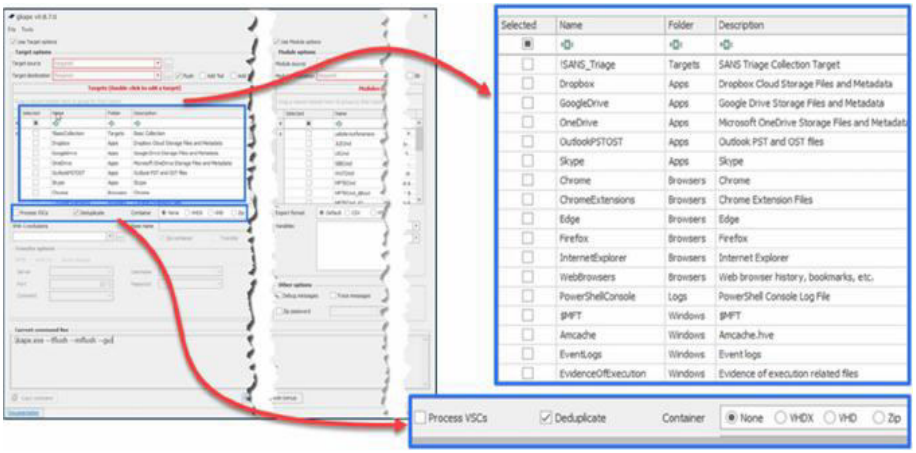

Figure 5. Creating triage data with KAPE

KAPE also streamlines additional forensic tasks, such as extracting Volume Shadow Copies with a single click, eliminating the need for multiple manual steps. Additionally, collected data can be saved as a VHDX file, which is automatically compressed into a ZIP archive for efficient storage.

While KAPE originally operated as a command-line tool, the GUI (GKAPE) was introduced later for ease of use. The command line remains a powerful option, enabling automation of data collection

and processing. Analysts can review generated commands in the GUI to better understand and optimize KAPE's CLI usage. Enabling the "Use Target Options" checkbox in KAPE's GUI grants access to the Target selection panel, where users define which forensic artifacts to collect.

Define Source and Destination – Select the drive letter (e.g., C:, D:) or UNC path for data collection. KAPE does not process forensic images (E01) directly; users must first mount them using Arsenal Image Mounter (AIM). The destination should be an external drive, network share, or cloud storage (SFTP, AWS S3, Azure).

Append Machine Name – Checking the %m option ensures that the collected data is tagged with the machine name, useful when gathering evidence from multiple systems.

Select Targets – Choose the artifacts or groups of artifacts to collect. KAPE includes predefined targets but also allows for customization.

Process Volume Shadow Copies (VSCs) – Checking the "Process VSCs" box enables KAPE to collect data from VSCs, automatically organizing them by snapshot.

Choose Output Format – Select from various storage formats such as ZIP, VHD, XHDX, or compressed VHDX for efficient data management.

Execute Collection – Clicking "Execute" initiates the collection process, displaying progress in a command window.

This structured workflow allows investigators to efficiently gather and store forensic data while maintaining flexibility in output options(Figure 6).

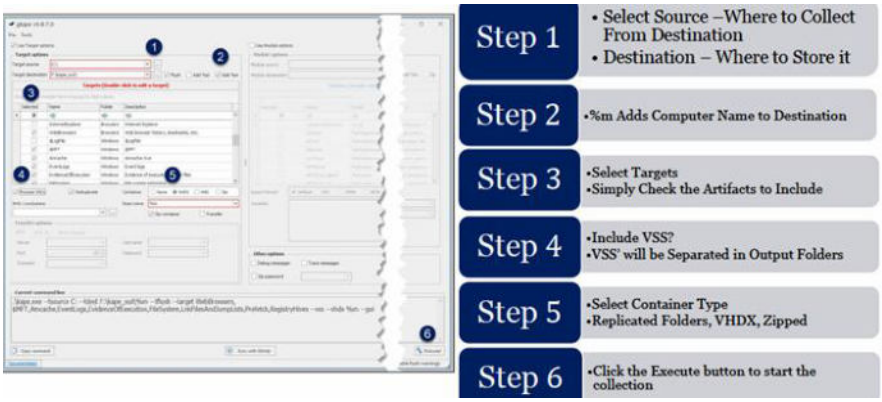

Figure 6. Definition of collection criteria

In Figure 7, KAPE dynamically generates the corresponding command line as users select Targets and Modules in the GUI. This feature helps users familiarize themselves with KAPE's CLI syntax.

While most KAPE functions can be executed via the GUI, scripting remains exclusive to the command line. Scripting is essential for automation and large-scale deployment, enabling forensic teams to streamline data collection across multiple systems efficiently[6-7].

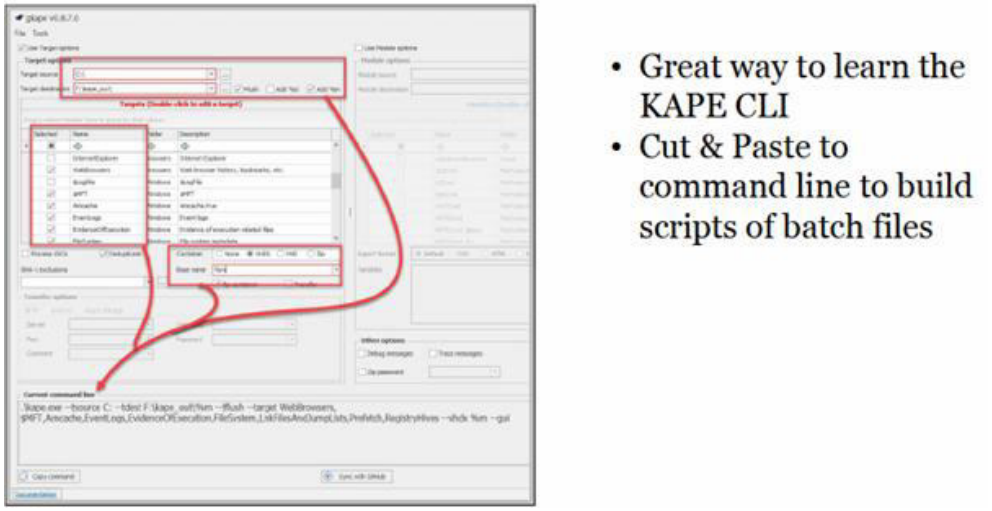

Figure 7. KAPE can build the command line

KAPE uses double dashes (--) before each command-line parameter. Understanding CLI syntax is essential for automation and scripting forensic collections.

One key feature of KAPE is its variety of output container formats. Users can choose between an uncompressed replicated folder structure or a highly compressed VHDX.[8] While VHDX is already a compressed format, further compression can significantly reduce storage requirements, making it possible to store data from multiple systems on a single USB drive(Figure 8).

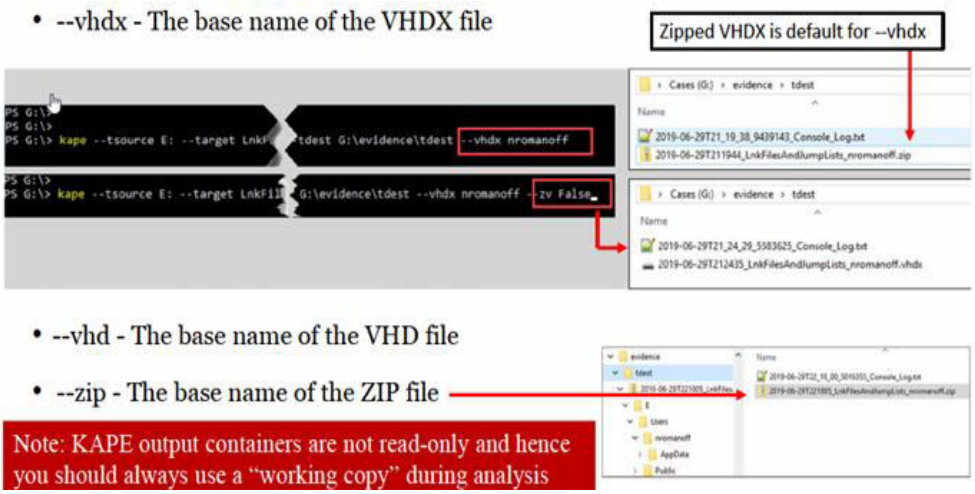

Figure 8. Containers for Target output

KAPE Targets control how the collected folder structure is replicated. When the "Recreate Directories" option is enabled, the output maintains the original folder hierarchy, mirroring its structure in Windows Explorer.

Additionally, KAPE can extract data from Volume Shadow Copies (VSCs), applying the same directory replication rules. This ensures that forensic artifacts from VSCs are organized consistently, preserving their original context for analysis (Figure 9).

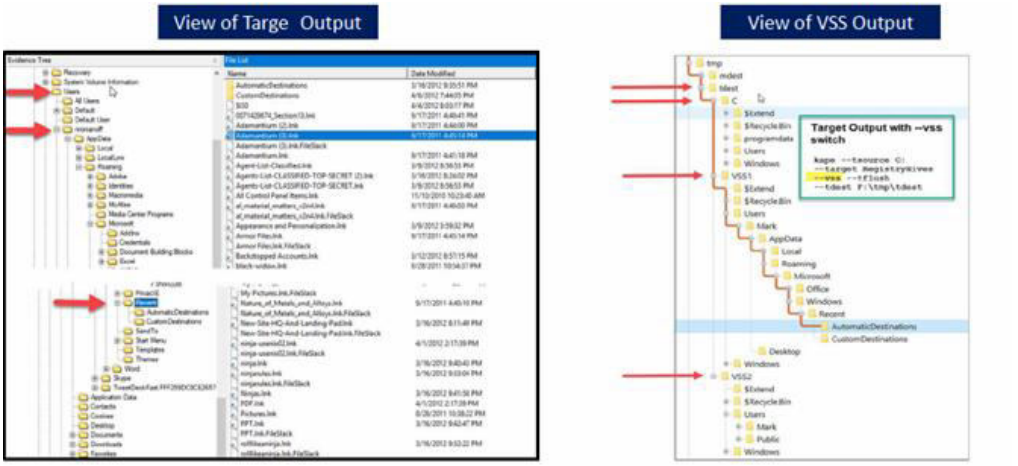

Figure 9. Output folder structure

IV. Triage Imaging with KAPE

KAPE enables the creation of a Triage VHDX, allowing investigators to quickly collect and analyze key forensic artifacts. The triage image can then be examined using tools like Windows SIFT Workstation to extract critical evidence efficiently(Figure 10).

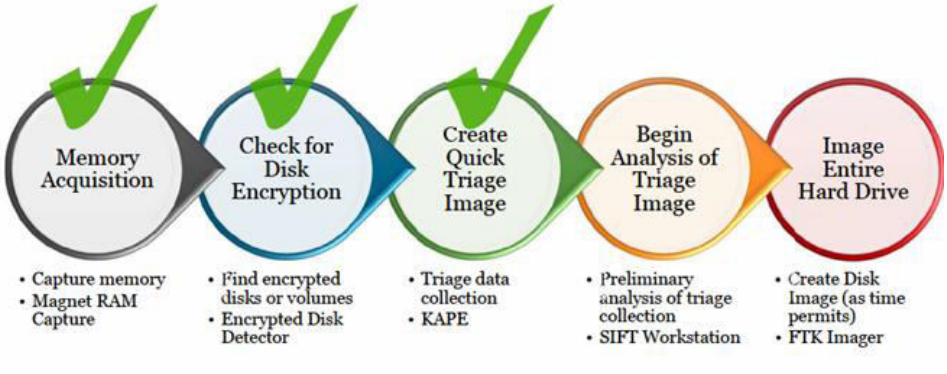

Figure 10. Triage Acquisition: step-by step overview

While triage imaging provides 95% of the most relevant artifacts, it may miss hidden folders, encrypted containers, or non-standard cloud storage. A full disk image ensures deeper analysis but is time-consuming and requires significant storage. In high-priority cases, such as insider threats, employee terminations, or law enforcement investigations, full disk imaging is recommended. However, in incident response, time constraints may necessitate selective collection from affected systems[9-10].

V. Recommendations

To enhance the efficiency of KAPE in digital forensic investigations, it is essential to focus on automation, integration, and accuracy. KAPE should be used for rapid triage collection, allowing investigators to quickly gather key artifacts while minimizing system impact. When necessary, full disk imaging should complement triage-based analysis to ensure no critical evidence is missed.

Integrating KAPE with forensic tools such as Autopsy, FTK, X-Ways, and Velociraptor improves investigative depth and efficiency. Scripting and automation should be prioritized to streamline large-scale forensic operations and reduce manual workload. Ensuring the proper handling of forensic artifacts, including metadata preservation and chain-of-custody verification, is critical for maintaining data integrity and admissibility.Investigators should leverage KAPE's ability to process Volume Shadow Copies (VSCs) to recover historical data while understanding its limitations in selective extraction. Regular updates to KAPE's configurations, targets, and modules are necessary to keep pace with

evolving forensic challenges. Periodic validation of KAPE's performance through testing and accuracy assessments will help refine collection and analysis processes over time.

By implementing these strategies, forensic teams can maximize KAPE's capabilities, improving efficiency, reliability, and the overall effectiveness of digital investigations.

VI. Conclusion

KAPE is a highly efficient tool for rapid forensic data collection and processing, allowing investigators to quickly gather critical artifacts while minimizing system impact. By leveraging targets and modules, KAPE provides a structured approach to forensic investigations, ensuring flexibility and scalability.While triage imaging with KAPE covers a significant portion of forensic needs, it is important to recognize its limitations. Hidden files, encrypted containers, and certain cloud storage artifacts may not be captured during triage, making full disk imaging necessary in complex cases such as insider threats, employee terminations, and law enforcement investigations. In incident response scenarios, time constraints may require selective data collection rather than full imaging. Despite these limitations, KAPE significantly reduces investigation time by enabling quick identification of key artifacts and automating forensic workflows.

Ensuring proper artifact handling, metadata preservation, and chain-of-custody verification is critical for maintaining data integrity and evidentiary value. The ability to process Volume Shadow Copies (VSCs) further enhances KAPE's effectiveness by recovering historical system states. Additionally, automating forensic workflows through scripting and batch processing allows for large-scale investigations with improved efficiency. The integration of KAPE with forensic analysis tools such as SIFT Workstation and other post-processing solutions further strengthens its role in digital forensic investigations.

To maximize its potential, investigators should regularly update KAPE's configurations, targets, and modules to keep pace with evolving forensic challenges and cyber threats. Future advancements in cloud forensics, integration with SIEM platforms, and AI-assisted forensic analysis will likely enhance KAPE's capabilities, making it an even more valuable tool for forensic professionals.

By combining KAPE's speed, automation, and adaptability, forensic experts can enhance the efficiency and reliability of digital investigations. As technology and forensic methodologies continue to evolve, KAPE will remain a critical component of modern forensic workflows, enabling investigators to respond effectively to cyber incidents and digital crimes.

References

1.B. Carrier, "File System Forensic Analysis," Addison-Wesley, 2005.

2. H. Carvey, "Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 10," Syngress, 2018.

3.B. Shavers, E. Zimmerman, "X-Ways Forensics Practitioner's Guide," Syngress, 2013. 4.Kroll Cyber Security, "KAPE (Kroll Artifact Parser and Extractor) Documentation," Kroll, Available: https://www.kroll.com/en/services/cyber-risk/kape.

5. AccessData, "FTK Imager User Guide," AccessData, 2019. Available: https://ad-pdf.s3.amazonaws.com/AD-FTK-Imager-UserGuide.pdf.

6.SANS Institute, "Velociraptor: Digging Deeper for DFIR," SANS Institute, 2020. Available: https://www.sans.org/blog/velociraptor-digging-deeper-for-dfir/.

7.A. J. Nelson, "Digital Forensics and Incident Response," Packt Publishing, 2019.

8.C. Hargreaves, "Incident Response & Computer Forensics," McGraw-Hill, 2020.

9.D. Cowen, "Computer Forensics: A Beginner's Guide," McGraw-Hill, 2021.

10. A. Ligh, M. Case, J. Levy, and C. Walters, "The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory," Wiley, 2014.