Live Acquisition: KAPE

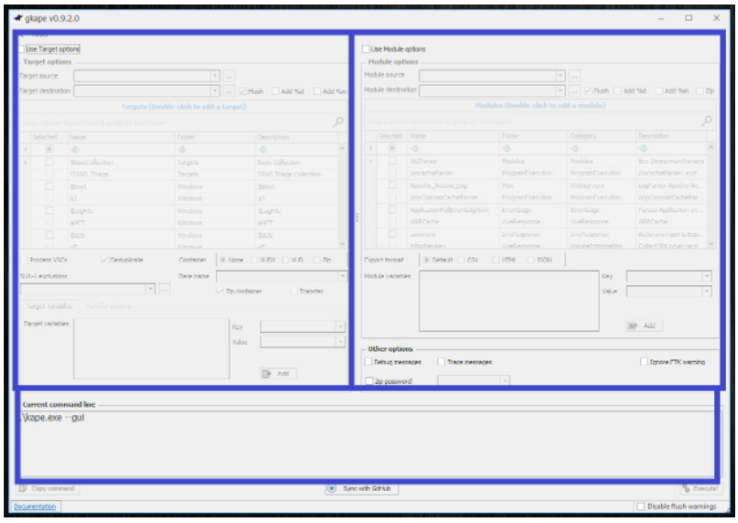
In this lesson, we're going to look at the forensic tool KAPE: the Kroll Artifact Parser and Extractor. KAPE is an efficient and highly configurable triage program that will target essentially any device or storage location, find forensically useful artifacts, and parse them within a few minutes. It is suggested that during a digital investigation a disk imager should be initialized to collect a full disk image of the target system, and KAPE should be run alongside to immediately collect important evidence, even before the full disk image has been acquired. This means that law enforcement and security teams can get results extremely quickly, which can generate new leads for investigation.

It is possible to deploy KAPE on a large scale using PowerShell to download, run, and send the results from KAPE back to the security team, making it an incredibly useful digital forensics and incident response triage tool.

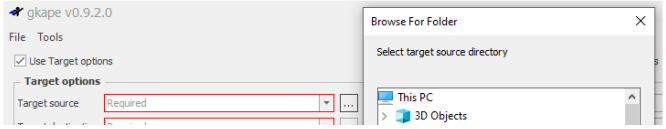
Below we're going to show you KAPE in action, performing live acquisition against our own running system just to demonstrate some of the functionality and information that this tool can retrieve in an extremely short space of time.

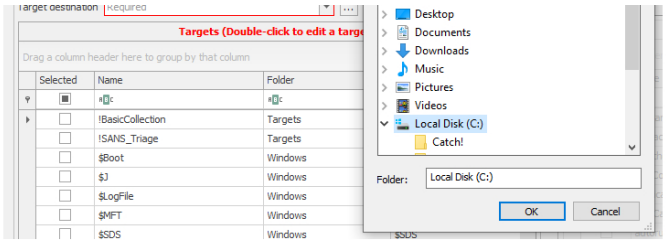
Looking in the KAPE folder, there are two executable files, kape.exe and gkape.exe. We'll be using gkape.exe, which is the graphical version of this tool. Let's run it. We can split the interface into three section:

- **Top Left –** Targets are how we can choose exactly what information we want to retrieve from the target system, so we can get it as quickly as possible. This can be anything from system memory to web browser data.
- **Top Right –** Modules provide additional functionality and allow operations to be conducted with the retrieved data, such as analysis of information collected from the target system. These build on the Target options and allow us to fine-tune the information we want to collect.
- **Bottom –** The Command Line section builds up the query which is passed to KAPE for execution.

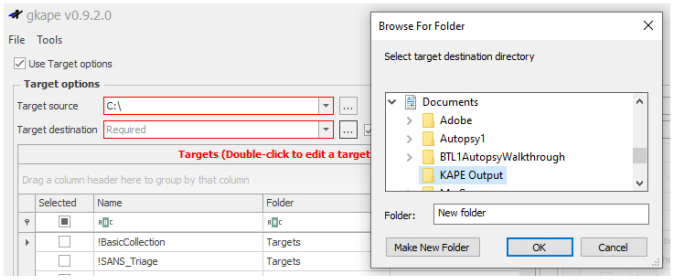


When we click the checkbox to enable Targets in the top left we first need to provide the target source. This would typically be a disk image, but for this walkthrough we're going to use our host system's C drive.



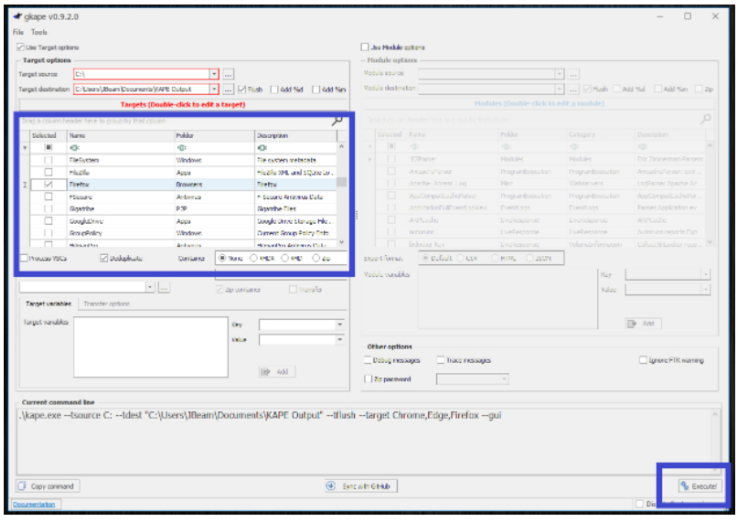


Next, we need to set a location for where files collected by KAPE will be saved. We've set it to a new folder in our Documents called KAPE Output.

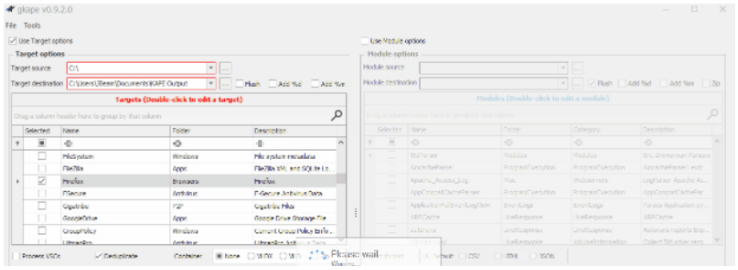


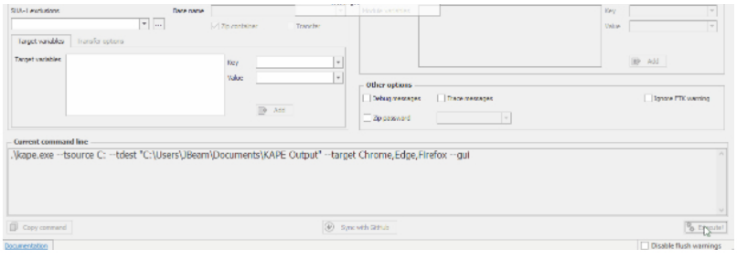
Next, we can select our targets. For the first example, let's collect information from the most popular web browsers out there; Chrome, Edge, and Firefox. We can scroll down the Targets box and find them.

Once we have all of our Targets selected, we can click the Execute button at the bottom right to start KAPE.

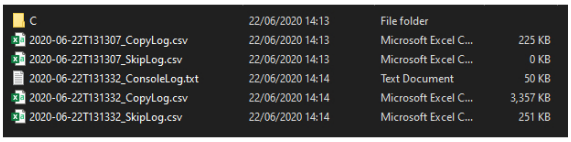


KAPE will open a terminal and start retrieving copies of the files we have requested.

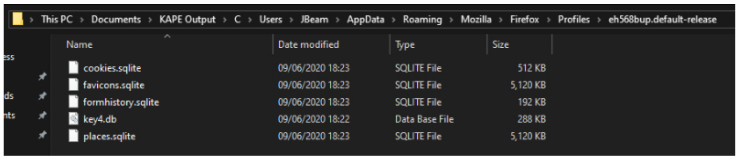




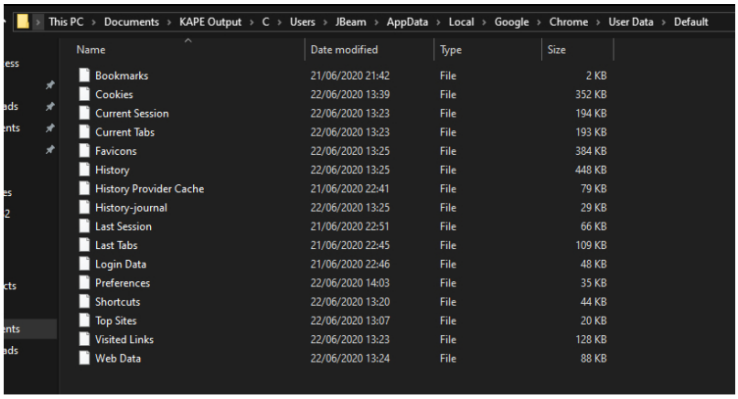
Let's see what KAPE found by navigating to the directory we set as our Target destination earlier. We can see that are a number of logs, telling us exactly what KAPE did during the acquisition. We also have a folder named "C" after our host system's C drive.



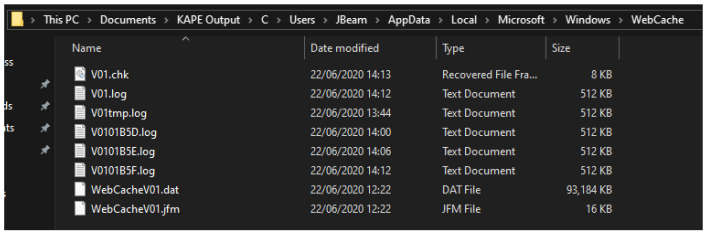
At the following file path, we can see that KAPE found some interesting files regarding activity conducted using the Firefox browser on this system, including cookies (which can tell us what sites the user has visited) and formhistory which could include personal information such as addresses, names, date of birth, and more.



In the below screenshot we can see that KAPE has also retrieved some really useful information regarding Google Chrome.



And finally, we have some files from Internet Explorer/Edge such as web caches.



KAPE can be used to quickly retrieve tons of information, such as; Windows event logs, antivirus logs, file system metadata, log files, deleted files, emails, and absolutely tons more. We strongly recommend that students install KAPE and use it to analyze their own systems to become more familiar with using this tool. You can download KAPE

for free here – https://www.kroll.com/en/services/cyber-risk/investigate-and-respond/kroll-artifact-parser-extractor-kape

Previous Topic

Mark Complete

Next Topic

Back to Lesson