

Blue Team Level 1 Certification
(Standard)

Introduction to BTL1

Welcome to Blue Team Level 1

4 Topics

Lab and Forum Access

SECURITY FUNDAMENTALS DOMAIN

Introduction to Security Fundamentals

1 Topic

Soft Skills

7 Topics

Security Controls

5 Topics 1 Quiz

Networking Basics

6 Topics 1 Quiz

Management Principles

4 Topics 1 Quiz

PHISHING ANALYSIS DOMAIN

PA1) Introduction to Emails and Phishing

7 Topics 1 Quiz

PA2) Types of Phishing Emails

10 Topics 2 Quizzes

PA3) Tactics and Techniques Used

12 Topics 2 Quizzes

PA4) Investigating a Phishing Email

8 Topics 2 Quizzes

PA5) Analysing URLs, Attachments, and Artifacts

8 Topics 1 Quiz

PA6) Taking Defensive Actions

12 Topics 1 Quiz

PA7) Report Writing

7 Topics 1 Quiz

PA8) Phishing Response Challenge

3 Topics 1 Quiz

THREAT INTELLIGENCE DOMAIN

TI1) Introduction to Threat Intelligence

7 Topics

TI2) Threat Actors & APTs

6 Topics 2 Quizzes

TI3) Operational Threat Intelligence

7 Topics 1 Quiz

TI4) Tactical Threat Intelligence

7 Topics 1 Quiz

TI5) Strategic Threat Intelligence

5 Topics 1 Quiz

TI6) Malware and Global Campaigns

6 Topics 1 Quiz

DIGITAL FORENSICS DOMAIN

DF1) Introduction to Digital Forensics

5 Topics

DF2) Forensics Fundamentals

10 Topics 5 Quizzes

Live Acquisition: KAPE

Blue Team Level 1 Certification (Standard) > DF3) Digital Evidence Collection > Live Acquisition:...

IN PROGRESS



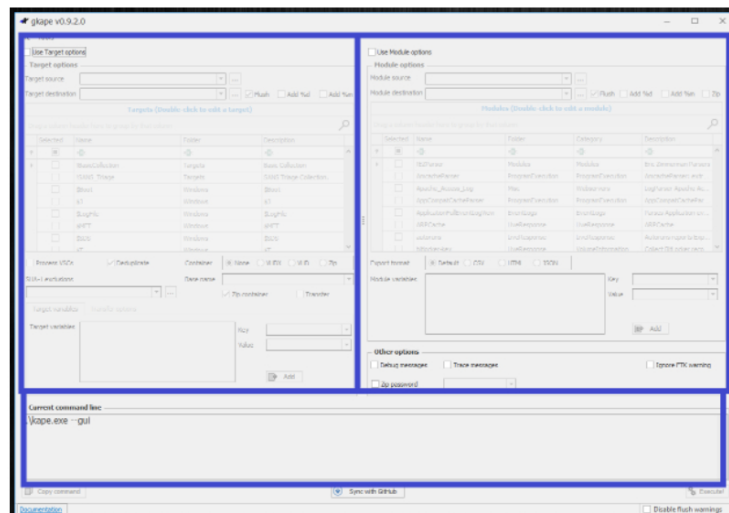
In this lesson, we're going to look at the forensic tool KAPE: the Kroll Artifact Parser and Extractor. KAPE is an efficient and highly configurable triage program that will target essentially any device or storage location, find forensically useful artifacts, and parse them within a few minutes. It 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.

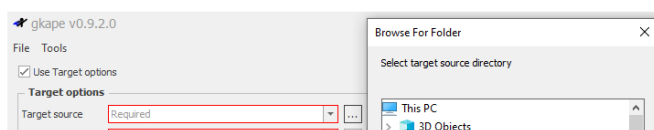
Below we're going to show you KAPE in action, performing live acquisition against our own running system just to demonstrate some of the functionality and information that this tool can retrieve in an extremely short space of time.

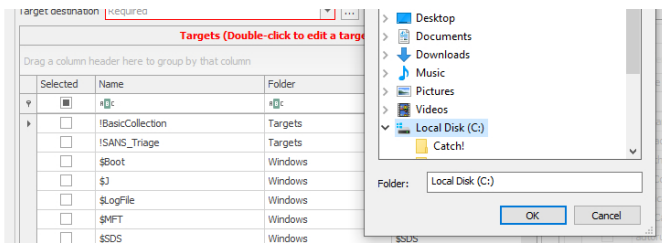
Looking in the KAPE folder, there are two executable files, kape.exe and gkape.exe. We'll be using gkape.exe, which is the graphical version of this tool. Let's run it. We can split the interface into three sections:

- 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.

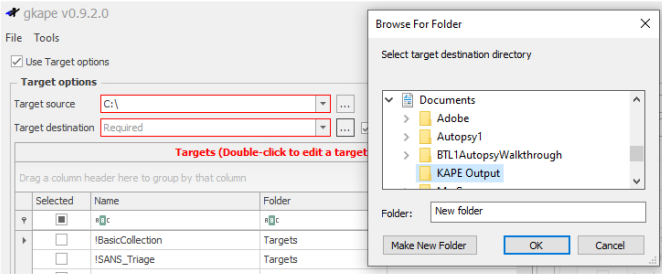


When we click the checkbox to enable Targets in the top left we first need to provide the target source. This would typically be a disk image, but for this walkthrough we're going to use our host system's C drive.





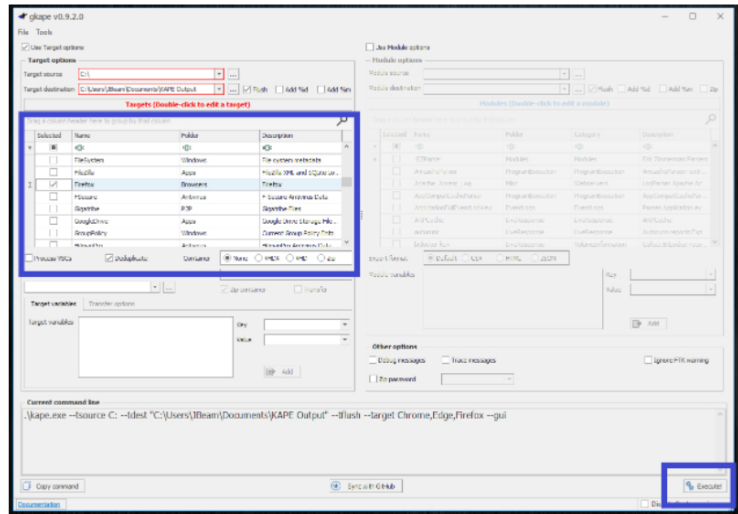
Next, we need to set a location for where files collected by KAPE will be saved. We've set it to a new folder in our Documents called KAPE Output.



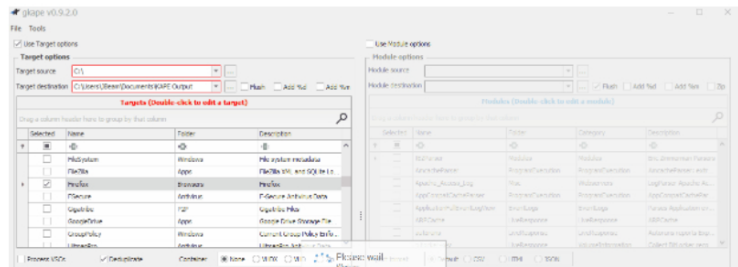
Next, we can select our targets. For the first example, let's collect information from the most popular web browsers out there; Chrome, Edge, and Firefox. We can scroll down the Targets box and find them.

<input checked="" type="checkbox"/>	Edge	Browsers	Edge
<input checked="" type="checkbox"/>	Firefox	Browsers	Firefox
<input checked="" type="checkbox"/>	Chrome	Browsers	Chrome

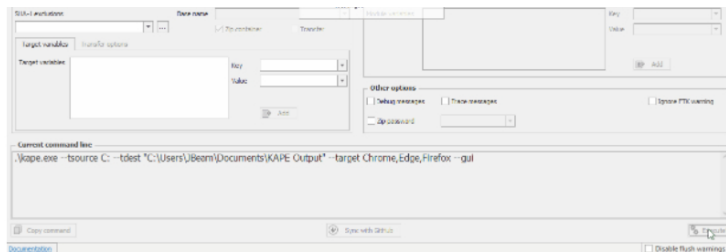
Once we have all of our Targets selected, we can click the Execute button at the bottom right to start KAPE.



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



<ul style="list-style-type: none"> DF3) Digital Evidence Collection <ul style="list-style-type: none"> 8 Topics 1 Quiz Section Introduction, Evidence Collection Equipment ACPO Principles of Digital Evidence Collection & Preservation Chain of Custody Disk Imaging: FTK Imager Live Forensics Live Acquisition: KAPE Evidence Destruction Activity) End of Section Review, Evidence Collection
<ul style="list-style-type: none"> DF4) Windows Investigations <ul style="list-style-type: none"> 3 Topics 3 Quizzes DF5) Linux Investigations <ul style="list-style-type: none"> 4 Topics 2 Quizzes DF6) Volatility <ul style="list-style-type: none"> 3 Topics 1 Quiz DF7) Autopsy <ul style="list-style-type: none"> 4 Topics 1 Quiz
<h3>SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN</h3> <ul style="list-style-type: none"> SI1) Introduction to SIEM <ul style="list-style-type: none"> 7 Topics 1 Quiz SI2) Logging <ul style="list-style-type: none"> 6 Topics 2 Quizzes SI3) Aggregation <ul style="list-style-type: none"> 2 Topics 1 Quiz SI4) Correlation <ul style="list-style-type: none"> 6 Topics 1 Quiz SI5) Using Splunk <ul style="list-style-type: none"> 5 Topics 2 Quizzes
<h3>INCIDENT RESPONSE DOMAIN</h3> <ul style="list-style-type: none"> IR1) Introduction to Incident Response <ul style="list-style-type: none"> 8 Topics 1 Quiz IR2) Preparation Phase <ul style="list-style-type: none"> 10 Topics 2 Quizzes IR3) Detection and Analysis Phase <ul style="list-style-type: none"> 7 Topics 4 Quizzes IR4) Containment, Eradication, and Recovery Phase <ul style="list-style-type: none"> 5 Topics 1 Quiz IR5) Lessons Learned and Reporting <ul style="list-style-type: none"> 7 Topics IR6) MITRE ATT&CK <ul style="list-style-type: none"> 13 Topics 2 Quizzes
<h3>BTL1 EXAM</h3> <ul style="list-style-type: none"> Exam Preparation Using RDP and SSH How to Start Your Exam



Let's see what KAPE found by navigating to the directory we set as our Target destination earlier. We can see that there 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.

C	22/06/2020 14:13	File folder	
2020-06-22T131307_CopyLog.csv	22/06/2020 14:13	Microsoft Excel C...	225 KB
2020-06-22T131307_SkipLog.csv	22/06/2020 14:13	Microsoft Excel C...	0 KB
2020-06-22T131332_ConsoleLog.txt	22/06/2020 14:14	Text Document	50 KB
2020-06-22T131332_CopyLog.csv	22/06/2020 14:14	Microsoft Excel C...	3,357 KB
2020-06-22T131332_SkipLog.csv	22/06/2020 14:14	Microsoft Excel C...	251 KB

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.

Name	Date modified	Type	Size
cookies.sqlite	09/06/2020 18:23	SQLITE File	512 KB
favicons.sqlite	09/06/2020 18:23	SQLITE File	5,120 KB
formhistory.sqlite	09/06/2020 18:23	SQLITE File	192 KB
key4.db	09/06/2020 18:22	Data Base File	288 KB
places.sqlite	09/06/2020 18:23	SQLITE File	5,120 KB

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

Name	Date modified	Type	Size
Bookmarks	21/06/2020 21:42	File	2 KB
Cookies	22/06/2020 13:39	File	352 KB
Current Session	22/06/2020 13:23	File	194 KB
Current Tabs	22/06/2020 13:23	File	193 KB
Favicons	22/06/2020 13:25	File	384 KB
History	22/06/2020 13:25	File	448 KB
History Provider Cache	21/06/2020 22:41	File	79 KB
History-journal	22/06/2020 13:25	File	29 KB
Last Session	21/06/2020 22:51	File	66 KB
Last Tabs	21/06/2020 22:45	File	109 KB
Login Data	21/06/2020 22:46	File	48 KB
Preferences	22/06/2020 14:03	File	35 KB
Shortcuts	22/06/2020 13:20	File	44 KB
Top Sites	22/06/2020 13:07	File	20 KB
Visited Links	22/06/2020 13:23	File	128 KB
Web Data	22/06/2020 13:24	File	88 KB

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

Name	Date modified	Type	Size
V01.chk	22/06/2020 14:13	Recovered File Fra...	8 KB
V01.log	22/06/2020 14:12	Text Document	512 KB
V01tmp.log	22/06/2020 13:44	Text Document	512 KB
V0101B5D.log	22/06/2020 14:00	Text Document	512 KB
V0101B5E.log	22/06/2020 14:06	Text Document	512 KB
V0101B5F.log	22/06/2020 14:12	Text Document	512 KB
WebCacheV01.dat	22/06/2020 12:22	DAT File	93,184 KB
WebCacheV01.jfm	22/06/2020 12:22	JFM File	16 KB

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 ✓
Back to Lesson

Next Topic >

Privacy & Cookies Policy

