



# LEARN TO FLY WITH KAPE

Become an incident response superhero



# WHO ARE YOU?

Name

- [censored]

Employed by

- SBB AG (CyberART Organisation)

Employed as

- Security Analyst / Engineer

I often ...

- Develop and maintain the SIEM environment, including technical use cases

I sometimes ...

- Support incident response efforts and malware analysis specifically

I recently discovered ...

- Machine learning image processing

# CONTENT

What is KAPE and why should I care?

Fine then, how does KAPE even work?

I want to fly, show me how to use it!

More, give me more!

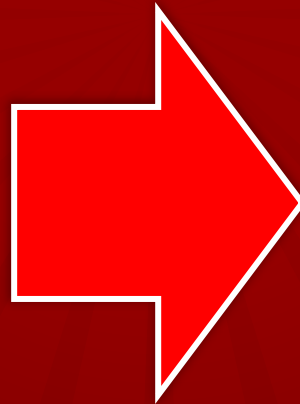
I demand answers!

# WHAT IS KAPE?

The “Kroll Artifact Parser and Extractor” explained

ML Instruction:

Picture of a  
cybersecurity superhero



# KROLL ARTIFACT PARSER AND EXTRACTOR

## KAPE is ...

- a triage program that targets windows systems of any version
- closed source but free for personal and business use
- can be extended, modified and customized with configuration files
- needs a license for commercial engagements

## Developed and maintained by Eric Zimmerman

- Former FBI Forensics Specialist
- Senior Director at Kroll Inc.
- SANS Instructor for Forensic Trainings
- Author of over 50 open source security tools



# WHAT CAN IT DO?

## Collect files from a live windows system

- Can copy hidden files, system files and files in access
- Run live response modules to collect transient data

## Run tools against a system or data collection

- Many well known tools have modules out of the box
- Data can be collected, directly processed or a combination of both

## Why is it awesome?

- Adding new modules just requires a text file
- The tool is portable and can be used manually with an GUI or as a CMD app
- It's really quite fast and also runs reasonably well on weaker systems
- Results can be uploaded in various formats directly to FTP/S3/Azure

# WHERE, WHEN AND HOW IS IT USED?

## KAPE == Triage

- Triage tools are used early and often during incident response steps
- Usually the goal is to quickly find the most relevant data and guide decisions
- Increasingly often triage tools are also used for root cause analysis post-incident
- Triage is often «good enough» to deal with most daily incidents

## KAPE != Forensics

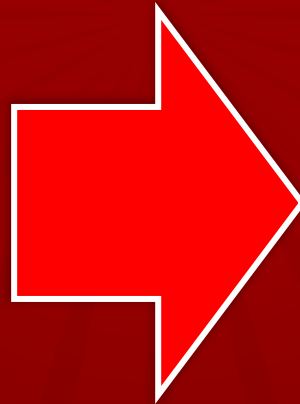
- Forensic methods are deployed when missing any kind of data is not an option
- It's usually done on a low level data copy of the target storage device
- Some techniques and tools are similar or even identical to triage operations
- Investigations are time consuming, complicated and are mostly done post-event

# HOW DOES KAPE WORK?

Short overview of the capabilities (and some theory)

ML Instruction:

Picture of a  
marvel superhero  
fighting against  
computer crime





# WORKFLOW

## COLLECTION

### Source

- Live System
- Mounted Image

### KAPE TARGETS

- Process all selected target definitions
- Search and copy data to destination

### Destination

- Copied data with the same source folder structure

### KAPE MODULES

- Module selection
- Run scripts and binaries against destination/system and write results to output

### Output

- Categorized module output data (CSV,JSON,HTML,Other)

### KAPE RESULTS

- Encapsulate destination data (VHDX,VHD,ZIP,None)
- Upload and transfer destination and output data

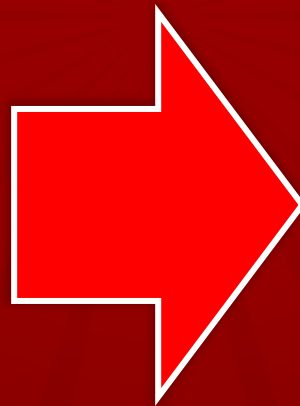
## PROCESSING

# HOW IS KAPE USED?

A demonstration of how to fight your everyday battles

ML Instruction:

Picture of a  
marvel superhero  
fighting against  
computer crime  
using his superpower



# SHORT DEMONSTRATION

gkape v1.2.0.0

File Tools

☒ Use Target options

**Target options**

Target source: c:\

Target destination: C:\KAPE\Destination

☒ Flush ☐ Add %d ☐ Add %m

**Targets (Double-click to edit a target)**

Drag a column header here to group by that column

Selected	Name	Folder	Description
<input type="checkbox"/>	!BasicCollection	Compound	Basic Collection
<input checked="" type="checkbox"/>	!SANS_Triage	Compound	SANS Triage Collection
<input type="checkbox"/>	!SBB_Test	!Local	SBB Triage Test
<input type="checkbox"/>	!SBB_Triage	!Local	SBB Triage
<input type="checkbox"/>	\$Boot	Windows	\$Boot
<input type="checkbox"/>	\$J	Windows	\$J
<input type="checkbox"/>	\$LogFile	Windows	\$LogFile

☐ Process VSCs ☒ Deduplicate

Container: ☐ None ☒ VHDX ☐ VHD ☐ Zip

SHA-1 exclusions:

Base name: Base

☒ Zip container ☒ Transfer

Target variables: **Transfer options**

SFTP **S3** AWS S3 Presigned URL Azure storage

**General** Credentials

Region: Required Bucket: Required

Provider: Required Key prefix:

Comment:

For Oracle S3, use the CLI as --s3o is required

**Module options**

Module source: C:\KAPE\Destination

Module destination: C:\KAPE\Results

☒ Flush ☐ Add %d ☐ Add %m ☐ Zip

**Modules (Double-click to edit a module)**

Drag a column header here to group by that column

Name	Folder	Category	Description
!ToolSync	Compound	Sync	Sync for new Maps, Batch Files, Targets and Modules
<input checked="" type="checkbox"/> IEZParser	Compound	Modules	Eric Zimmerman Parsers
<input type="checkbox"/> !SBB_Test	!Local	Modules	SBB Live Modules Test
<input type="checkbox"/> !SBB_Triage	!Local	Modules	SBB Modules
<input type="checkbox"/> AmcacheParser	EZTools	ProgramE...	AmcacheParser: extract program execution informat...
<input type="checkbox"/> AppCompatCacheParser	EZTools	ProgramE...	AppCompatCacheParser: extract AppCompatCache ...
<input type="checkbox"/> BMC-Tools_RDPBitmapCa...	Git-Hub	Remote A...	BMC-Tools: RDP Bitmap Cache parser
<input type="checkbox"/> hstrings	Compound	Modules	Run all hstrings Modules

Export format: ☒ Default ☐ CSV ☐ HTML ☐ JSON

Module variables:

Key:

Value:

Add

**Other options**

☐ Debug messages ☐ Trace messages ☐ Ignore FTK warning

☐ Zip password:

☐ Retain local copies

**Current command line**

```
.\kape.exe --tsource c: --tdest C:\KAPE\Destination --tflush --target !SANS_Triage --vhdx Base --msource C:\KAPE\Destination --mdest C:\KAPE\Results --mflush --module IEZParser --gui
```

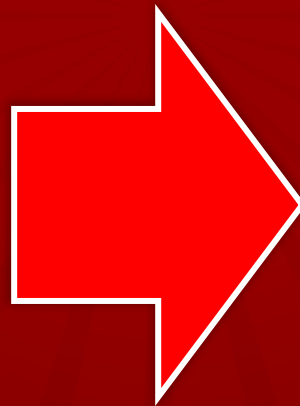


# WHERE CAN I LEARN MORE?

Resources and help to get you flying in no time

ML Instruction:

Picture of a  
marvel superhero  
helping an employee  
with his laptop





# RESOURCES AND REPOSITORIES

GitHub Repository for your convenience

- [tinyurl.com/kape2022](https://tinyurl.com/kape2022)

Links to public/official resources

- [www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape](https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape)
- [github.com/EricZimmerman/KapeDocs](https://github.com/EricZimmerman/KapeDocs)
- [github.com/EricZimmerman/KapeFiles](https://github.com/EricZimmerman/KapeFiles)
- [github.com/AndrewRathbun/Awesome-KAPE](https://github.com/AndrewRathbun/Awesome-KAPE)



# QUESTIONS AND FEEDBACK?

GitHub Link: [tinyurl.com/kape2022](https://tinyurl.com/kape2022)

