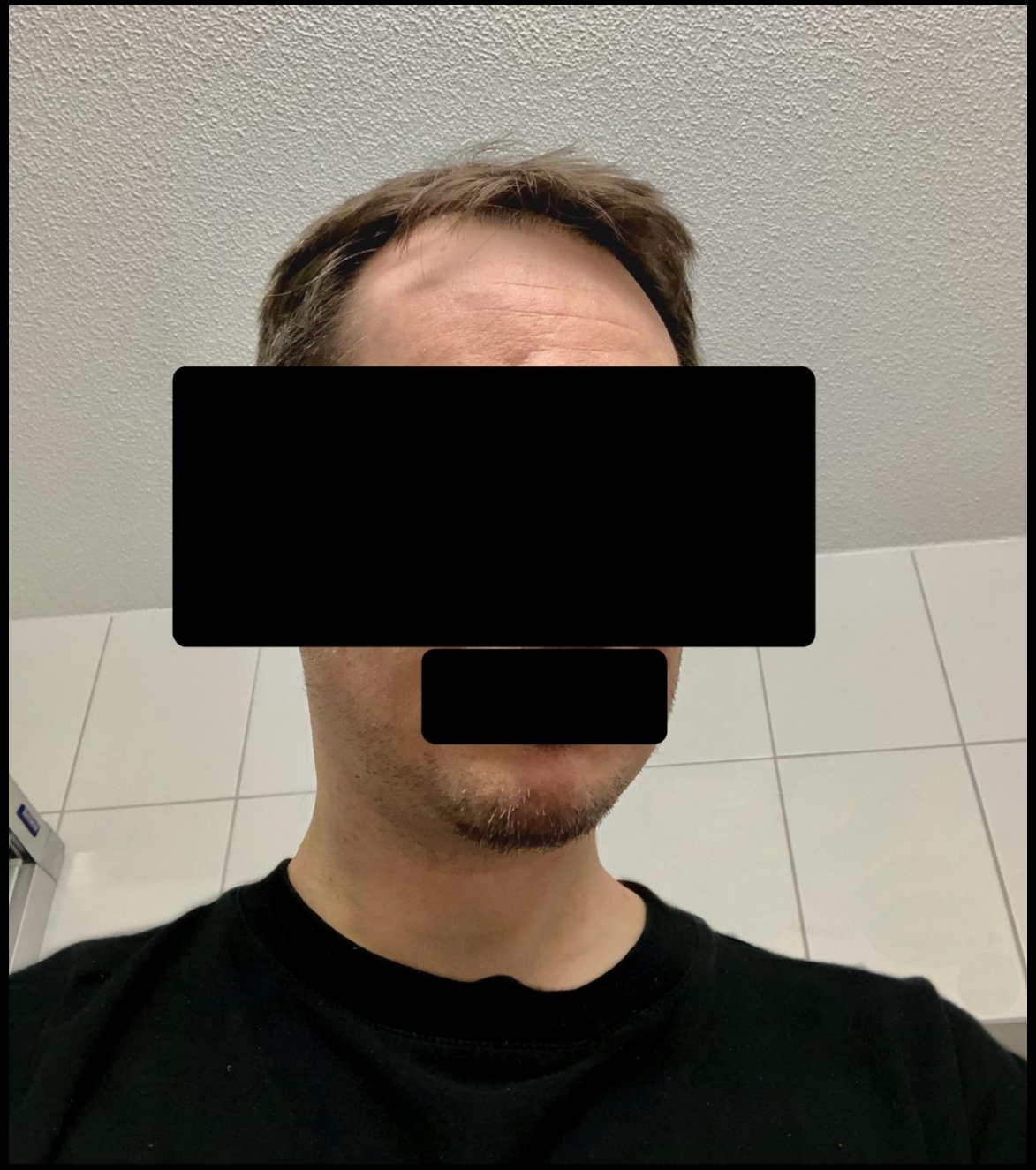
LEARN TO FLY WITH KAPE

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/linux/mac systems
- can be extended, modified and customized with configuration files
- closed source but free for personal and business use
- 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 live 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

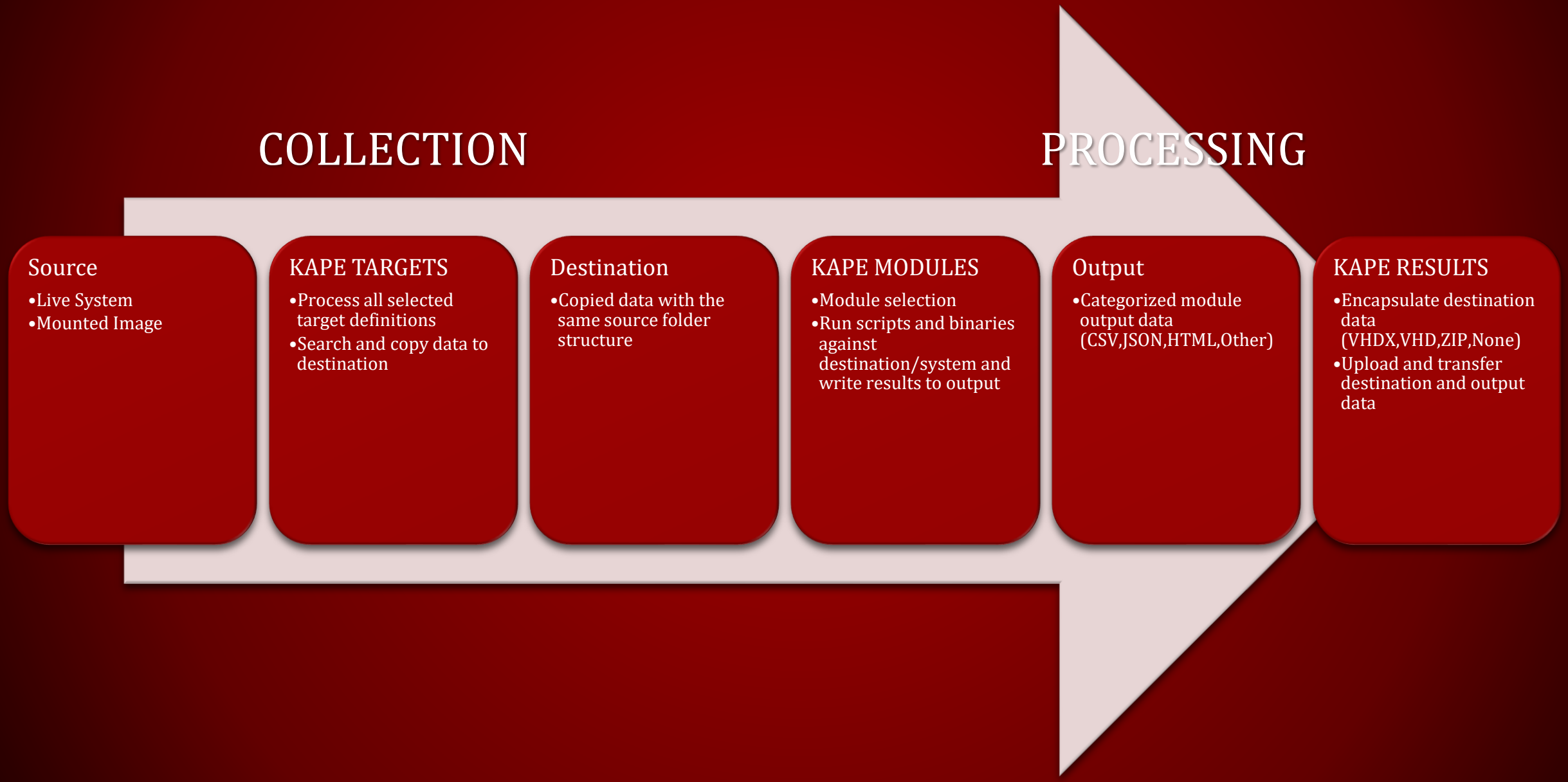
HOW DOES KAPE WORK?

Short overview of the triage process

ML Instruction:

Picture of a
marvel superhero
fighting against
computer crime

WORKFLOW


COLLECTION
PROCESSING
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

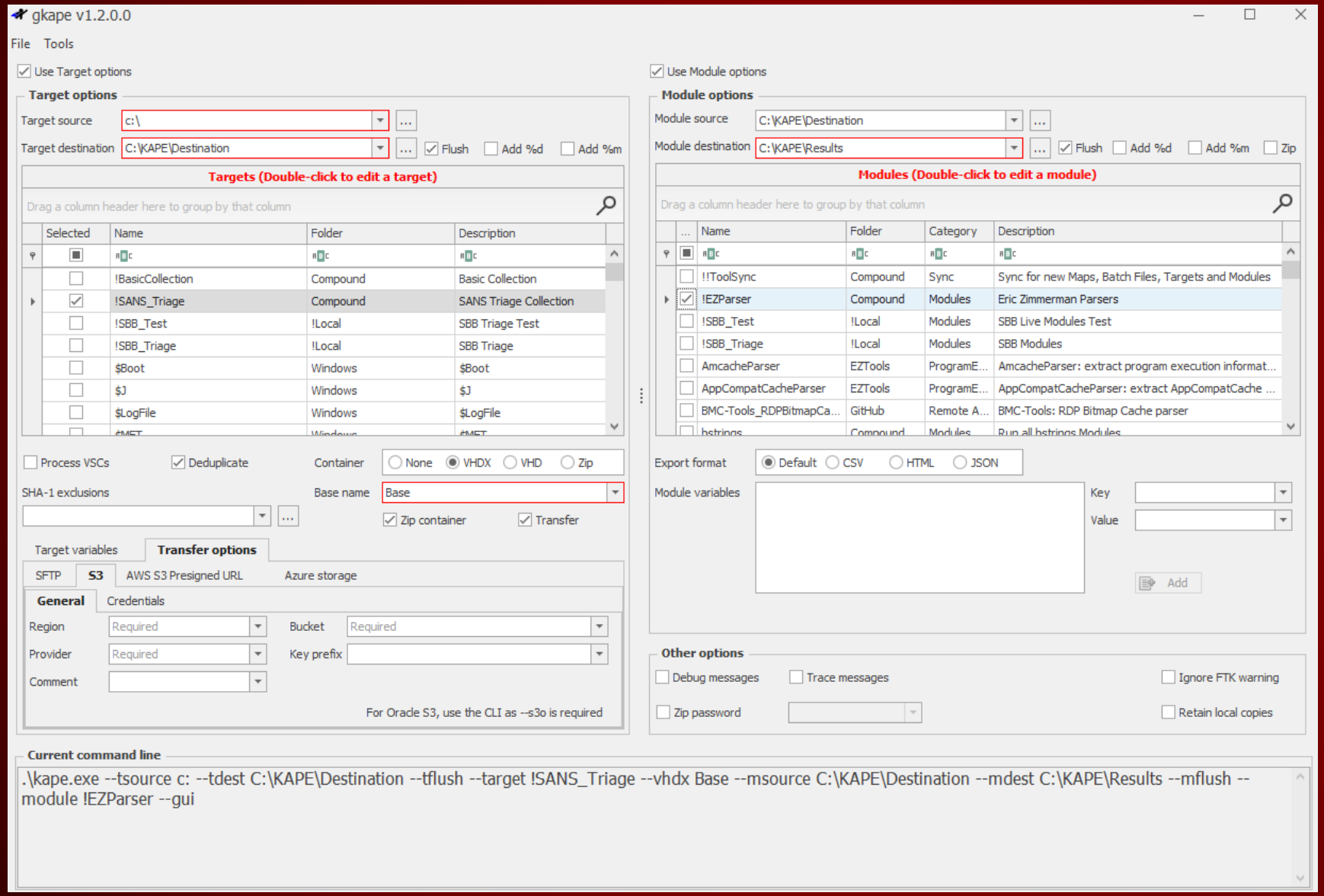
HOW IS KAPE USED?

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



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

Links to public/official resources

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

QUESTIONS AND FEEDBACK?

GitHub Link: tinyurl.com/kape2022