Luca Tännler

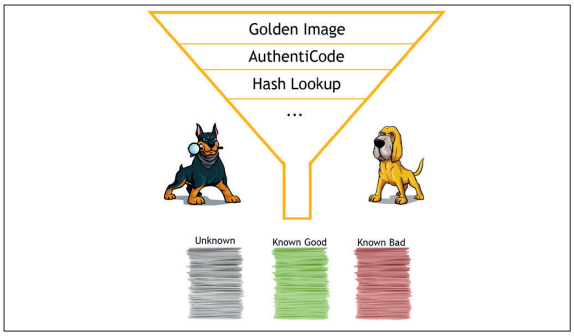
Mathias Vetsch

Graduate Candidates	Luca Tännler, Mathias Vetsch
Examiner	Cyrill Brunschwiler
Co-Examiner	Dr. Benjamin Fehrensen
Subject Area	Sicherheit
Project Partner	Compass Security Schweiz AG, Jona, SG

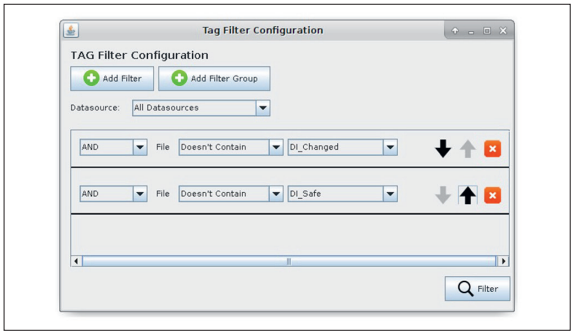
Forensic Triage Toolkit

Forensic analysis of Windows systems

Computer Forensics has to deal with a nearly unmanageable amount of data.



Automated Forensic Analysis with Autopsy dramatically reduces the amount of data to analyse.



The Tag Filter module helps to visualize the results of the developed Autopsy modules.

Introduction: Nowadays it is a daily routine of an IT Forensics Analyst or a Computer Incident Response Team (CIRT) to analyze potentially infected workstations or server systems. An IT Forensic Analyst examines the hard disk and tries to find out if there is any malware, spyware or other indication of compromise. Usually, this kind of work (a.k.a. triage) is very time-consuming. The primary goal of this project is to automate as many steps as possible to merge out known good data and give hints on possible infected data so the analyst has to focus on a small amount of data only.

Approach/Technologies: In a first step we evaluated existing triage techniques and existing open source projects with a focus on forensic triage capabilities. After the initial research, we created a feature list in collaboration with our supervisor. The list contained the most important features to optimize the forensic triage process. We decided to build on the existing open source project Autopsy. The project provides a variety of fundamental features which were required to achieve our goal. The project has a modular architecture, which allows to implement additional features.

Result: During our development phase we managed to significantly improve the Autopsy platform. The Bitlocker module allows to add volumes from encrypted Windows workstations into Autopsy. The module is designed in a way, which allows simple implementations for other disk encryption software. Additional modules were developed to automate differentiation between known-good and known-bad files.

- The golden image module to exclude known-good files from a reference data source
- The AuthentiCode verification module allows to identify the publisher of a software through code signing certificates
- The hash-database update feature automates the import of white- and blacklists from the internet
- The VirusTotal online check module performs a hash lookup to a free online database

All these modules mark files on the evidence. To visualize the results, we added the tag filter module. This module provides a generic filter for the tagged files. This allows the analyst to focus work efforts on interesting content.