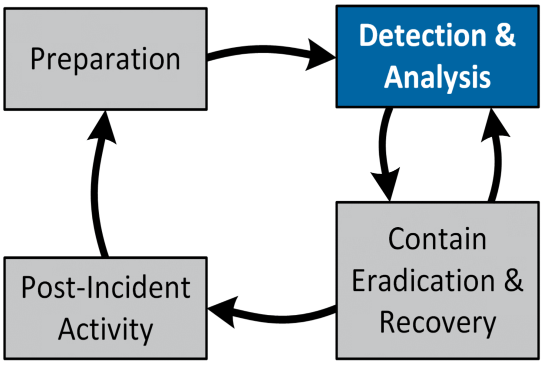
Roman
Ehrbar

Oliver
Nietlispach

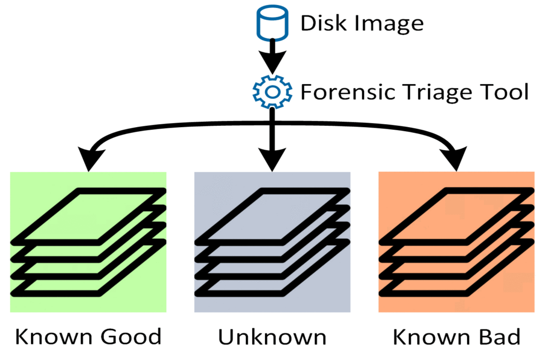
Students	Roman Ehrbar, Oliver Nietlispach
Lecturers	Cyrill Brunschwiler
Advisors	- -
Topic	Security

Malware Hunting

Forensic Triage Toolkit



Incident Response Lifecycle as defined by the National Institute of Standards and Technology (NIST).



A Forensic Triage Toolkit reduces the amount of files which need to be analyzed by a CIRT member.

Introduction: The analysis of potentially compromised workstations and servers has become daily routine for members of a Computer Incident Response Team (CIRT). To help during the detection and analysis process, a triage toolkit is used which uses various methods to categorize data of a potentially comprised system. A good triage toolkit removes as much known data from the list, which leaves less work for a CIRT member. One example is using white- and blacklists of known software components. During a previous bachelor thesis (Tännler, Luca and Vetsch, Mathias (2016) Forensic Triage Kit), Autopsy, which is based on The Sleuth Kit (TSK), was determined as a good basis for further development. The task of this term project was to increase automation of the triage process by building upon these developments or to build something entirely new which encompasses the specified requirements.

Approach/Technologies: At first, the results of the previous bachelor thesis were evaluated. The conclusion was, that Autopsy is designed as a digital forensics tool for law enforcement rather than CIRT members. Additionally, the current version of Autopsy suffers from performance and stability issues, which further complicated the process. It was therefore decided to create a new framework which encompasses the requirements stated in the bachelor thesis with the addition of automation. The framework was designed with an event-driven architecture because these systems support unpredictable behavior.The project was separated into multiple week-long iterations for which the goals and results were individually defined. During this process, Elasticsearch was chosen to speed up lookups of aggregated meta data and results generated by other tools. TSK is still used to extract files and meta data from disk images.

Result: A concept was created which demonstrated that the event-driven framework can be used to analyze and display data from a disk image. Some implementations of the framework's interfaces currently encompass only basic functionality, but they can be extended to meet all requirements. As of now, hashes can be calculated from the extracted files of a disk image and linked with the file meta data. This enables a comparison with known hash data sets. The aggregated meta data and calculated hashes can be viewed and analyzed directly through Elasticsearch. This is a precedent to show how the integration of components can be achieved in the future.