

Cross-Computer Malware Detection in Digital Forensics



Anders Orsten Flaglien

Supervised by André Årnes and Katrin Franke



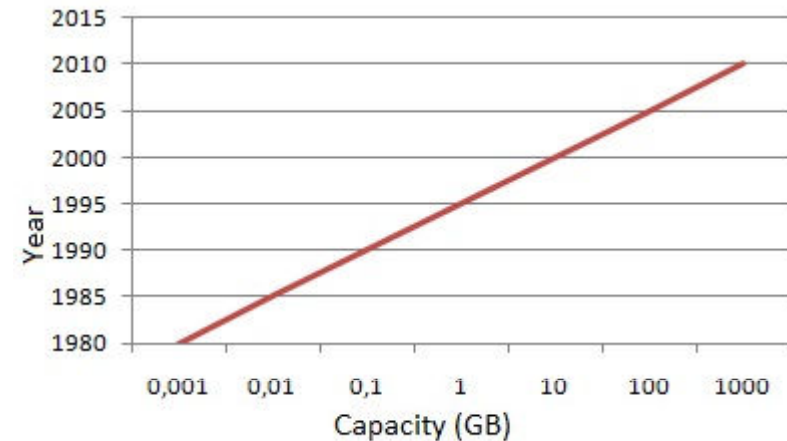
Master of Science in Information Security
Gjøvik University College

Outline

- Motivation and Background
- Task and Research Questions
- The proposed *Correlation Method for Malware Detection in Digital Forensics*
- Experiment Execution and Results
- Conclusions and Future Work

Motivation and Background

- **Increasing data volumes** makes it hard and resource consuming to perform digital forensics
- **Workstation-centric tools**
- **Sophisticated malware**, using obscurity techniques for hiding their presence
- **Robot networks (botnets)**, established with malware are used to improve the value and effect of computer crime
- These challenges makes it crucial to examine new methods to improve the **efficiency** and **effectiveness** of detecting malware in digital forensics.



The Task and corresponding Research Questions

- The main scenario for the problem faced is defined as:

Is it possible to identify traces of malware by using correlation techniques against data stored on multiple seized computers?



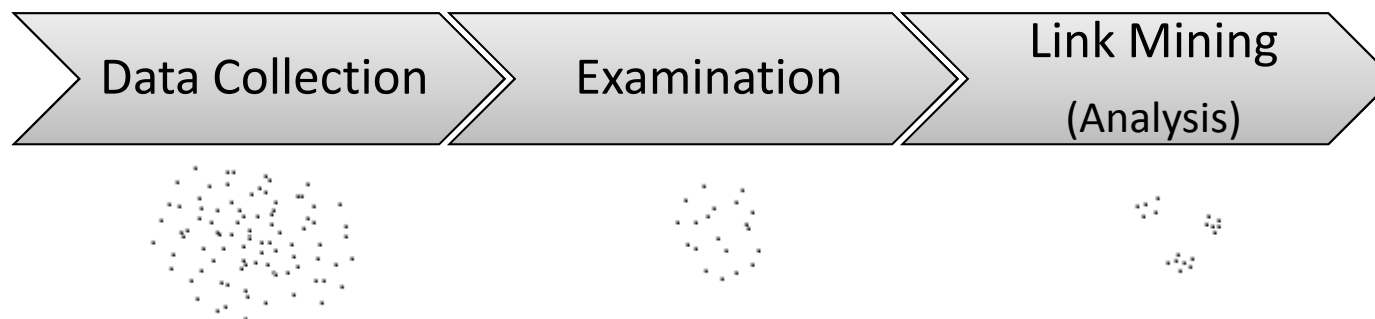
- Research Questions:

- Which features can be used to correlate and identify malware?
- How can correlation techniques be applied to digital forensics?
- How will the correlation techniques affect the efficiency and effectiveness?

- A correlation method, an implementation of it and proper experiments are required.

A new Correlation Method for Malware Detection

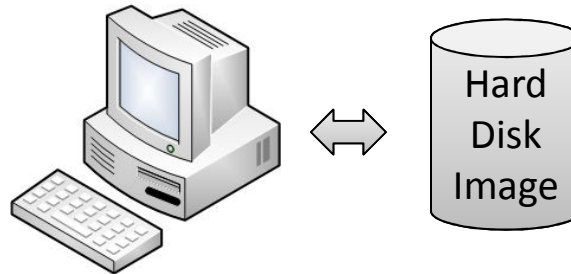
- The method complies with the challenges faced by combining three disciplines
 - Digital Forensics
 - Malware Detection
 - Data and Link Mining



- Practical Implementation based on open-source (e.g., TSK, Fiwalk, Weka) and self developed tools (in Python)

Data Collection

The foundation for later Examination and Link Mining



- Identification of machines involved with an incident
- Post-mortem (system powered off)
- Collection and copying of data from seized machines, bit-by-bit
- Integrity verification using one-way hash functions
- Read-only access
- Focus on computer hard-disks, especially partitions

Examination and Feature Extraction

Creation of a textual and structured representation of interesting files

- Feature extraction
 - Case specific metadata
 - Machine and media ID
 - File metadata
 - Timestamps, allocation and location specific information, integrity validation values etc.
 - Content-based
 - IP, Email and URL strings, content entropy and file content characteristics
- Total of 17 features + content-based ($3 * n$)
- Removal of *all* known and good files from the Feature File (Hash databases, clean system hashes)

File Object 1.... Feature A, B, C, D, E,...

...

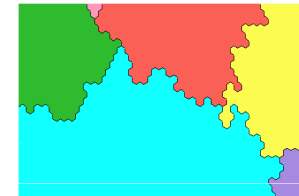
File Object n.... Feature A, B, C, D, E,...

Feature File, Machine 1

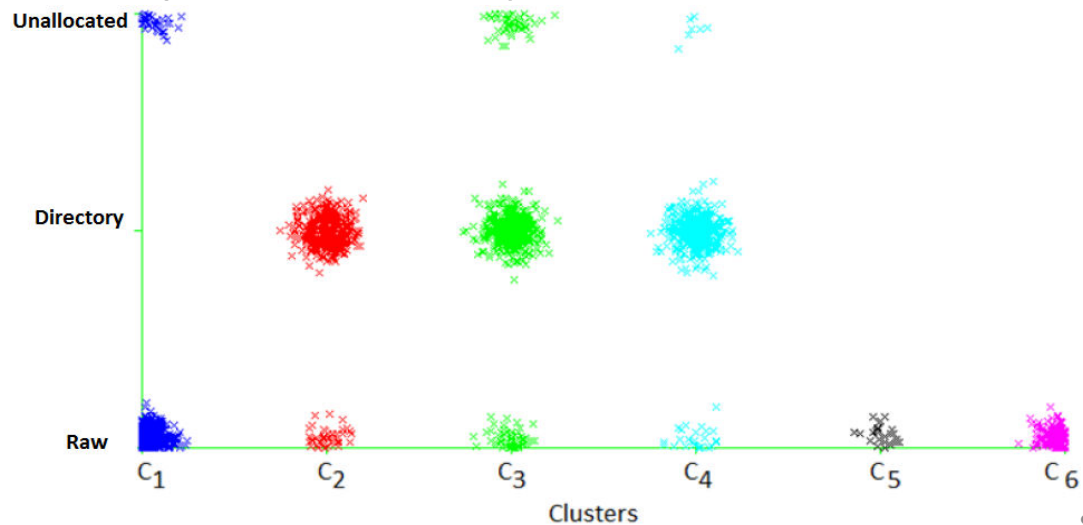
Link-based Cluster Analysis

Grouping file objects with common characteristics (to identify links)

- Evaluation of properly selected and pre-processed features
- Combining all to one Case File = {Machine 1-n}
- Estimation of natural data segments (k) using Self Organized Maps
- Cluster correlated File Objects to verify links between machines
 - Utilized to identify clusters with high level of malware characteristics

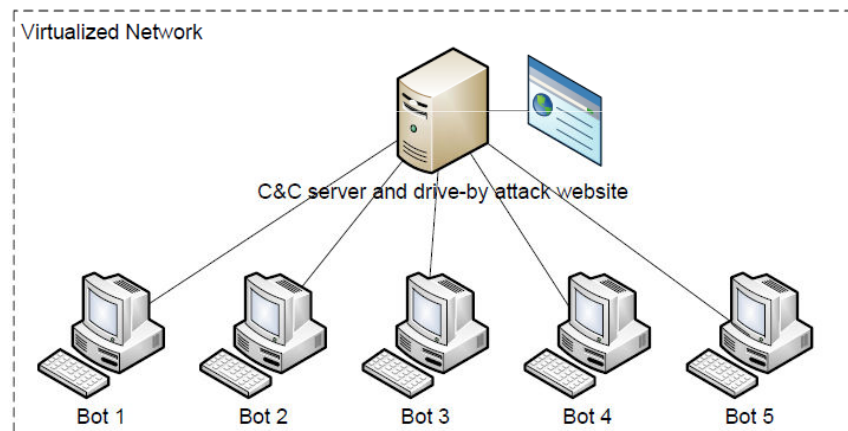


SOM diagram of segments



Experiment Execution

- Three experiments:
 - *Proof-of-Concept*, single machine
 - *Keylogger Bot Malware*, multiple machines (5)
 - *Malware from the wild (Spybot v1.3)*, multiple machines (5)



- Online Banking Attack Scenario

- Virtual environment

- Linux machine with correlation method implemented (Xubuntu)
- Infected Windows XP machines

Experiment Analysis and Results

Summary of key findings

- Reduced number of data objects down to 3%
 - Mainly caused by the homogeneous experiment machines, also resulting in many correlations
 - Reflect the effect of perfect hash-based removal conditions

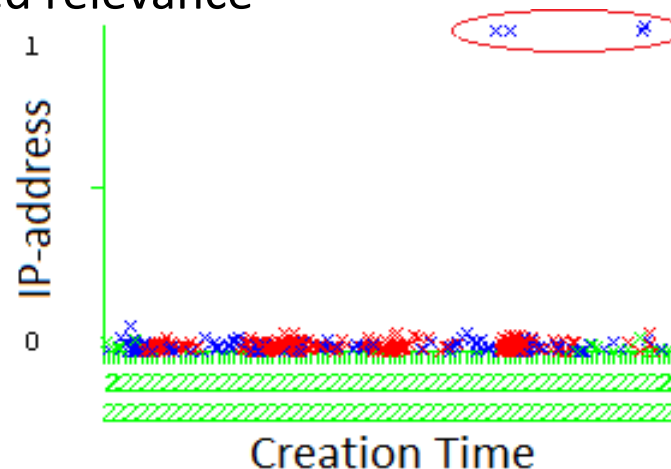
Machine ID	Initial	Filtered
All (5)	69335	2206

Table 1: Filtered file objects

Cluster	Number of Objects	Percentage
1	411	19%
2	506	23%
3	603	27%
4	503	23%
5	25	1%
6	158	7%

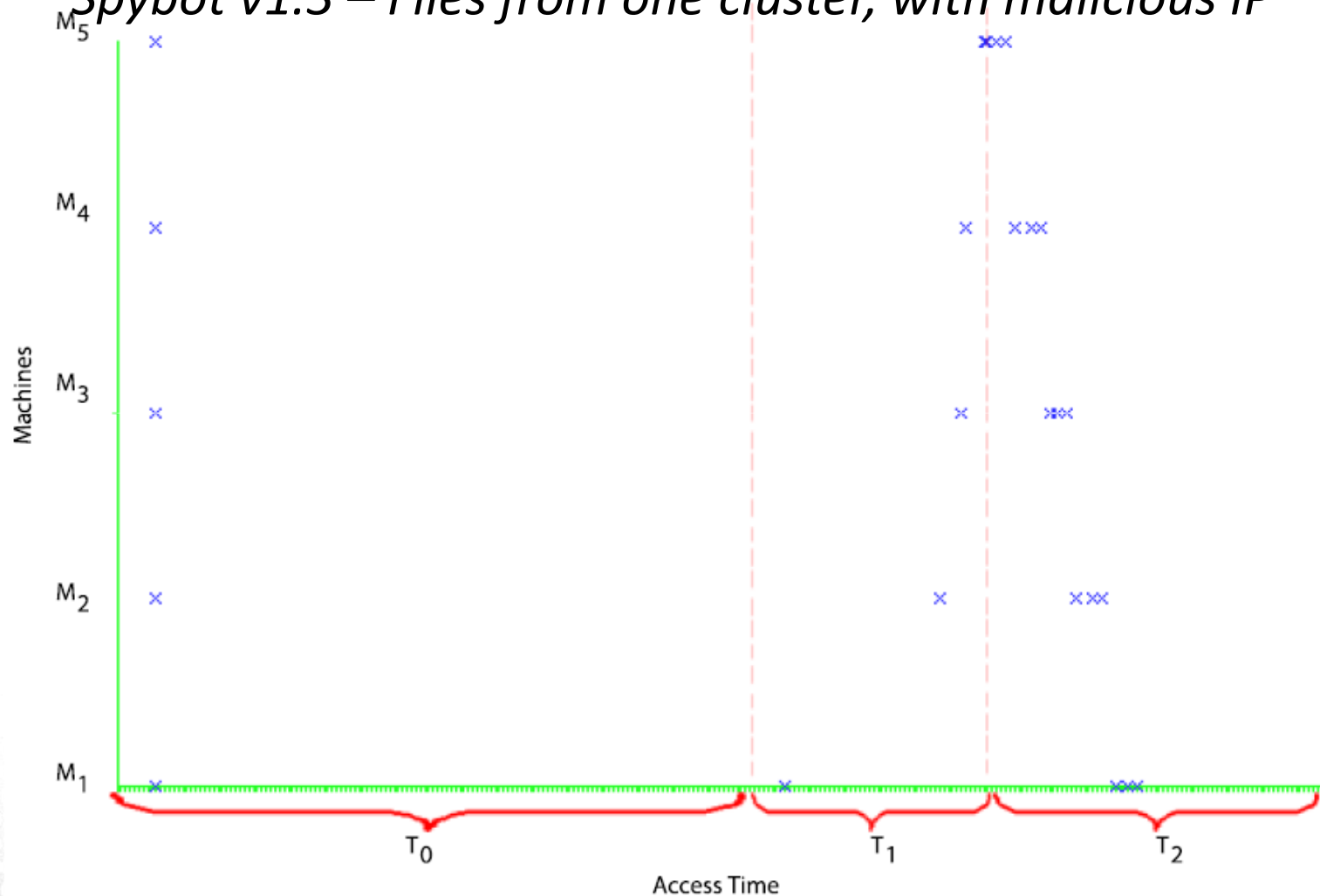
Table 2: Clustered Instances

- Correlations over all machines, with varied relevance
 - Common characteristics within clusters
 - Distinctive characteristics between clusters
- Content-based features improved detection of abnormalities further



Experiment Analysis and Results cont.

Spybot v1.3 – Files from one cluster, with malicious IP



T0: IE history files accessed, T1: Infection file accessed, T2: Additional infections files accessed

Conclusions and Future Work

Conclusions

- The features represent files well and improves identification of malware
- Focus on metadata and special content-based features improves efficiency of analysis
- Correlation techniques improves knowledge of data from multiple machines
- Overall result show that the correlation method has an effect on the effectiveness and efficiency of malware detection in digital forensics.

Future work

- More machines, and use of machines from the wild (infected and uninfected)
- *feature selection* to improve clustering results
- Perform thorough *cluster evaluations*
- Use of more *hash databases* for filtering
- Utilize correlation results to improve *presentation of digital evidence*