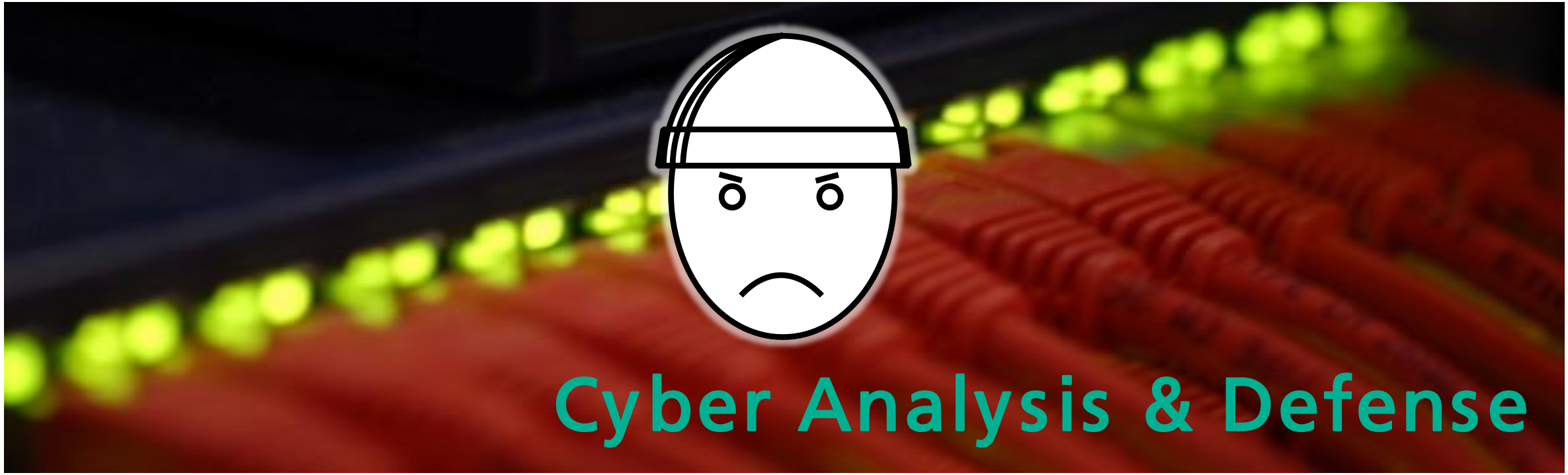
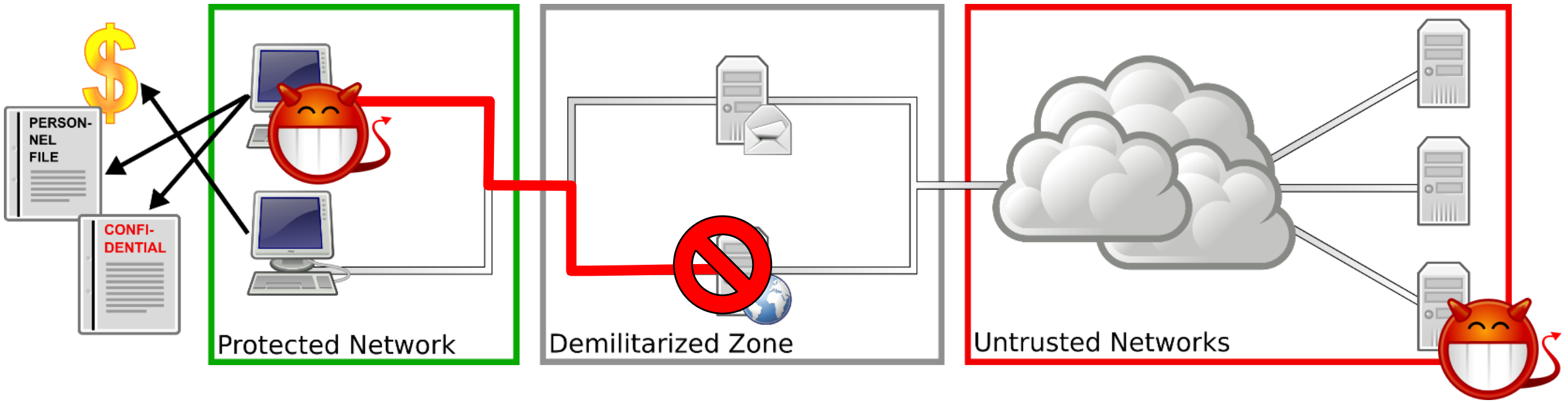
SAD THUG:
STRUCTURAL ANOMALY DETECTION FOR TRANSMISSIONS OF HIGH-VALUE INFORMATION USING GRAPHICS

Jonathan P. Chapman



offen
© Fraunhofer

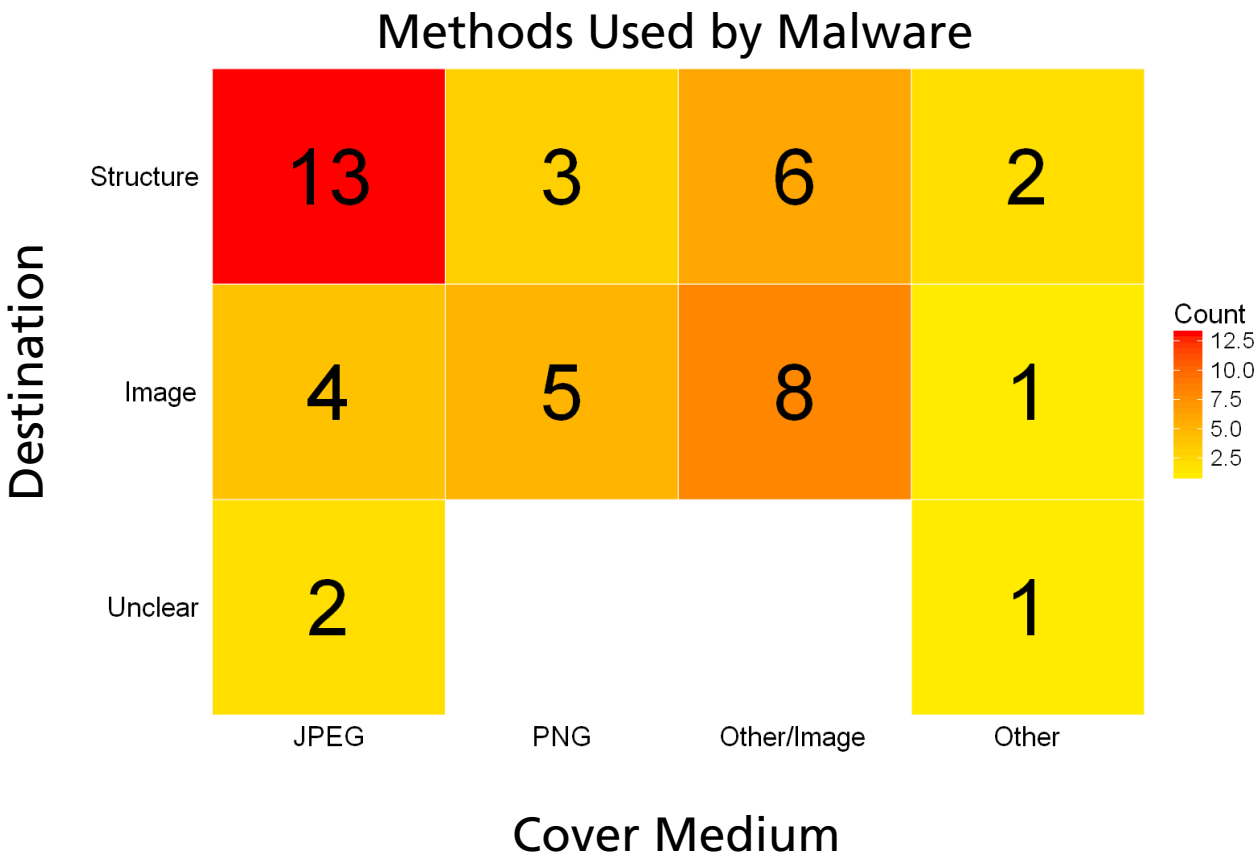
Threat Model

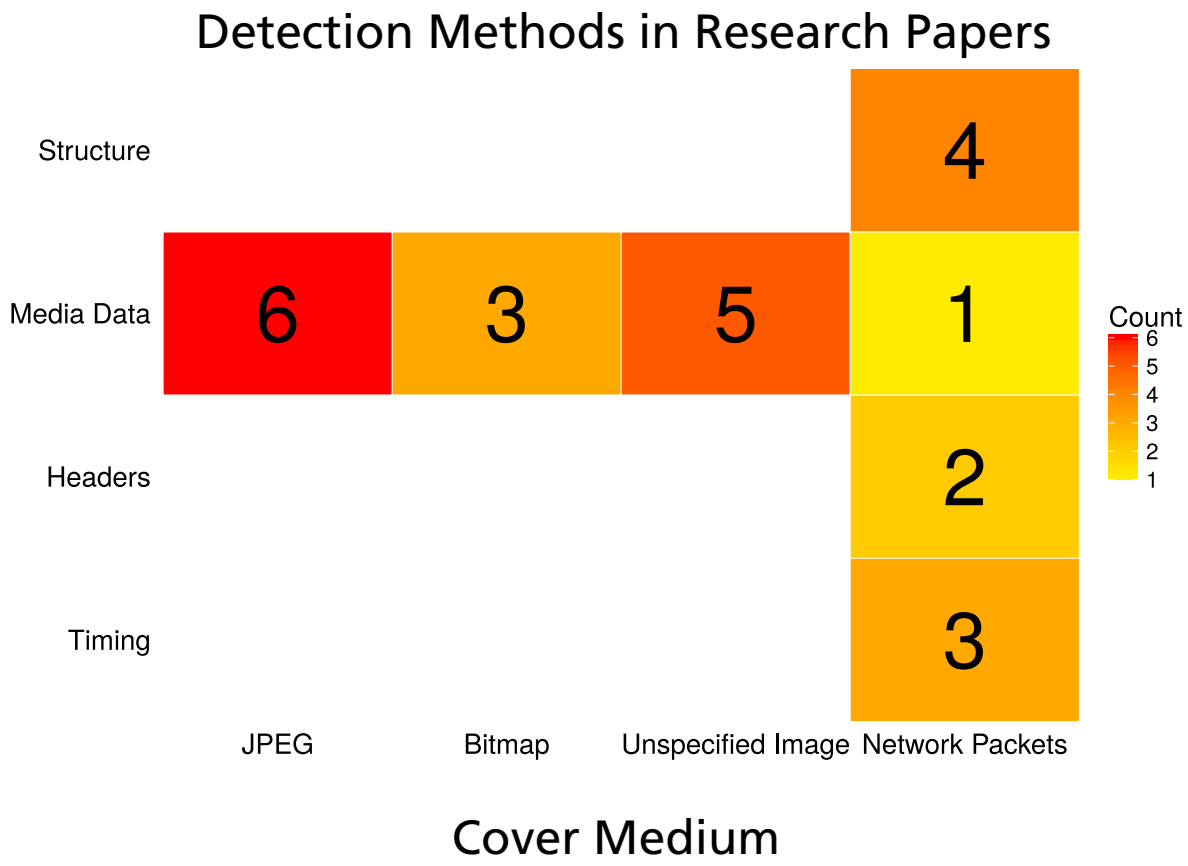


Icons: Tango Project

© Fraunhofer

Steganography in Malware



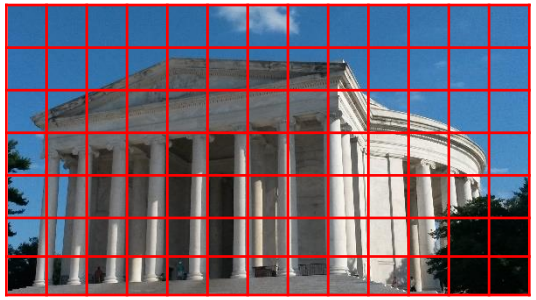


© Fraunhofer

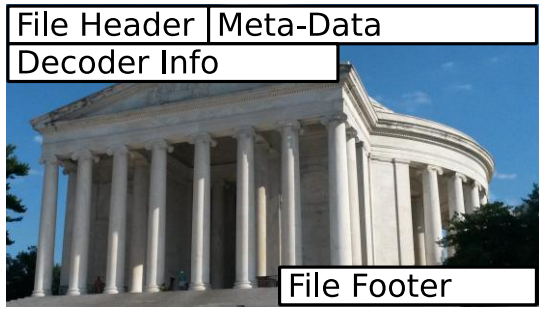
Storing Compressed Image Data



Raw image data



Encoding

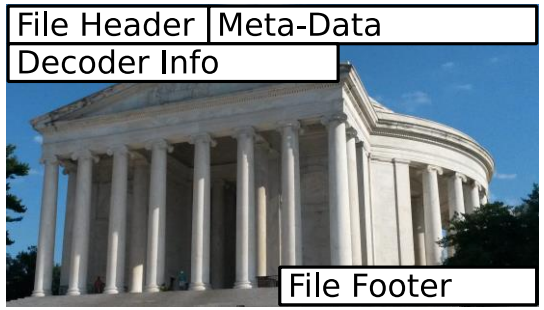


Storage

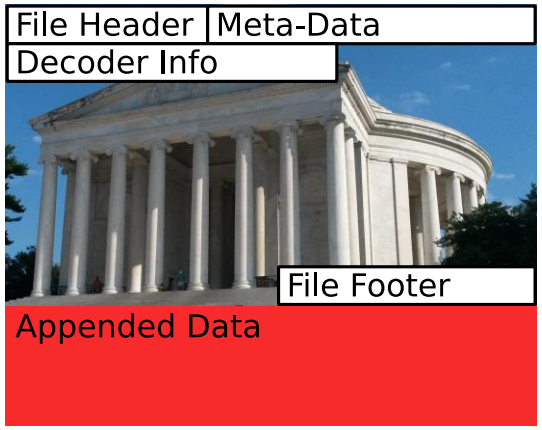
SOI	APP1	DQT0	DQT1	Scan	EOI
2	50	69	69	247027	2

© Fraunhofer

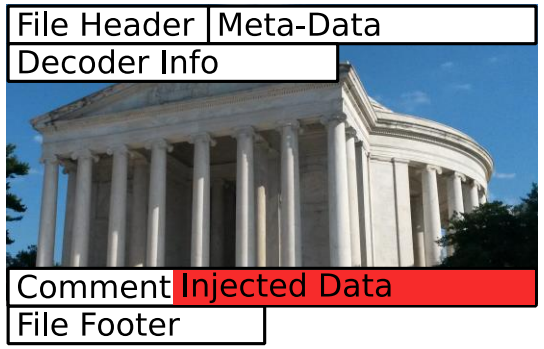
Structural Embedding Approaches



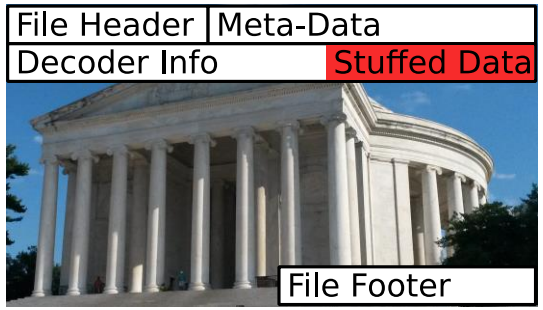
Clean



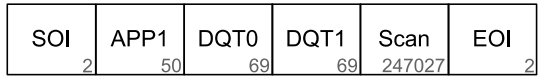
Appending

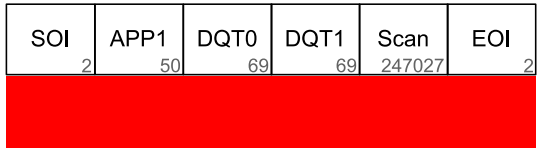


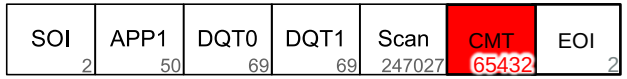
Segment Injection

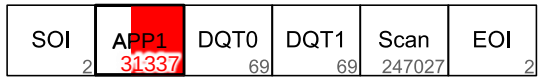


Byte Stuffing









© Fraunhofer

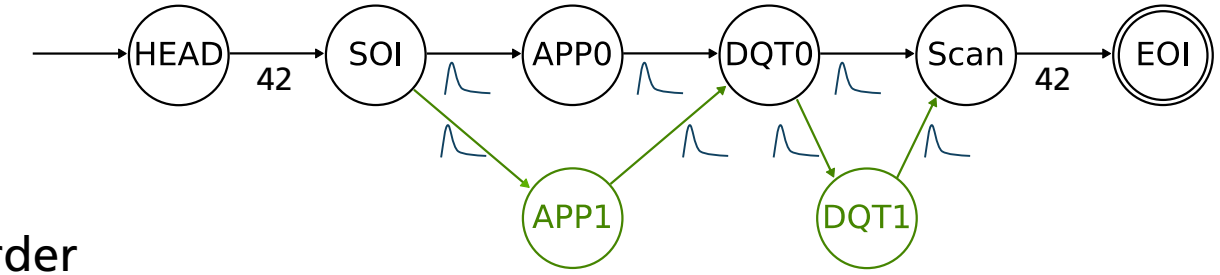
The SAD THUG Approach: Cornerstones

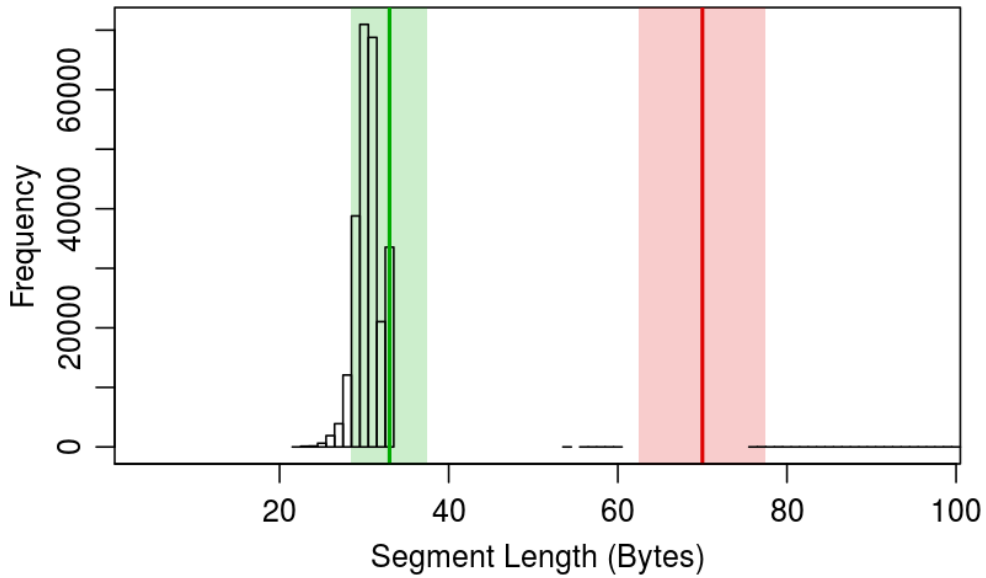
- Interpret file type as formal language
  - Works for any structured file type
    (proof of concept: JPEG, PNG)
- Build approximate model from training data
- Match files against model, adding restrictions
  - Threshold τ: minimum observation count
  - Factor α: Defines acceptance range

© Fraunhofer

The SAD THUG Approach: Model

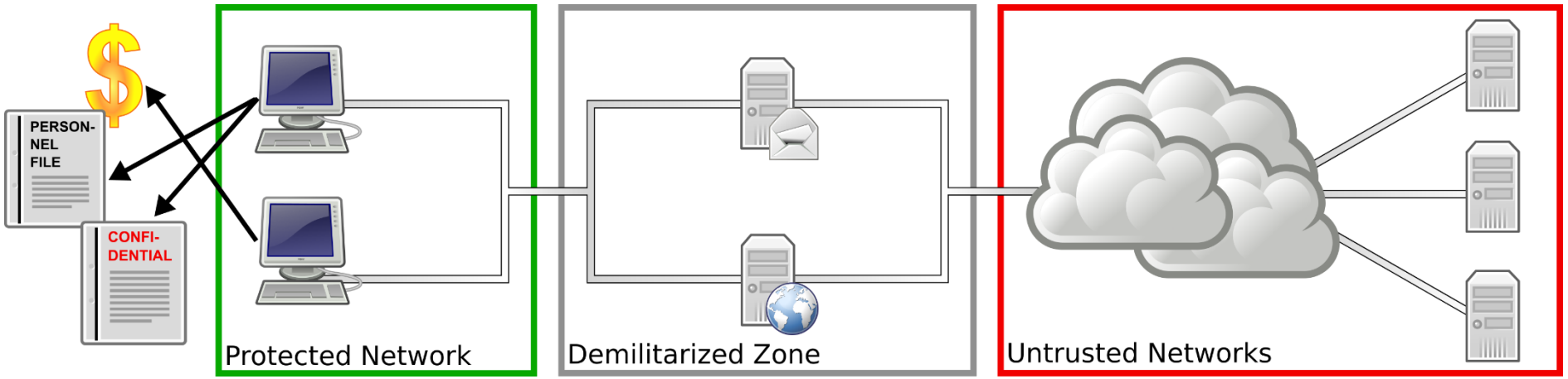
- Deterministic finite automaton, models clean files
- States = Segment types
- Directed Edges = Segments observed in that order
- Annotations to edges:
  - Second segment has fixed length: Count of observations
  - Variable length: Distribution of observed lengths





offen
© Fraunhofer

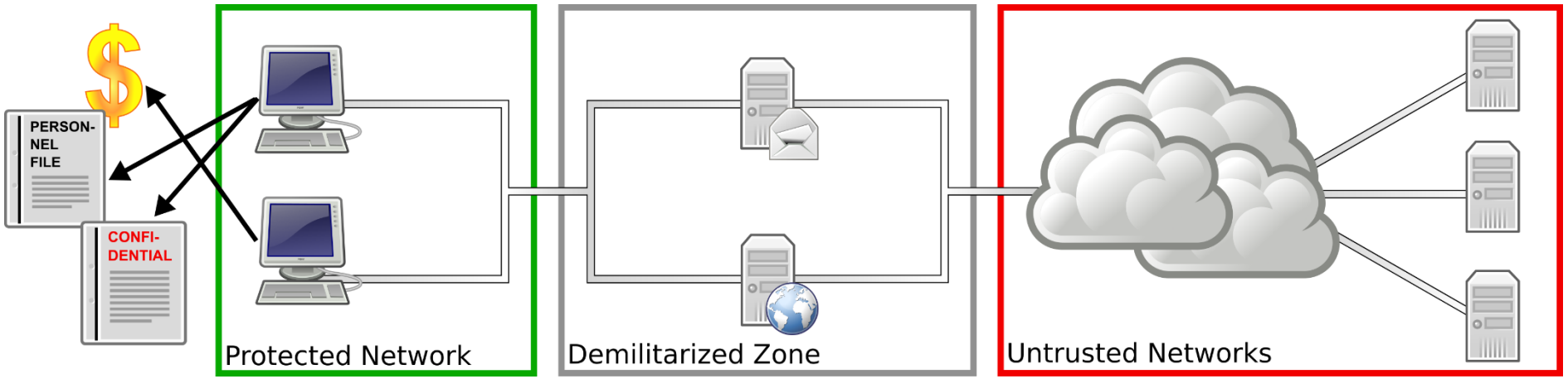
Evaluation Setup



- Base data set
  - Recursive crawling of Alexa Top 25 websites
  - ~300,000 image files
    - 270,000 JPEG
    - 33,000 PNG

© Fraunhofer

Evaluation Setup

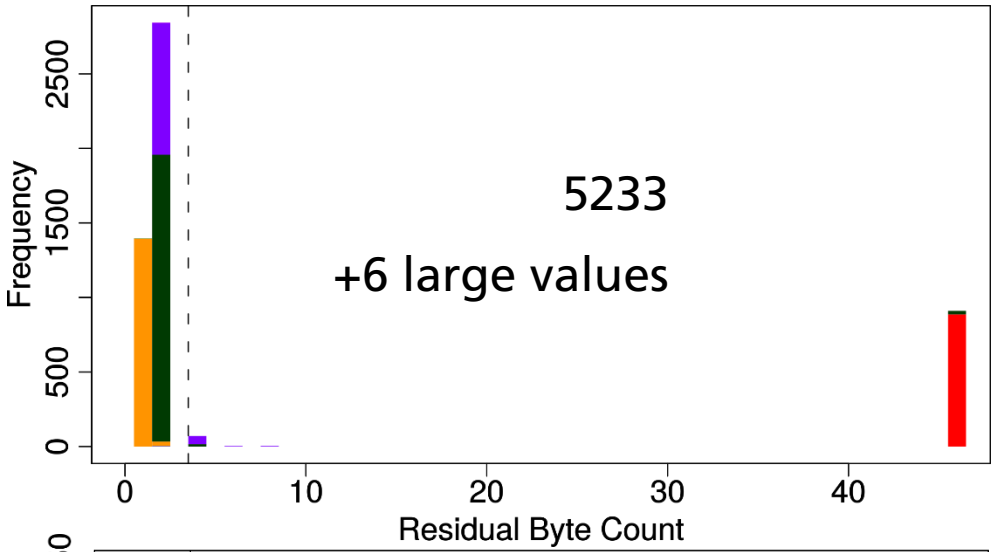


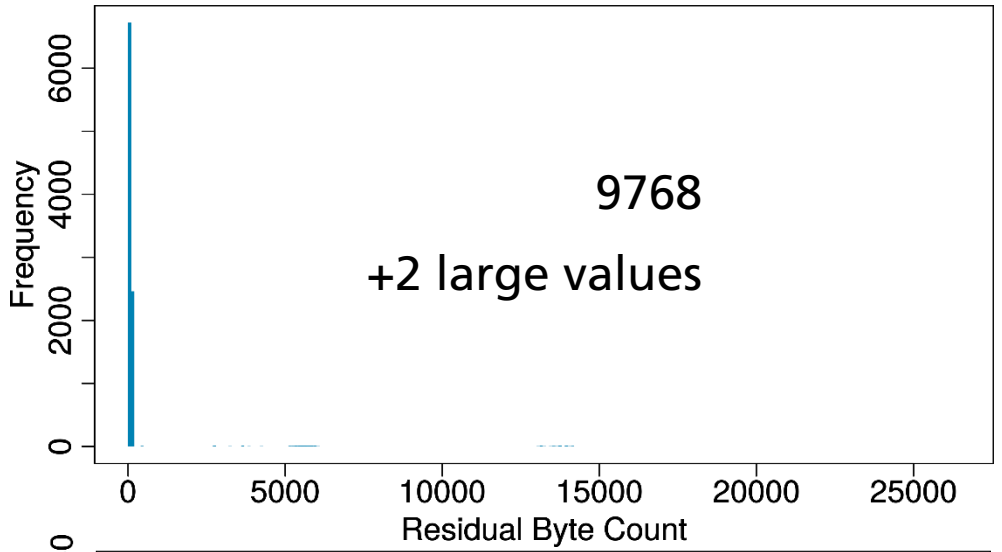
- 10-fold cross-validation
- Test set
  - Unmodified files
  - Live images (ZeusVM)
  - Embedding with malware methods and real/resembling data
- JPEG only: Stegdetect: Append and Invisible Secrets methods

© Fraunhofer

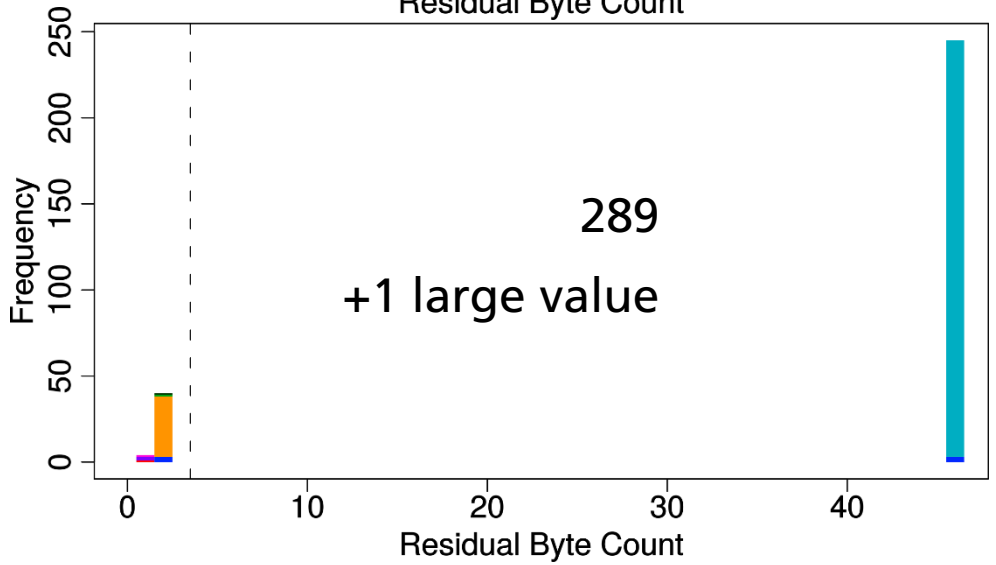
Evaluation: Residual Bytes in Base Data Set

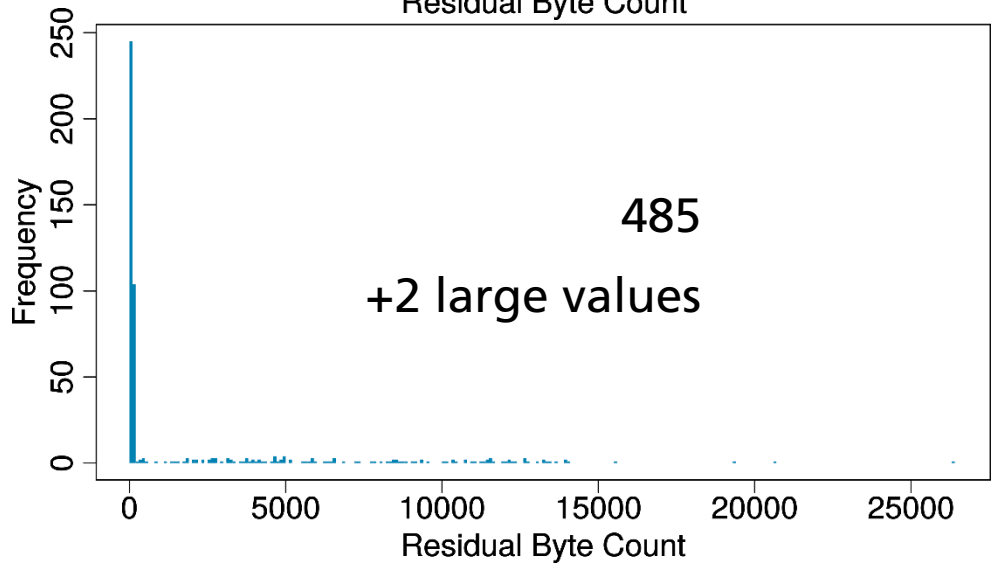
JPEG





PNG





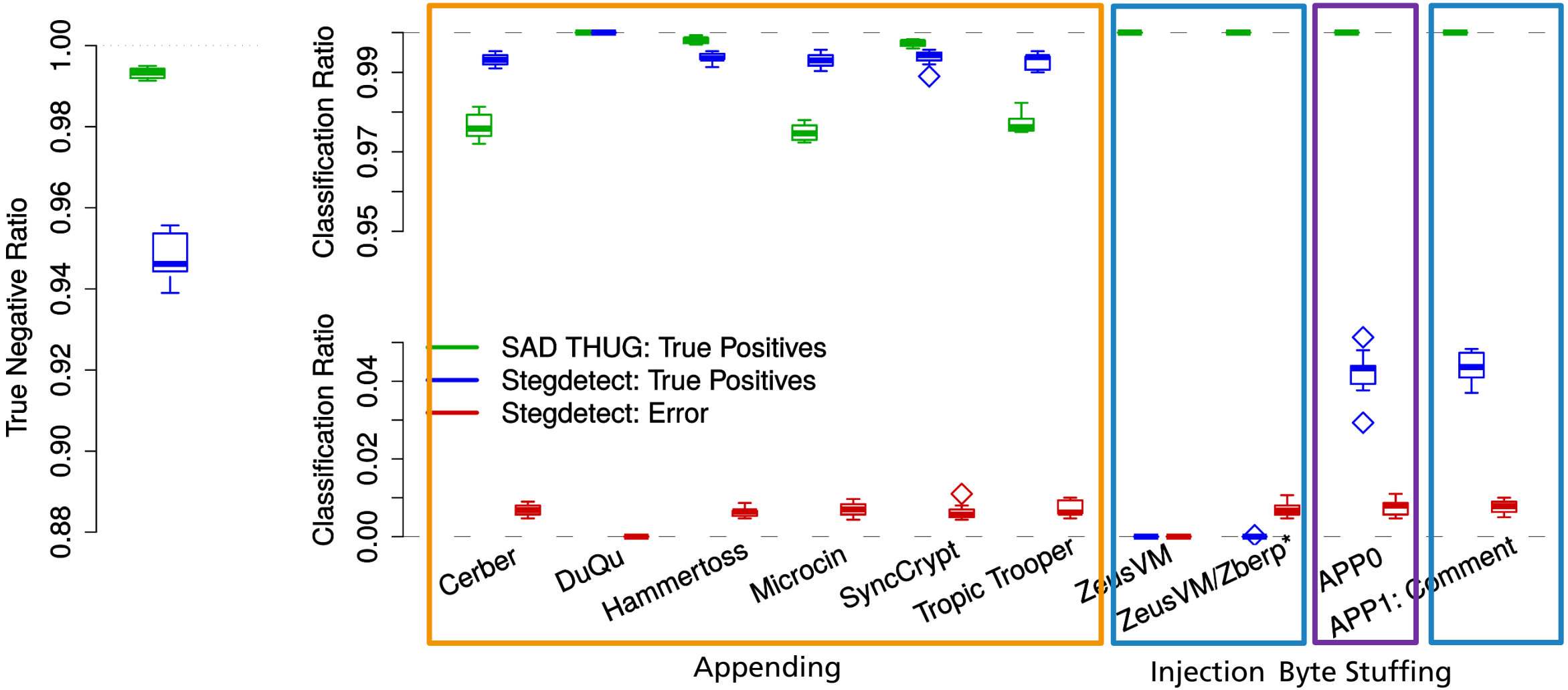
© Fraunhofer

Evaluation Setup: JPEG

Name	Method	Industry
Cerber	Appending	Ransomware
DuQu (1 & 2)	Appending	APT/Government
Hammertoss	Appending	APT/Government
Microcin	Appending	APT/Government
SyncCrypt	Appending	Ransomware
Tropic Trooper	Appending	APT/Government
ZeusVM/Zberp	Injection	Banking-Trojan
APP0	*Byte Stuffing*	*Fraunhofer FKIE*
APP1: Comment	*Injection*	*Fraunhofer FKIE*

© Fraunhofer

Evaluation Results: JPEG



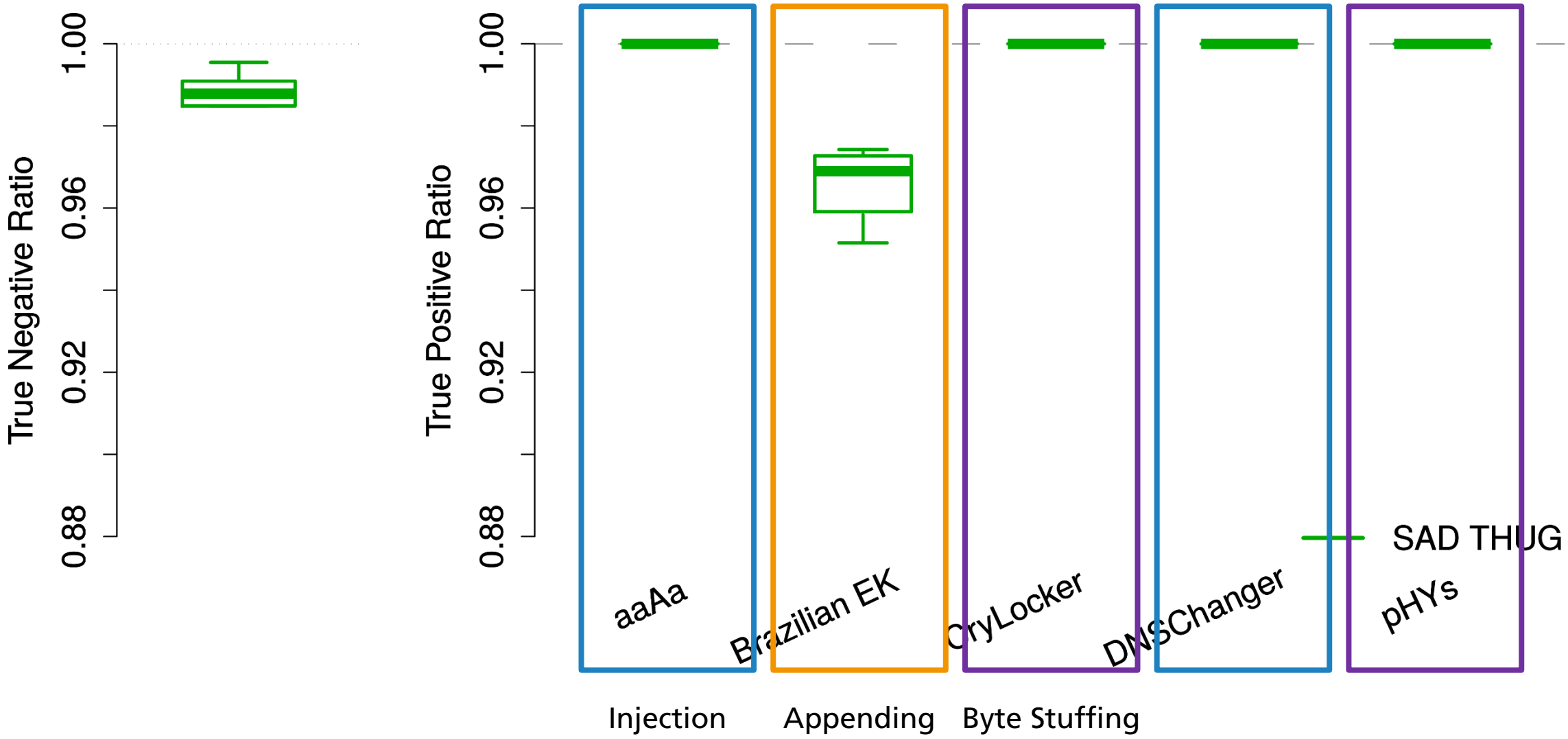
© Fraunhofer

Evaluation Setup: PNG

Name	Method	Industry
“Brazilian EK“	Appending	Exploit Kit
CryLocker	Byte Stuffing	Ransomware
DNSChanger	Injection	Exploit Kit
aaAa	*Injection*	*Fraunhofer FKIE*
pHYs	*Byte Stuffing*	*Fraunhofer FKIE*

© Fraunhofer

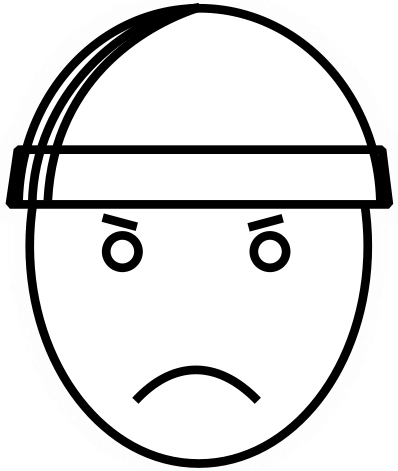
Evaluation Results: PNG



© Fraunhofer

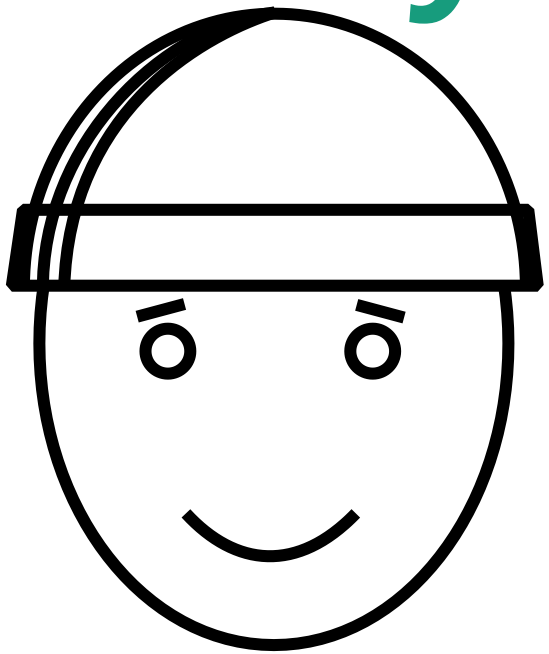
Key Takeaways

- SAD THUG makes thugs sad!
- Structural embedding methods as prevalent as image data-based methods!
- SAD THUG detects them, including unknown methods!
- SAD THUG can be used for any structured file type



© Fraunhofer

Thank you!



© Fraunhofer