Hochschule Worms
University of Applied Sciences

NETWORK INFORMATION HIDING

CH. 8: REPLICATING EXPERIMENTS

Prof. Dr. Steffen Wendzel
Worms University of Applied Sciences

https://www.wendzel.de (EN) | https://www.hs-worms.de/wendzel/ (DE) @cdp_xe (Twitter)

Online Class: https://github.com/cdpxe/Network-Covert-Channels-A-University-level-Course/

Why Replicating Experiments?

- Replication studies …
  - allow to validate research results, either before or after their publication.
    - In some sciences, e.g. Psychology, there was even a replication crisis, where several (even standard textbook results) could not be replicated and were thus (partially) rejected.
  - allow to extend experiments and thus allow to gain more insights.

cf. Steffen Wendzel, Luca Caviglione, Wojciech Mazurczyk, Jean-Francois Lalande: Network Information Hiding and Science 2.0: Can it be a Match?, *Int. Journal of Electronics and Telecommunications*, Vol. 63(2), pp. 217-222, 2017.

Replicating Experiments

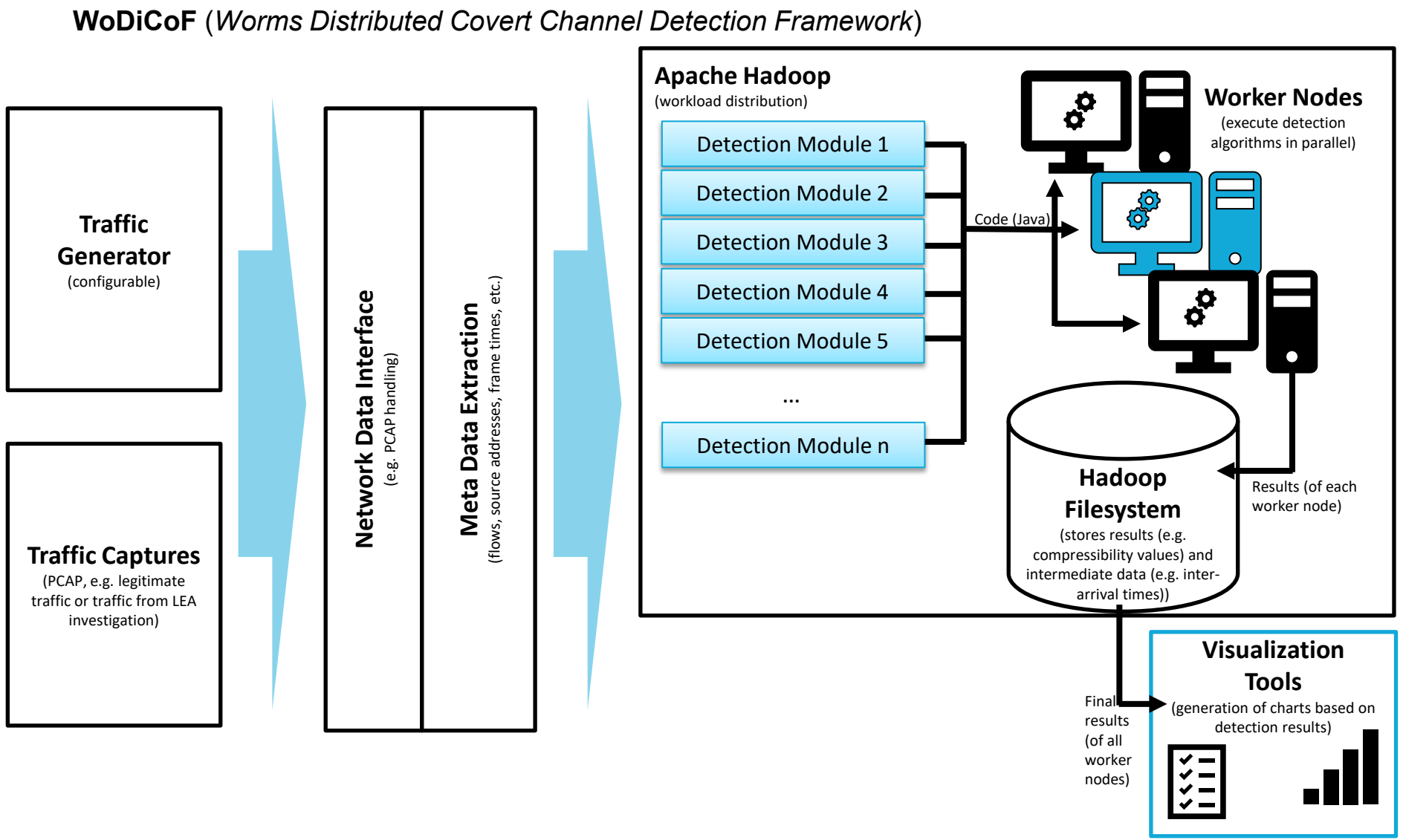
- Almost nobody seems to replicate experimental results of other researchers in the covert channel domain.
  - Manifold reasons, e.g. it is difficult to publish replication studies, no data available, no code available, no time, …
  - Replication studies should be honored as valid contributions in research.

- But: How trustworthy are provided results during review and in papers?
  - Well, conference and journal quality is a good indicator, but not perfect.
  - Publisher name is not a good indicator, e.g. Springer, IEEE, ACM, … they all feature crappy papers with horrible research.

- Thus, we initiated the
  Int'l Workshop on Information Security Methodology and Replication Studies (IWSMR)

cf. Steffen Wendzel, Luca Caviglione, Wojciech Mazurczyk, Jean-Francois Lalande: Network Information Hiding and Science 2.0: Can it be a Match?, *Int. Journal of Electronics and Telecommunications*, Vol. 63(2), pp. 217-222, 2017.

Replicating Experiments



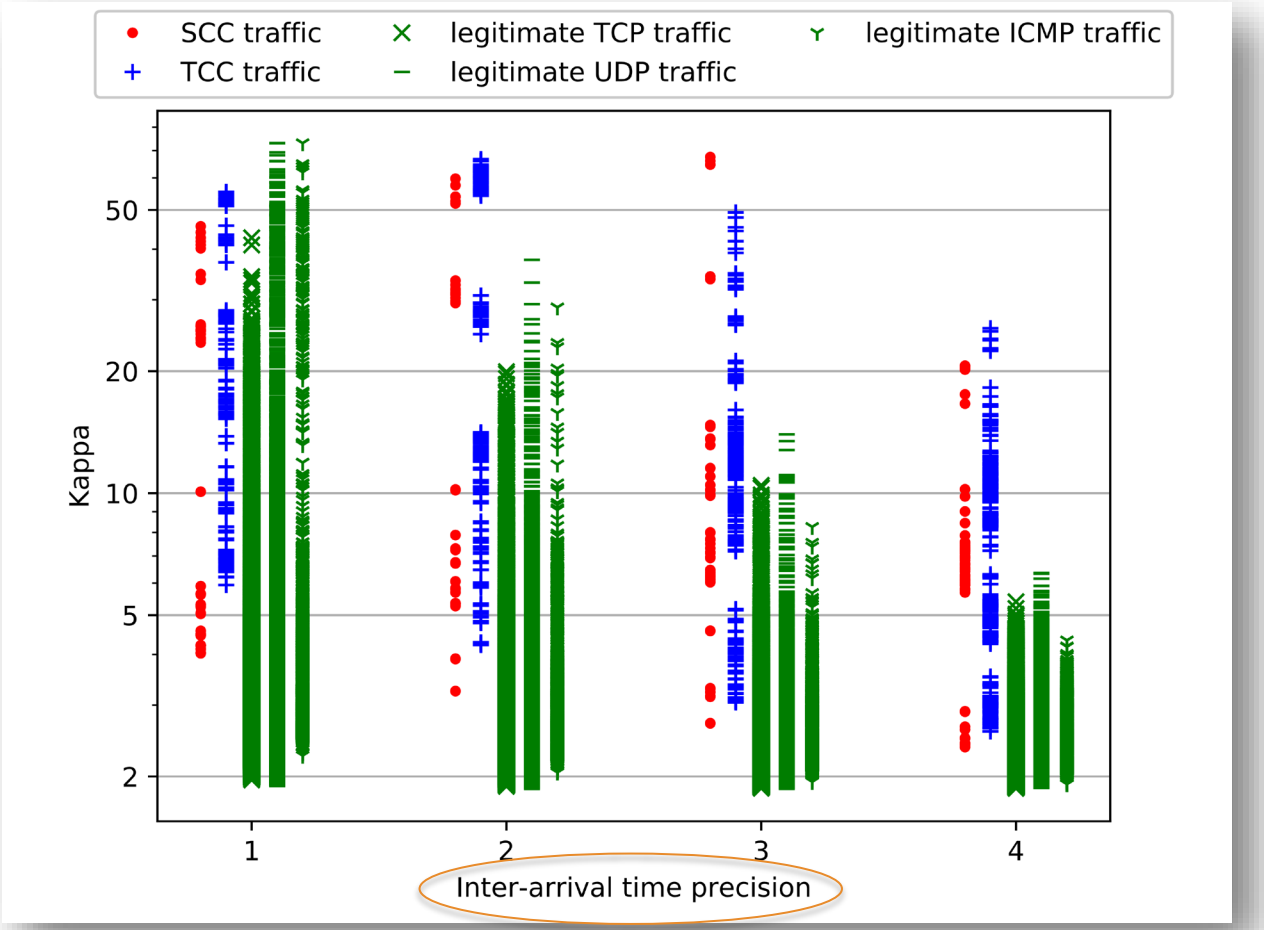
R. Keidel, S. Wendzel, S. Zillien et al.: WoDiCoF - A Testbed for the Evaluation of (Parallel) Covert Channel Detection Algorithms, J.UCS, Vol. 24(5), 2018.

Replication Study: Compressibility of Cabuk et al.

- Published in ACM Transactions on Information and System Security (TISSEC), as an extended version of an ACM CCS paper.
  - 147/508 citations *(May-22-2020, src: Google Scholar)*
  - However, compressibility was only covered in the journal version.

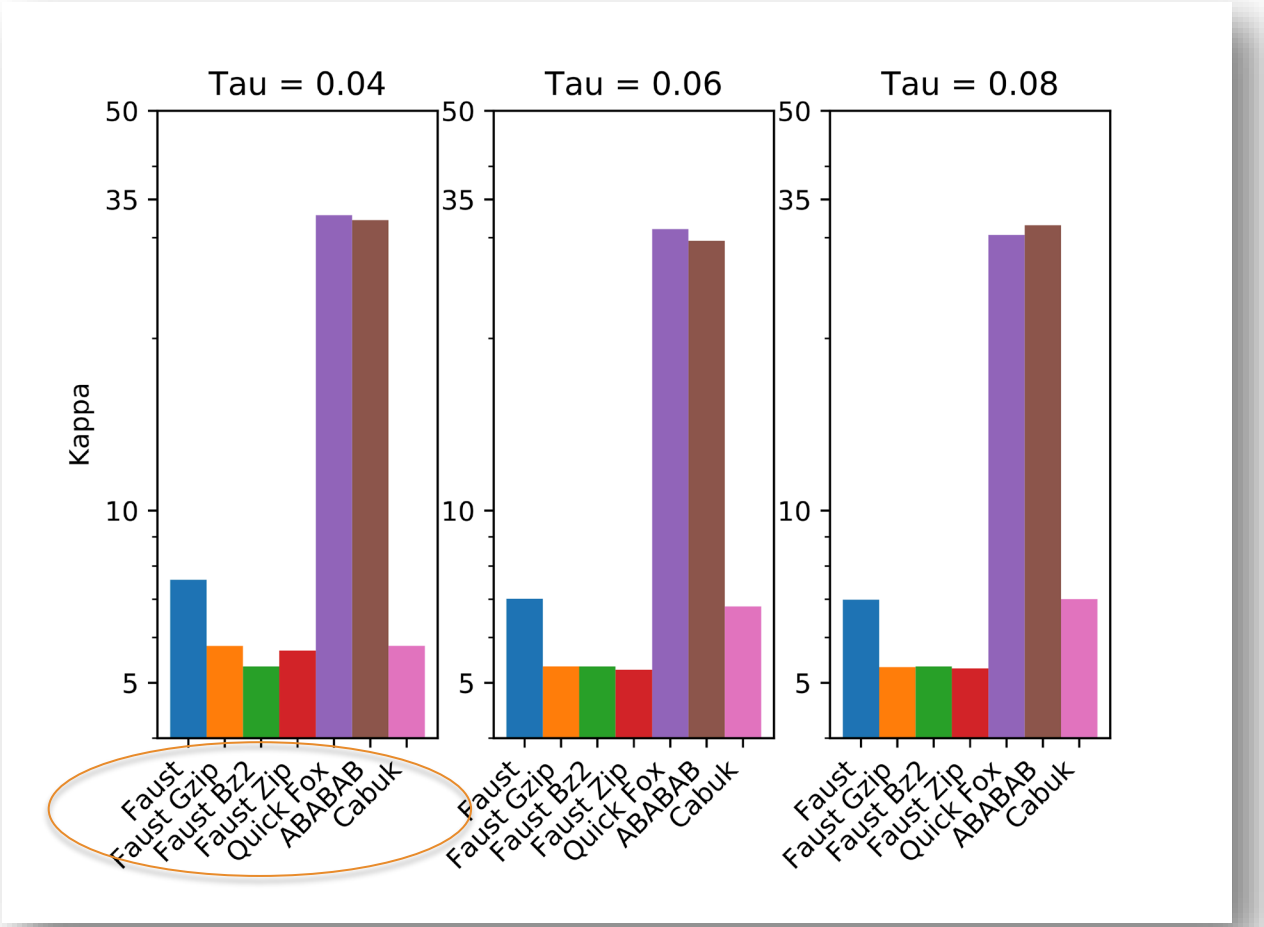
Replication Study: Compressibility of Cabuk et al.

Let's see how the precision of the measured IAT values influences Kappa…



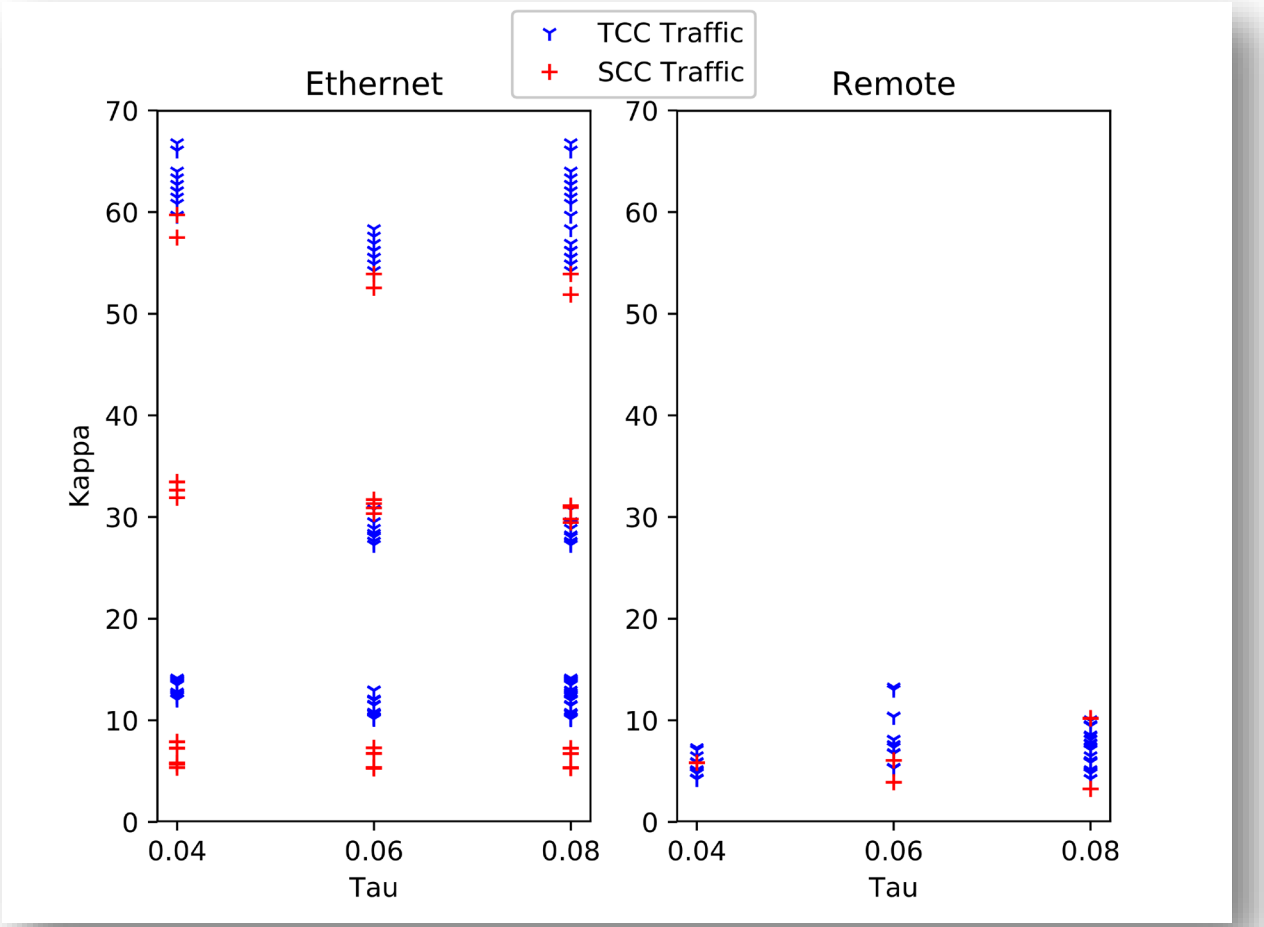
Replication Study: Compressibility of Cabuk et al.

Let’s see what happens if we transfer slightly different data over the covert channel …



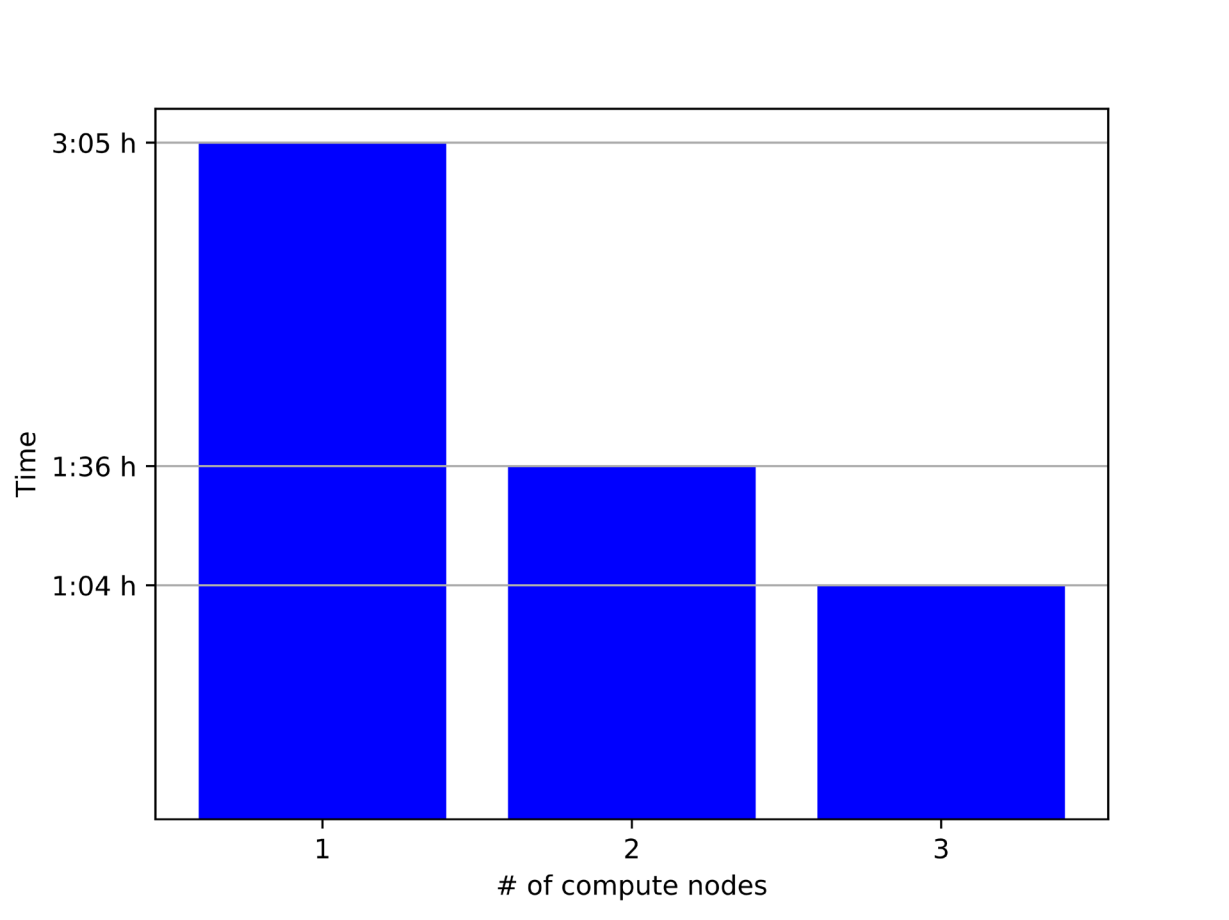
Replication Study: Compressibility of Cabuk et al.

Let’s see how Kappa differs when we utilize a different network connection …



Finally: Testing Parallel Performance

Parallelization using Apache Hadoop with several gigabytes of PCAP recordings.



NeFiAS (available soon on GitHub!)

README.md

NeFiAS – Network Forensics and Anomaly Detection System

NeFiAS is a simple and portable tool for network anomaly detection/network forensics, mostly tailored for the domain of network covert channels (network steganography). It was (initially) written by Steffen Wendzel.

Features

- Very tiny framework: core system contains less than 1.000 lines of code
- Super portable (core system entirely written in `bash` and `awk` (see the *story* below)
- Provides a good performance due to beowulf cluster, i.e. can be easily spread among many nodes
- Requires only standard Linux, no special libraries or tools required (see *requirements* below)

Summary

- Replication can lead to new insights:

  Even if previous work (such as in case of Cabuk et al.) is not “wrong”, replication studies can extend our understanding of how a method performs under changing circumstances.