Tampering Digital Evidence is Hard: The Case of Main Memory Images

Janine Schneider

March 29, 2020

IT Security Infrastructures Lab
Department of Computer Science
Friedrich-Alexander University Erlangen-Nürnberg (FAU)

Beyond a reasonable doubt

Georges Biard, Michael Douglas César 2016 3, https://commons.wikimedia.org/wiki/File:Michael_Douglas_C%C3%A9sar_2016_3.jpg, 2016, https://creativecommons.org/licenses/by-sa/3.0/deed.en

Introduction

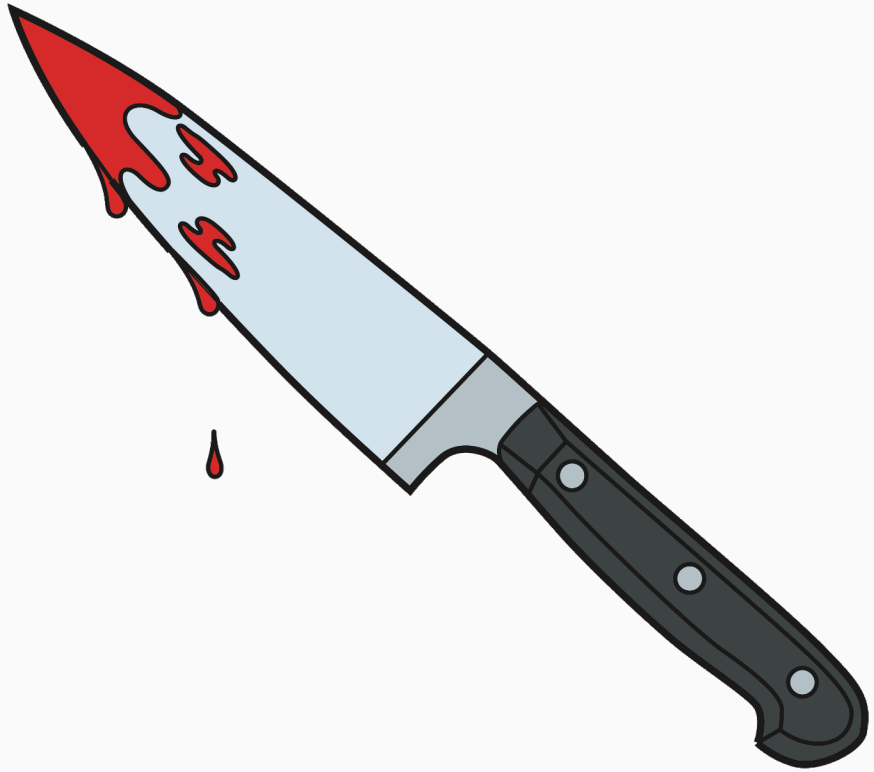
The Washington Post
Democracy Dies in Darkness

A Florida cop planted meth on random drivers, police say. One lost custody of his daughter.

Former deputy Zachary Wester was arrested July 10 for allegedly targeting innocent drivers, planting drugs in their vehicles in Jackson County, Fla. (WJHG)

https://www.washingtonpost.com/nation/2019/07/11/florida-cop-meth-drugs-arrests-scandal/

Introduction

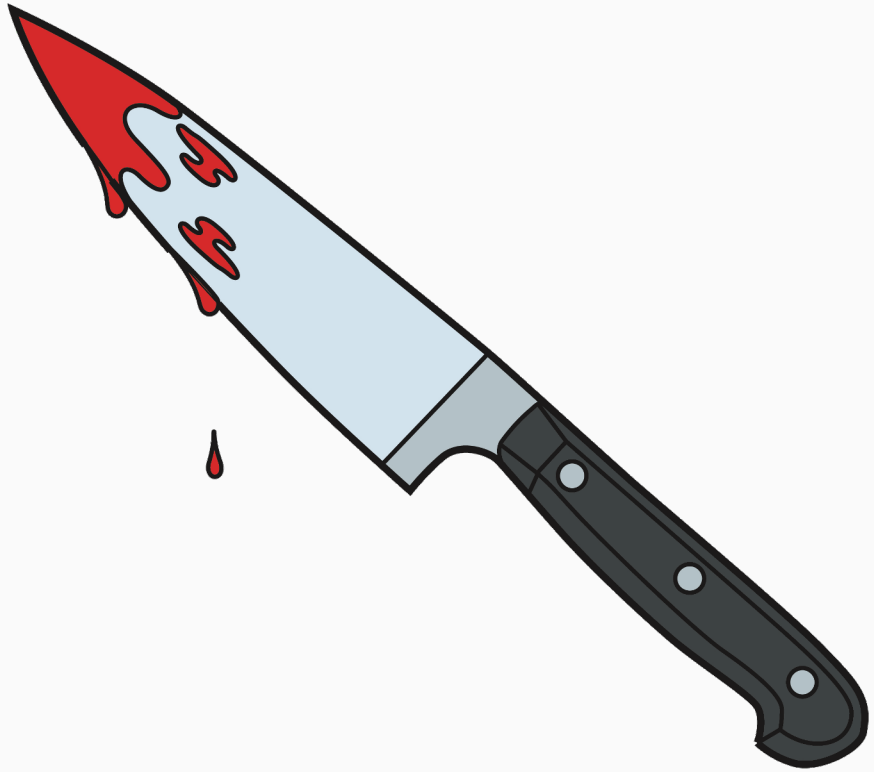


Left: Western Digital WD2500JD-00HBC0 20051228, 2007, https://commons.wikimedia.org/wiki/File:Western_Digital_WD2500JD-00HBC0_20051228.jpg, https://commons.wikimedia.org/wiki/Commons:GNU_Free_Documentation_License,_version_1.2

Right: The Clear Communication People, Bloody knife, 2013, https://www.flickr.com/photos/easy-pics/9665996132, https://creativecommons.org/licenses/by-nc-nd/2.0/

Introduction

d2d9 0c14 5e9c 54d4 8749 9c82 6056 953f

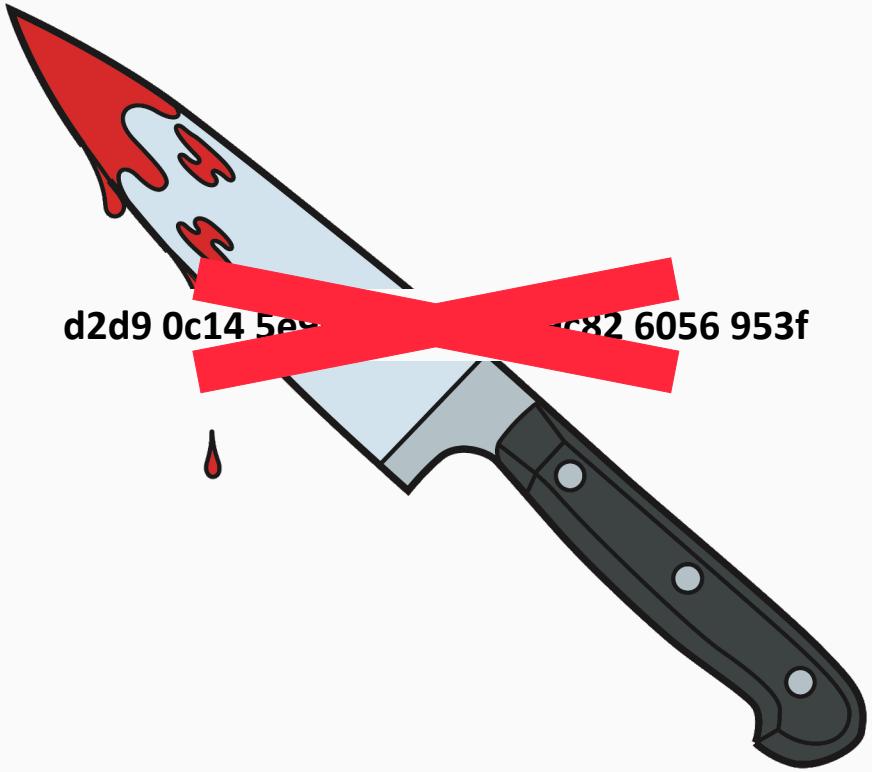


Left: Western Digital WD2500JD-00HBC0 20051228, 2007, https://commons.wikimedia.org/wiki/File:Western_Digital_WD2500JD-00HBC0_20051228.jpg, https://commons.wikimedia.org/wiki/Commons:GNU_Free_Documentation_License,_version_1.2

Right: The Clear Communication People, Bloody knife, 2013, https://www.flickr.com/photos/easy-pics/9665996132, https://creativecommons.org/licenses/by-nc-nd/2.0/

Introduction

d2d9 0c14 5e9c 54d4 8749 9c82 6056 953f



d2d9 0c14 5e[illegible] [illegible]c82 6056 953f

Left: Western Digital WD2500JD-00HBC0 20051228, 2007, https://commons.wikimedia.org/wiki/File:Western_Digital_WD2500JD-00HBC0_20051228.jpg, https://commons.wikimedia.org/wiki/Commons:GNU_Free_Documentation_License,_version_1.2

Right: The Clear Communication People, Bloody knife, 2013, https://www.flickr.com/photos/easy-pics/9665996132, https://creativecommons.org/licenses/by-nc-nd/2.0/

Introduction

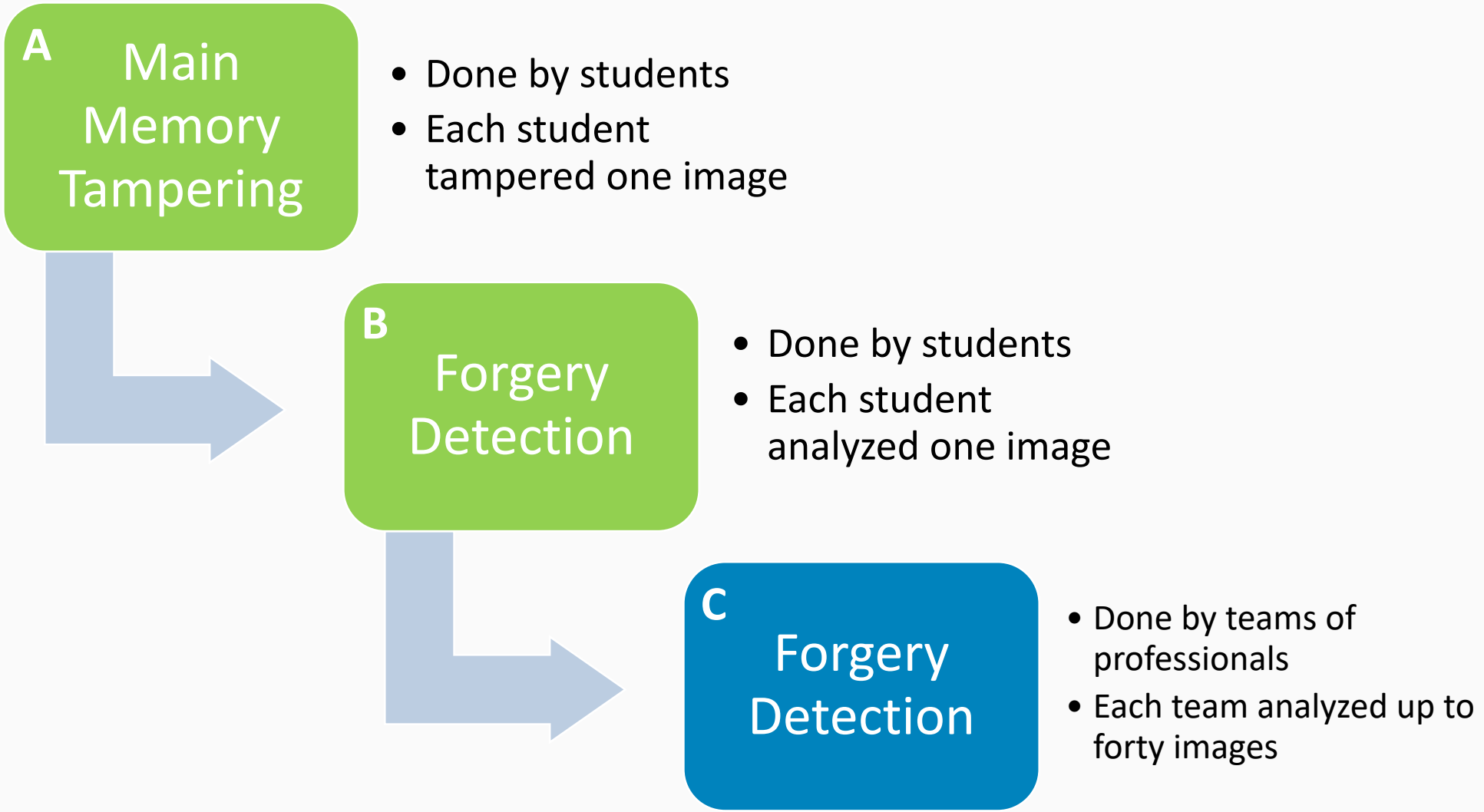
If there are no clear signs of evidence tampering, the effort of tampering is high, and neither motivation nor competence of a possible manipulative actor for performing the tampering task is evident, then it is improbable that the evidence was tampered with.

Research Goals

Freiling and Hösch show that HDD tampering is "hard" and the effort to create forgeries is "high":

- Does that depend on the type of evidence manipulated?
- What factors influence the success of manipulations
- What factors influence the speed of tampering analysis? Is there a positive effect of training?

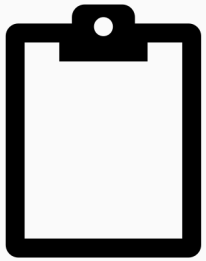
Experimental Design



Fictious Scenario

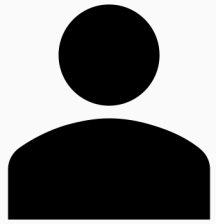
- Police identifies a server, which runs an illegal website selling drugs
- Werner Weber is suspected to be the administrator
- Police acquires a main memory dump of his laptop
- A policemen, involved in the investigation, is a personal enemy of Werner Weber

General Considerations



Pre-study questionnaire:

- Motivation
- Experience
- Demographic data



Person effort:

- Part A and B
- Logged by participants
- Minutes
- > 30 min

Team effort:

- Part C
- Logged automatically
- Seconds

Part A

Material

Participants were given:

- A clean main memory image, i.e. from which the server was never accessed
- ssh-key to access the server
- sudo password for the administration of the server

Task

The task was to tamper with the main memory image so that an analyst comes to the following conclusions:

- There was definitely an active network connection to the server at the time of main memory backup or before that.
- Administrative commands were executed on the server over this network connection.

Participants

- 23 participants
- Mostly computer science master students
- Moderate motivation

Comparison

	our work (Part A, $n = 23$)	HDD experiment (Phase 1.A (Freiling and Hösch, 2018), $n = 13$)
Min/max	300/2300	120/1260
Average	927	532
Stddev.	466	325
Median	810	450

Tampering effort measured in minutes for Part A (left) and comparison with HDD manipulation results (Freiling and Hösch, 2018) (right)

Part B

Material

Participants received:

- Randomly chosen main memory image
- Kernel module used to create the image
- Volatility profile
- ssh-keys and sudo password of the server

Participants

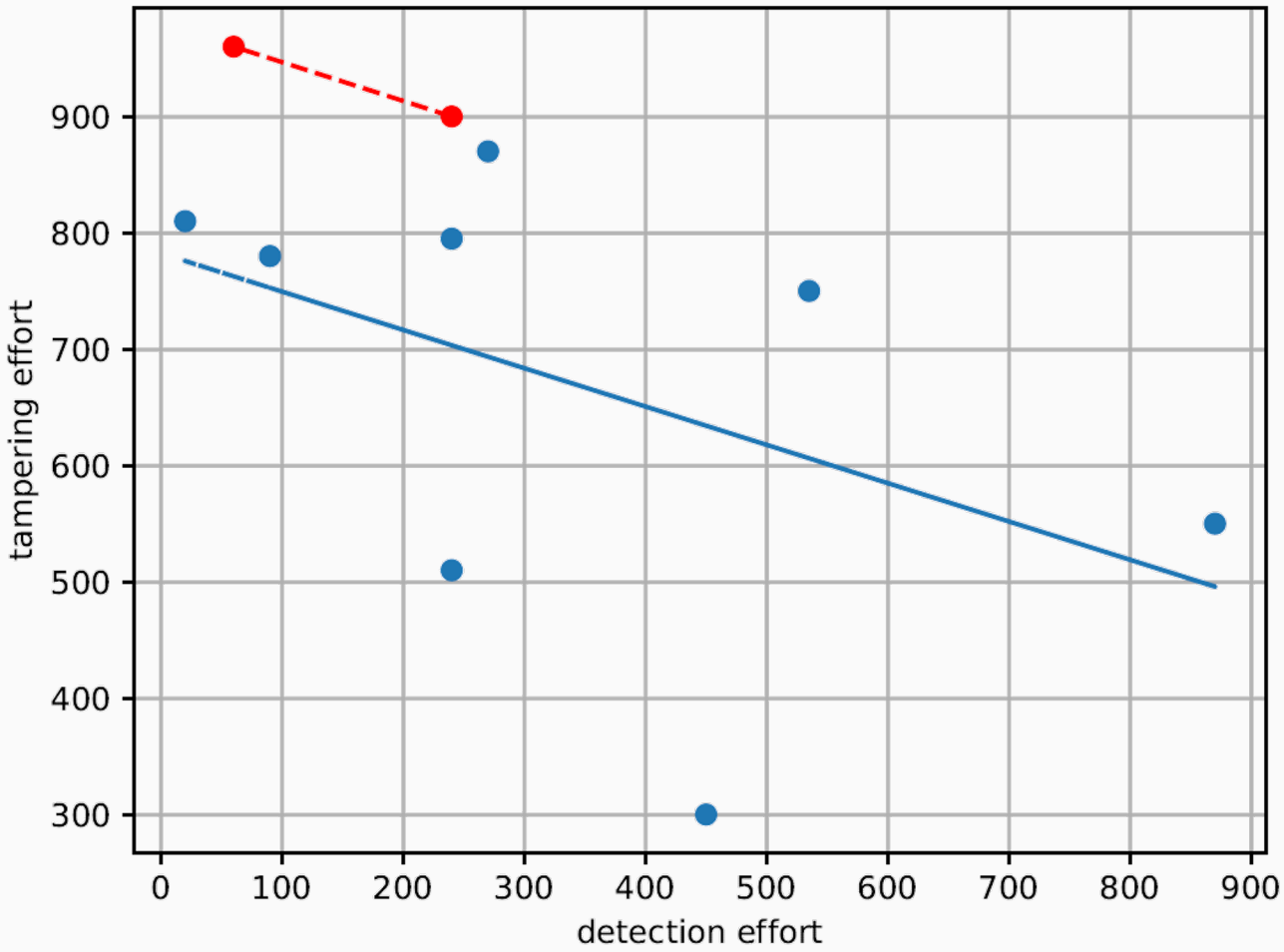
- 22 participants
- Intersection between Part A and B = 19 participants

Results

	classified as original	classified as forgery
original	12	0
person effort range	150–795	–
person effort average	426.25	–
person effort median	385	–
forgery	2	8
person effort range	60–240	20–870
person effort average	150	375
person effort median	150	270

Results of Part B of our experiment (individual detection, person effort measured in minutes).

Relation between efforts



Relation between tampering and detection effort for correctly (blue) and incorrectly (red) classified forgeries with a linear regression line for both cases.

Influencing factors

Participants who created successful forgeries:

- Computer science master students
- Participated in the preliminary course
- Highly motivated
- Invested more time than other participants

Influencing factors

Participants who did a wrong classification:

- Computer science master and bachelor students
- Highly motivated
- Bachelor student not participated in the preliminary course
- Master student invested less time than other participants

Tampering Approaches

Tampering approaches:

- Simulate-and-Sweep
- Manual-Fix
- Manual-Fix++

Detection Approaches

Detection Approaches:

- Missing information
- Tool traces
- Time and data structure inconsistencies
- Network connections

Part C

Structure

- Teams received a sequence of 40 memory dumps (called challenges) from the random pool
- 20 originals
- 20 forgeries

Participants

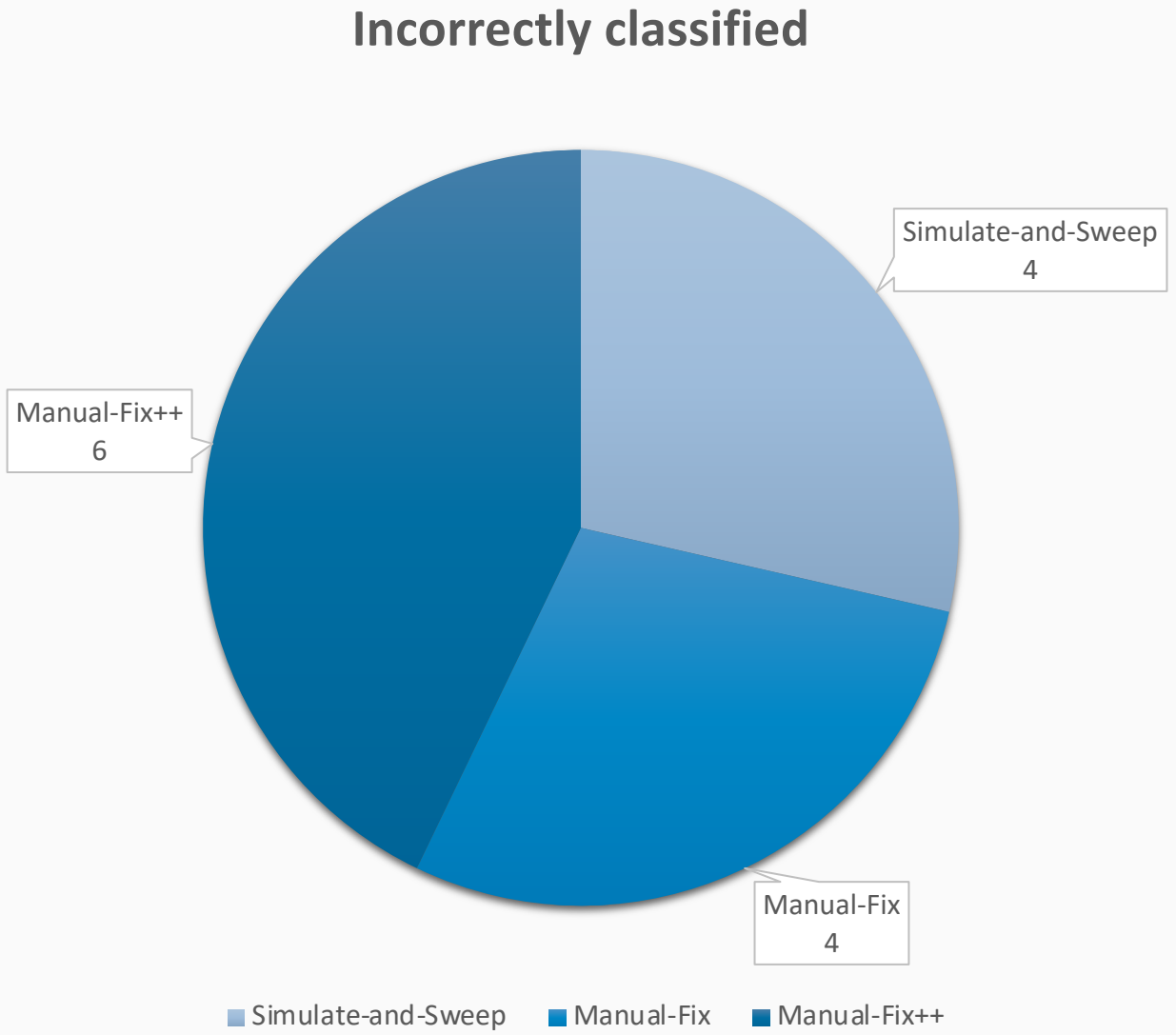
- 15 teams
- 66 participants
- Most stated that they are averaged experienced or academics
- 105 minutes
- 5 team results were analyzed

Results

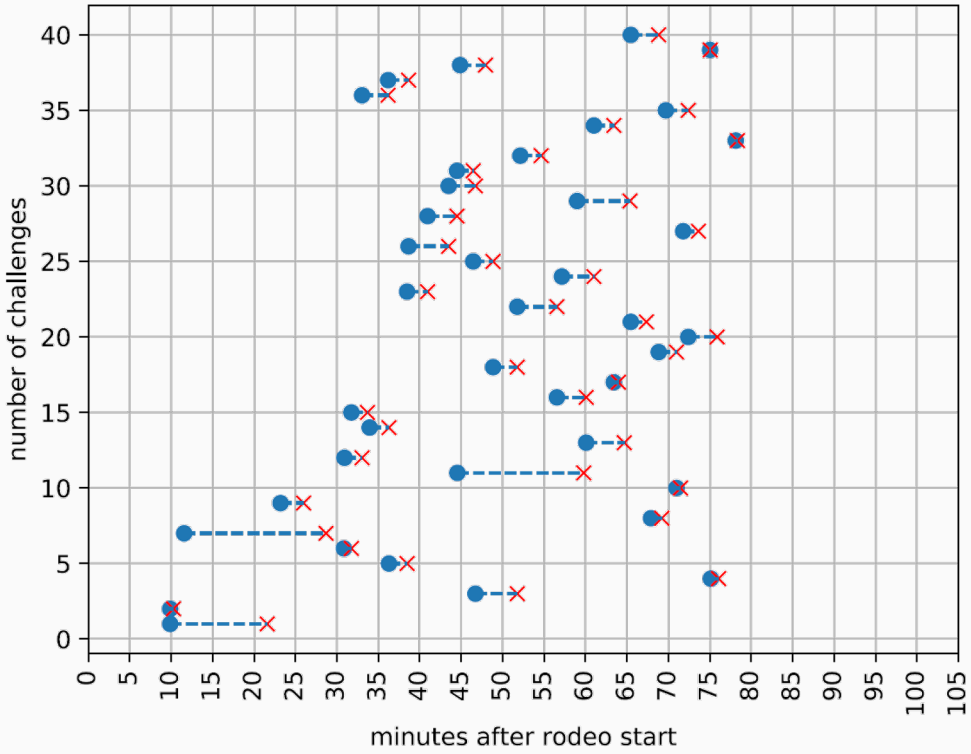
	classified as original	classified as forgery
original	84	8
team effort range	0–2610	3–643
team effort average	198.89	162.75
team effort median	133	173
forgery	16	75
team effort range	2–182	3–1852
team effort average	52.81	192.05
team effort median	8	123

Results of team 4, 5, 9, 10, 11 of Part C of the experiment (team effort given in seconds)

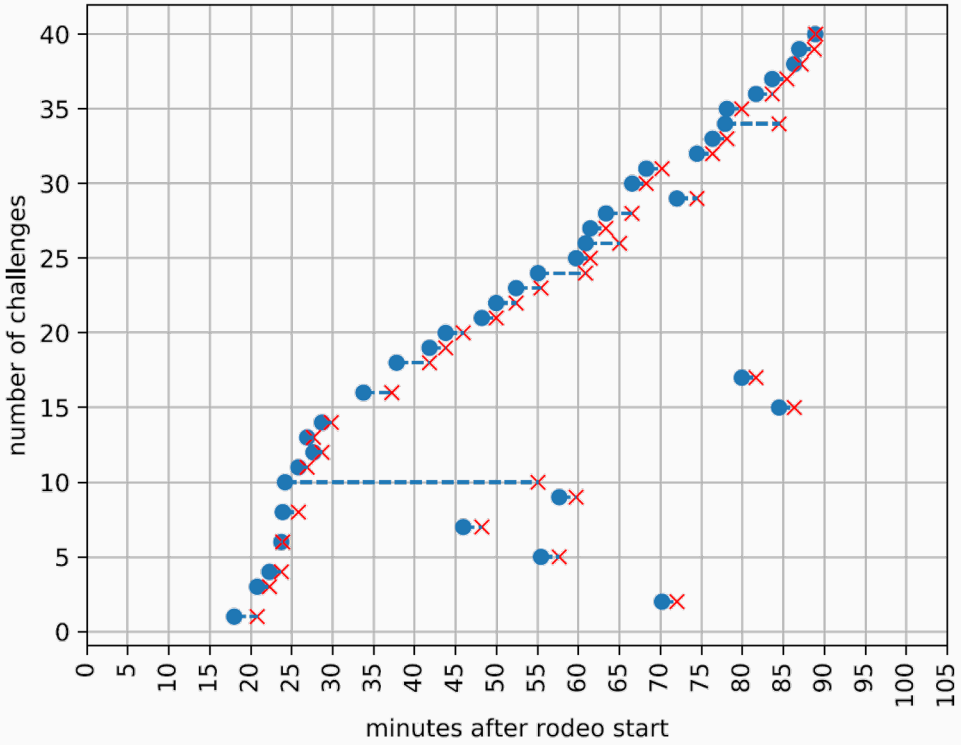
Incorrectly classified images



Parallel Processing

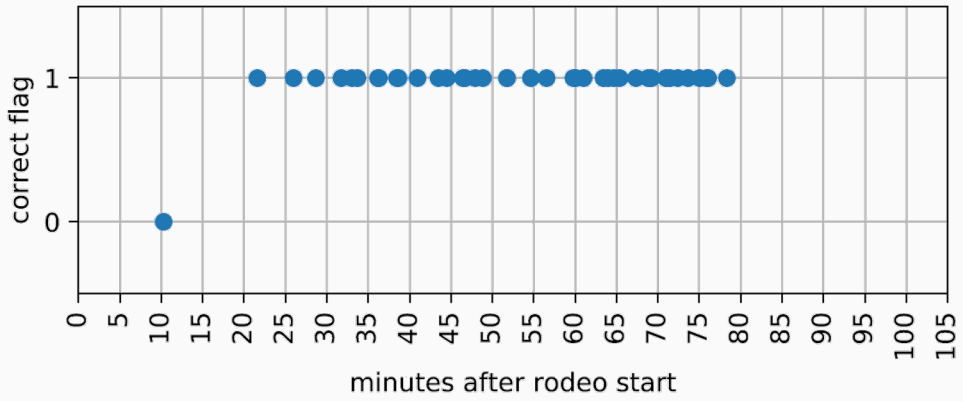


LST and SAT times per challenge for team 4. LST is depicted as blue circles and SAT is depicted as red x

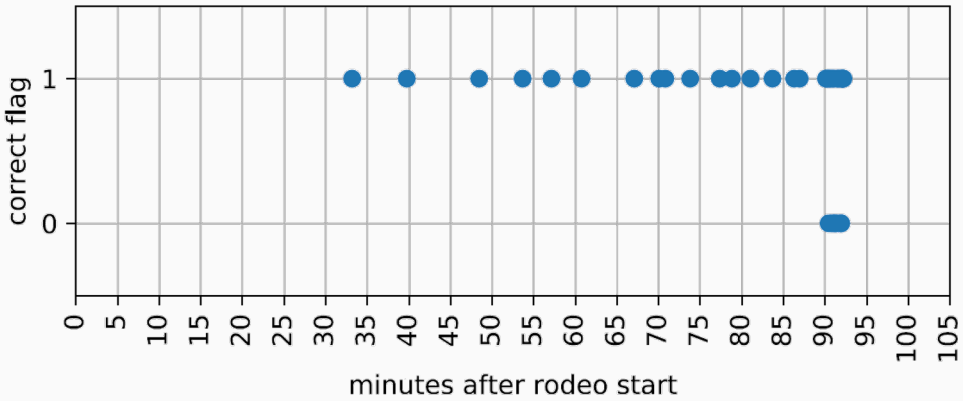


LST and SAT times per challenge for team 11. LST is depicted as blue circles and SAT is depicted as red x.

Guessing

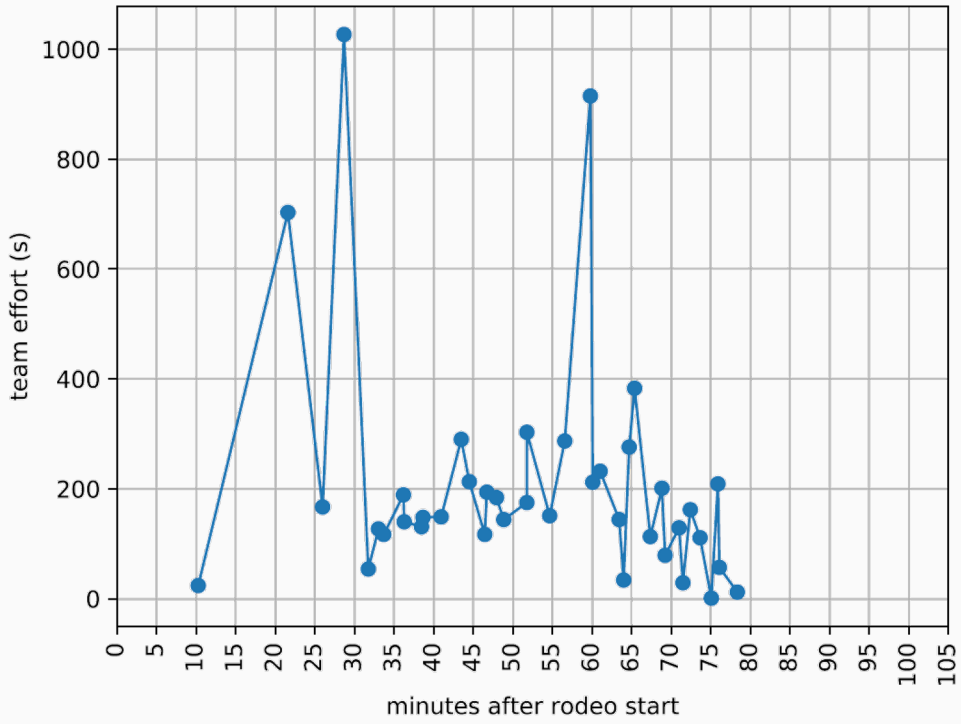


Distribution of correct and incorrect answers over time for team 4

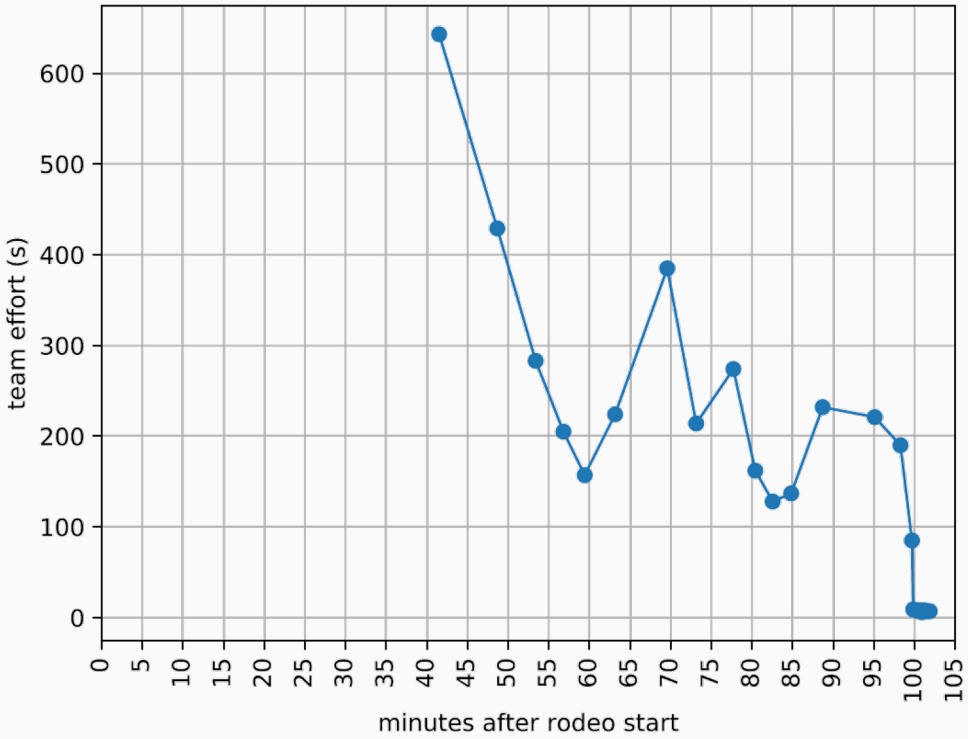


Distribution of correct and incorrect answers over time for team 10

Repetition



Team effort per challenge for submission added time (SAT) for team 4.
Effort is measured in seconds



Team effort per challenge for submission added time (SAT) for team 9.
Effort is measured in seconds.

Conclusion

Conclusion

- Probability that a manipulation is detected is high
- Clear differences between HDD and main memory experiments
- Producing a good forgery generally requires more effort than detecting the forgery
- Different tampering approaches were similar to those documented by Freiling and Hösch (2018) for hard disc images

Thank you!