Raspberry Pi-based video filtration system

A novel approach to reversible PII anonymization in videostreams using commodity hardware

C.H.J Kuipers & S. Scholtes

February 6, 2018

Research Project 1
Master of System and Network Engineering
Institute of Informatics
University of Amsterdam

Introduction

Research question

How can commodity hardware be used to filter PII from video streams?

Research question

How can commodity hardware be used to filter PII from video streams?

1. What types of PII?

Research question

How can commodity hardware be used to filter PII from video streams?

1. What types of PII?
2. What anonymization techniques?

Research question

How can commodity hardware be used to filter PII from video streams?

1. What types of PII?
2. What anonymization techniques?
3. Tailoring to commodity hardware?

Process

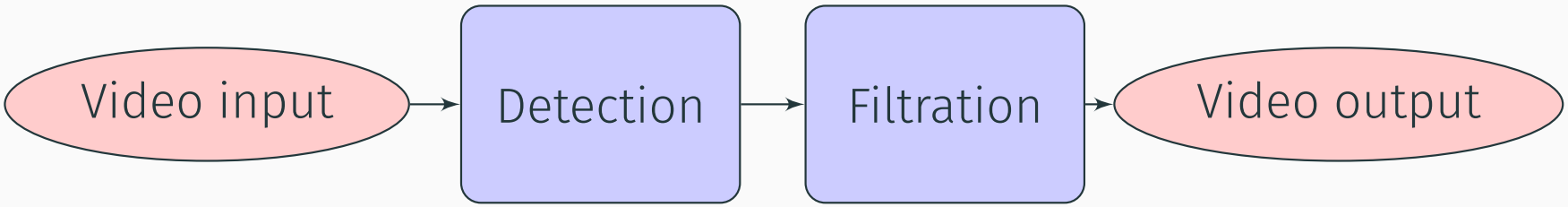


Figure 1: Video processing overview

Personally Identifiable Information

Definition

Any information related to a natural person, that can be used to directly or indirectly identify the person[1].

[1] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)". In: *Official Journal of the European Union* L119 (May 2016), pp. 1–88. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC.

Filtration

Filtration

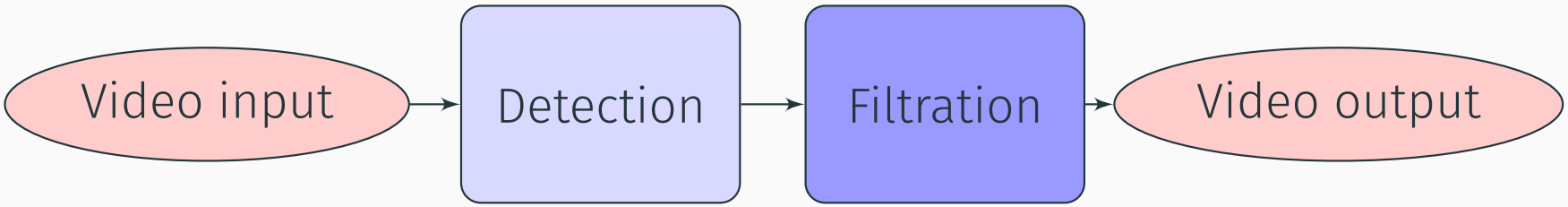


Figure 2: The filtration process

Filtration

Reversibility of the filtration process

- Contextual

- Container

Filtration

Reversibility of the filtration process

- **Contextual**

  Image manipulation
- **Container**

  Encryption in transit & at rest

Filtration - anonymization techniques

Reversible methods:

- Pixelrelocation
- Warping
- Chaos Cryptography

Filtration - anonymization techniques

Reversible methods:

- Pixelrelocation
- Warping
- Chaos Cryptography

One-way methods:

- Masking
- Blurring (a.k.a. Normalized Blurring)

Filtration - techniques

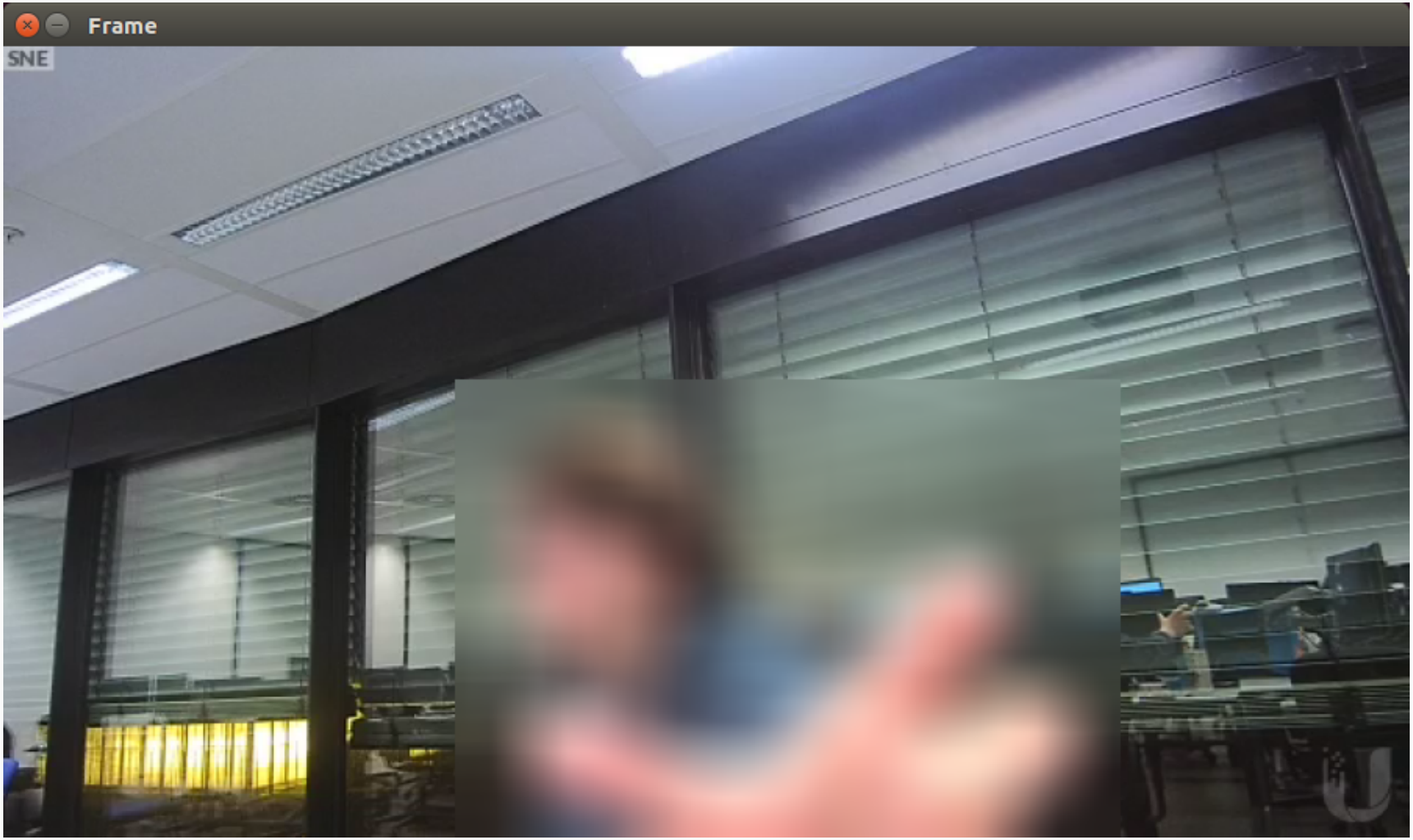


Figure 3: Blur

Filtration - techniques

Reversible methods:

- Pixelrelocation
- Warping
- Chaos Cryptography

One-way methods:

- Masking
- Blurring (a.k.a. Normalized Blurring)
- Gaussian blurring

Filtration - techniques

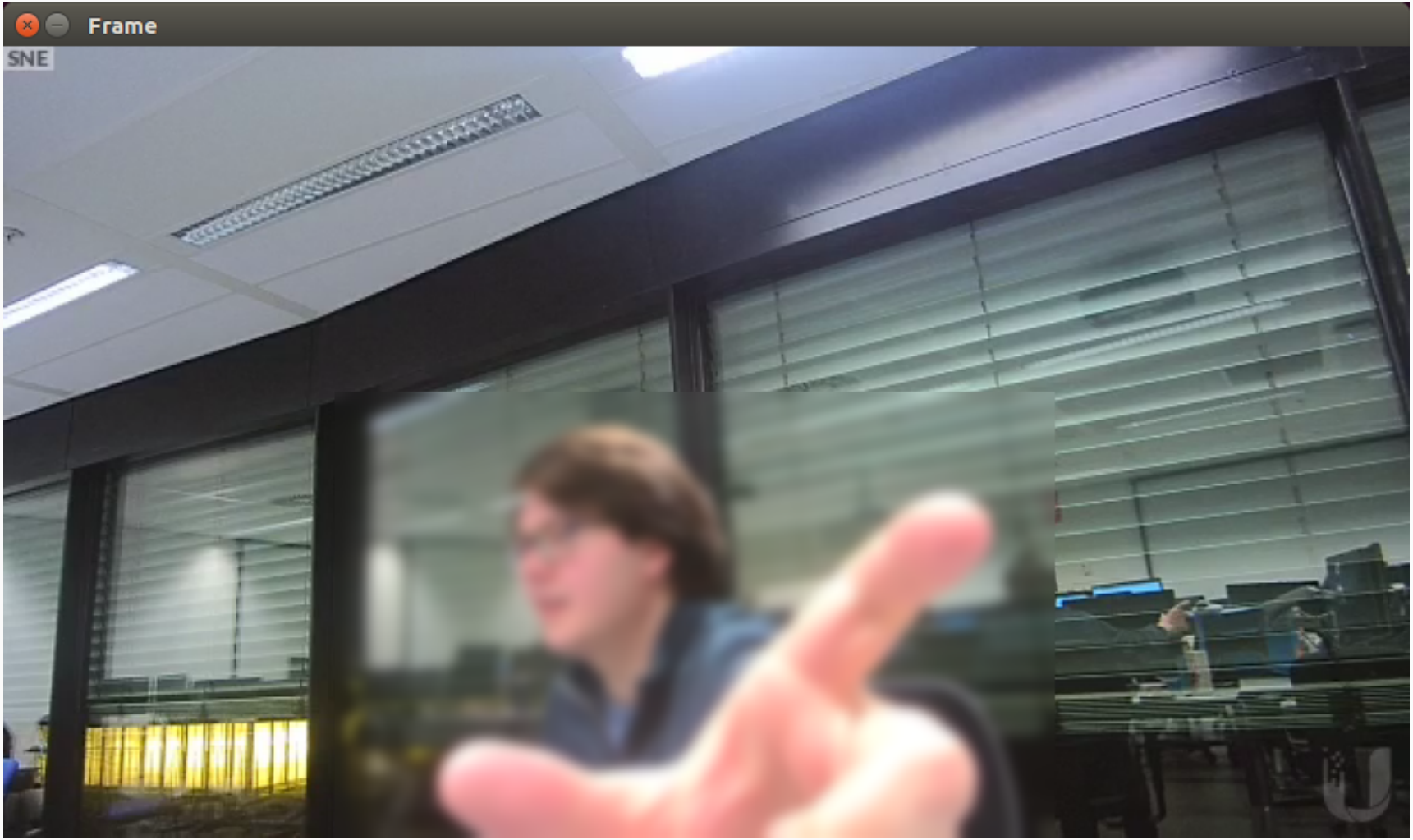


Figure 4: Gaussian blur

Proof of Concept

Proof of Concept

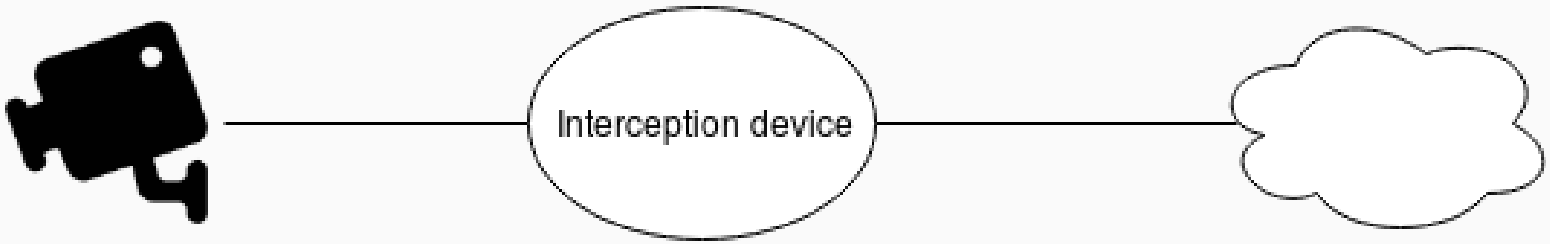


Figure 5: Overview

Proof of Concept

Components used for the Proof of Concept

Hardware:

- IP Camera
- Interception device
- Router

Proof of Concept

Components used for the Proof of Concept

Hardware:

- IP Camera
- Interception device
- Router

Software:

- Ubuntu 16.0.4.3 LTS
- Stretch 9.3
- Python 3.5.1-3
- OpenCV 3.3.0
- Caffenet Caffemodel

Proof of Concept

Test overview

Proof of Concept

Test overview

- Baseline

Proof of Concept

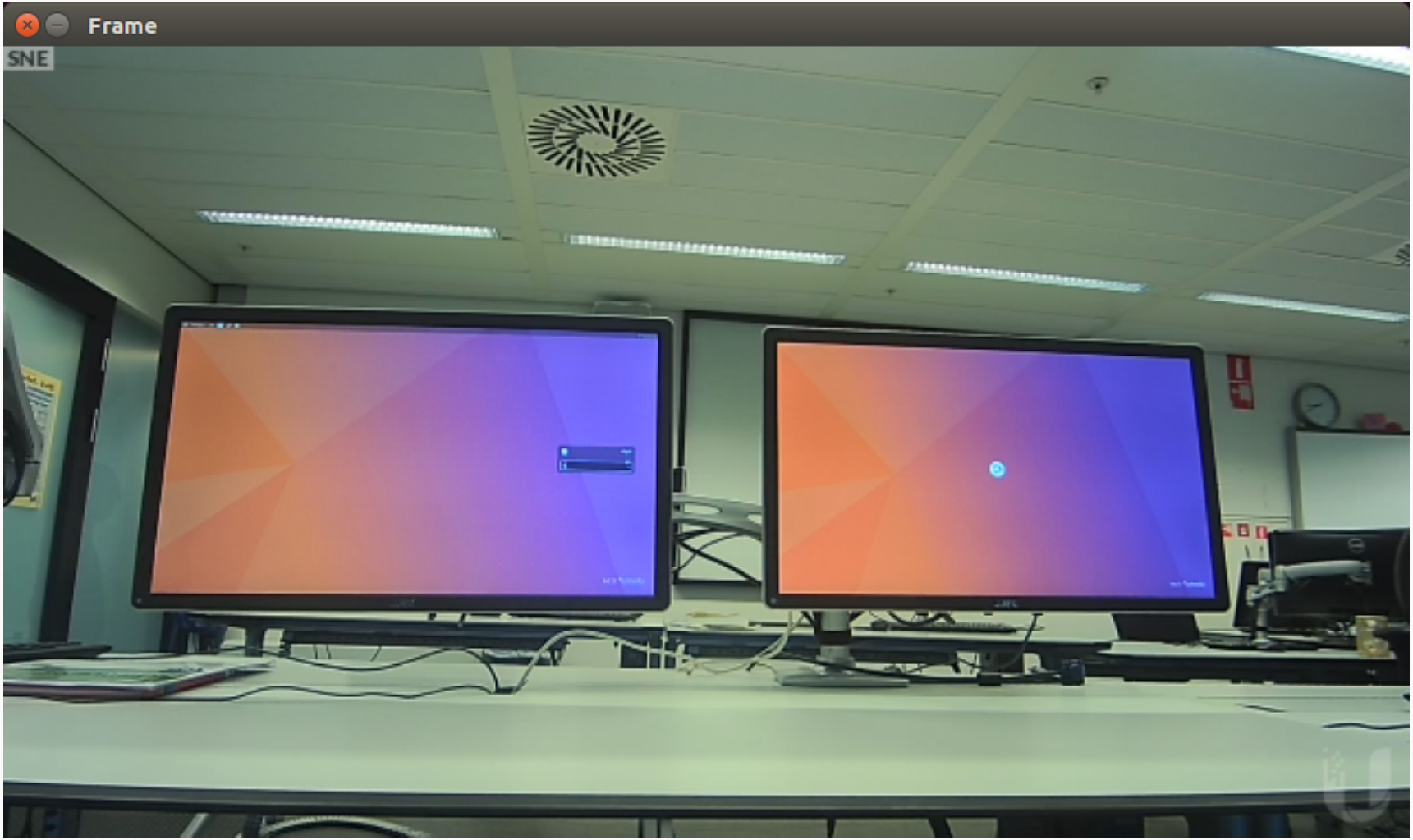


Figure 6: Baseline

Proof of Concept

Test overview

- Baseline

Proof of Concept

Test overview

- Baseline
- Detection

Proof of Concept

Test overview

- Baseline
- Detection
- Draw boxes

Proof of Concept

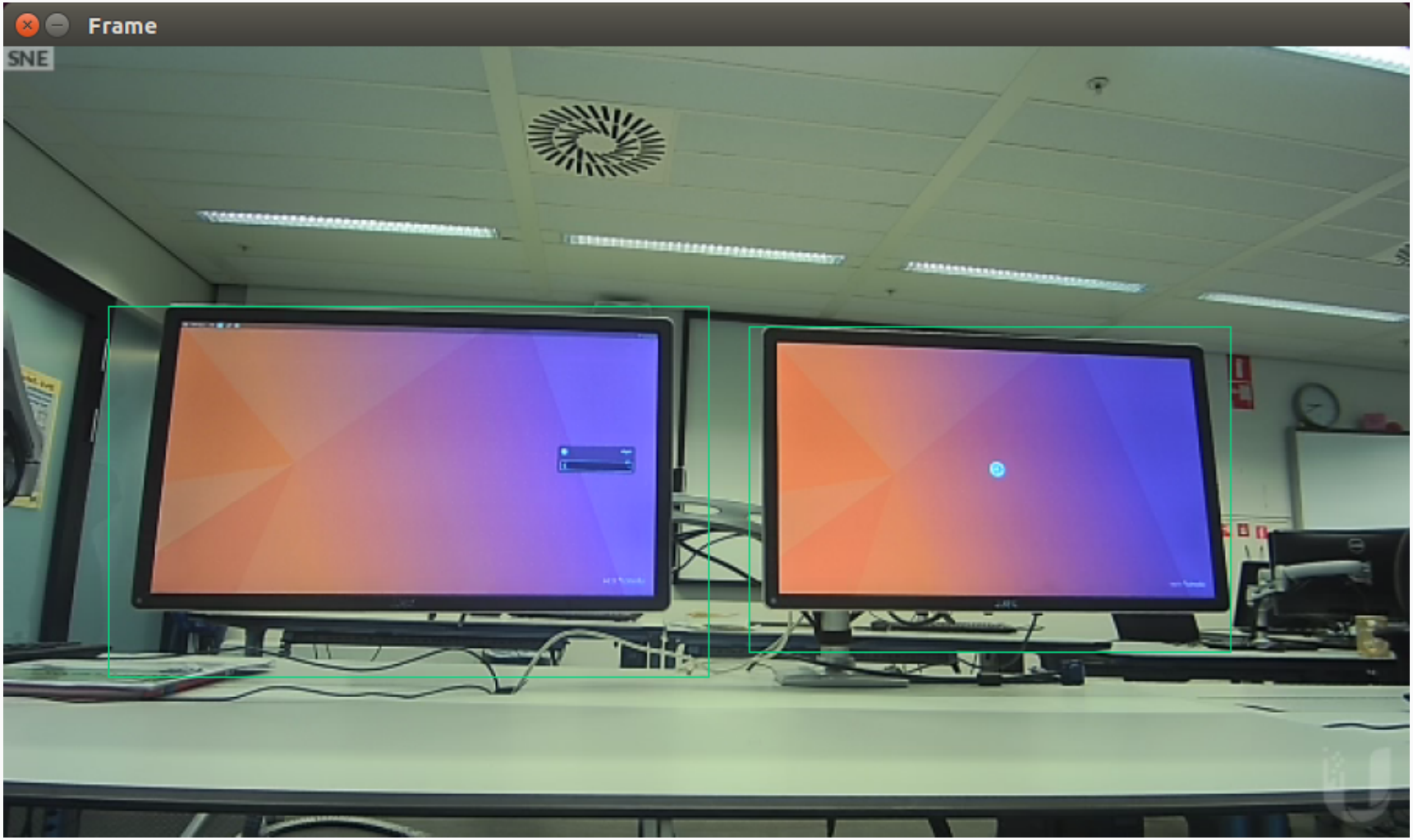


Figure 7: Draw boxes

Proof of Concept

Test overview

- Baseline
- Detection
- Draw boxes

Proof of Concept

Test overview

- Baseline
- Detection
- Draw boxes
- Labels

Proof of Concept

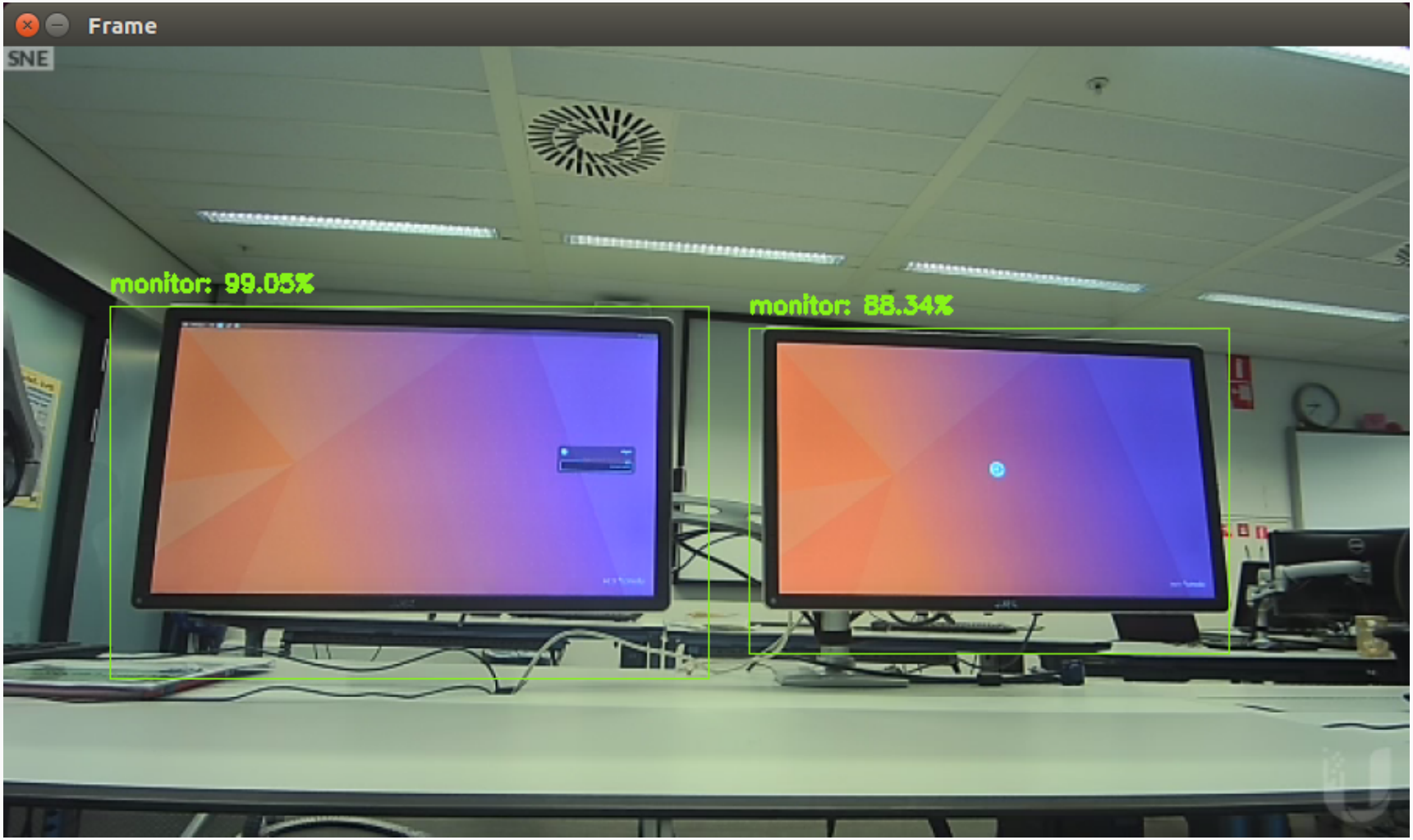


Figure 8: Label detections

Proof of Concept

Test overview

- Baseline
- Detection
- Draw boxes
- Labels

Proof of Concept

Test overview

- Baseline
- Detection
- Draw boxes
- Labels
- Save anonymized stream

Proof of Concept

Test overview

- Baseline
- Detection
- Draw boxes
- Labels
- Save anonymized stream
- Save original stream

Proof of Concept

Test overview

- Baseline
- Detection
- Draw boxes
- Labels
- Save anonymized stream
- Save original stream
- Encrypt original stream

Proof of Concept

Test overview

- Baseline
- Detection
- Draw boxes
- Labels
- Save anonymized stream
- Save original stream
- Encrypt original stream
- Re-stream anonymized stream

Proof of Concept

Test overview

- Baseline
- Detection
- Draw boxes
- Labels
- Save anonymized stream
- Save original stream
- Encrypt original stream
- Re-stream anonymized stream
- Blurring

Proof of Concept

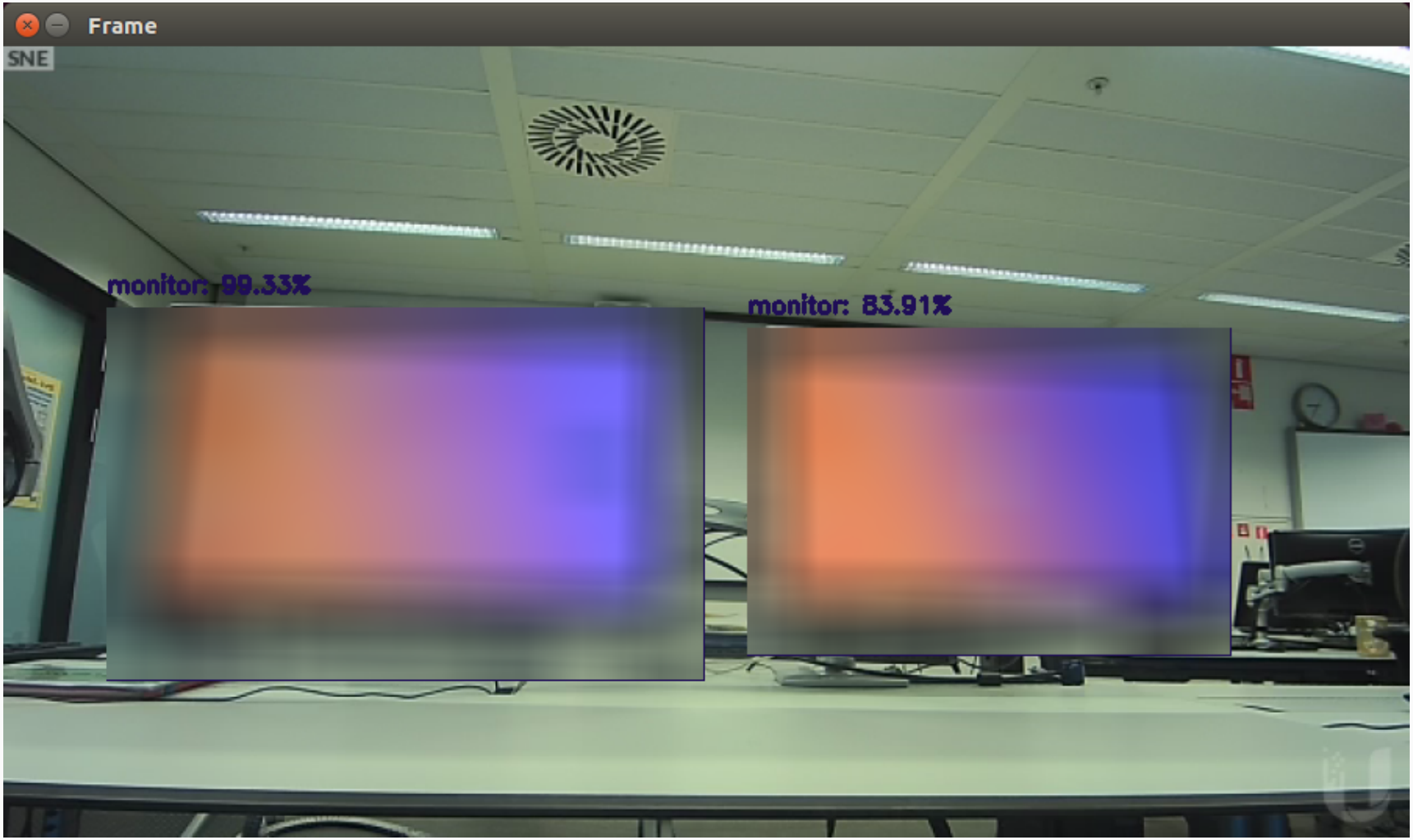


Figure 9: Blurring detections

Proof of Concept

Test overview

- Baseline
- Detection
- Draw boxes
- Labels
- Save anonymized stream
- Save original stream
- Encrypt original stream
- Re-stream anonymized stream
- Blurring

Proof of Concept

Test overview

- Baseline
- Detection
- Draw boxes
- Labels
- Save anonymized stream
- Save original stream
- Encrypt original stream
- Re-stream anonymized stream
- Blurring
- Blurring + padding

Proof of Concept

Test overview

- Baseline
- Detection
- Draw boxes
- Labels
- Save anonymized stream
- Save original stream
- Encrypt original stream
- Re-stream anonymized stream
- Blurring
- Blurring + padding
- Gaussian blurring

Proof of Concept

Figure 10: Gaussian blurring

Proof of Concept

Test overview

- Baseline
- Detection
- Draw boxes
- Labels
- Save anonymized stream
- Save original stream
- Encrypt original stream
- Re-stream anonymized stream
- Blurring
- Blurring + padding
- Gaussian blurring

Proof of Concept

Test overview

- Baseline
- Detection
- Draw boxes
- Labels
- Save anonymized stream
- Save original stream
- Encrypt original stream
- Re-stream anonymized stream
- Blurring
- Blurring + padding
- Gaussian blurring
- Gaussian blurring + padding

Proof of Concept

Test overview

- Baseline
- Detection
- Draw boxes
- Labels
- Save anonymized stream
- Save original stream
- Encrypt original stream
- Re-stream anonymized stream
- Blurring
- Blurring + padding
- Gaussian blurring
- Gaussian blurring + padding
- Masking

Proof of Concept

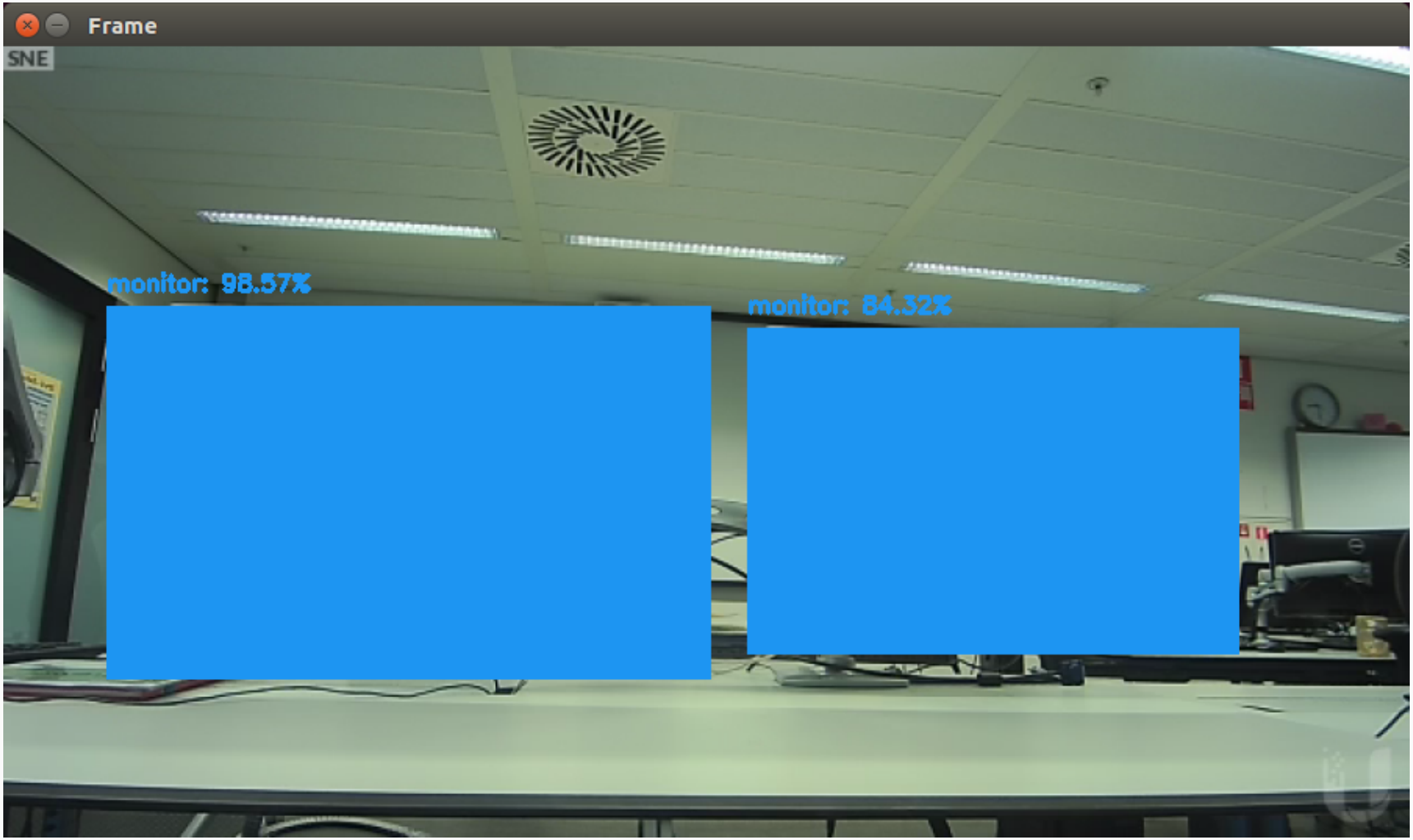


Figure 11: Masking detections

Proof of Concept

Test overview

- Baseline
- Detection
- Draw boxes
- Labels
- Save anonymized stream
- Save original stream
- Encrypt original stream
- Re-stream anonymized stream
- Blurring
- Blurring + padding
- Gaussian blurring
- Gaussian blurring + padding
- Masking

Proof of Concept

Test overview

- Baseline
- Detection
- Draw boxes
- Labels
- Save anonymized stream
- Save original stream
- Encrypt original stream
- Re-stream anonymized stream
- Blurring
- Blurring + padding
- Gaussian blurring
- Gaussian blurring + padding
- Masking
- Masking + padding

Proof of Concept

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Baseline	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Detection		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Drawing boxes			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Labeling				✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Save anonymized stream					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Save original stream						✓	✓	✓	✓	✓	✓	✓	✓	✓
AES Encrypting original stream							✓	✓	✓	✓	✓	✓	✓	✓
Re-stream								✓	✓	✓	✓	✓	✓	✓
Blur									✓	✓				
Blur + padding										✓				
Gaussian blur											✓	✓		
Gaussian blur + padding												✓		
Masking													✓	✓
Masking + padding														✓

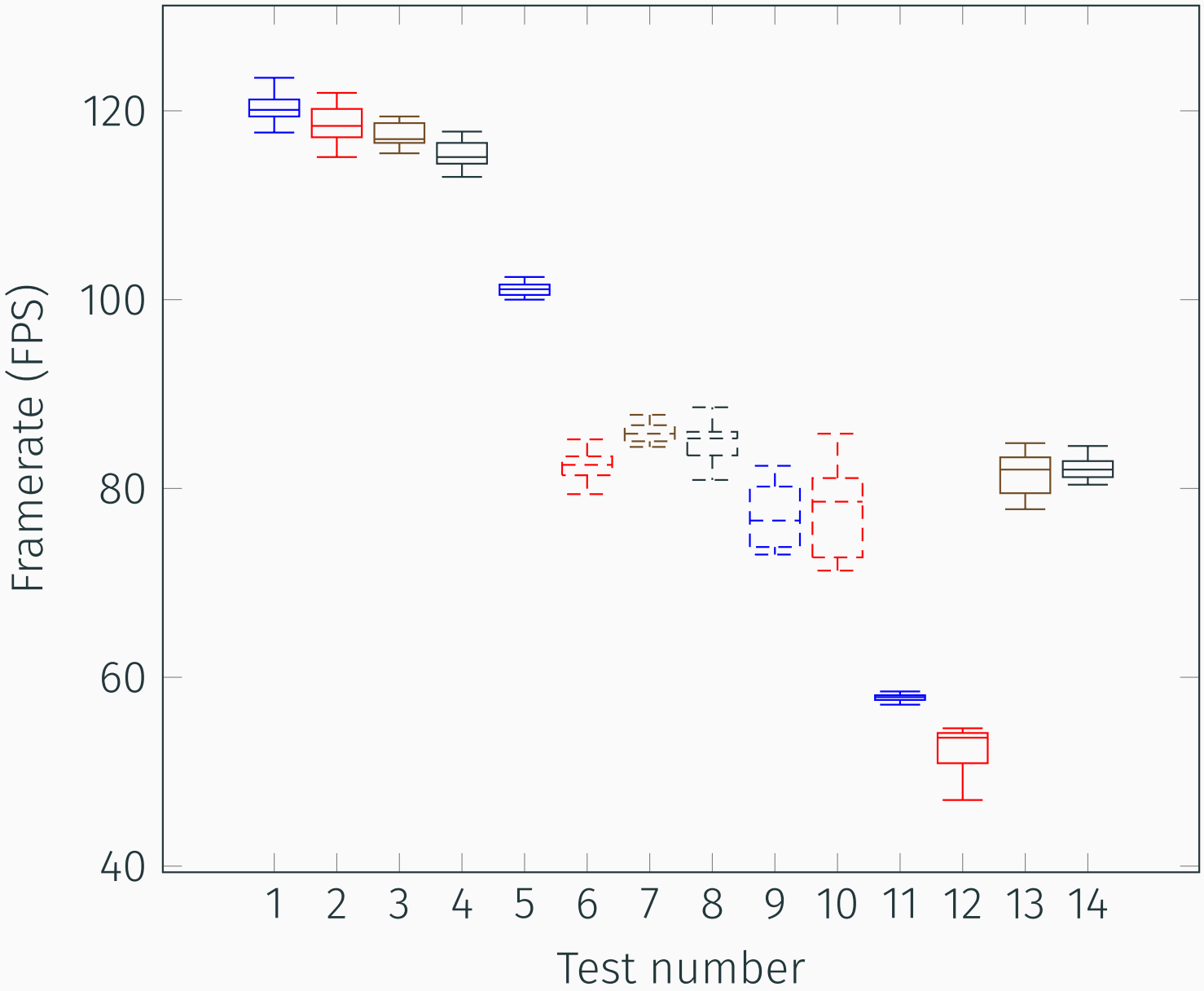
Table 1: Shows how the different tests are constructed

FPS overview

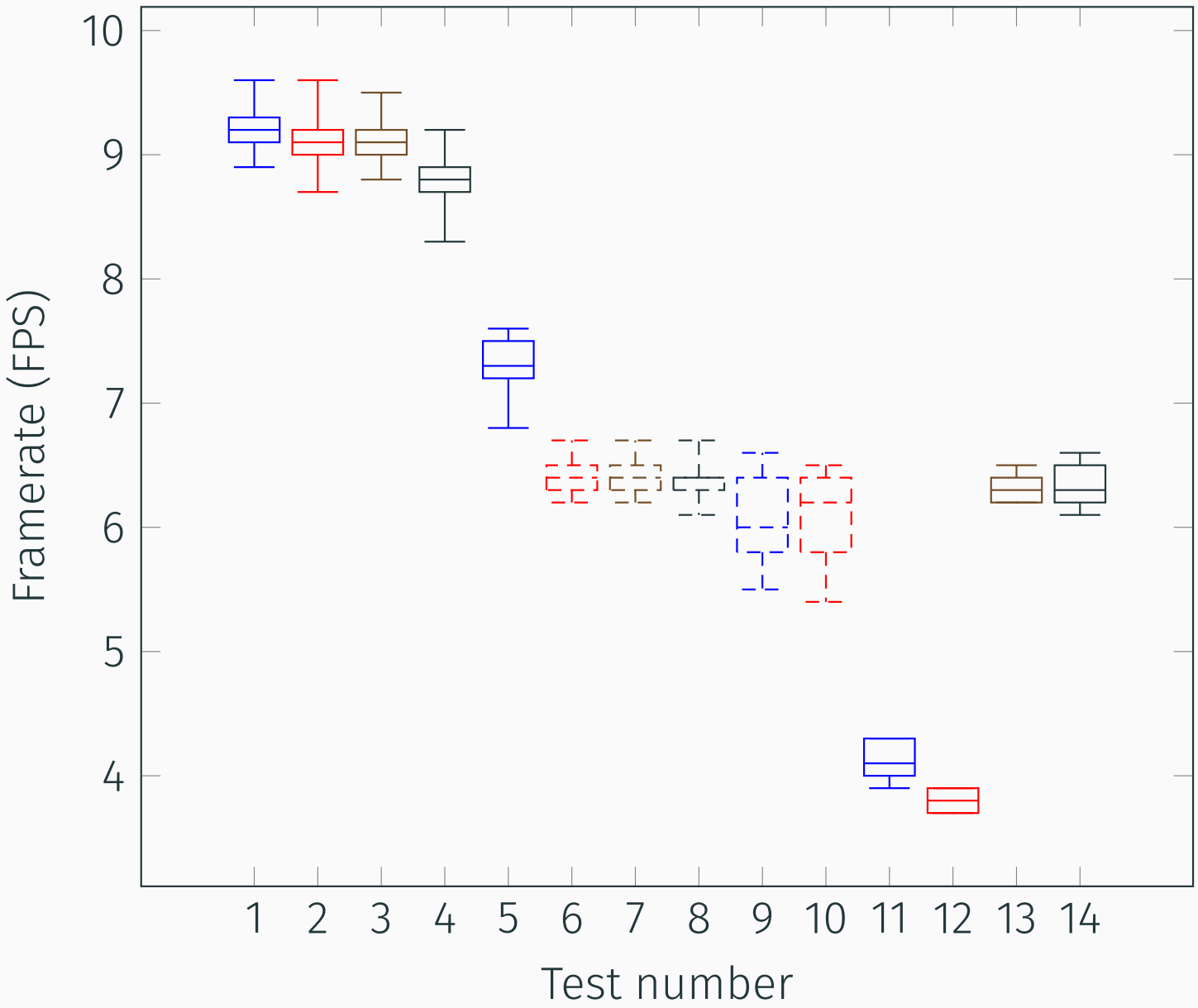
	Dell desktop	Raspberry Pi 3	Atom Server	Atom Laptop
Test 1	120.1	9.2	7.9	3.46
Test 2	118.4	9.1	7.8	3.42
Test 3	117	9.1	7.8	3.45
Test 4	115.1	8.8	7.6	3.42
Test 5	101.1	7.3	6.2	3.06
Test 6	82.5	6.4	5.3	2.91
Test 7	85.8	6.4	5.3	2.92
Test 8	85.3	6.4	5.3	2.96
Test 9	76.6	6.0	5.4	2.87
Test 10	78.6	6.2	5.3	2.82
Test 11	57.9	4.1	4.78	2.5
Test 12	53.6	3.8	4.79	2.58
Test 13	82.0	6.3	5.4	2.88
Test 14	82.0	6.3	5.3	2.91

Table 2: Shows the relation between the baseline measurement and the performance hit in frames per seconds

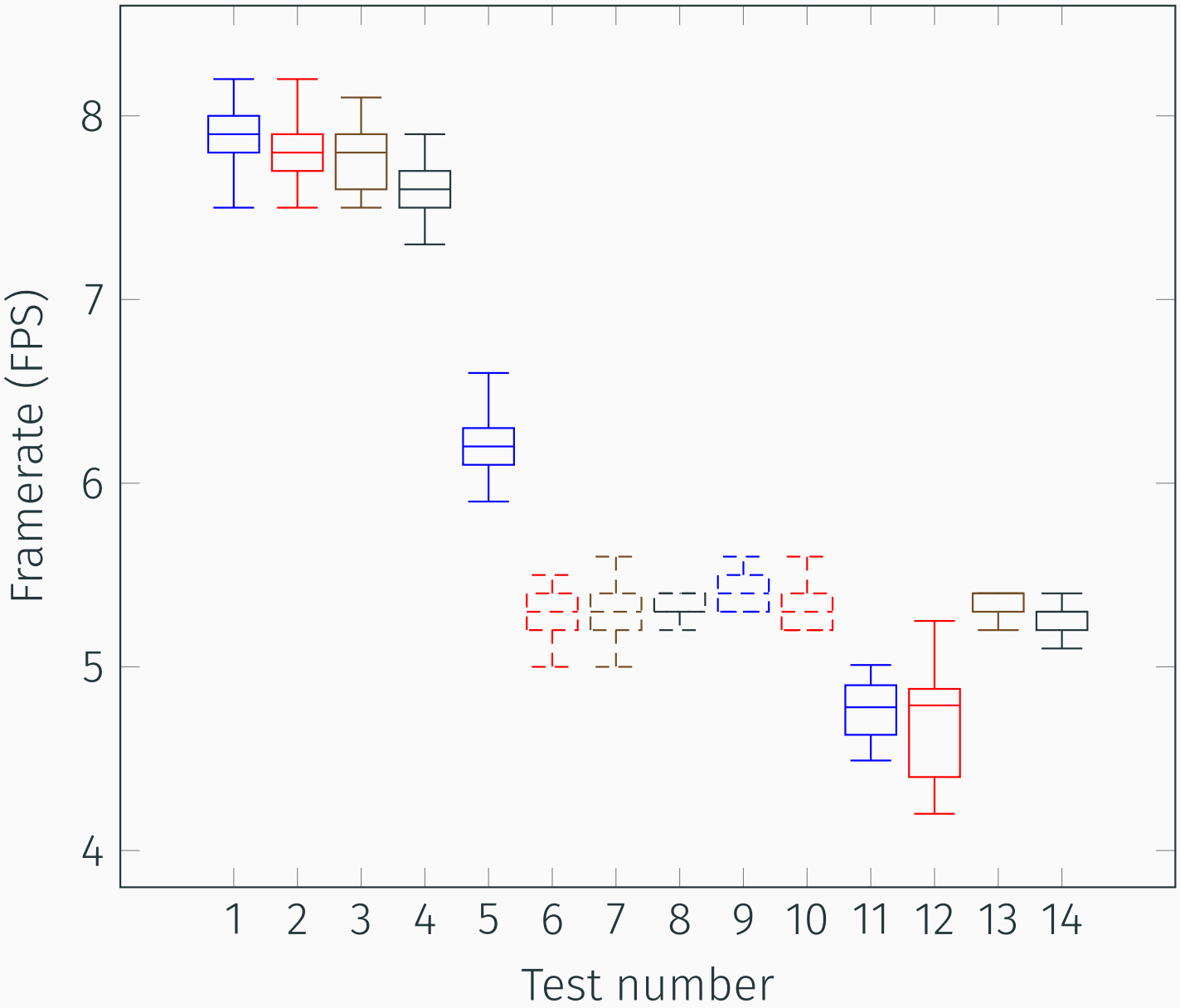
Results Dell Desktop



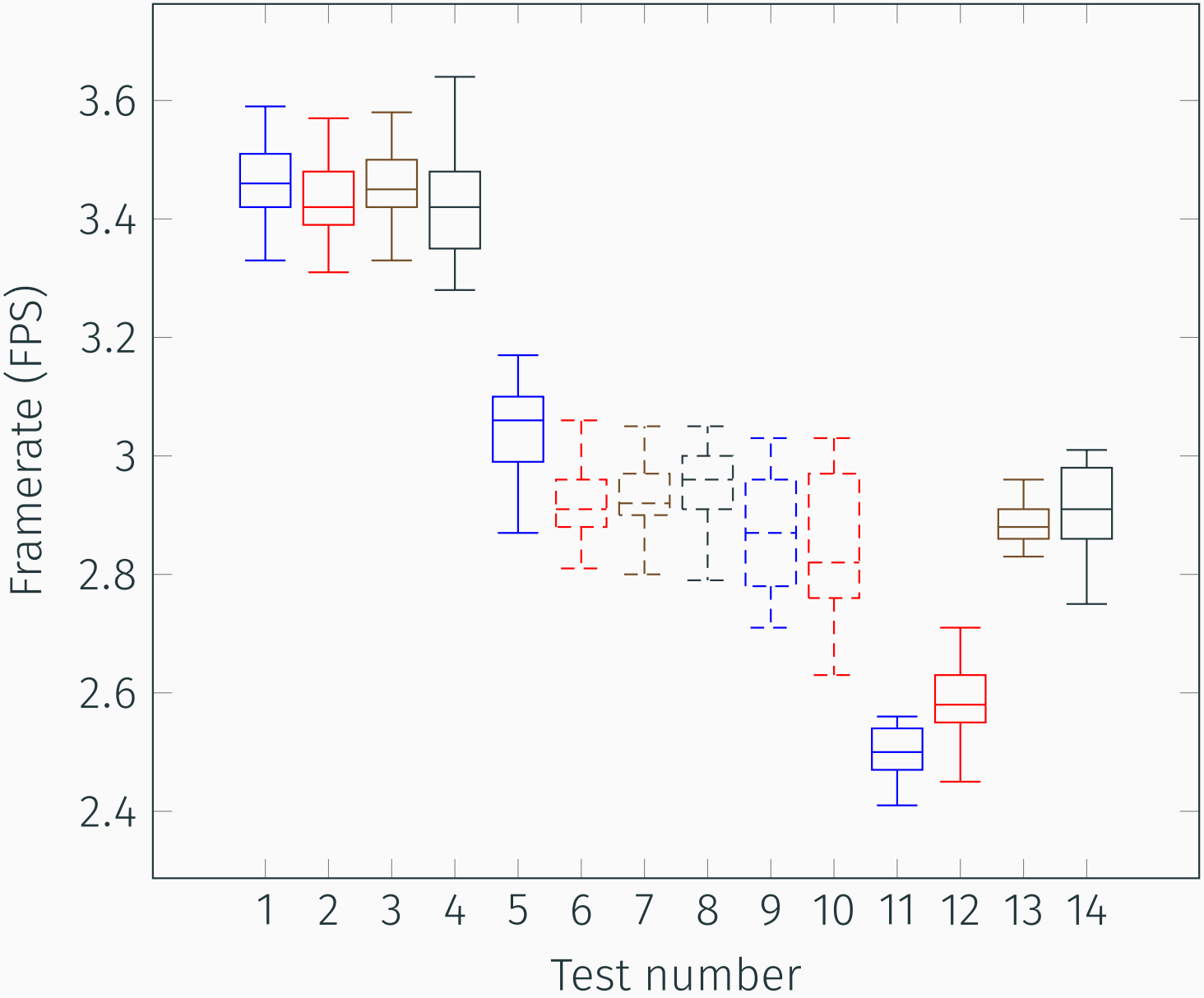
Results Raspberry Pi 3



Results Intel Atom Server



Results Intel Atom laptop



FPS overview (percentage)

	Dell desktop	Raspberry Pi 3	Atom Server	Atom Laptop
Test 1	100%	100%	100%	100%
Test 2	98.58%	98.91%	98.73%	98.84%
Test 3	97.42%	98.91%	98.73%	99.71%
Test 4	95.84%	95.65%	96.20%	98.84%
Test 5	84.18%	79.35%	78.48%	88.44%
Test 6	68.70%	69.56%	67.09%	84.10%
Test 7	71.44%	69.56%	67.09%	84.39%
Test 8	71.02%	69.56%	67.09%	85.55%
Test 9	63.78%	65.22%	68.35%	82.95%
Test 10	65.44%	67.39%	67.09%	81.50%
Test 11	48.21%	44.56%	60.50%	72.25%
Test 12	44.63%	41.30%	60.63%	74.57%
Test 13	68.28%	68.48%	68.35%	83.24%
Test 14	68.28%	68.48%	67.09%	84.10%

Table 3: Shows the relation between the baseline measurement and the performance hit relative to the baseline measurement in percentages

Conclusion & Discussion

Conclusion

How can commodity hardware be used to filter PII from video streams?

Discussion

- Effectiveness anonymization techniques
- Edge detection
- False positives
- False negatives
- Raspberry Pi stability
- Hardware temperatures

Future Work

- Encryption
- Codecs
- Automation
- Distributing & clustering
- Anonymization techniques
- Overclocking the Pi

Questions?

Additional slides

Raspberry Pi setup

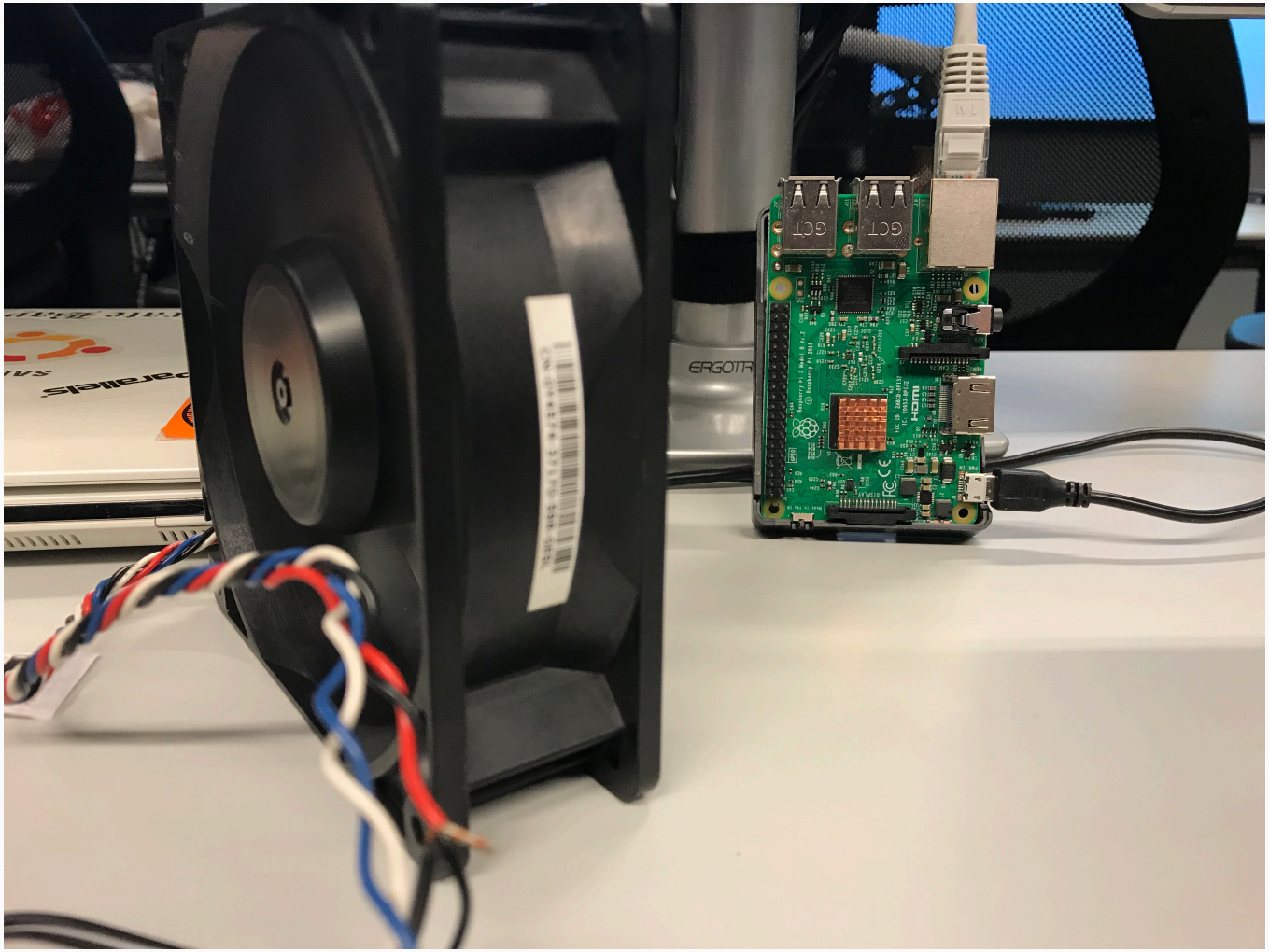


Figure 12: Raspberry Pi cooling issues

Raspberry Pi setup

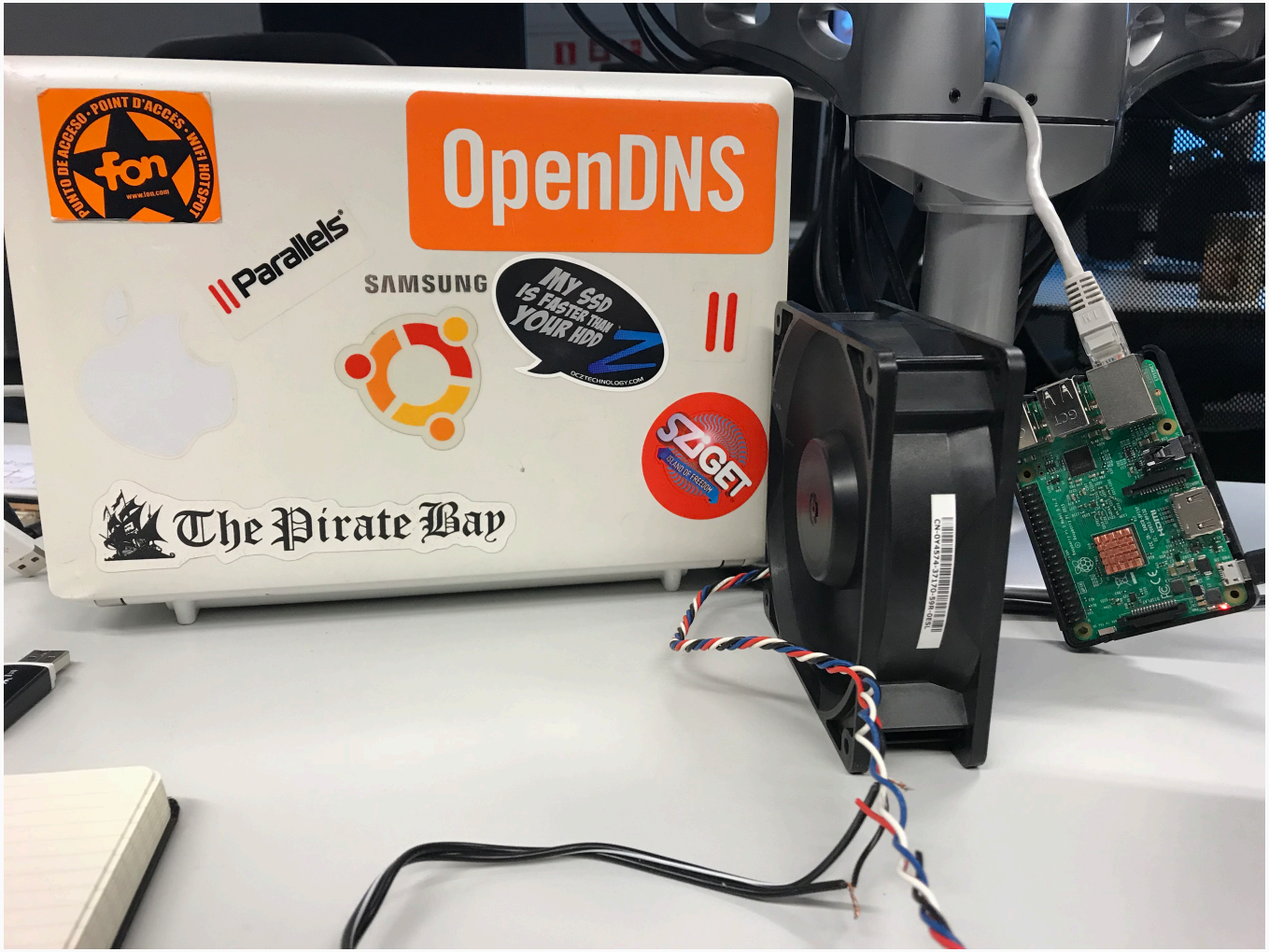


Figure 13: Netbook and Raspberry Pi

DNN Accuracy

Snapshot of iteration 310.000:[2]
Best performance at iteration 313.000
Values at iteration 313.000:

- Validation accuracy: 57,412%
- Loss: 1,82328

Our snapshot:

- Top-1 accuracy: 57,4%
- Top-5 accuracy: 80,4%

[2]Source: Jeff Donahue @jeffdonahue