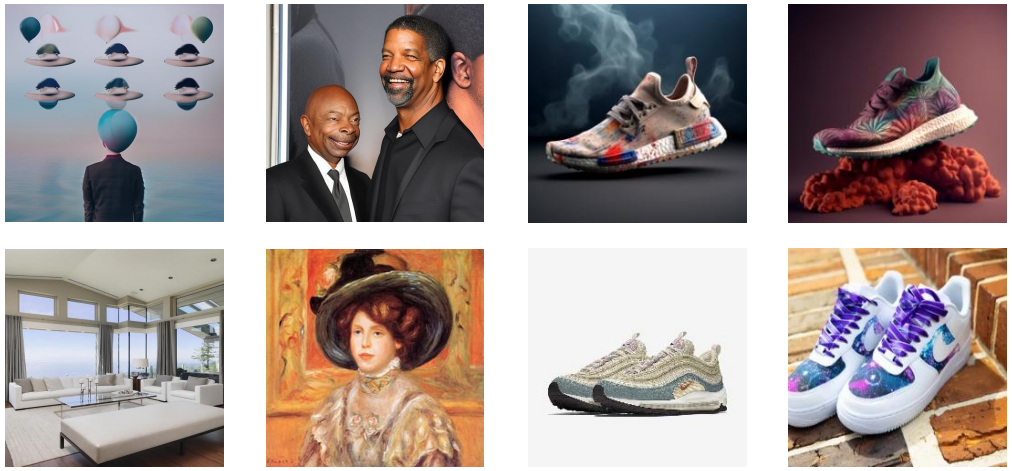
Faculty of Informatics, Mathematics, and Computer Science

Department of Information Systems and Technology

June, 2024

Synthetics Detection

Student: Alex Dadukin



Train split

Test split

Train

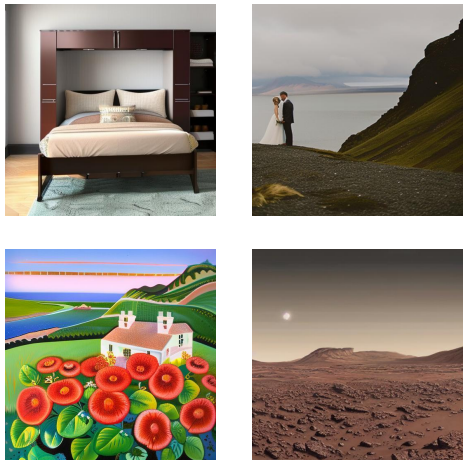
- about 18k images of size **512x512**
- 10k fake, 8k real (1.25:1)

Test

- about 5k images of size **240x240**
- 1.3k fake, 0.8 real (1.625:1)

Classes

- REAL
- FAKE



Fake vs. Real
Q: Can you spot real images?

Train

- There is no clear **visual** difference between fake and real images
- Real images contain drawings (including contemporary art)

Test

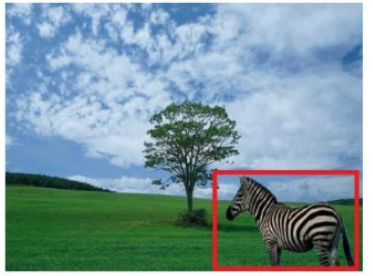
- Images are **4.5 times smaller** (2.3 times along single dimension) then train set
  - Downscaling **train** to **240x240**: potentially, losing important information
  - Upscaling **test** to **512x512**: potentially, adding noise/introducing
- Images are not as diverse as the **train split**
- Real class from both **train and test** have visual distortions which makes objects look less “real”
- Both test and train has slightly different fake to real ratio

Original aspect ratio is not preserved

J. Muindi et. al. Deep Fake Detector: Using ML techniques to Distinguish Real Images From Fakes // Stanford CS230, 2021

N. AlShariah et. al. Detecting Fake Images on Social Media using Machine Learning // IJACSA, 2019

(a) Authentic Image



(b) Fake Image

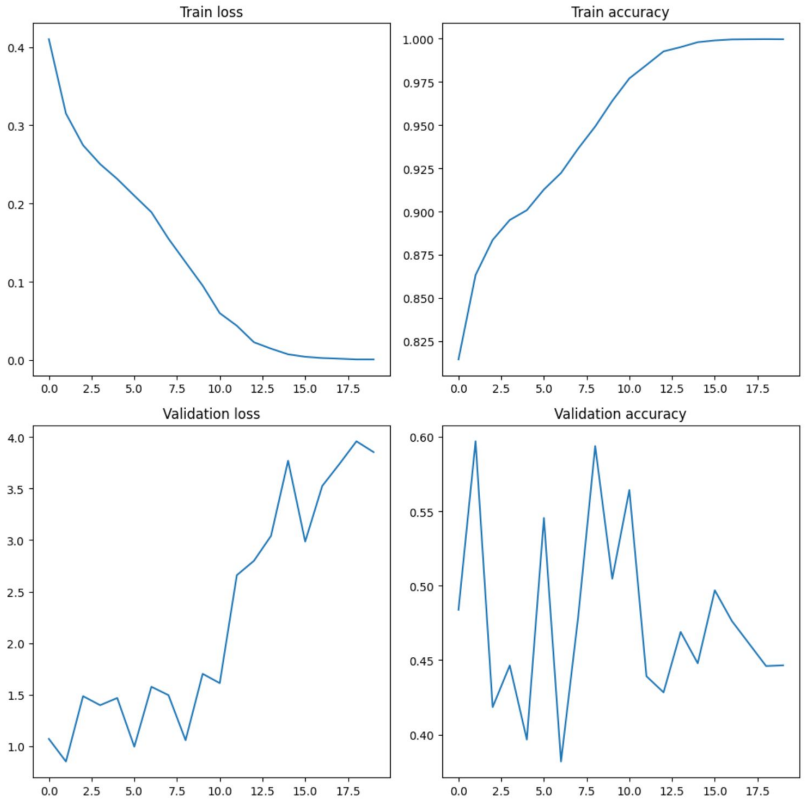
Fakes are defined more broadly: everything that is not a real photo

*"Of the numerous CNN architectures that we tested, we found that the **ResNet** architecture outperformed the others in terms of the dev set accuracy, with DenseNet coming in at a second..."*

Baseline accuracy: **75%**

Model architecture	Accuracy on raw
AlexNet	67%
VGG16	68%
Inception	64%
ResNet	75%
DenseNet	67%

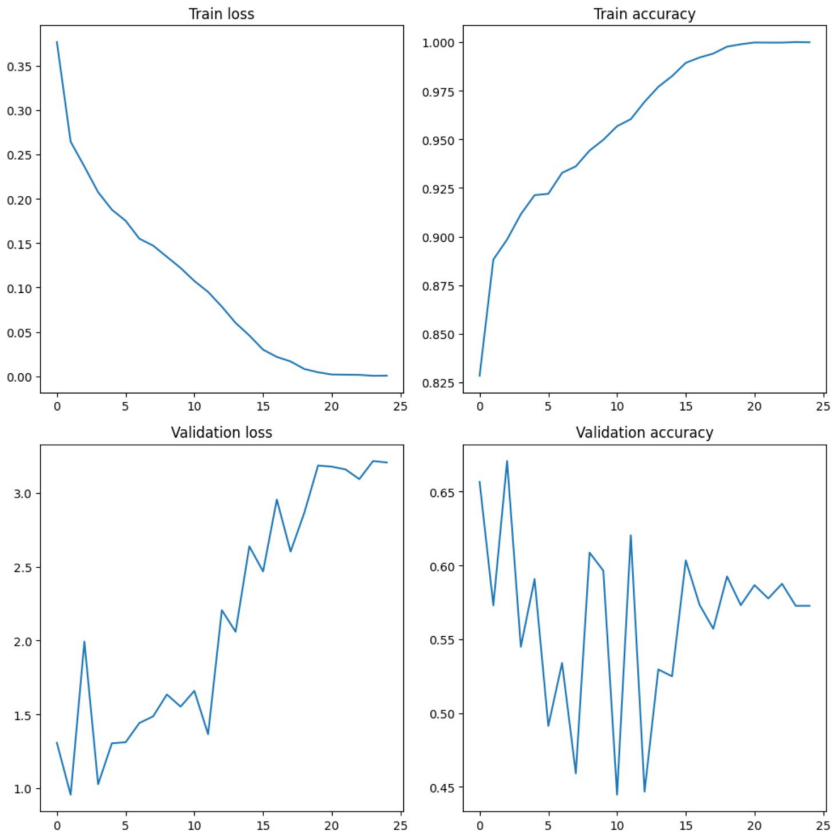
ResNet demonstrated superiority over other models



ResNet 18

- No Weights
- Num Classes: **2**
- Batch Size: **8**
- Gradient Clip: **disabled**
- Weight Decay: **disabled**
- Learning rate: **3e-4**
- Epochs: **20**

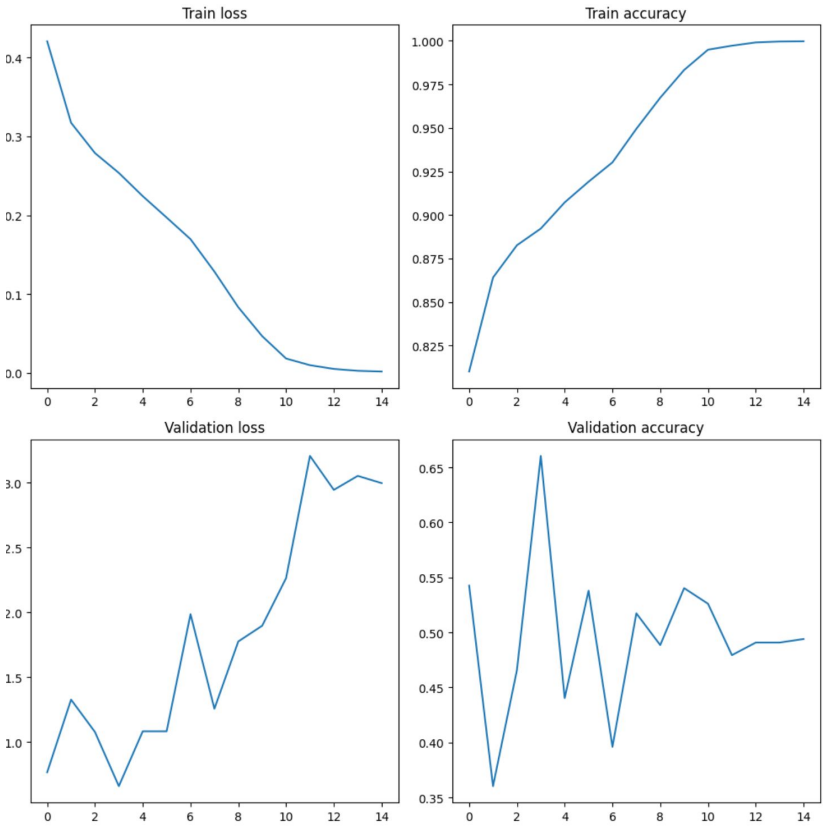
Best Accuracy: **0.60**



ResNet 18 (More batches)

- No Pre-Trained Weights
- Num Classes: **2**
- Batch Size: **32**
- Gradient Clip: **0.1**
- Weight Decay: **0.0003**
- Learning rate: **3e-4**
- Epochs: **25**

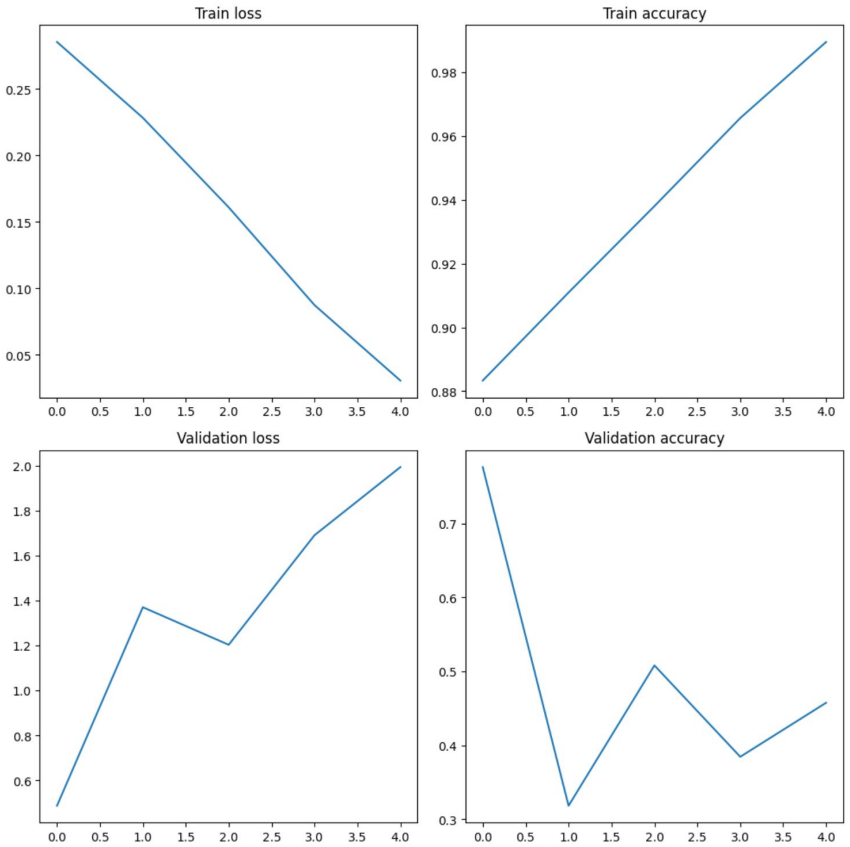
Best Accuracy: **0.67**



ResNet 18 (Balanced classes)

- No Weights
- Num Classes: **2**
- Batch Size: **8**
- Gradient Clip: **disabled**
- Weight Decay: **disabled**
- Learning rate: **3e-4**
- Epochs: **15**

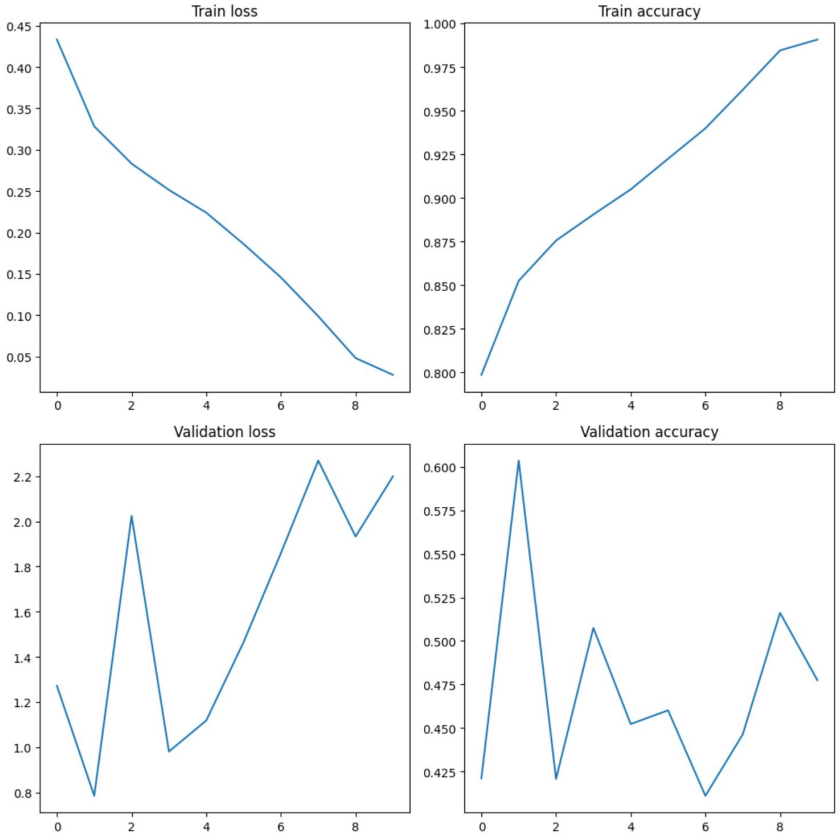
Best Accuracy: **0.66**



ResNet 18 (FT)

- ImageNet Weights (v1)
- Num Classes: **2**
- Batch Size: **8**
- Gradient Clip: **disabled**
- Weight Decay: **disabled**
- Learning rate: **3e-4**
- Epochs: **5**

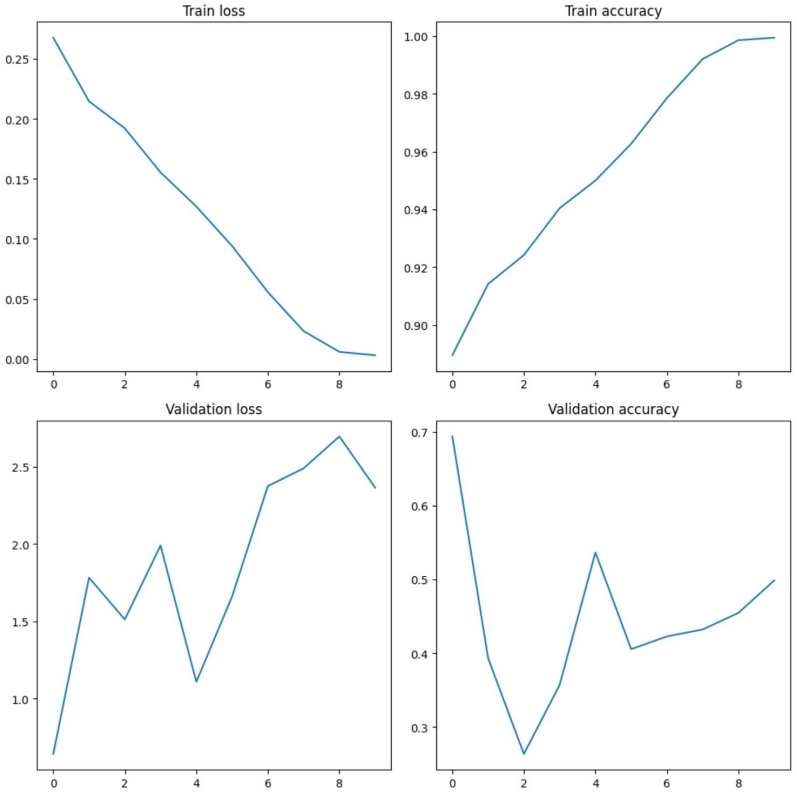
Best Accuracy: **0.78**



ResNet 34

- No Weights
- Num Classes: **2**
- Batch Size: **8**
- Gradient Clip: **disabled**
- Weight Decay: **disabled**
- Learning rate: **3e-4**
- Epochs: **10**

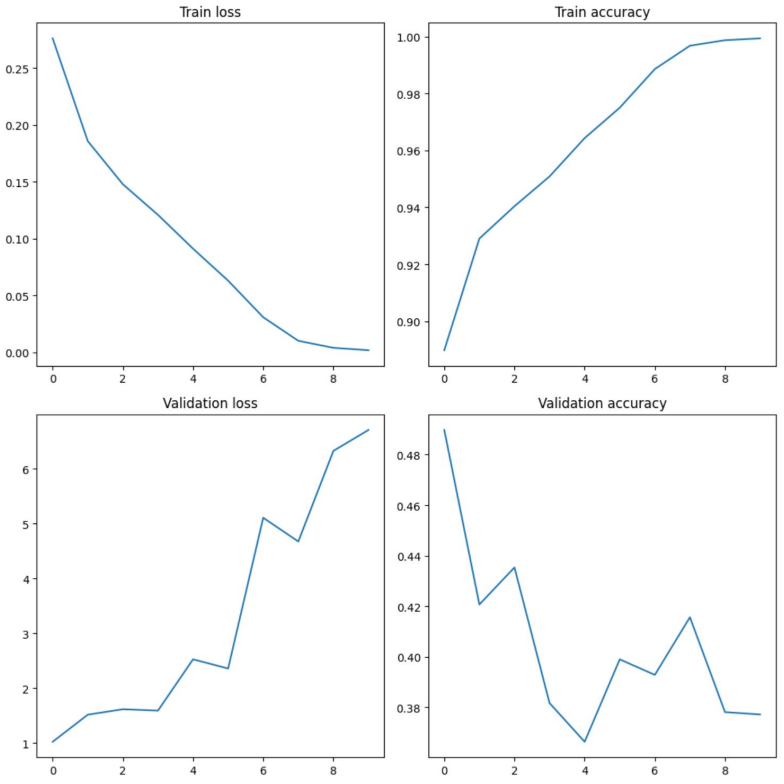
Best Accuracy: **0.60**



ResNet 34 (FT)

- ImageNet Weights
- Num Classes: **2**
- Batch Size: **8**
- Gradient Clip: **disabled**
- Weight Decay: **disabled**
- Learning rate: **3e-4**
- Epochs: **10**

Best Accuracy: **0.69**

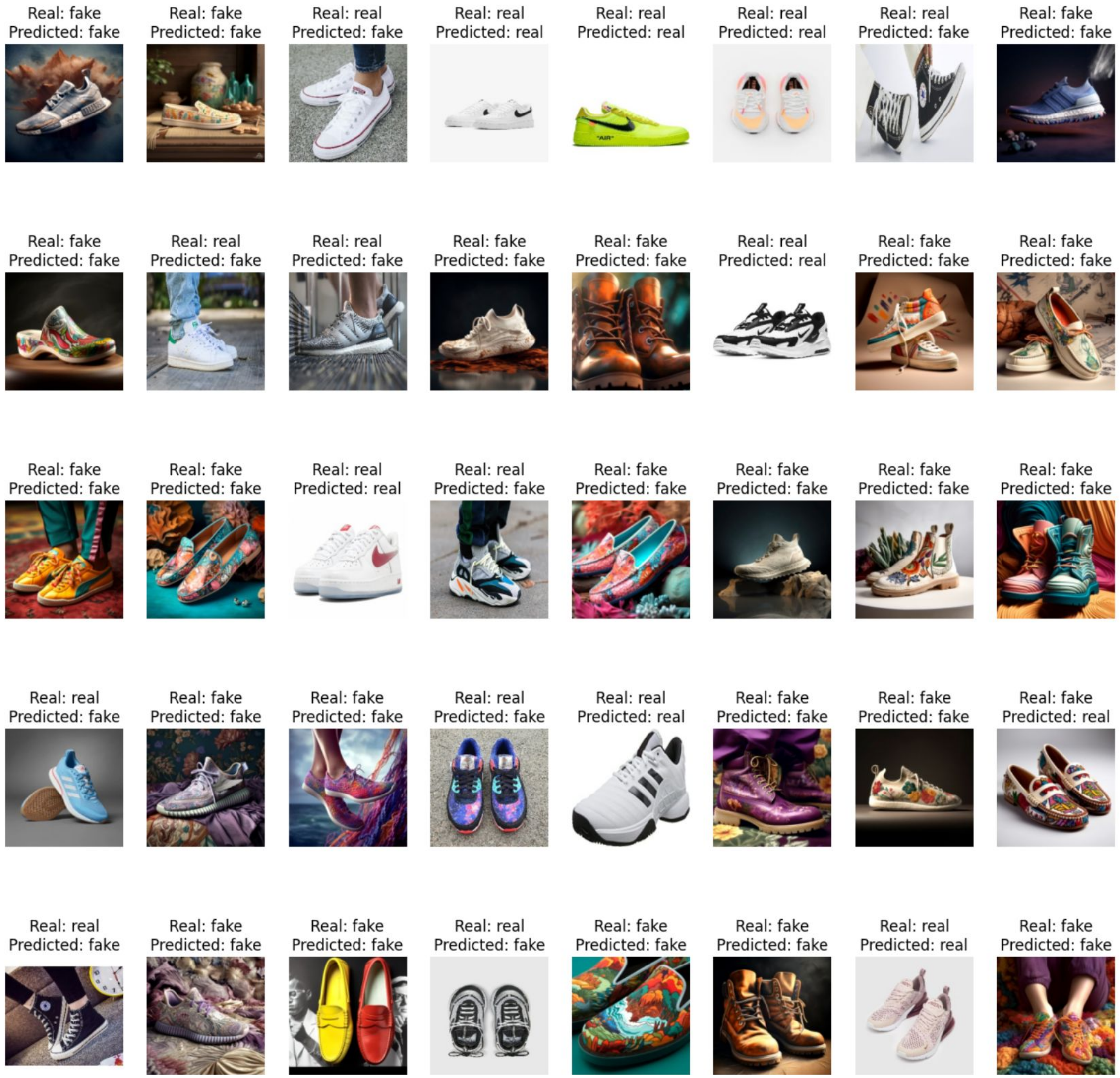


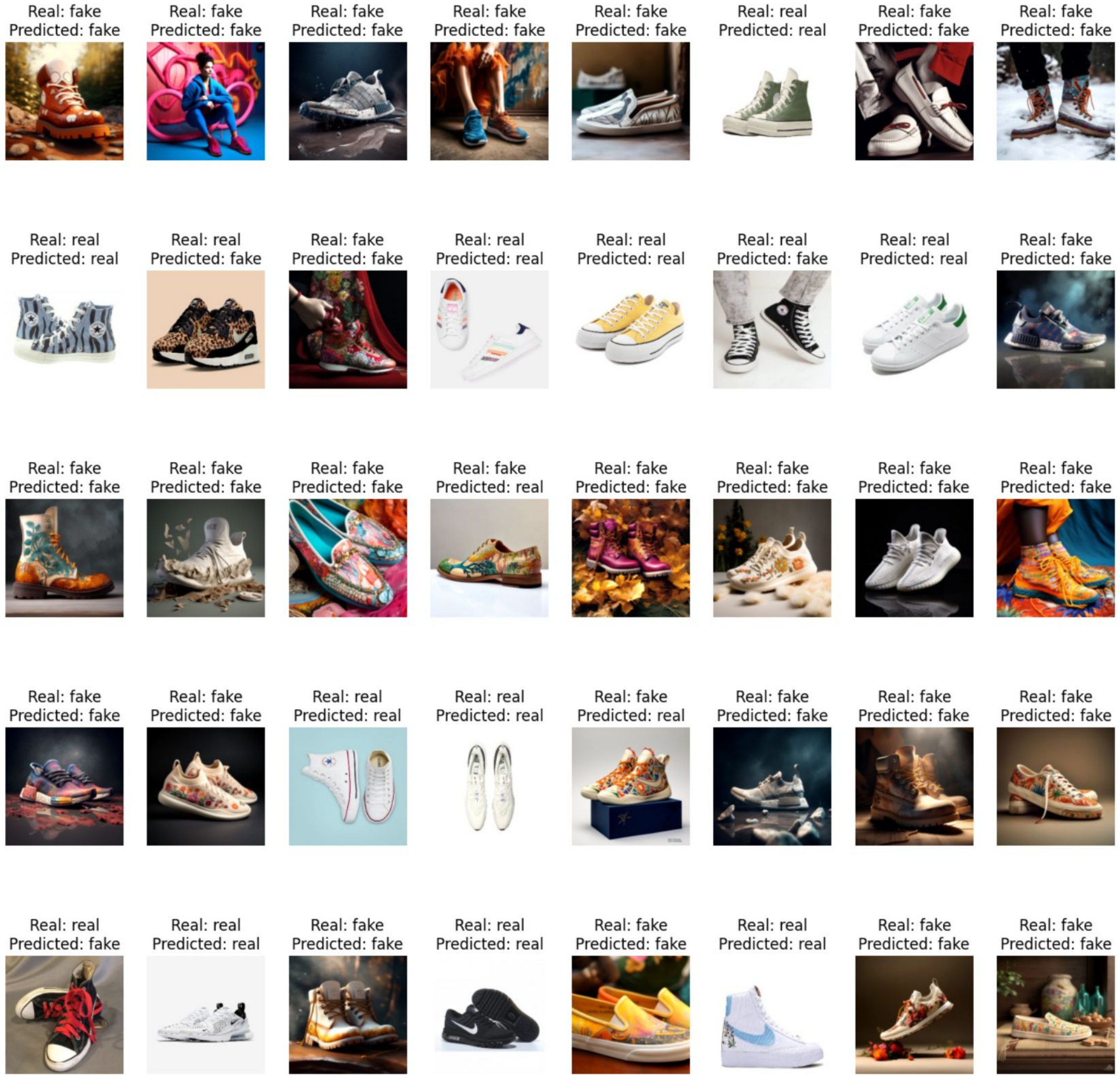
ResNet 50 (FT)

- ImageNet Weights
- Num Classes: **2**
- Batch Size: **8**
- Gradient Clip: **disabled**
- Weight Decay: **disabled**
- Learning rate: **3e-4**
- Epochs: **10**

Best Accuracy: **0.49**

Code


Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: real
Predicted: fake
Real: real
Predicted: real
Real: real
Predicted: real
Real: real
Predicted: real
Real: real
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: real
Predicted: fake
Real: real
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: real
Predicted: real
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: real
Predicted: real
Real: real
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: real
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: real
Predicted: fake
Real: real
Predicted: real
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: real
Real: real
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: real
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: real
Predicted: real
Real: fake
Predicted: fake


Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: real
Predicted: real
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: real
Predicted: real
Real: real
Predicted: fake
Real: fake
Predicted: fake
Real: real
Predicted: real
Real: real
Predicted: real
Real: real
Predicted: fake
Real: real
Predicted: real
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: real
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: real
Predicted: real
Real: real
Predicted: real
Real: fake
Predicted: real
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: fake
Predicted: fake
Real: real
Predicted: fake
Real: real
Predicted: real
Real: fake
Predicted: fake
Real: real
Predicted: real
Real: fake
Predicted: fake
Real: real
Predicted: real
Real: fake
Predicted: fake
Real: fake
Predicted: fake

ResNet ??

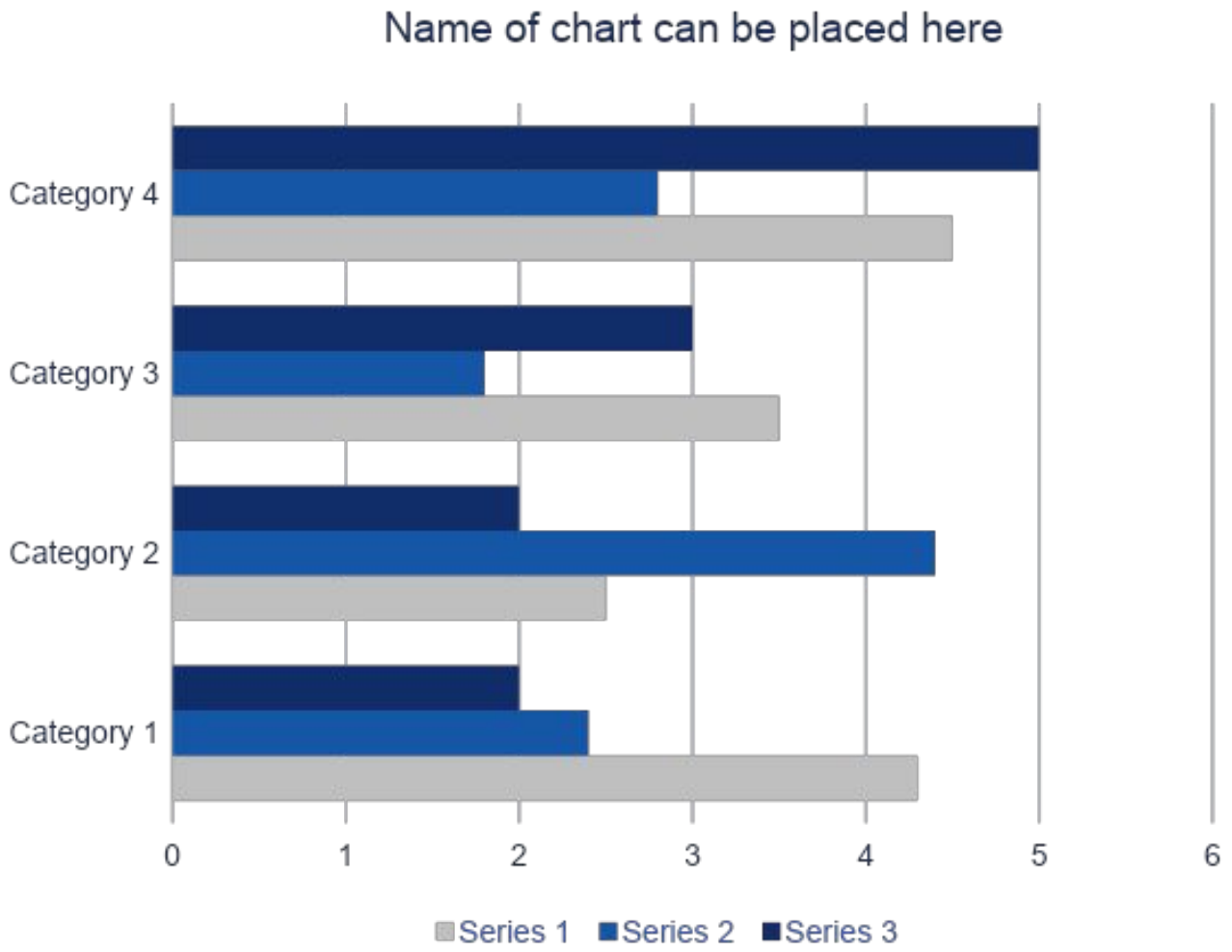
- ?? Weights
- Num Classes: **?**
- Batch Size: **??**
- Learning rate: **???**
- Epochs: **???**

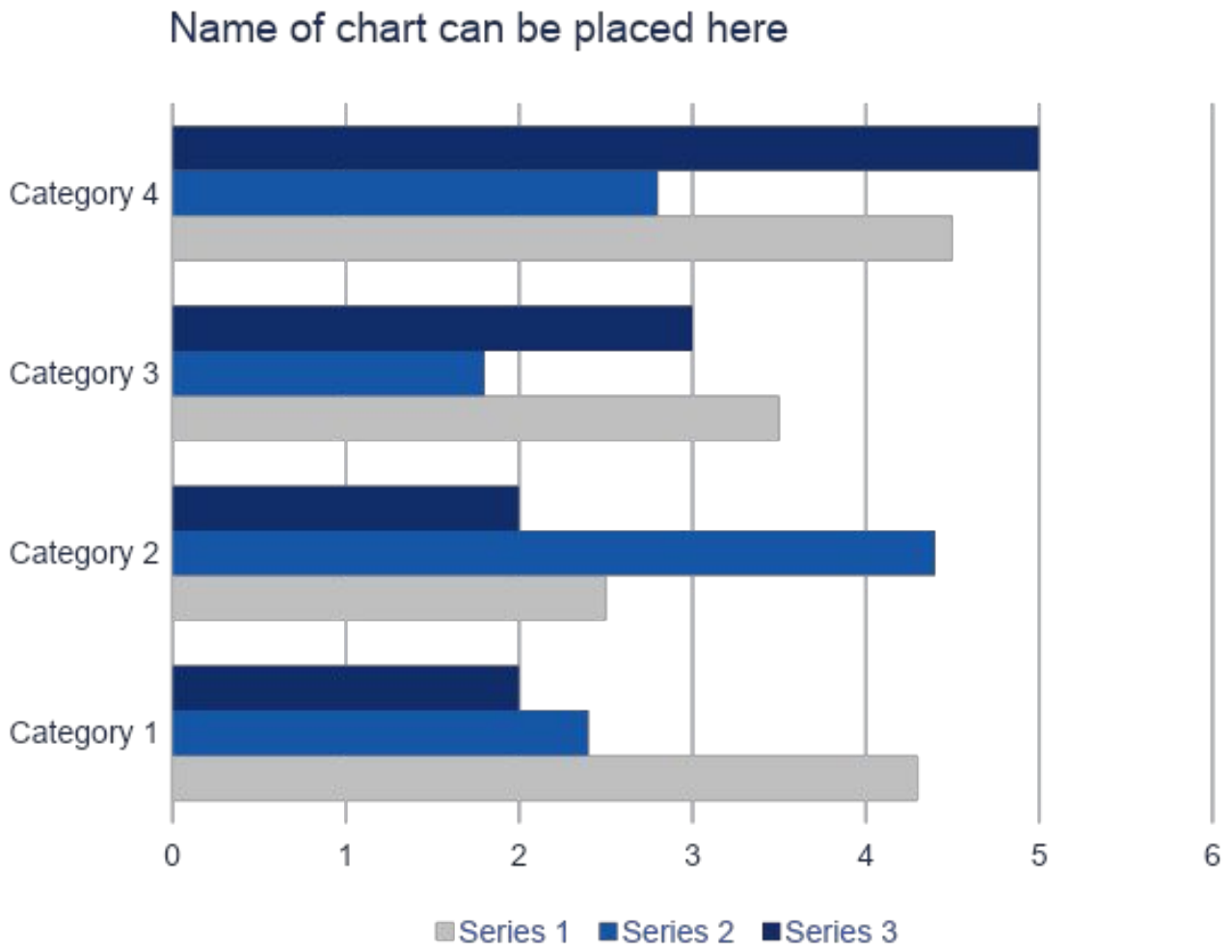
Best Accuracy: **???**

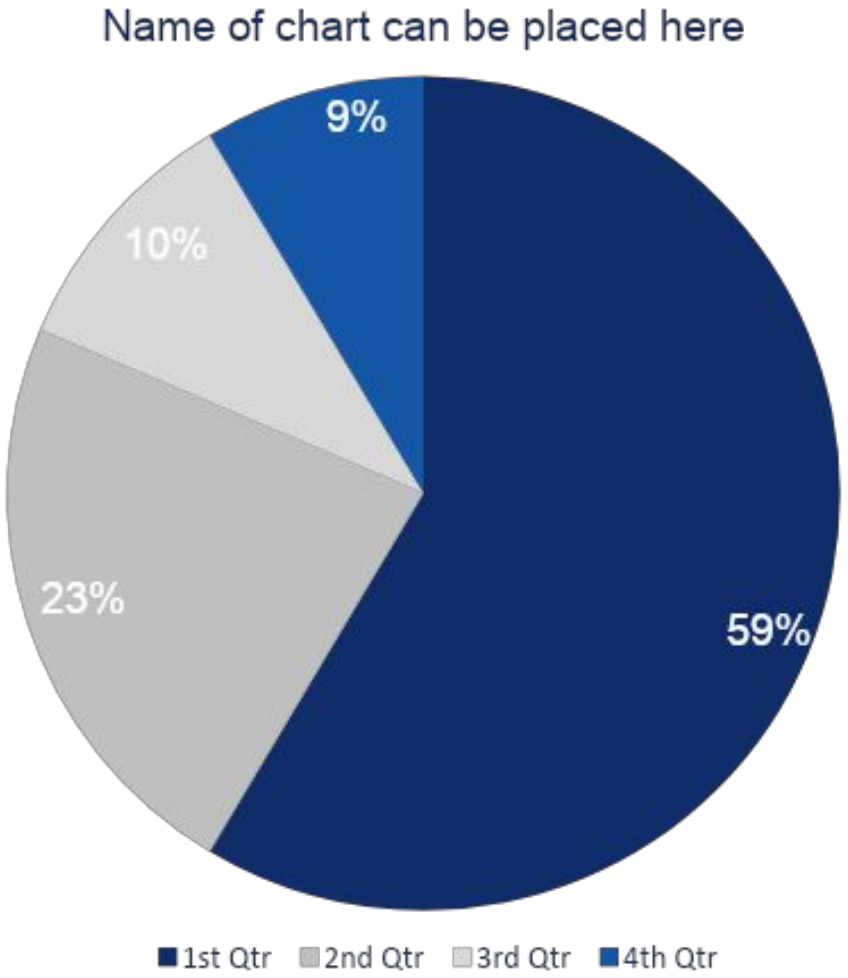
Code

Release 0.9.9: weights + presentation + code


HSE UNIVERSITY
EST 1992

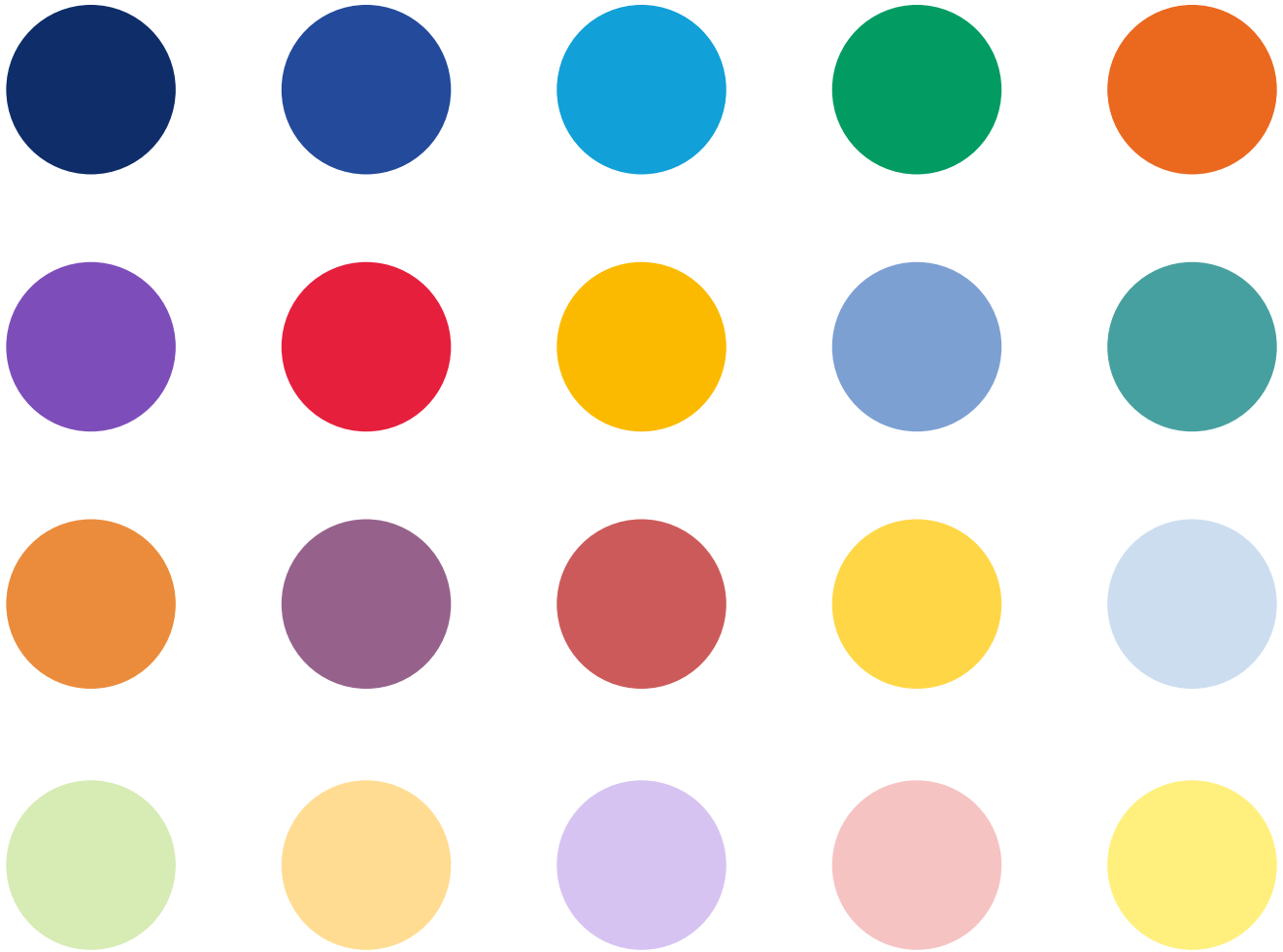

Name of chart can be placed here
Category 4
Category 3
Category 2
Category 1
0
1
2
3
4
5
6
Series 1
Series 2
Series 3

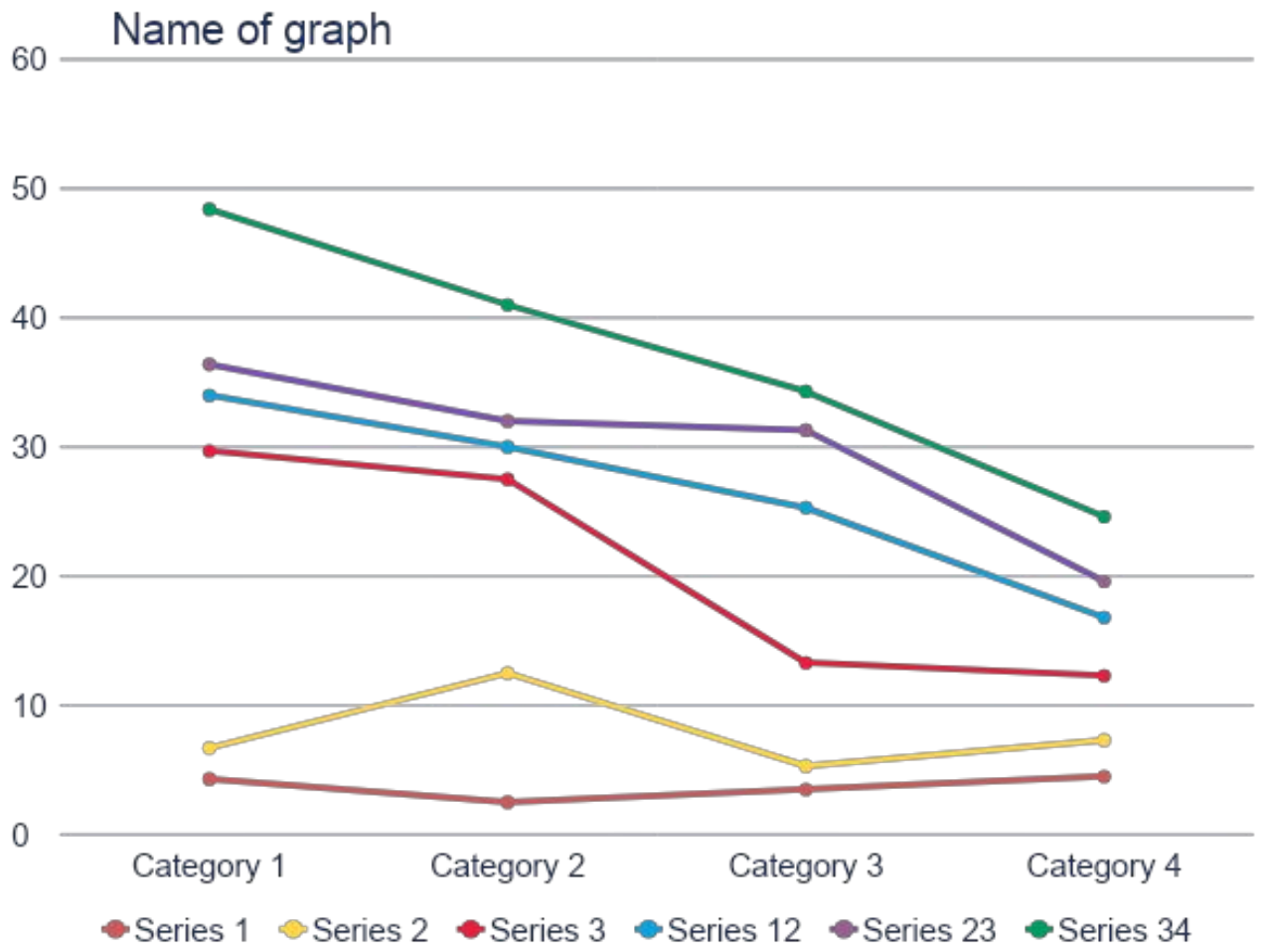

Name of chart can be placed here
Category 4
Category 3
Category 2
Category 1
0
1
2
3
4
5
6
Series 1
Series 2
Series 3

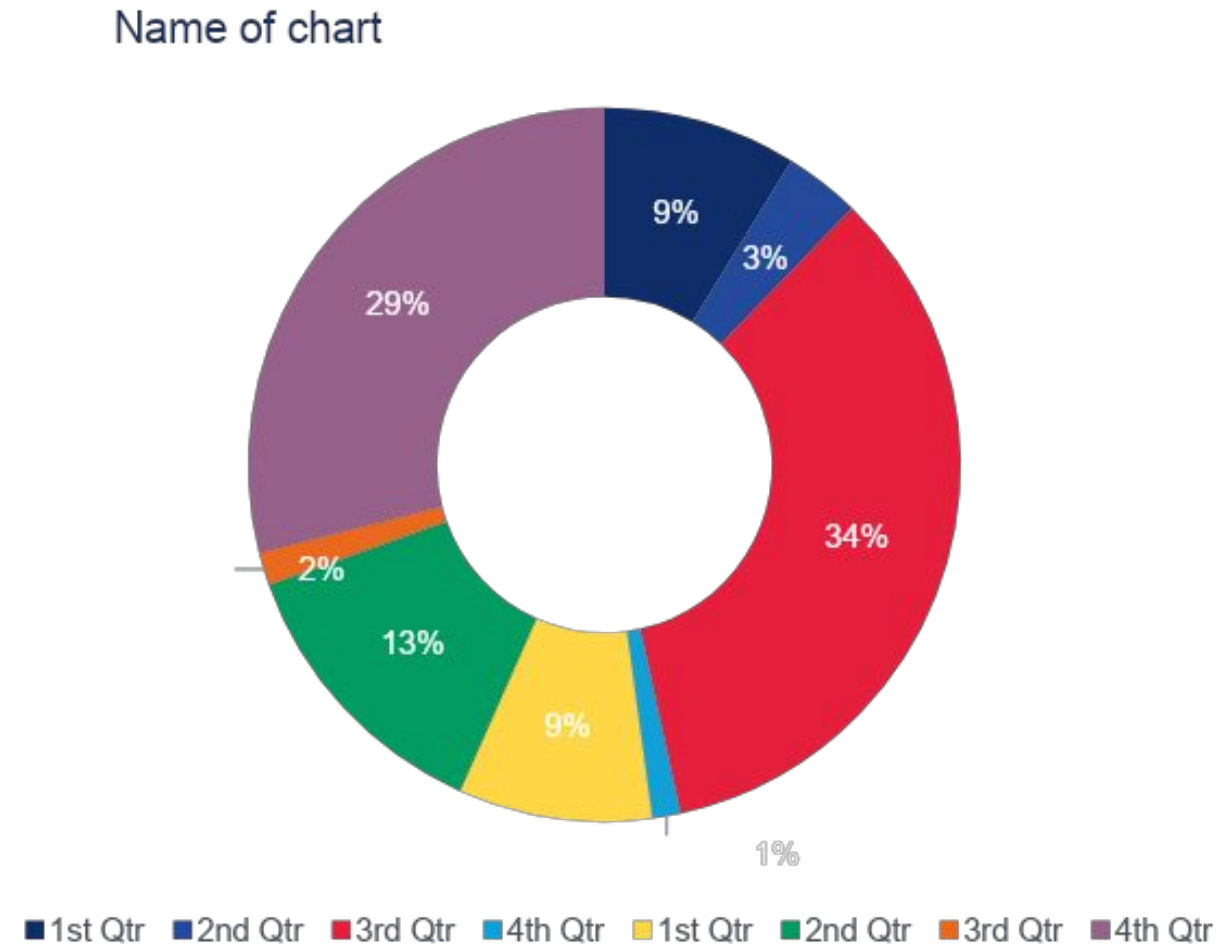

Name of chart can be placed here
9%
10%
23%
59%
1st Qtr
2nd Qtr
3rd Qtr
4th Qtr

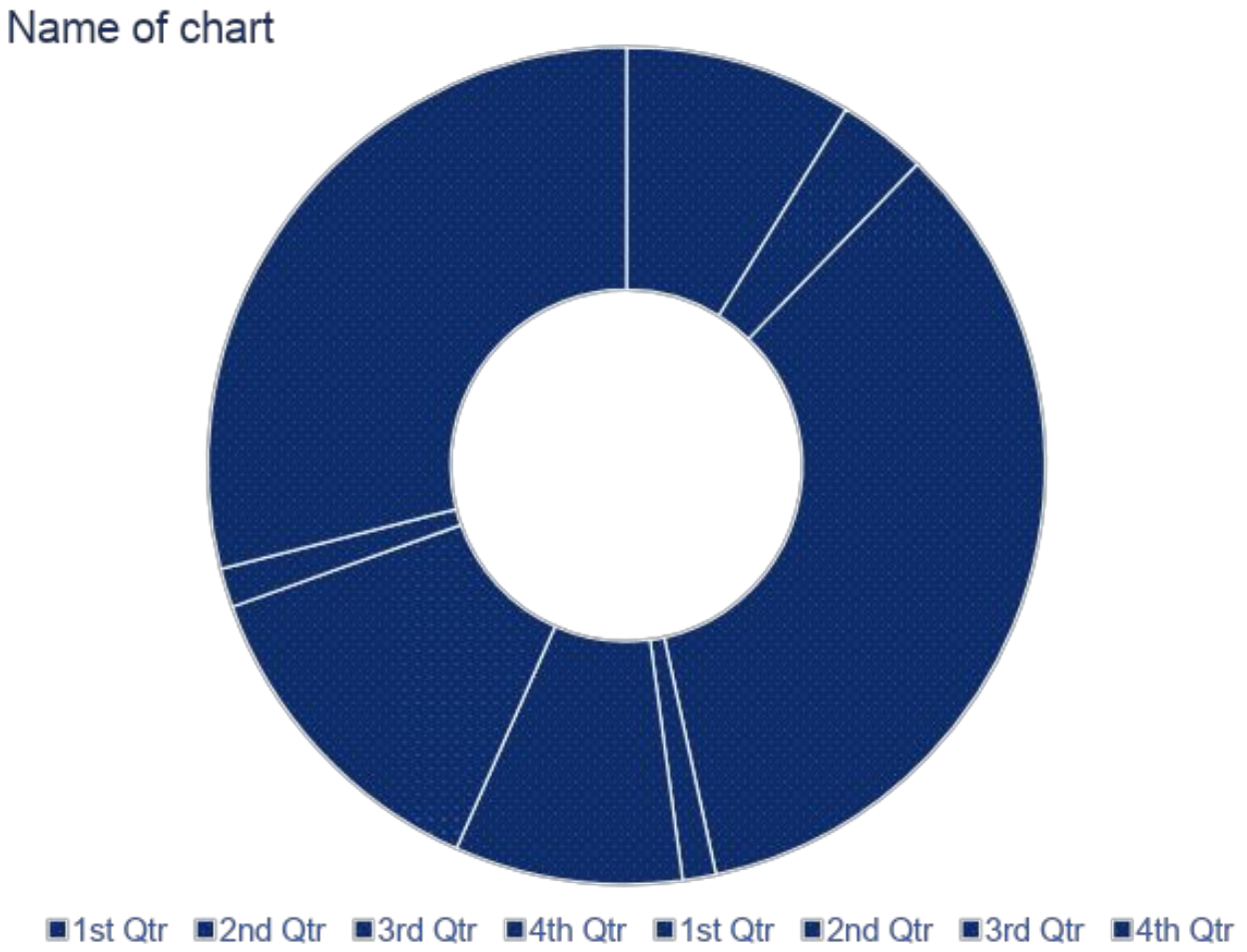
Название столбца	Кооперация	Минимизация	Актуализация	Верификация	Буферизация
Показатели эффективности	12 343 567	3 287 498	34 353	456 578 678	23 424
Еще показатели, но эффективности ли?	345 353	28 764	67 868	909 837 459	900 077
И еще немного показателей	67 868	1 293 090	23 324 213	12 334	34 567
ИТОГО	**63 836 746**	**35 216 735**	**75 984 375**	**3 984 759 835**	**34 785**

Название столбца	Актуализация	Верификация	Буферизация
Показатели эффективности	34 353	456 578 678	23 424
Еще показатели, но эффективности ли?	67 868	909 837 459	900 077
И еще немного показателей	23 324 213	12 334	34 567
ИТОГО	**75 984 375**	**3 984 759 835**	**34 785**




Name of graph
60
50
40
30
20
10
0
Category 1
Category 2
Category 3
Category 4
Series 1
Series 2
Series 3
Series 12
Series 23
Series 34


Name of chart
9%
3%
34%
1%
9%
13%
2%
29%
1st Qtr
2nd Qtr
3rd Qtr
4th Qtr
1st Qtr
2nd Qtr
3rd Qtr
4th Qtr


Name of chart
1st Qtr
2nd Qtr
3rd Qtr
4th Qtr
1st Qtr
2nd Qtr
3rd Qtr
4th Qtr