FeatureImportance_GoldenEye

June 28, 2021

[1]:
```
##############################################################################
# Random Forest Classification Model (TensorFlow)                            #
# Based on the Implementation of:                                            #
# For GoldenEye Dataset                                                      #
# https://www.tensorflow.org/decision_forests/tutorials/beginner_colab       #
##############################################################################
```

[2]:
```
# Installieren aller benötigten Pakete
!pip install pandas
!pip install tensorflow_decision_forests
!pip install wurlitzer
!pip install matplotlib
!pip install ipython
```

```
Requirement already satisfied: pandas in /home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (1.2.5)
Requirement already satisfied: python-dateutil>=2.7.3 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from pandas)
(2.8.1)
Requirement already satisfied: pytz>=2017.3 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from pandas)
(2021.1)
Requirement already satisfied: numpy>=1.16.5 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from pandas)
(1.19.2)
Requirement already satisfied: six>=1.5 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from python-
dateutil>=2.7.3->pandas) (1.15.0)
Requirement already satisfied: tensorflow_decision_forests in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (0.1.7)
Requirement already satisfied: absl-py in /home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow_decision_forests) (0.13.0)
```

```
Requirement already satisfied: tensorflow~=2.5 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow_decision_forests) (2.5.0)
Requirement already satisfied: numpy in /home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow_decision_forests) (1.19.2)
Requirement already satisfied: wheel in /home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow_decision_forests) (0.35.0)
Requirement already satisfied: pandas in /home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow_decision_forests) (1.2.5)
Requirement already satisfied: six in /home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow_decision_forests) (1.15.0)
Requirement already satisfied: gast==0.4.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (0.4.0)
Requirement already satisfied: google-pasta~=0.2 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (0.2.0)
Requirement already satisfied: tensorboard~=2.5 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (2.5.0)
Requirement already satisfied: grpcio~=1.34.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (1.34.1)
Requirement already satisfied: tensorflow-estimator<2.6.0,>=2.5.0rc0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (2.5.0)
Requirement already satisfied: keras-preprocessing~=1.1.2 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (1.1.2)
Requirement already satisfied: termcolor~=1.1.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (1.1.0)
Requirement already satisfied: opt-einsum~=3.3.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (3.3.0)
```

```
Requirement already satisfied: wrapt~=1.12.1 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (1.12.1)
Requirement already satisfied: flatbuffers~=1.12.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (1.12)
Requirement already satisfied: typing-extensions~=3.7.4 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (3.7.4.3)
Requirement already satisfied: astunparse~=1.6.3 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (1.6.3)
Requirement already satisfied: keras-nightly~=2.5.0.dev in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (2.5.0.dev2021032900)
Requirement already satisfied: protobuf>=3.9.2 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (3.17.3)
Requirement already satisfied: h5py~=3.1.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (3.1.0)
Requirement already satisfied: packaging>=20.2 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
wheel->tensorflow_decision_forests) (20.9)
Requirement already satisfied: pytz>=2017.3 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
pandas->tensorflow_decision_forests) (2021.1)
Requirement already satisfied: python-dateutil>=2.7.3 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
pandas->tensorflow_decision_forests) (2.8.1)
Requirement already satisfied: google-auth-oauthlib<0.5,>=0.4.1 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (0.4.4)
Requirement already satisfied: markdown>=2.6.8 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (3.3.4)
```

```
Requirement already satisfied: google-auth<2,>=1.6.3 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (1.32.0)
Requirement already satisfied: setuptools>=41.0.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (44.0.0)
Requirement already satisfied: tensorboard-data-server<0.7.0,>=0.6.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (0.6.1)
Requirement already satisfied: requests<3,>=2.21.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (2.25.1)
Requirement already satisfied: tensorboard-plugin-wit>=1.6.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (1.8.0)
Requirement already satisfied: werkzeug>=0.11.15 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (2.0.1)
Requirement already satisfied: pyparsing>=2.0.2 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
packaging>=20.2->wheel->tensorflow_decision_forests) (2.4.7)
Requirement already satisfied: requests-oauthlib>=0.7.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from google-auth-
oauthlib<0.5,>=0.4.1->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_for
ests) (1.3.0)
Requirement already satisfied: pyasn1-modules>=0.2.1 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from google-
auth<2,>=1.6.3->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests)
(0.2.8)
Requirement already satisfied: cachetools<5.0,>=2.0.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from google-
auth<2,>=1.6.3->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests)
(4.2.2)
Requirement already satisfied: rsa<5,>=3.1.4; python_version >= "3.6" in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from google-
auth<2,>=1.6.3->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests)
(4.7.2)
```

```
Requirement already satisfied: chardet<5,>=3.0.2 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from requests<3,>
=2.21.0->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (4.0.0)
Requirement already satisfied: certifi>=2017.4.17 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from requests<3,>
=2.21.0->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests)
(2021.5.30)
Requirement already satisfied: idna<3,>=2.5 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from requests<3,>
=2.21.0->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (2.10)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from requests<3,>
=2.21.0->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests)
(1.26.6)
Requirement already satisfied: oauthlib>=3.0.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from requests-
oauthlib>=0.7.0->google-auth-oauthlib<0.5,>=0.4.1->tensorboard~=2.5->tensorflow~
=2.5->tensorflow_decision_forests) (3.1.1)
Requirement already satisfied: pyasn1<0.5.0,>=0.4.6 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
pyasn1-modules>=0.2.1->google-
auth<2,>=1.6.3->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests)
(0.4.8)
Requirement already satisfied: wurlitzer in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (2.1.0)
Requirement already satisfied: matplotlib in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (3.4.2)
Requirement already satisfied: cycler>=0.10 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from matplotlib)
(0.10.0)
Requirement already satisfied: kiwisolver>=1.0.1 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from matplotlib)
(1.3.1)
Requirement already satisfied: python-dateutil>=2.7 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from matplotlib)
(2.8.1)
Requirement already satisfied: pyparsing>=2.2.1 in
```

```
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from matplotlib)
(2.4.7)
Requirement already satisfied: numpy>=1.16 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from matplotlib)
(1.19.2)
Requirement already satisfied: pillow>=6.2.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from matplotlib)
(8.2.0)
Requirement already satisfied: six in /home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
cycler>=0.10->matplotlib) (1.15.0)
Collecting ipython
  Using cached ipython-7.25.0-py3-none-any.whl (786 kB)
Collecting jedi>=0.16
  Using cached jedi-0.18.0-py2.py3-none-any.whl (1.4 MB)
Collecting backcall
  Using cached backcall-0.2.0-py2.py3-none-any.whl (11 kB)
Collecting pickleshare
  Using cached pickleshare-0.7.5-py2.py3-none-any.whl (6.9 kB)
Collecting matplotlib-inline
  Using cached matplotlib_inline-0.1.2-py3-none-any.whl (8.2 kB)
Collecting pexpect>4.3; sys_platform != "win32"
  Using cached pexpect-4.8.0-py2.py3-none-any.whl (59 kB)
Collecting decorator
  Using cached decorator-5.0.9-py3-none-any.whl (8.9 kB)
Collecting prompt-toolkit!=3.0.0,!=3.0.1,<3.1.0,>=2.0.0
  Using cached prompt_toolkit-3.0.19-py3-none-any.whl (368 kB)
Collecting traitlets>=4.2
  Using cached traitlets-5.0.5-py3-none-any.whl (100 kB)
Collecting pygments
  Using cached Pygments-2.9.0-py3-none-any.whl (1.0 MB)
Requirement already satisfied: setuptools>=18.5 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from ipython)
(44.0.0)
Collecting parso<0.9.0,>=0.8.0
  Using cached parso-0.8.2-py2.py3-none-any.whl (94 kB)
Collecting ptyprocess>=0.5
  Using cached ptyprocess-0.7.0-py2.py3-none-any.whl (13 kB)
Collecting wcwidth
  Using cached wcwidth-0.2.5-py2.py3-none-any.whl (30 kB)
Collecting ipython-genutils
  Using cached ipython_genutils-0.2.0-py2.py3-none-any.whl (26 kB)
Installing collected packages: parso, jedi, backcall, pickleshare, ipython-
genutils, traitlets, matplotlib-inline, ptyprocess, pexpect, decorator, wcwidth,
```

```
prompt-toolkit, pygments, ipython
Successfully installed backcall-0.2.0 decorator-5.0.9 ipython-7.25.0 ipython-
genutils-0.2.0 jedi-0.18.0 matplotlib-inline-0.1.2 parso-0.8.2 pexpect-4.8.0
pickleshare-0.7.5 prompt-toolkit-3.0.19 ptyprocess-0.7.0 pygments-2.9.0
traitlets-5.0.5 wcwidth-0.2.5
```

[3]:
```python
# Laden der benötigten Python Pakete
import pandas as pd
import numpy as np
import tensorflow_decision_forests as tfdf
from wurlitzer import sys_pipes
import matplotlib.pyplot as plt
```

[4]:
```python
# Prüfung der installierten TensorFlow Decision Forests Version
print(f"Found TensorFlow Decision Forests v{tfdf.__version__}")
```

```
Found TensorFlow Decision Forests v0.1.7
```

[5]:
```python
# Laden der Netzwerk Traffic Daten für den GoldenEye Angriff
data_GoldenEye = pd.read_csv('../Data/Optimized/
 ↪Thursday-15-02-2018_GoldenEye-Attack.csv')
```

[6]:
```python
# Suchen und Ersetzen von NaN Werten im Dataset
nan_count = data_GoldenEye.isna().sum().sum()
print(f"Initial Count of NaN in Dataset: {nan_count}")

data_GoldenEye = data_GoldenEye.replace([np.inf, -np.inf], np.nan)
data_GoldenEye = data_GoldenEye.interpolate()

nan_count = data_GoldenEye.isna().sum().sum()
print(f"Count of NaN in Dataset after Cleanse: {nan_count}")
```

```
Initial Count of NaN in Dataset: 4921
Count of NaN in Dataset after Cleanse: 0
```

[7]:
```python
# Festlegen des Wertes der bestimmten Variable
label = 'label'
```

[8]:
```python
# Aufteilen des Datasets in Training- und Test-Daten
def split_dataset(dataset,  test_ratio=0.30):
    """Splits a panda dataframe in two dataframes."""
    test_indices = np.random.rand(len(dataset)) < test_ratio
    return dataset[~test_indices], dataset[test_indices]

training_data_GoldenEye, testing_data_GoldenEye = split_dataset(data_GoldenEye)

print("{} examples in training, {} examples for testing.".format(
    len(training_data_GoldenEye), len(testing_data_GoldenEye)))
```

```
726480 examples in training, 311105 examples for testing.
```

[9]:
```
# Konvertieren des Panda Dataframes in ein TensorFlow Dataset
print("Converting Panda Dataframe into TensorFlow Dataset...")
training_dataset_GoldenEye = tfdf.keras.
 ↪pd_dataframe_to_tf_dataset(training_data_GoldenEye, label=label)
testing_dataset_GoldenEye = tfdf.keras.
 ↪pd_dataframe_to_tf_dataset(testing_data_GoldenEye, label=label)
```

```
Converting Panda Dataframe into TensorFlow Dataset…
```

[10]:
```
# Erstellen des Random Forest Modells
model = tfdf.keras.RandomForestModel()
model.compile(metrics=["accuracy"])
```

[11]:
```
# Trainieren des Modells
print("Training the Model: ")
with sys_pipes():
    model.fit(x=training_dataset_GoldenEye)
```

```
Training the Model:
2021-06-28 14:57:03.047266: I
tensorflow/compiler/mlir/mlir_graph_optimization_pass.cc:176] None of the MLIR
Optimization Passes are enabled (registered 2)
2021-06-28 14:57:03.079364: I
tensorflow/core/platform/profile_utils/cpu_utils.cc:114] CPU Frequency:
2199995000 Hz
11352/11352 [==============================] - 68s 6ms/step
[INFO kernel.cc:746] Start Yggdrasil model training
[INFO kernel.cc:747] Collect training examples
[INFO kernel.cc:392] Number of batches: 11352
[INFO kernel.cc:393] Number of examples: 726480
[INFO data_spec_inference.cc:289] 31744 item(s) have been pruned (i.e. they are
considered out of dictionary) for the column timestamp (2000 item(s) left)
because min_value_count=5 and max_number_of_unique_values=2000
[INFO kernel.cc:769] Dataset:
Number of records: 726480
Number of columns: 80

Number of columns by type:
        NUMERICAL: 78 (97.5%)
        CATEGORICAL: 2 (2.5%)

Columns:

NUMERICAL: 78 (97.5%)
        0: "ack_flag_cnt" NUMERICAL mean:0.285002 min:0 max:1 sd:0.451415
        1: "active_max" NUMERICAL mean:148222 min:0 max:1.11992e+08
```

```
sd:1.07137e+06
        2: "active_mean" NUMERICAL mean:84931.5 min:0 max:1.11992e+08 sd:814317
        3: "active_min" NUMERICAL mean:62469.4 min:0 max:1.11992e+08 sd:768439
        4: "active_std" NUMERICAL mean:39071.8 min:0 max:5.86304e+07 sd:347667
        5: "bwd_blk_rate_avg" NUMERICAL mean:0 min:0 max:0 sd:0
        6: "bwd_byts/b_avg" NUMERICAL mean:0 min:0 max:0 sd:0
        7: "bwd_header_len" NUMERICAL mean:135.199 min:0 max:383632 sd:1967.65
        8: "bwd_iat_max" NUMERICAL mean:3.10959e+06 min:0 max:1.19913e+08
sd:1.08092e+07
        9: "bwd_iat_mean" NUMERICAL mean:942709 min:0 max:1.19913e+08
sd:4.0715e+06
        10: "bwd_iat_min" NUMERICAL mean:270331 min:0 max:1.19913e+08
sd:3.49435e+06
        11: "bwd_iat_std" NUMERICAL mean:1.0444e+06 min:0 max:8.45025e+07
sd:3.54535e+06
        12: "bwd_iat_tot" NUMERICAL mean:9.39539e+06 min:0 max:1.2e+08
sd:2.84657e+07
        13: "bwd_pkt_len_max" NUMERICAL mean:333.842 min:0 max:2708 sd:495.132
        14: "bwd_pkt_len_mean" NUMERICAL mean:121.775 min:0 max:1457.94
sd:185.713
        15: "bwd_pkt_len_min" NUMERICAL mean:34.0133 min:0 max:1176 sd:55.8469
        16: "bwd_pkt_len_std" NUMERICAL mean:121.651 min:0 max:1329.36
sd:207.433
        17: "bwd_pkts/b_avg" NUMERICAL mean:0 min:0 max:0 sd:0
        18: "bwd_pkts/s" NUMERICAL mean:3357.56 min:0 max:2e+06 sd:42159.1
        19: "bwd_psh_flags" NUMERICAL mean:0 min:0 max:0 sd:0
        20: "bwd_seg_size_avg" NUMERICAL mean:121.775 min:0 max:1457.94
sd:185.713
        21: "bwd_urg_flags" NUMERICAL mean:0 min:0 max:0 sd:0
        22: "cwe_flag_count" NUMERICAL mean:0 min:0 max:0 sd:0
        23: "down/up_ratio" NUMERICAL mean:0.579061 min:0 max:126 sd:0.746608
        24: "dst_port" NUMERICAL mean:7485.54 min:0 max:65534 sd:17631.4
        25: "ece_flag_cnt" NUMERICAL mean:0.0613492 min:0 max:1 sd:0.23997
        26: "fin_flag_cnt" NUMERICAL mean:0.00579369 min:0 max:1 sd:0.0758955
        27: "flow_byts/s" NUMERICAL mean:433861 min:0 max:1.2985e+09
sd:5.41791e+06
        28: "flow_duration" NUMERICAL mean:1.36669e+07 min:0 max:1.2e+08
sd:3.25844e+07
        29: "flow_iat_max" NUMERICAL mean:6.32273e+06 min:0 max:1.19964e+08
sd:1.63608e+07
        30: "flow_iat_mean" NUMERICAL mean:2.95333e+06 min:0 max:1.19964e+08
sd:1.12159e+07
        31: "flow_iat_min" NUMERICAL mean:2.3825e+06 min:0 max:1.19964e+08
sd:1.10625e+07
        32: "flow_iat_std" NUMERICAL mean:1.25785e+06 min:0 max:8.43107e+07
sd:4.45397e+06
        33: "flow_pkts/s" NUMERICAL mean:43005.2 min:0.0166716 max:4e+06
sd:265059
```

```
        34: "fwd_act_data_pkts" NUMERICAL mean:1.84772 min:0 max:1412 sd:5.64362
        35: "fwd_blk_rate_avg" NUMERICAL mean:0 min:0 max:0 sd:0
        36: "fwd_byts/b_avg" NUMERICAL mean:0 min:0 max:0 sd:0
        37: "fwd_header_len" NUMERICAL mean:103.82 min:0 max:204920 sd:797.336
        38: "fwd_iat_max" NUMERICAL mean:5.98896e+06 min:0 max:1.19964e+08
sd:1.62041e+07
        39: "fwd_iat_mean" NUMERICAL mean:3.35053e+06 min:0 max:1.19964e+08
sd:1.1672e+07
        40: "fwd_iat_min" NUMERICAL mean:2.56224e+06 min:0 max:1.19964e+08
sd:1.15742e+07
        41: "fwd_iat_std" NUMERICAL mean:1.30273e+06 min:0 max:8.43894e+07
sd:4.51473e+06
        42: "fwd_iat_tot" NUMERICAL mean:1.31775e+07 min:0 max:1.2e+08
sd:3.24942e+07
        43: "fwd_pkt_len_max" NUMERICAL mean:151.874 min:0 max:64440 sd:280.919
        44: "fwd_pkt_len_mean" NUMERICAL mean:44.3607 min:0 max:16529.3
sd:60.8472
        45: "fwd_pkt_len_min" NUMERICAL mean:14.0744 min:0 max:1460 sd:23.773
        46: "fwd_pkt_len_std" NUMERICAL mean:50.8409 min:0 max:18401.6
sd:92.4182
        47: "fwd_pkts/b_avg" NUMERICAL mean:0 min:0 max:0 sd:0
        48: "fwd_pkts/s" NUMERICAL mean:37149.9 min:0 max:4e+06 sd:252318
        49: "fwd_psh_flags" NUMERICAL mean:0.0484322 min:0 max:1 sd:0.214678
        50: "fwd_seg_size_avg" NUMERICAL mean:44.3607 min:0 max:16529.3
sd:60.8472
        51: "fwd_seg_size_min" NUMERICAL mean:16.4071 min:0 max:48 sd:7.29571
        52: "fwd_urg_flags" NUMERICAL mean:0 min:0 max:0 sd:0
        53: "idle_max" NUMERICAL mean:4.16038e+06 min:0 max:1.19964e+08
sd:1.36992e+07
        54: "idle_mean" NUMERICAL mean:4.01772e+06 min:0 max:1.19964e+08
sd:1.33225e+07
        55: "idle_min" NUMERICAL mean:3.85466e+06 min:0 max:1.19964e+08
sd:1.31257e+07
        56: "idle_std" NUMERICAL mean:176486 min:0 max:6.61412e+07
sd:1.92879e+06
        57: "init_bwd_win_byts" NUMERICAL mean:5651.66 min:-1 max:65535
sd:17200.2
        58: "init_fwd_win_byts" NUMERICAL mean:5083.24 min:-1 max:65535 sd:10415
        59: "pkt_len_max" NUMERICAL mean:342.48 min:0 max:64440 sd:515.851
        60: "pkt_len_mean" NUMERICAL mean:80.1481 min:0 max:3326.99 sd:119.476
        61: "pkt_len_min" NUMERICAL mean:13.9494 min:0 max:1460 sd:22.5373
        62: "pkt_len_std" NUMERICAL mean:110.175 min:0 max:10579.8 sd:164.357
        63: "pkt_len_var" NUMERICAL mean:39151.9 min:0 max:1.11932e+08 sd:185602
        64: "pkt_size_avg" NUMERICAL mean:93.4709 min:0 max:3328.3 sd:123.057
        65: "protocol" NUMERICAL mean:9.5572 min:0 max:17 sd:5.3196
        66: "psh_flag_cnt" NUMERICAL mean:0.360401 min:0 max:1 sd:0.480117
        67: "rst_flag_cnt" NUMERICAL mean:0.061352 min:0 max:1 sd:0.239975
        68: "subflow_bwd_byts" NUMERICAL mean:4971.93 min:0 max:2.79052e+07
```

```
sd:140221
        69: "subflow_bwd_pkts" NUMERICAL mean:6.46444 min:0 max:19181 sd:98.1016
        70: "subflow_fwd_byts" NUMERICAL mean:435.18 min:0 max:8.66172e+06
sd:30201.7
        71: "subflow_fwd_pkts" NUMERICAL mean:5.1062 min:1 max:9021 sd:34.1614
        72: "syn_flag_cnt" NUMERICAL mean:0.0484322 min:0 max:1 sd:0.214678
        74: "tot_bwd_pkts" NUMERICAL mean:6.46444 min:0 max:19181 sd:98.1016
        75: "tot_fwd_pkts" NUMERICAL mean:5.1062 min:1 max:9021 sd:34.1614
        76: "totlen_bwd_pkts" NUMERICAL mean:4971.93 min:0 max:2.79052e+07
sd:140221
        77: "totlen_fwd_pkts" NUMERICAL mean:435.18 min:0 max:8.66172e+06
sd:30201.7
        78: "urg_flag_cnt" NUMERICAL mean:0.0482078 min:0 max:1 sd:0.214205

CATEGORICAL: 2 (2.5%)
        73: "timestamp" CATEGORICAL has-dict vocab-size:2001 num-oods:31744
(4.36956%) most-frequent:"<OOD>" 31744 (4.36956%)
        79: "__LABEL" CATEGORICAL integerized vocab-size:3 no-ood-item

Terminology:
        nas: Number of non-available (i.e. missing) values.
        ood: Out of dictionary.
        manually-defined: Attribute which type is manually defined by the user
i.e. the type was not automatically inferred.
        tokenized: The attribute value is obtained through tokenization.
        has-dict: The attribute is attached to a string dictionary e.g. a
categorical attribute stored as a string.
        vocab-size: Number of unique values.

[INFO kernel.cc:772] Configure learner
[INFO kernel.cc:797] Training config:
learner: "RANDOM_FOREST"
features: "ack_flag_cnt"
features: "active_max"
features: "active_mean"
features: "active_min"
features: "active_std"
features: "bwd_blk_rate_avg"
features: "bwd_byts/b_avg"
features: "bwd_header_len"
features: "bwd_iat_max"
features: "bwd_iat_mean"
features: "bwd_iat_min"
features: "bwd_iat_std"
features: "bwd_iat_tot"
features: "bwd_pkt_len_max"
features: "bwd_pkt_len_mean"
features: "bwd_pkt_len_min"
```

```
features: "bwd_pkt_len_std"
features: "bwd_pkts/b_avg"
features: "bwd_pkts/s"
features: "bwd_psh_flags"
features: "bwd_seg_size_avg"
features: "bwd_urg_flags"
features: "cwe_flag_count"
features: "down/up_ratio"
features: "dst_port"
features: "ece_flag_cnt"
features: "fin_flag_cnt"
features: "flow_byts/s"
features: "flow_duration"
features: "flow_iat_max"
features: "flow_iat_mean"
features: "flow_iat_min"
features: "flow_iat_std"
features: "flow_pkts/s"
features: "fwd_act_data_pkts"
features: "fwd_blk_rate_avg"
features: "fwd_byts/b_avg"
features: "fwd_header_len"
features: "fwd_iat_max"
features: "fwd_iat_mean"
features: "fwd_iat_min"
features: "fwd_iat_std"
features: "fwd_iat_tot"
features: "fwd_pkt_len_max"
features: "fwd_pkt_len_mean"
features: "fwd_pkt_len_min"
features: "fwd_pkt_len_std"
features: "fwd_pkts/b_avg"
features: "fwd_pkts/s"
features: "fwd_psh_flags"
features: "fwd_seg_size_avg"
features: "fwd_seg_size_min"
features: "fwd_urg_flags"
features: "idle_max"
features: "idle_mean"
features: "idle_min"
features: "idle_std"
features: "init_bwd_win_byts"
features: "init_fwd_win_byts"
features: "pkt_len_max"
features: "pkt_len_mean"
features: "pkt_len_min"
features: "pkt_len_std"
features: "pkt_len_var"
```

```
features: "pkt_size_avg"
features: "protocol"
features: "psh_flag_cnt"
features: "rst_flag_cnt"
features: "subflow_bwd_byts"
features: "subflow_bwd_pkts"
features: "subflow_fwd_byts"
features: "subflow_fwd_pkts"
features: "syn_flag_cnt"
features: "timestamp"
features: "tot_bwd_pkts"
features: "tot_fwd_pkts"
features: "totlen_bwd_pkts"
features: "totlen_fwd_pkts"
features: "urg_flag_cnt"
label: "__LABEL"
task: CLASSIFICATION
[yggdrasil_decision_forests.model.random_forest.proto.random_forest_config] {
  num_trees: 300
  decision_tree {
    max_depth: 16
    min_examples: 5
    in_split_min_examples_check: true
    missing_value_policy: GLOBAL_IMPUTATION
    allow_na_conditions: false
    categorical_set_greedy_forward {
      sampling: 0.1
      max_num_items: -1
      min_item_frequency: 1
    }
    growing_strategy_local {
    }
    categorical {
      cart {
      }
    }
    num_candidate_attributes_ratio: -1
    axis_aligned_split {
    }
    internal {
      sorting_strategy: PRESORTED
    }
  }
  winner_take_all_inference: true
  compute_oob_performances: true
  compute_oob_variable_importances: false
  adapt_bootstrap_size_ratio_for_maximum_training_duration: false
}
```

```
[INFO kernel.cc:800] Deployment config:

[INFO kernel.cc:837] Train model
[INFO random_forest.cc:303] Training random forest on 726480 example(s) and 79
feature(s).
[INFO random_forest.cc:578] Training of tree  1/300 (tree index:0) done
accuracy:0.999978 logloss:0.000807194
[INFO random_forest.cc:578] Training of tree  11/300 (tree index:9) done
accuracy:0.99999 logloss:0.000133517
[INFO random_forest.cc:578] Training of tree  21/300 (tree index:20) done
accuracy:0.999993 logloss:9.47712e-05
[INFO random_forest.cc:578] Training of tree  31/300 (tree index:30) done
accuracy:0.999995 logloss:9.21377e-05
[INFO random_forest.cc:578] Training of tree  41/300 (tree index:38) done
accuracy:0.999993 logloss:8.95192e-05
[INFO random_forest.cc:578] Training of tree  51/300 (tree index:49) done
accuracy:0.999996 logloss:9.12801e-05
[INFO random_forest.cc:578] Training of tree  61/300 (tree index:59) done
accuracy:0.999996 logloss:4.48004e-05
[INFO random_forest.cc:578] Training of tree  71/300 (tree index:73) done
accuracy:0.999996 logloss:4.61115e-05
[INFO random_forest.cc:578] Training of tree  81/300 (tree index:81) done
accuracy:0.999996 logloss:4.58013e-05
[INFO random_forest.cc:578] Training of tree  91/300 (tree index:92) done
accuracy:0.999997 logloss:4.53838e-05
[INFO random_forest.cc:578] Training of tree  101/300 (tree index:98) done
accuracy:0.999996 logloss:4.55602e-05
[INFO random_forest.cc:578] Training of tree  111/300 (tree index:108) done
accuracy:0.999996 logloss:4.64331e-05
[INFO random_forest.cc:578] Training of tree  121/300 (tree index:120) done
accuracy:0.999996 logloss:4.5799e-05
[INFO random_forest.cc:578] Training of tree  131/300 (tree index:132) done
accuracy:0.999996 logloss:4.5801e-05
[INFO random_forest.cc:578] Training of tree  141/300 (tree index:142) done
accuracy:0.999997 logloss:4.44065e-05
[INFO random_forest.cc:578] Training of tree  151/300 (tree index:151) done
accuracy:0.999996 logloss:4.37733e-05
[INFO random_forest.cc:578] Training of tree  161/300 (tree index:164) done
accuracy:0.999996 logloss:4.4593e-05
[INFO random_forest.cc:578] Training of tree  171/300 (tree index:170) done
accuracy:0.999996 logloss:4.51117e-05
[INFO random_forest.cc:578] Training of tree  181/300 (tree index:180) done
accuracy:0.999996 logloss:4.53929e-05
[INFO random_forest.cc:578] Training of tree  191/300 (tree index:194) done
accuracy:0.999996 logloss:4.53991e-05
[INFO random_forest.cc:578] Training of tree  201/300 (tree index:201) done
accuracy:0.999996 logloss:4.5151e-05
```

```
[INFO random_forest.cc:578] Training of tree  211/300 (tree index:207) done
accuracy:0.999996 logloss:4.55226e-05
[INFO random_forest.cc:578] Training of tree  221/300 (tree index:218) done
accuracy:0.999996 logloss:4.56777e-05
[INFO random_forest.cc:578] Training of tree  231/300 (tree index:230) done
accuracy:0.999995 logloss:4.5955e-05
[INFO random_forest.cc:578] Training of tree  241/300 (tree index:242) done
accuracy:0.999995 logloss:4.61304e-05
[INFO random_forest.cc:578] Training of tree  251/300 (tree index:244) done
accuracy:0.999995 logloss:4.56269e-05
[INFO random_forest.cc:578] Training of tree  261/300 (tree index:257) done
accuracy:0.999995 logloss:4.59369e-05
[INFO random_forest.cc:578] Training of tree  271/300 (tree index:273) done
accuracy:0.999995 logloss:4.5509e-05
[INFO random_forest.cc:578] Training of tree  281/300 (tree index:283) done
accuracy:0.999995 logloss:4.53777e-05
[INFO random_forest.cc:578] Training of tree  291/300 (tree index:289) done
accuracy:0.999995 logloss:4.55151e-05
[INFO random_forest.cc:578] Training of tree  300/300 (tree index:298) done
accuracy:0.999995 logloss:4.55272e-05
[INFO random_forest.cc:645] Final OOB metrics: accuracy:0.999995
logloss:4.55272e-05
[INFO kernel.cc:856] Export model in log directory: /tmp/tmp81yjfb25
[INFO kernel.cc:864] Save model in resources
[INFO kernel.cc:960] Loading model from path
[INFO decision_forest.cc:590] Model loaded with 300 root(s), 20952 node(s), and
66 input feature(s).
[INFO abstract_model.cc:973] Engine "RandomForestGeneric" built
[INFO kernel.cc:820] Use fast generic engine
```

[12]:
```python
# Evaluation des trainierten Modells mit den Testdaten
print("Evaluating the Model...")
evaluation = model.evaluate(testing_dataset_GoldenEye, return_dict=True)

print()

for name, value in evaluation.items():
    print(f"{name}: {value:.4f}")
```

```
Evaluating the Model…
4862/4862 [==============================] - 30s 6ms/step - loss: 0.0000e+00 -
accuracy: 1.0000

loss: 0.0000
accuracy: 1.0000
```

[13]:
```
# Erstellen einer Bilanz für das trainierte Modell
model.summary()
```

```
.196333 ################
   10.    "fwd_byts/b_avg"  6.196333 ################
   11.    "fwd_pkts/b_avg"  6.196333 ################
   12.     "fwd_urg_flags"  6.196333 ################
   13.      "rst_flag_cnt"  6.196333 ################
   14.           "__LABEL"  6.196333 ################
   15.   "bwd_pkt_len_min"  6.196174 ###############
   16.     "fwd_psh_flags"  6.195752 ###############
   17.      "syn_flag_cnt"  6.195395 ###############
   18.        "active_std"  6.186666 ###############
   19.          "protocol"  6.185479 ###############
   20.      "urg_flag_cnt"  6.185220 ###############
   21.       "pkt_len_min"  6.163760 ###############
   22.   "fwd_pkt_len_min"  6.161323 ###############
   23.     "down/up_ratio"  6.146889 ###############
   24.       "bwd_iat_max"  6.144748 ###############
   25.       "bwd_iat_tot"  6.132439 ###############
   26.          "idle_std"  6.131485 ###############
   27.          "idle_max"  6.110771 ###############
   28.         "idle_mean"  6.110162 ###############
   29.   "totlen_fwd_pkts"  6.100082 ###############
   30.          "idle_min"  6.088318 ###############
   31.  "subflow_fwd_byts"  6.078703 ##############
   32.       "active_mean"  6.076018 ##############
   33.        "active_min"  6.075307 ##############
   34.        "active_max"  6.065359 ##############
   35.      "psh_flag_cnt"  6.060368 ##############
   36.       "bwd_iat_min"  6.059368 ##############
   37.       "bwd_iat_std"  6.056878 ##############
   38.      "pkt_size_avg"  6.053871 ##############
   39. "fwd_act_data_pkts"  6.052673 ##############
   40.      "pkt_len_mean"  6.046496 ##############
   41.       "flow_byts/s"  6.035912 ##############
   42. "init_bwd_win_byts"  6.033605 ##############
   43.  "fwd_seg_size_avg"  6.027662 ##############
   44.       "fwd_iat_std"  6.025702 ##############
   45.      "bwd_iat_mean"  6.019866 ##############
   46.       "pkt_len_std"  6.000939 ##############
   47.   "totlen_bwd_pkts"  5.995096 ##############
   48.  "fwd_pkt_len_mean"  5.986585 ##############
   49.      "flow_iat_std"  5.975480 ##############
   50.  "subflow_fwd_pkts"  5.970263 ##############
   51.  "subflow_bwd_byts"  5.966350 ##############
   52.      "tot_fwd_pkts"  5.957343 #############
```

```
   53.   "fwd_pkt_len_max"  5.942622 #############
   54.  "bwd_seg_size_avg"  5.930834 #############
   55.      "ack_flag_cnt"  5.930407 #############
   56.        "bwd_pkts/s"  5.923935 #############
   57.   "bwd_pkt_len_max"  5.923673 #############
   58.  "bwd_pkt_len_mean"  5.918741 #############
   59.       "pkt_len_var"  5.905684 #############
   60.   "bwd_pkt_len_std"  5.867505 #############
   61.  "subflow_bwd_pkts"  5.860475 #############
   62.   "fwd_pkt_len_std"  5.858490 #############
   63.    "bwd_header_len"  5.852646 #############
   64.       "pkt_len_max"  5.851105 #############
   65.      "tot_bwd_pkts"  5.812395 ############
   66.       "fwd_iat_min"  5.625428 ###########
   67.      "flow_iat_min"  5.520944 ##########
   68.       "fwd_iat_tot"  5.461815 #########
   69.      "fwd_iat_mean"  5.440457 #########
   70.     "flow_duration"  5.425080 #########
   71.       "fwd_iat_max"  5.367465 ########
   72.        "fwd_pkts/s"  5.355653 ########
   73.      "flow_iat_max"  5.324052 ########
   74.    "fwd_header_len"  5.315583 ########
   75.         "timestamp"  5.307326 ########
   76.          "dst_port"  5.268064 ########
   77.     "flow_iat_mean"  5.063705 ######
   78.       "flow_pkts/s"  5.037486 ######
   79.  "fwd_seg_size_min"  4.508160 #
   80. "init_fwd_win_byts"  4.331581



Winner take all: true
Out-of-bag evaluation: accuracy:0.999995 logloss:4.55272e-05
Number of trees: 300
Total number of nodes: 20952

Number of nodes by tree:
Count: 300 Average: 69.84 StdDev: 30.9854
Min: 17 Max: 197 Ignored: 0
---------------------------------------------
[  17,  26) 15   5.00%   5.00% ####
[  26,  35) 23   7.67%  12.67% #####
[  35,  44) 31  10.33%  23.00% #######
[  44,  53) 22   7.33%  30.33% #####
[  53,  62) 39  13.00%  43.33% #########
[  62,  71) 28   9.33%  52.67% #######
[  71,  80) 42  14.00%  66.67% ##########
[  80,  89) 18   6.00%  72.67% ####
```

```
[  89,  98) 35  11.67%  84.33% ########
[  98, 107) 10   3.33%  87.67% ##
[ 107, 116) 10   3.33%  91.00% ##
[ 116, 125) 15   5.00%  96.00% ####
[ 125, 134)  5   1.67%  97.67% #
[ 134, 143)  1   0.33%  98.00%
[ 143, 152)  3   1.00%  99.00% #
[ 152, 161)  1   0.33%  99.33%
[ 161, 170)  0   0.00%  99.33%
[ 170, 179)  0   0.00%  99.33%
[ 179, 188)  0   0.00%  99.33%
[ 188, 197]  2   0.67% 100.00%

Depth by leafs:
Count: 10626 Average: 6.47092 StdDev: 2.0629
Min: 1 Max: 15 Ignored: 0
------------------------------------------------
[  1,  2)   63   0.59%   0.59%
[  2,  3)  147   1.38%   1.98% #
[  3,  4)  450   4.23%   6.21% ##
[  4,  5) 1012   9.52%  15.73% #####
[  5,  6) 1767  16.63%  32.36% ########
[  6,  7) 2140  20.14%  52.50% ##########
[  7,  8) 2048  19.27%  71.78% ##########
[  8,  9) 1408  13.25%  85.03% #######
[  9, 10)  785   7.39%  92.41% ####
[ 10, 11)  435   4.09%  96.51% ##
[ 11, 12)  217   2.04%  98.55% #
[ 12, 13)  103   0.97%  99.52%
[ 13, 14)   28   0.26%  99.78%
[ 14, 15)   17   0.16%  99.94%
[ 15, 15]    6   0.06% 100.00%

Number of training obs by leaf:
Count: 10626 Average: 20510.4 StdDev: 81391.6
Min: 5 Max: 687484 Ignored: 0
------------------------------------------------
[      5,  34379) 9736  91.62%  91.62% ##########
[  34379,  68753)  261   2.46%  94.08%
[  68753, 103127)  157   1.48%  95.56%
[ 103127, 137501)   96   0.90%  96.46%
[ 137501, 171875)   34   0.32%  96.78%
[ 171875, 206249)   11   0.10%  96.88%
[ 206249, 240623)   11   0.10%  96.99%
[ 240623, 274997)   10   0.09%  97.08%
[ 274997, 309371)    9   0.08%  97.17%
[ 309371, 343745)   20   0.19%  97.36%
[ 343745, 378119)   58   0.55%  97.90%
```

```
[ 378119, 412493)   55   0.52%  98.42%
[ 412493, 446867)   36   0.34%  98.76%
[ 446867, 481241)   39   0.37%  99.12%
[ 481241, 515615)   21   0.20%  99.32%
[ 515615, 549989)   12   0.11%  99.44%
[ 549989, 584363)   13   0.12%  99.56%
[ 584363, 618737)    2   0.02%  99.58%
[ 618737, 653111)    0   0.00%  99.58%
[ 653111, 687484]   45   0.42% 100.00%

Attribute in nodes:
        934 : init_fwd_win_byts [NUMERICAL]
        896 : fwd_seg_size_min [NUMERICAL]
        529 : fwd_header_len [NUMERICAL]
        510 : dst_port [NUMERICAL]
        373 : flow_iat_min [NUMERICAL]
        327 : timestamp [CATEGORICAL]
        309 : fwd_iat_min [NUMERICAL]
        273 : flow_iat_mean [NUMERICAL]
        264 : fwd_pkts/s [NUMERICAL]
        262 : fwd_iat_mean [NUMERICAL]
        235 : flow_pkts/s [NUMERICAL]
        233 : flow_duration [NUMERICAL]
        228 : fwd_iat_max [NUMERICAL]
        210 : fwd_iat_tot [NUMERICAL]
        210 : flow_iat_max [NUMERICAL]
        195 : ack_flag_cnt [NUMERICAL]
        159 : pkt_len_max [NUMERICAL]
        154 : subflow_bwd_pkts [NUMERICAL]
        148 : flow_iat_std [NUMERICAL]
        148 : bwd_pkts/s [NUMERICAL]
        148 : bwd_header_len [NUMERICAL]
        145 : tot_bwd_pkts [NUMERICAL]
        139 : init_bwd_win_byts [NUMERICAL]
        138 : fwd_seg_size_avg [NUMERICAL]
        134 : bwd_pkt_len_std [NUMERICAL]
        133 : fwd_pkt_len_mean [NUMERICAL]
        132 : pkt_len_var [NUMERICAL]
        121 : fwd_pkt_len_std [NUMERICAL]
        119 : totlen_fwd_pkts [NUMERICAL]
        116 : fwd_pkt_len_max [NUMERICAL]
        112 : subflow_fwd_byts [NUMERICAL]
        111 : pkt_size_avg [NUMERICAL]
        105 : bwd_iat_min [NUMERICAL]
        104 : subflow_fwd_pkts [NUMERICAL]
        104 : bwd_pkt_len_max [NUMERICAL]
        101 : totlen_bwd_pkts [NUMERICAL]
        101 : subflow_bwd_byts [NUMERICAL]
```

```
        101 : psh_flag_cnt [NUMERICAL]
        100 : tot_fwd_pkts [NUMERICAL]
        98 : flow_byts/s [NUMERICAL]
        97 : idle_mean [NUMERICAL]
        95 : pkt_len_mean [NUMERICAL]
        93 : bwd_pkt_len_mean [NUMERICAL]
        92 : idle_min [NUMERICAL]
        91 : pkt_len_std [NUMERICAL]
        88 : fwd_iat_std [NUMERICAL]
        88 : bwd_iat_mean [NUMERICAL]
        85 : idle_max [NUMERICAL]
        84 : bwd_seg_size_avg [NUMERICAL]
        70 : active_mean [NUMERICAL]
        62 : bwd_iat_std [NUMERICAL]
        60 : active_max [NUMERICAL]
        58 : bwd_iat_max [NUMERICAL]
        54 : fwd_act_data_pkts [NUMERICAL]
        45 : bwd_iat_tot [NUMERICAL]
        44 : fwd_pkt_len_min [NUMERICAL]
        42 : active_min [NUMERICAL]
        31 : idle_std [NUMERICAL]
        21 : urg_flag_cnt [NUMERICAL]
        19 : down/up_ratio [NUMERICAL]
        17 : protocol [NUMERICAL]
        16 : active_std [NUMERICAL]
        10 : pkt_len_min [NUMERICAL]
        2 : syn_flag_cnt [NUMERICAL]
        2 : fwd_psh_flags [NUMERICAL]
        1 : bwd_pkt_len_min [NUMERICAL]

Attribute in nodes with depth <= 0:
        43 : fwd_seg_size_min [NUMERICAL]
        39 : init_fwd_win_byts [NUMERICAL]
        35 : flow_pkts/s [NUMERICAL]
        31 : flow_iat_mean [NUMERICAL]
        21 : fwd_pkts/s [NUMERICAL]
        21 : fwd_header_len [NUMERICAL]
        19 : fwd_iat_max [NUMERICAL]
        18 : flow_iat_max [NUMERICAL]
        12 : timestamp [CATEGORICAL]
        11 : fwd_iat_tot [NUMERICAL]
        11 : flow_duration [NUMERICAL]
        8 : fwd_iat_mean [NUMERICAL]
        5 : fwd_pkt_len_std [NUMERICAL]
        5 : dst_port [NUMERICAL]
        5 : bwd_pkts/s [NUMERICAL]
        3 : pkt_len_var [NUMERICAL]
        3 : bwd_iat_std [NUMERICAL]
```

```
        2 : fwd_pkt_len_mean [NUMERICAL]
        2 : fwd_pkt_len_max [NUMERICAL]
        2 : bwd_iat_mean [NUMERICAL]
        1 : subflow_bwd_byts [NUMERICAL]
        1 : fwd_seg_size_avg [NUMERICAL]
        1 : bwd_pkt_len_std [NUMERICAL]
        1 : bwd_iat_min [NUMERICAL]

Attribute in nodes with depth <= 1:
        96 : init_fwd_win_byts [NUMERICAL]
        90 : fwd_seg_size_min [NUMERICAL]
        46 : flow_pkts/s [NUMERICAL]
        45 : flow_iat_mean [NUMERICAL]
        38 : flow_iat_max [NUMERICAL]
        34 : dst_port [NUMERICAL]
        29 : fwd_pkts/s [NUMERICAL]
        29 : fwd_iat_tot [NUMERICAL]
        28 : fwd_header_len [NUMERICAL]
        27 : fwd_iat_max [NUMERICAL]
        27 : flow_duration [NUMERICAL]
        23 : timestamp [CATEGORICAL]
        19 : fwd_pkt_len_std [NUMERICAL]
        18 : fwd_iat_mean [NUMERICAL]
        17 : bwd_pkt_len_std [NUMERICAL]
        17 : bwd_pkt_len_mean [NUMERICAL]
        15 : subflow_bwd_pkts [NUMERICAL]
        15 : pkt_len_var [NUMERICAL]
        15 : bwd_pkt_len_max [NUMERICAL]
        14 : subflow_bwd_byts [NUMERICAL]
        14 : fwd_pkt_len_max [NUMERICAL]
        14 : bwd_seg_size_avg [NUMERICAL]
        13 : tot_bwd_pkts [NUMERICAL]
        11 : pkt_len_max [NUMERICAL]
        11 : bwd_iat_std [NUMERICAL]
        10 : bwd_iat_mean [NUMERICAL]
        9 : flow_iat_min [NUMERICAL]
        9 : bwd_header_len [NUMERICAL]
        8 : totlen_bwd_pkts [NUMERICAL]
        7 : pkt_len_std [NUMERICAL]
        7 : pkt_len_mean [NUMERICAL]
        7 : fwd_act_data_pkts [NUMERICAL]
        6 : tot_fwd_pkts [NUMERICAL]
        6 : subflow_fwd_pkts [NUMERICAL]
        6 : bwd_pkts/s [NUMERICAL]
        5 : pkt_size_avg [NUMERICAL]
        5 : fwd_pkt_len_mean [NUMERICAL]
        5 : active_max [NUMERICAL]
        4 : idle_std [NUMERICAL]
```

```
        4 : fwd_pkt_len_min [NUMERICAL]
        4 : fwd_iat_std [NUMERICAL]
        4 : fwd_iat_min [NUMERICAL]
        4 : bwd_iat_tot [NUMERICAL]
        3 : subflow_fwd_byts [NUMERICAL]
        3 : fwd_seg_size_avg [NUMERICAL]
        3 : flow_byts/s [NUMERICAL]
        3 : active_min [NUMERICAL]
        2 : bwd_iat_min [NUMERICAL]
        2 : bwd_iat_max [NUMERICAL]
        1 : totlen_fwd_pkts [NUMERICAL]
        1 : pkt_len_min [NUMERICAL]
        1 : idle_mean [NUMERICAL]
        1 : flow_iat_std [NUMERICAL]
        1 : down/up_ratio [NUMERICAL]
        1 : active_mean [NUMERICAL]

Attribute in nodes with depth <= 2:
        169 : init_fwd_win_byts [NUMERICAL]
        165 : fwd_seg_size_min [NUMERICAL]
        75 : dst_port [NUMERICAL]
        65 : flow_iat_mean [NUMERICAL]
        63 : flow_pkts/s [NUMERICAL]
        62 : flow_iat_max [NUMERICAL]
        47 : fwd_pkts/s [NUMERICAL]
        46 : subflow_bwd_pkts [NUMERICAL]
        46 : fwd_header_len [NUMERICAL]
        46 : flow_duration [NUMERICAL]
        45 : flow_iat_min [NUMERICAL]
        44 : bwd_pkt_len_std [NUMERICAL]
        42 : timestamp [CATEGORICAL]
        42 : fwd_iat_mean [NUMERICAL]
        41 : fwd_iat_max [NUMERICAL]
        39 : tot_bwd_pkts [NUMERICAL]
        38 : bwd_pkt_len_max [NUMERICAL]
        37 : fwd_iat_tot [NUMERICAL]
        36 : pkt_len_var [NUMERICAL]
        35 : pkt_len_max [NUMERICAL]
        35 : bwd_seg_size_avg [NUMERICAL]
        33 : fwd_pkt_len_std [NUMERICAL]
        33 : fwd_iat_min [NUMERICAL]
        32 : subflow_bwd_byts [NUMERICAL]
        32 : bwd_pkt_len_mean [NUMERICAL]
        31 : bwd_header_len [NUMERICAL]
        29 : bwd_pkts/s [NUMERICAL]
        27 : totlen_bwd_pkts [NUMERICAL]
        22 : fwd_pkt_len_max [NUMERICAL]
        20 : pkt_len_std [NUMERICAL]
```

```
        19 : fwd_pkt_len_mean [NUMERICAL]
        17 : pkt_len_mean [NUMERICAL]
        16 : subflow_fwd_pkts [NUMERICAL]
        15 : tot_fwd_pkts [NUMERICAL]
        15 : bwd_iat_mean [NUMERICAL]
        14 : fwd_act_data_pkts [NUMERICAL]
        13 : fwd_seg_size_avg [NUMERICAL]
        13 : flow_byts/s [NUMERICAL]
        13 : bwd_iat_std [NUMERICAL]
        12 : pkt_size_avg [NUMERICAL]
        12 : fwd_iat_std [NUMERICAL]
        12 : flow_iat_std [NUMERICAL]
        10 : init_bwd_win_byts [NUMERICAL]
        10 : fwd_pkt_len_min [NUMERICAL]
        10 : active_max [NUMERICAL]
        9 : subflow_fwd_byts [NUMERICAL]
        8 : idle_std [NUMERICAL]
        8 : bwd_iat_tot [NUMERICAL]
        8 : bwd_iat_min [NUMERICAL]
        8 : active_min [NUMERICAL]
        7 : active_mean [NUMERICAL]
        5 : totlen_fwd_pkts [NUMERICAL]
        5 : down/up_ratio [NUMERICAL]
        5 : ack_flag_cnt [NUMERICAL]
        4 : psh_flag_cnt [NUMERICAL]
        4 : idle_min [NUMERICAL]
        4 : idle_mean [NUMERICAL]
        3 : idle_max [NUMERICAL]
        3 : bwd_iat_max [NUMERICAL]
        3 : active_std [NUMERICAL]
        1 : pkt_len_min [NUMERICAL]
        1 : bwd_pkt_len_min [NUMERICAL]

Attribute in nodes with depth <= 3:
        309 : init_fwd_win_byts [NUMERICAL]
        279 : fwd_seg_size_min [NUMERICAL]
        122 : dst_port [NUMERICAL]
        107 : fwd_header_len [NUMERICAL]
        101 : flow_iat_min [NUMERICAL]
        99 : flow_iat_mean [NUMERICAL]
        84 : timestamp [CATEGORICAL]
        84 : flow_pkts/s [NUMERICAL]
        80 : flow_iat_max [NUMERICAL]
        79 : fwd_iat_mean [NUMERICAL]
        74 : bwd_pkt_len_std [NUMERICAL]
        73 : subflow_bwd_pkts [NUMERICAL]
        73 : fwd_pkts/s [NUMERICAL]
        72 : flow_duration [NUMERICAL]
```

70 : fwd_iat_min [NUMERICAL]
69 : tot_bwd_pkts [NUMERICAL]
63 : bwd_header_len [NUMERICAL]
60 : pkt_len_max [NUMERICAL]
59 : fwd_iat_max [NUMERICAL]
57 : subflow_bwd_byts [NUMERICAL]
57 : bwd_pkt_len_max [NUMERICAL]
55 : bwd_seg_size_avg [NUMERICAL]
54 : fwd_iat_tot [NUMERICAL]
53 : bwd_pkt_len_mean [NUMERICAL]
51 : totlen_bwd_pkts [NUMERICAL]
51 : pkt_len_var [NUMERICAL]
48 : fwd_pkt_len_std [NUMERICAL]
48 : bwd_pkts/s [NUMERICAL]
40 : fwd_pkt_len_mean [NUMERICAL]
38 : init_bwd_win_byts [NUMERICAL]
37 : fwd_pkt_len_max [NUMERICAL]
37 : flow_iat_std [NUMERICAL]
33 : pkt_len_std [NUMERICAL]
32 : tot_fwd_pkts [NUMERICAL]
32 : bwd_iat_min [NUMERICAL]
31 : subflow_fwd_pkts [NUMERICAL]
31 : ack_flag_cnt [NUMERICAL]
30 : fwd_seg_size_avg [NUMERICAL]
30 : flow_byts/s [NUMERICAL]
29 : bwd_iat_mean [NUMERICAL]
27 : pkt_len_mean [NUMERICAL]
26 : totlen_fwd_pkts [NUMERICAL]
26 : pkt_size_avg [NUMERICAL]
25 : fwd_iat_std [NUMERICAL]
24 : subflow_fwd_byts [NUMERICAL]
21 : active_max [NUMERICAL]
20 : fwd_pkt_len_min [NUMERICAL]
20 : fwd_act_data_pkts [NUMERICAL]
20 : active_mean [NUMERICAL]
19 : bwd_iat_std [NUMERICAL]
16 : psh_flag_cnt [NUMERICAL]
14 : active_min [NUMERICAL]
11 : idle_min [NUMERICAL]
11 : idle_max [NUMERICAL]
11 : bwd_iat_tot [NUMERICAL]
10 : idle_std [NUMERICAL]
10 : idle_mean [NUMERICAL]
8 : bwd_iat_max [NUMERICAL]
7 : down/up_ratio [NUMERICAL]
7 : active_std [NUMERICAL]
1 : syn_flag_cnt [NUMERICAL]
1 : protocol [NUMERICAL]

```
        1 : pkt_len_min [NUMERICAL]
        1 : bwd_pkt_len_min [NUMERICAL]

Attribute in nodes with depth <= 5:
        619 : init_fwd_win_byts [NUMERICAL]
        600 : fwd_seg_size_min [NUMERICAL]
        330 : dst_port [NUMERICAL]
        322 : fwd_header_len [NUMERICAL]
        227 : flow_iat_min [NUMERICAL]
        182 : fwd_iat_min [NUMERICAL]
        174 : timestamp [CATEGORICAL]
        165 : flow_iat_mean [NUMERICAL]
        161 : fwd_iat_mean [NUMERICAL]
        144 : flow_pkts/s [NUMERICAL]
        138 : fwd_pkts/s [NUMERICAL]
        138 : fwd_iat_max [NUMERICAL]
        138 : flow_duration [NUMERICAL]
        133 : flow_iat_max [NUMERICAL]
        127 : subflow_bwd_pkts [NUMERICAL]
        121 : tot_bwd_pkts [NUMERICAL]
        119 : pkt_len_max [NUMERICAL]
        117 : ack_flag_cnt [NUMERICAL]
        116 : bwd_header_len [NUMERICAL]
        114 : bwd_pkt_len_std [NUMERICAL]
        112 : fwd_iat_tot [NUMERICAL]
        107 : flow_iat_std [NUMERICAL]
        105 : init_bwd_win_byts [NUMERICAL]
        100 : bwd_pkts/s [NUMERICAL]
        96 : fwd_seg_size_avg [NUMERICAL]
        96 : fwd_pkt_len_mean [NUMERICAL]
        95 : pkt_len_var [NUMERICAL]
        91 : fwd_pkt_len_std [NUMERICAL]
        90 : subflow_bwd_byts [NUMERICAL]
        88 : fwd_pkt_len_max [NUMERICAL]
        88 : bwd_pkt_len_max [NUMERICAL]
        86 : totlen_bwd_pkts [NUMERICAL]
        79 : subflow_fwd_byts [NUMERICAL]
        77 : subflow_fwd_pkts [NUMERICAL]
        76 : totlen_fwd_pkts [NUMERICAL]
        75 : bwd_pkt_len_mean [NUMERICAL]
        73 : pkt_size_avg [NUMERICAL]
        72 : bwd_seg_size_avg [NUMERICAL]
        72 : bwd_iat_min [NUMERICAL]
        70 : pkt_len_std [NUMERICAL]
        69 : tot_fwd_pkts [NUMERICAL]
        68 : flow_byts/s [NUMERICAL]
        66 : pkt_len_mean [NUMERICAL]
        65 : psh_flag_cnt [NUMERICAL]
```

```
        59 : bwd_iat_mean [NUMERICAL]
        54 : fwd_iat_std [NUMERICAL]
        46 : active_max [NUMERICAL]
        42 : active_mean [NUMERICAL]
        41 : idle_min [NUMERICAL]
        39 : bwd_iat_std [NUMERICAL]
        38 : fwd_pkt_len_min [NUMERICAL]
        35 : idle_mean [NUMERICAL]
        35 : bwd_iat_max [NUMERICAL]
        33 : idle_max [NUMERICAL]
        33 : fwd_act_data_pkts [NUMERICAL]
        33 : active_min [NUMERICAL]
        30 : bwd_iat_tot [NUMERICAL]
        24 : idle_std [NUMERICAL]
        17 : down/up_ratio [NUMERICAL]
        12 : active_std [NUMERICAL]
        6 : protocol [NUMERICAL]
        5 : pkt_len_min [NUMERICAL]
        3 : urg_flag_cnt [NUMERICAL]
        1 : syn_flag_cnt [NUMERICAL]
        1 : fwd_psh_flags [NUMERICAL]
        1 : bwd_pkt_len_min [NUMERICAL]

Condition type in nodes:
        9999 : HigherCondition
        172 : ContainsBitmapCondition
        155 : ContainsCondition
Condition type in nodes with depth <= 0:
        288 : HigherCondition
        12 : ContainsBitmapCondition
Condition type in nodes with depth <= 1:
        814 : HigherCondition
        23 : ContainsBitmapCondition
Condition type in nodes with depth <= 2:
        1722 : HigherCondition
        42 : ContainsBitmapCondition
Condition type in nodes with depth <= 3:
        3084 : HigherCondition
        81 : ContainsBitmapCondition
        3 : ContainsCondition
Condition type in nodes with depth <= 5:
        6615 : HigherCondition
        139 : ContainsBitmapCondition
        35 : ContainsCondition
Node format: NOT_SET

Training OOB:
        trees: 1, Out-of-bag evaluation: accuracy:0.999978 logloss:0.000807194
```

```
trees: 11, Out-of-bag evaluation: accuracy:0.99999 logloss:0.000133517
trees: 21, Out-of-bag evaluation: accuracy:0.999993 logloss:9.47712e-05
trees: 31, Out-of-bag evaluation: accuracy:0.999995 logloss:9.21377e-05
trees: 41, Out-of-bag evaluation: accuracy:0.999993 logloss:8.95192e-05
trees: 51, Out-of-bag evaluation: accuracy:0.999996 logloss:9.12801e-05
trees: 61, Out-of-bag evaluation: accuracy:0.999996 logloss:4.48004e-05
trees: 71, Out-of-bag evaluation: accuracy:0.999996 logloss:4.61115e-05
trees: 81, Out-of-bag evaluation: accuracy:0.999996 logloss:4.58013e-05
trees: 91, Out-of-bag evaluation: accuracy:0.999997 logloss:4.53838e-05
trees: 101, Out-of-bag evaluation: accuracy:0.999996 logloss:4.55602e-05
trees: 111, Out-of-bag evaluation: accuracy:0.999996 logloss:4.64331e-05
trees: 121, Out-of-bag evaluation: accuracy:0.999996 logloss:4.5799e-05
trees: 131, Out-of-bag evaluation: accuracy:0.999996 logloss:4.5801e-05
trees: 141, Out-of-bag evaluation: accuracy:0.999997 logloss:4.44065e-05
trees: 151, Out-of-bag evaluation: accuracy:0.999996 logloss:4.37733e-05
trees: 161, Out-of-bag evaluation: accuracy:0.999996 logloss:4.4593e-05
trees: 171, Out-of-bag evaluation: accuracy:0.999996 logloss:4.51117e-05
trees: 181, Out-of-bag evaluation: accuracy:0.999996 logloss:4.53929e-05
trees: 191, Out-of-bag evaluation: accuracy:0.999996 logloss:4.53991e-05
trees: 201, Out-of-bag evaluation: accuracy:0.999996 logloss:4.5151e-05
trees: 211, Out-of-bag evaluation: accuracy:0.999996 logloss:4.55226e-05
trees: 221, Out-of-bag evaluation: accuracy:0.999996 logloss:4.56777e-05
trees: 231, Out-of-bag evaluation: accuracy:0.999995 logloss:4.5955e-05
trees: 241, Out-of-bag evaluation: accuracy:0.999995 logloss:4.61304e-05
trees: 251, Out-of-bag evaluation: accuracy:0.999995 logloss:4.56269e-05
trees: 261, Out-of-bag evaluation: accuracy:0.999995 logloss:4.59369e-05
trees: 271, Out-of-bag evaluation: accuracy:0.999995 logloss:4.5509e-05
trees: 281, Out-of-bag evaluation: accuracy:0.999995 logloss:4.53777e-05
trees: 291, Out-of-bag evaluation: accuracy:0.999995 logloss:4.55151e-05
trees: 300, Out-of-bag evaluation: accuracy:0.999995 logloss:4.55272e-05
```

[14]:
```
# Erstellen der Feature Importance Kriterien aus Sicht des TensorFlow Modells
model.make_inspector().variable_importances()
```

[14]:
```
{'NUM_AS_ROOT': [("fwd_seg_size_min" (1; #51), 43.0),
  ("init_fwd_win_byts" (1; #58), 39.0),
  ("flow_pkts/s" (1; #33), 35.0),
  ("flow_iat_mean" (1; #30), 31.0),
  ("fwd_header_len" (1; #37), 21.0),
  ("fwd_pkts/s" (1; #48), 21.0),
  ("fwd_iat_max" (1; #38), 19.0),
  ("flow_iat_max" (1; #29), 18.0),
  ("timestamp" (4; #73), 12.0),
  ("fwd_iat_tot" (1; #42), 11.0),
  ("flow_duration" (1; #28), 11.0),
  ("fwd_iat_mean" (1; #39), 8.0),
```

```
("dst_port" (1; #24), 5.0),
("fwd_pkt_len_std" (1; #46), 5.0),
("bwd_pkts/s" (1; #18), 5.0),
("bwd_iat_std" (1; #11), 3.0),
("pkt_len_var" (1; #63), 3.0),
("fwd_pkt_len_max" (1; #43), 2.0),
("bwd_iat_mean" (1; #9), 2.0),
("fwd_pkt_len_mean" (1; #44), 2.0),
("fwd_seg_size_avg" (1; #50), 1.0),
("subflow_bwd_byts" (1; #68), 1.0),
("bwd_pkt_len_std" (1; #16), 1.0),
("bwd_iat_min" (1; #10), 1.0)]}
```