RandomForest_LOIC

July 1, 2021

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

[2]:
```
# Installieren der benötigten Python Pakete
!python -m pip install tensorflow_decision_forests
!python -m pip install numpy==1.19.5
!python -m pip install six==1.15.0
!python -m pip install wheel==0.35
!python -m pip install pandas
!python -m pip install wurlitzer
!python -m pip install matplotlib
```

```
Requirement already satisfied: tensorflow_decision_forests in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages
(0.1.7)
Requirement already satisfied: numpy in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow_decision_forests) (1.19.5)
Requirement already satisfied: absl-py in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow_decision_forests) (0.13.0)
Requirement already satisfied: tensorflow~=2.5 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow_decision_forests) (2.5.0)
Requirement already satisfied: six in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow_decision_forests) (1.15.0)
Requirement already satisfied: pandas in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow_decision_forests) (1.2.5)
Requirement already satisfied: wheel in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow_decision_forests) (0.35.0)
Requirement already satisfied: astunparse~=1.6.3 in
```

```
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (1.6.3)
Requirement already satisfied: keras-nightly~=2.5.0.dev in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (2.5.0.dev2021032900)
Requirement already satisfied: tensorflow-estimator<2.6.0,>=2.5.0rc0 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (2.5.0)
Requirement already satisfied: gast==0.4.0 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (0.4.0)
Requirement already satisfied: termcolor~=1.1.0 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (1.1.0)
Requirement already satisfied: keras-preprocessing~=1.1.2 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (1.1.2)
Requirement already satisfied: h5py~=3.1.0 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (3.1.0)
Requirement already satisfied: typing-extensions~=3.7.4 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (3.7.4.3)
Requirement already satisfied: google-pasta~=0.2 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (0.2.0)
Requirement already satisfied: tensorboard~=2.5 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (2.5.0)
Requirement already satisfied: protobuf>=3.9.2 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (3.17.3)
Requirement already satisfied: flatbuffers~=1.12.0 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (1.12)
Requirement already satisfied: grpcio~=1.34.0 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (1.34.1)
Requirement already satisfied: wrapt~=1.12.1 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (1.12.1)
Requirement already satisfied: opt-einsum~=3.3.0 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (3.3.0)
Requirement already satisfied: markdown>=2.6.8 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (3.3.4)
Requirement already satisfied: tensorboard-plugin-wit>=1.6.0 in
```

```
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (1.8.0)
Requirement already satisfied: google-auth<2,>=1.6.3 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (1.32.0)
Requirement already satisfied: requests<3,>=2.21.0 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (2.25.1)
Requirement already satisfied: tensorboard-data-server<0.7.0,>=0.6.0 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (0.6.1)
Requirement already satisfied: google-auth-oauthlib<0.5,>=0.4.1 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (0.4.4)
Requirement already satisfied: setuptools>=41.0.0 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (57.0.0)
Requirement already satisfied: werkzeug>=0.11.15 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (2.0.1)
Requirement already satisfied: pyasn1-modules>=0.2.1 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/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/ML.Proxy.FeatureImportance/lib/python3.9/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 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
google-
auth<2,>=1.6.3->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests)
(4.7.2)
Requirement already satisfied: requests-oauthlib>=0.7.0 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
google-auth-oauthlib<0.5,>=0.4.1->tensorboard~=2.5->tensorflow~=2.5->tensorflow_
decision_forests) (1.3.0)
Requirement already satisfied: pyasn1<0.5.0,>=0.4.6 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/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: idna<3,>=2.5 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
requests<3,>=2.21.0->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_fore
sts) (2.10)
```

```
Requirement already satisfied: urllib3<1.27,>=1.21.1 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
requests<3,>=2.21.0->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_fore
sts) (1.26.6)
Requirement already satisfied: chardet<5,>=3.0.2 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
requests<3,>=2.21.0->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_fore
sts) (4.0.0)
Requirement already satisfied: certifi>=2017.4.17 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
requests<3,>=2.21.0->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_fore
sts) (2021.5.30)
Requirement already satisfied: oauthlib>=3.0.0 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
requests-oauthlib>=0.7.0->google-auth-oauthlib<0.5,>=0.4.1->tensorboard~=2.5->te
nsorflow~=2.5->tensorflow_decision_forests) (3.1.1)
Requirement already satisfied: packaging>=20.2 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
wheel->tensorflow_decision_forests) (20.9)
Requirement already satisfied: pyparsing>=2.0.2 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
packaging>=20.2->wheel->tensorflow_decision_forests) (2.4.7)
Requirement already satisfied: python-dateutil>=2.7.3 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
pandas->tensorflow_decision_forests) (2.8.1)
Requirement already satisfied: pytz>=2017.3 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
pandas->tensorflow_decision_forests) (2021.1)
Requirement already satisfied: numpy==1.19.5 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages
(1.19.5)
Requirement already satisfied: six==1.15.0 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages
(1.15.0)
Requirement already satisfied: wheel==0.35 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages
(0.35.0)
Requirement already satisfied: packaging>=20.2 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
wheel==0.35) (20.9)
Requirement already satisfied: pyparsing>=2.0.2 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
packaging>=20.2->wheel==0.35) (2.4.7)
Requirement already satisfied: pandas in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages
(1.2.5)
Requirement already satisfied: numpy>=1.16.5 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
```

```
pandas) (1.19.5)
Requirement already satisfied: pytz>=2017.3 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
pandas) (2021.1)
Requirement already satisfied: python-dateutil>=2.7.3 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
pandas) (2.8.1)
Requirement already satisfied: six>=1.5 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
python-dateutil>=2.7.3->pandas) (1.15.0)
Requirement already satisfied: wurlitzer in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages
(2.1.0)
Requirement already satisfied: matplotlib in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages
(3.4.2)
Requirement already satisfied: pyparsing>=2.2.1 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
matplotlib) (2.4.7)
Requirement already satisfied: python-dateutil>=2.7 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
matplotlib) (2.8.1)
Requirement already satisfied: numpy>=1.16 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
matplotlib) (1.19.5)
Requirement already satisfied: pillow>=6.2.0 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
matplotlib) (8.2.0)
Requirement already satisfied: cycler>=0.10 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
matplotlib) (0.10.0)
Requirement already satisfied: kiwisolver>=1.0.1 in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
matplotlib) (1.3.1)
Requirement already satisfied: six in
/home/julianbuecher/ML.Proxy.FeatureImportance/lib/python3.9/site-packages (from
cycler>=0.10->matplotlib) (1.15.0)
```

[3]:
```python
# Importieren 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
import tensorflow as tf
```

```
2021-06-30 17:05:21.796349: W
tensorflow/stream_executor/platform/default/dso_loader.cc:64] Could not load
```

```
dynamic library 'libcudart.so.11.0'; dlerror: libcudart.so.11.0: cannot open
shared object file: No such file or directory
2021-06-30 17:05:21.796384: I tensorflow/stream_executor/cuda/cudart_stub.cc:29]
Ignore above cudart dlerror if you do not have a GPU set up on your machine.
```

[4]:
```
# Laden der Netzwerk Traffic Daten für den LOIC Angriff
data_LOIC = pd.read_csv('../Data/Optimized/Tuesday-20-02-2018_LOIC-Attack.csv')
```

[5]:
```
# Suchen und Ersetzen von NaN Werten im Dataset
nan_count = data_LOIC.isna().sum().sum()
print(f"Count of NaN in Dataset: {nan_count}")
```

```
Count of NaN in Dataset: 0
```

[6]:
```
# Festlegen der Label-Spalte innerhalb des Datasets
label = 'label'
```

[7]:
```
# 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_LOIC, testing_data_LOIC = split_dataset(data_LOIC)

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

```
5565312 examples in training, 2383436 examples for testing.
```

[8]:
```
# Konvertieren des Panda Dataframes in ein TensorFlow Dataset
print("Converting Panda Dataframe into TensorFlow Dataset...")
training_dataset_LOIC = tfdf.keras.
 ↪pd_dataframe_to_tf_dataset(training_data_LOIC, label=label)
testing_dataset_LOIC = tfdf.keras.pd_dataframe_to_tf_dataset(testing_data_LOIC,␣
 ↪label=label)
```

```
Converting Panda Dataframe into TensorFlow Dataset…

2021-06-30 17:07:04.753042: W
tensorflow/stream_executor/platform/default/dso_loader.cc:64] Could not load
dynamic library 'libcuda.so.1'; dlerror: libcuda.so.1: cannot open shared object
file: No such file or directory
2021-06-30 17:07:04.753101: W
tensorflow/stream_executor/cuda/cuda_driver.cc:326] failed call to cuInit:
UNKNOWN ERROR (303)
2021-06-30 17:07:04.753143: I
tensorflow/stream_executor/cuda/cuda_diagnostics.cc:156] kernel driver does not
```

```
appear to be running on this host (WS000252): /proc/driver/nvidia/version does
not exist
2021-06-30 17:07:04.754801: I tensorflow/core/platform/cpu_feature_guard.cc:142]
This TensorFlow binary is optimized with oneAPI Deep Neural Network Library
(oneDNN) to use the following CPU instructions in performance-critical
operations:  AVX2 FMA
To enable them in other operations, rebuild TensorFlow with the appropriate
compiler flags.
2021-06-30 17:07:04.762077: W
tensorflow/core/framework/cpu_allocator_impl.cc:80] Allocation of 44522496
exceeds 10% of free system memory.
2021-06-30 17:07:04.830362: W
tensorflow/core/framework/cpu_allocator_impl.cc:80] Allocation of 44522496
exceeds 10% of free system memory.
2021-06-30 17:07:04.836208: W
tensorflow/core/framework/cpu_allocator_impl.cc:80] Allocation of 44522496
exceeds 10% of free system memory.
2021-06-30 17:07:04.841641: W
tensorflow/core/framework/cpu_allocator_impl.cc:80] Allocation of 44522496
exceeds 10% of free system memory.
2021-06-30 17:07:04.846832: W
tensorflow/core/framework/cpu_allocator_impl.cc:80] Allocation of 44522496
exceeds 10% of free system memory.
```

[9]:
```
# Erstellen des Random Forest Modells
model = tfdf.keras.RandomForestModel()
model.compile(metrics=["accuracy"])
```

[10]:
```
# Trainieren des Modells
print("Training the Model...")
with sys_pipes():
    model.fit(x=training_dataset_LOIC)
```

```
Training the Model…

2021-06-30 17:07:17.764153: I
tensorflow/compiler/mlir/mlir_graph_optimization_pass.cc:176] None of the MLIR
Optimization Passes are enabled (registered 2)
2021-06-30 17:07:17.818498: I
tensorflow/core/platform/profile_utils/cpu_utils.cc:114] CPU Frequency:
3000005000 Hz

86958/86958 [==============================] - 268s 3ms/step

[INFO kernel.cc:746] Start Yggdrasil model training
[INFO kernel.cc:747] Collect training examples
[INFO kernel.cc:392] Number of batches: 86958
[INFO kernel.cc:393] Number of examples: 5565312
[INFO data_spec_inference.cc:289] 23592 item(s) have been pruned (i.e. they are
```

```
considered out of dictionary) for the column dst_ip (2000 item(s) left) because
min_value_count=5 and max_number_of_unique_values=2000
[INFO data_spec_inference.cc:289] 3979151 item(s) have been pruned (i.e. they
are considered out of dictionary) for the column flow_id (2000 item(s) left)
because min_value_count=5 and max_number_of_unique_values=2000
[INFO data_spec_inference.cc:289] 26905 item(s) have been pruned (i.e. they are
considered out of dictionary) for the column src_ip (2000 item(s) left) because
min_value_count=5 and max_number_of_unique_values=2000
[INFO data_spec_inference.cc:289] 35609 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: 5565312
Number of columns: 84

Number of columns by type:
        NUMERICAL: 79 (94.0476%)
        CATEGORICAL: 5 (5.95238%)

Columns:

NUMERICAL: 79 (94.0476%)
        0: "ack_flag_cnt" NUMERICAL mean:0.271283 min:0 max:1 sd:0.444622
        1: "active_max" NUMERICAL mean:386593 min:0 max:1.11423e+08
sd:4.29355e+06
        2: "active_mean" NUMERICAL mean:258887 min:0 max:1.11423e+08
sd:3.24434e+06
        3: "active_min" NUMERICAL mean:169360 min:0 max:1.11423e+08
sd:2.72905e+06
        4: "active_std" NUMERICAL mean:132689 min:0 max:7.52324e+07
sd:1.97688e+06
        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:137.82 min:0 max:516132 sd:3148.55
        8: "bwd_iat_max" NUMERICAL mean:3.21588e+06 min:0 max:1.19956e+08
sd:1.1346e+07
        9: "bwd_iat_mean" NUMERICAL mean:1.03978e+06 min:0 max:1.19956e+08
sd:5.0239e+06
        10: "bwd_iat_min" NUMERICAL mean:413038 min:0 max:1.19956e+08
sd:4.57932e+06
        11: "bwd_iat_std" NUMERICAL mean:1.01454e+06 min:0 max:8.48055e+07
sd:3.64765e+06
        12: "bwd_iat_tot" NUMERICAL mean:9.126e+06 min:0 max:1.2e+08
sd:2.81643e+07
        13: "bwd_pkt_len_max" NUMERICAL mean:391.229 min:0 max:65160 sd:526.301
        14: "bwd_pkt_len_mean" NUMERICAL mean:125.081 min:0 max:30375.1
sd:168.796
        15: "bwd_pkt_len_min" NUMERICAL mean:32.6208 min:0 max:1460 sd:54.4157
```

```
        16: "bwd_pkt_len_std" NUMERICAL mean:142.335 min:0 max:22448.4
sd:217.933
        17: "bwd_pkts/b_avg" NUMERICAL mean:0 min:0 max:0 sd:0
        18: "bwd_pkts/s" NUMERICAL mean:3273.36 min:0 max:2e+06 sd:32541.1
        19: "bwd_psh_flags" NUMERICAL mean:0 min:0 max:0 sd:0
        20: "bwd_seg_size_avg" NUMERICAL mean:125.081 min:0 max:30375.1
sd:168.796
        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:0.539062 min:0 max:311 sd:1.25652
        25: "dst_port" NUMERICAL mean:7355.01 min:0 max:65535 sd:17263.6
        26: "ece_flag_cnt" NUMERICAL mean:0.212103 min:0 max:1 sd:0.408798
        27: "fin_flag_cnt" NUMERICAL mean:0.00577578 min:0 max:1 sd:0.0757787
        28: "flow_byts/s" NUMERICAL mean:297168 min:0 max:1.618e+09
sd:3.9135e+06
        29: "flow_duration" NUMERICAL mean:1.3526e+07 min:0 max:1.2e+08
sd:3.24246e+07
        30: "flow_iat_max" NUMERICAL mean:6.34098e+06 min:0 max:1.2e+08
sd:1.64315e+07
        31: "flow_iat_mean" NUMERICAL mean:3.13474e+06 min:0 max:1.2e+08
sd:1.19968e+07
        32: "flow_iat_min" NUMERICAL mean:2.63966e+06 min:0 max:1.2e+08
sd:1.19686e+07
        33: "flow_iat_std" NUMERICAL mean:1.13478e+06 min:0 max:8.47984e+07
sd:3.80032e+06
        35: "flow_pkts/s" NUMERICAL mean:34849.7 min:0.0166667 max:5e+06
sd:226737
        36: "fwd_act_data_pkts" NUMERICAL mean:13.0801 min:0 max:280042
sd:1236.49
        37: "fwd_blk_rate_avg" NUMERICAL mean:0 min:0 max:0 sd:0
        38: "fwd_byts/b_avg" NUMERICAL mean:0 min:0 max:0 sd:0
        39: "fwd_header_len" NUMERICAL mean:197.806 min:0 max:2.24034e+06
sd:9970.08
        40: "fwd_iat_max" NUMERICAL mean:6.14366e+06 min:0 max:1.2e+08
sd:1.63671e+07
        41: "fwd_iat_mean" NUMERICAL mean:3.50992e+06 min:0 max:1.2e+08
sd:1.22005e+07
        42: "fwd_iat_min" NUMERICAL mean:2.71761e+06 min:0 max:1.2e+08
sd:1.20892e+07
        43: "fwd_iat_std" NUMERICAL mean:1.30992e+06 min:0 max:8.47984e+07
sd:4.64561e+06
        44: "fwd_iat_tot" NUMERICAL mean:1.32235e+07 min:0 max:1.2e+08
sd:3.2359e+07
        45: "fwd_pkt_len_max" NUMERICAL mean:170.659 min:0 max:1968 sd:259.916
        46: "fwd_pkt_len_mean" NUMERICAL mean:45.6675 min:0 max:1460 sd:50.3849
        47: "fwd_pkt_len_min" NUMERICAL mean:13.3114 min:0 max:1460 sd:24.2287
        48: "fwd_pkt_len_std" NUMERICAL mean:54.0462 min:0 max:1032.38
sd:87.3679
```

```
        49: "fwd_pkts/b_avg" NUMERICAL mean:0 min:0 max:0 sd:0
        50: "fwd_pkts/s" NUMERICAL mean:29318.6 min:0 max:5e+06 sd:215881
        51: "fwd_psh_flags" NUMERICAL mean:0.0574228 min:0 max:1 sd:0.232649
        52: "fwd_seg_size_avg" NUMERICAL mean:45.6675 min:0 max:1460 sd:50.3849
        53: "fwd_seg_size_min" NUMERICAL mean:15.9668 min:0 max:48 sd:6.18696
        54: "fwd_urg_flags" NUMERICAL mean:0 min:0 max:0 sd:0
        55: "idle_max" NUMERICAL mean:5.3226e+06 min:0 max:1.2e+08
sd:1.56216e+07
        56: "idle_mean" NUMERICAL mean:5.17446e+06 min:0 max:1.2e+08
sd:1.53288e+07
        57: "idle_min" NUMERICAL mean:5.00624e+06 min:0 max:1.2e+08
sd:1.51765e+07
        58: "idle_std" NUMERICAL mean:180734 min:0 max:7.6394e+07 sd:1.81093e+06
        59: "init_bwd_win_byts" NUMERICAL mean:9621.37 min:-1 max:65535
sd:21997.6
        60: "init_fwd_win_byts" NUMERICAL mean:5073.41 min:-1 max:65535
sd:10253.8
        61: "pkt_len_max" NUMERICAL mean:399.298 min:0 max:65160 sd:525.924
        62: "pkt_len_mean" NUMERICAL mean:81.036 min:0 max:16691.3 sd:102.954
        63: "pkt_len_min" NUMERICAL mean:13.1567 min:0 max:1460 sd:22.1163
        64: "pkt_len_std" NUMERICAL mean:122.873 min:0 max:22463.9 sd:164.259
        65: "pkt_len_var" NUMERICAL mean:42078.9 min:0 max:5.04626e+08 sd:258474
        66: "pkt_size_avg" NUMERICAL mean:94.1349 min:0 max:16801.1 sd:106.483
        67: "protocol" NUMERICAL mean:9.36653 min:0 max:17 sd:5.24853
        68: "psh_flag_cnt" NUMERICAL mean:0.390729 min:0 max:1 sd:0.487914
        69: "rst_flag_cnt" NUMERICAL mean:0.212101 min:0 max:1 sd:0.408796
        71: "src_port" NUMERICAL mean:45290.6 min:0 max:65535 sd:21111.9
        72: "subflow_bwd_byts" NUMERICAL mean:4965.1 min:0 max:3.75834e+07
sd:227166
        73: "subflow_bwd_pkts" NUMERICAL mean:6.68547 min:0 max:25806 sd:157.391
        74: "subflow_fwd_byts" NUMERICAL mean:708.702 min:0 max:8.96138e+06
sd:39628.4
        75: "subflow_fwd_pkts" NUMERICAL mean:16.8162 min:1 max:280043
sd:1237.79
        76: "syn_flag_cnt" NUMERICAL mean:0.0574228 min:0 max:1 sd:0.232649
        78: "tot_bwd_pkts" NUMERICAL mean:6.68547 min:0 max:25806 sd:157.391
        79: "tot_fwd_pkts" NUMERICAL mean:16.8162 min:1 max:280043 sd:1237.79
        80: "totlen_bwd_pkts" NUMERICAL mean:4965.1 min:0 max:3.75834e+07
sd:227166
        81: "totlen_fwd_pkts" NUMERICAL mean:708.702 min:0 max:8.96138e+06
sd:39628.4
        82: "urg_flag_cnt" NUMERICAL mean:0.0383515 min:0 max:1 sd:0.192043

CATEGORICAL: 5 (5.95238%)
        24: "dst_ip" CATEGORICAL has-dict vocab-size:2001 num-oods:23592
(0.423912%) most-frequent:"172.31.0.2" 1722060 (30.9427%)
        34: "flow_id" CATEGORICAL has-dict vocab-size:2001 num-oods:3979151
(71.4992%) most-frequent:"<OOD>" 3979151 (71.4992%)
```

```
        70: "src_ip" CATEGORICAL has-dict vocab-size:2001 num-oods:26905
(0.483441%) most-frequent:"8.6.0.1" 65615 (1.179%)
        77: "timestamp" CATEGORICAL has-dict vocab-size:2001 num-oods:35609
(0.639838%) most-frequent:"<OOD>" 35609 (0.639838%)
        83: "__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_ip"
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_id"
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: "src_ip"
features: "src_port"
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 5565312 example(s) and 83
feature(s).
[INFO random_forest.cc:578] Training of tree  1/300 (tree index:1) done
accuracy:0.999989 logloss:0.000387675
[INFO random_forest.cc:578] Training of tree  7/300 (tree index:10) done
```

```
accuracy:0.999996 logloss:0.000110349
[INFO random_forest.cc:578] Training of tree  12/300 (tree index:11) done
accuracy:0.999996 logloss:4.4888e-05
[INFO random_forest.cc:578] Training of tree  15/300 (tree index:14) done
accuracy:0.999998 logloss:1.98903e-05
[INFO random_forest.cc:578] Training of tree  20/300 (tree index:18) done
accuracy:0.999999 logloss:1.79278e-05
[INFO random_forest.cc:578] Training of tree  23/300 (tree index:23) done
accuracy:0.999999 logloss:1.05264e-05
[INFO random_forest.cc:578] Training of tree  26/300 (tree index:25) done
accuracy:0.999999 logloss:1.0468e-05
[INFO random_forest.cc:578] Training of tree  31/300 (tree index:32) done
accuracy:0.999999 logloss:1.01551e-05
[INFO random_forest.cc:578] Training of tree  35/300 (tree index:36) done
accuracy:0.999999 logloss:9.40367e-06
[INFO random_forest.cc:578] Training of tree  41/300 (tree index:42) done
accuracy:0.999999 logloss:9.3936e-06
[INFO random_forest.cc:578] Training of tree  47/300 (tree index:47) done
accuracy:0.999999 logloss:9.44069e-06
[INFO random_forest.cc:578] Training of tree  51/300 (tree index:51) done
accuracy:0.999999 logloss:9.45451e-06
[INFO random_forest.cc:578] Training of tree  56/300 (tree index:54) done
accuracy:0.999999 logloss:9.70042e-06
[INFO random_forest.cc:578] Training of tree  60/300 (tree index:59) done
accuracy:0.999999 logloss:9.52045e-06
[INFO random_forest.cc:578] Training of tree  63/300 (tree index:63) done
accuracy:0.999999 logloss:9.39215e-06
[INFO random_forest.cc:578] Training of tree  66/300 (tree index:64) done
accuracy:0.999999 logloss:9.34759e-06
[INFO random_forest.cc:578] Training of tree  70/300 (tree index:68) done
accuracy:0.999999 logloss:9.37471e-06
[INFO random_forest.cc:578] Training of tree  75/300 (tree index:74) done
accuracy:0.999999 logloss:9.35624e-06
[INFO random_forest.cc:578] Training of tree  81/300 (tree index:81) done
accuracy:0.999999 logloss:9.48176e-06
[INFO random_forest.cc:578] Training of tree  84/300 (tree index:83) done
accuracy:0.999999 logloss:9.62356e-06
[INFO random_forest.cc:578] Training of tree  88/300 (tree index:90) done
accuracy:0.999999 logloss:9.66675e-06
[INFO random_forest.cc:578] Training of tree  92/300 (tree index:93) done
accuracy:0.999999 logloss:9.63805e-06
[INFO random_forest.cc:578] Training of tree  97/300 (tree index:99) done
accuracy:0.999999 logloss:9.49868e-06
[INFO random_forest.cc:578] Training of tree  101/300 (tree index:100) done
accuracy:0.999999 logloss:9.4608e-06
[INFO random_forest.cc:578] Training of tree  104/300 (tree index:107) done
accuracy:0.999999 logloss:9.46038e-06
[INFO random_forest.cc:578] Training of tree  109/300 (tree index:106) done
```

```
accuracy:0.999999 logloss:9.49427e-06
[INFO random_forest.cc:578] Training of tree  112/300 (tree index:111) done
accuracy:0.999999 logloss:9.41738e-06
[INFO random_forest.cc:578] Training of tree  116/300 (tree index:115) done
accuracy:0.999999 logloss:9.63863e-06
[INFO random_forest.cc:578] Training of tree  120/300 (tree index:119) done
accuracy:0.999999 logloss:9.57974e-06
[INFO random_forest.cc:578] Training of tree  123/300 (tree index:122) done
accuracy:0.999999 logloss:9.58727e-06
[INFO random_forest.cc:578] Training of tree  127/300 (tree index:129) done
accuracy:0.999999 logloss:9.62461e-06
[INFO random_forest.cc:578] Training of tree  133/300 (tree index:133) done
accuracy:0.999999 logloss:9.72517e-06
[INFO random_forest.cc:578] Training of tree  139/300 (tree index:140) done
accuracy:0.999999 logloss:9.83346e-06
[INFO random_forest.cc:578] Training of tree  144/300 (tree index:143) done
accuracy:0.999999 logloss:9.77996e-06
[INFO random_forest.cc:578] Training of tree  148/300 (tree index:147) done
accuracy:0.999999 logloss:9.79225e-06
[INFO random_forest.cc:578] Training of tree  151/300 (tree index:149) done
accuracy:0.999999 logloss:9.83586e-06
[INFO random_forest.cc:578] Training of tree  156/300 (tree index:156) done
accuracy:0.999999 logloss:1.00301e-05
[INFO random_forest.cc:578] Training of tree  160/300 (tree index:160) done
accuracy:0.999999 logloss:1.00214e-05
[INFO random_forest.cc:578] Training of tree  163/300 (tree index:163) done
accuracy:0.999999 logloss:1.00815e-05
[INFO random_forest.cc:578] Training of tree  167/300 (tree index:166) done
accuracy:0.999999 logloss:1.02347e-05
[INFO random_forest.cc:578] Training of tree  171/300 (tree index:169) done
accuracy:0.999999 logloss:1.05445e-05
[INFO random_forest.cc:578] Training of tree  174/300 (tree index:174) done
accuracy:0.999999 logloss:1.06056e-05
[INFO random_forest.cc:578] Training of tree  179/300 (tree index:178) done
accuracy:0.999999 logloss:1.05279e-05
[INFO random_forest.cc:578] Training of tree  185/300 (tree index:188) done
accuracy:0.999999 logloss:1.05152e-05
[INFO random_forest.cc:578] Training of tree  191/300 (tree index:192) done
accuracy:0.999999 logloss:1.05195e-05
[INFO random_forest.cc:578] Training of tree  193/300 (tree index:191) done
accuracy:0.999999 logloss:1.05138e-05
[INFO random_forest.cc:578] Training of tree  198/300 (tree index:197) done
accuracy:0.999999 logloss:1.0463e-05
[INFO random_forest.cc:578] Training of tree  201/300 (tree index:198) done
accuracy:0.999999 logloss:1.04812e-05
[INFO random_forest.cc:578] Training of tree  204/300 (tree index:201) done
accuracy:0.999999 logloss:1.04716e-05
[INFO random_forest.cc:578] Training of tree  209/300 (tree index:208) done
```

```
accuracy:0.999999 logloss:1.04763e-05
[INFO random_forest.cc:578] Training of tree  215/300 (tree index:214) done
accuracy:0.999999 logloss:1.04089e-05
[INFO random_forest.cc:578] Training of tree  221/300 (tree index:222) done
accuracy:0.999999 logloss:1.0499e-05
[INFO random_forest.cc:578] Training of tree  226/300 (tree index:225) done
accuracy:0.999999 logloss:1.05068e-05
[INFO random_forest.cc:578] Training of tree  231/300 (tree index:229) done
accuracy:0.999999 logloss:1.05698e-05
[INFO random_forest.cc:578] Training of tree  233/300 (tree index:232) done
accuracy:0.999999 logloss:1.05411e-05
[INFO random_forest.cc:578] Training of tree  238/300 (tree index:238) done
accuracy:0.999999 logloss:1.08798e-05
[INFO random_forest.cc:578] Training of tree  242/300 (tree index:242) done
accuracy:0.999999 logloss:1.0928e-05
[INFO random_forest.cc:578] Training of tree  246/300 (tree index:245) done
accuracy:0.999999 logloss:1.09242e-05
[INFO random_forest.cc:578] Training of tree  249/300 (tree index:248) done
accuracy:0.999999 logloss:1.09359e-05
[INFO random_forest.cc:578] Training of tree  255/300 (tree index:258) done
accuracy:0.999999 logloss:1.09759e-05
[INFO random_forest.cc:578] Training of tree  261/300 (tree index:262) done
accuracy:0.999999 logloss:1.09999e-05
[INFO random_forest.cc:578] Training of tree  267/300 (tree index:267) done
accuracy:0.999999 logloss:1.0965e-05
[INFO random_forest.cc:578] Training of tree  273/300 (tree index:272) done
accuracy:0.999999 logloss:1.10039e-05
[INFO random_forest.cc:578] Training of tree  279/300 (tree index:281) done
accuracy:0.999999 logloss:1.09377e-05
[INFO random_forest.cc:578] Training of tree  284/300 (tree index:280) done
accuracy:0.999999 logloss:1.09686e-05
[INFO random_forest.cc:578] Training of tree  287/300 (tree index:287) done
accuracy:0.999999 logloss:1.09746e-05
[INFO random_forest.cc:578] Training of tree  291/300 (tree index:288) done
accuracy:0.999999 logloss:1.1007e-05
[INFO random_forest.cc:578] Training of tree  296/300 (tree index:294) done
accuracy:0.999999 logloss:1.09636e-05
[INFO random_forest.cc:578] Training of tree  300/300 (tree index:299) done
accuracy:0.999999 logloss:1.10132e-05
[INFO random_forest.cc:645] Final OOB metrics: accuracy:0.999999
logloss:1.10132e-05
[INFO kernel.cc:856] Export model in log directory: /tmp/tmpea5i9632
[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), 35148 node(s), and
70 input feature(s).
[INFO abstract_model.cc:973] Engine "RandomForestGeneric" built
[INFO kernel.cc:820] Use fast generic engine
```

[11]:
```python
# Evaluieren des trainierten Modells
print("Evaluating the Model...")
evaluation = model.evaluate(testing_dataset_LOIC, return_dict=True)
print()
for name, value in evaluation.items():
    print(f"{name}: {value:.4f}")
```

```
Evaluating the Model…
37242/37242 [==============================] - 126s 3ms/step - loss: 0.0000e+00
- accuracy: 1.0000

loss: 0.0000
accuracy: 1.0000
```

[12]:
```python
# Erstellen einer Bilanz für das trainierte Modell
model.summary()
```

```
Model: "random_forest_model"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
Total params: 1
Trainable params: 0
Non-trainable params: 1
_________________________________________________________________
Type: "RANDOM_FOREST"
Task: CLASSIFICATION
Label: "__LABEL"

Input Features (83):
        ack_flag_cnt
        active_max
        active_mean
        active_min
        active_std
        bwd_blk_rate_avg
        bwd_byts/b_avg
        bwd_header_len
        bwd_iat_max
        bwd_iat_mean
        bwd_iat_min
        bwd_iat_std
        bwd_iat_tot
        bwd_pkt_len_max
        bwd_pkt_len_mean
        bwd_pkt_len_min
        bwd_pkt_len_std
        bwd_pkts/b_avg
```

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

```
        pkt_size_avg
        protocol
        psh_flag_cnt
        rst_flag_cnt
        src_ip
        src_port
        subflow_bwd_byts
        subflow_bwd_pkts
        subflow_fwd_byts
        subflow_fwd_pkts
        syn_flag_cnt
        timestamp
        tot_bwd_pkts
        tot_fwd_pkts
        totlen_bwd_pkts
        totlen_fwd_pkts
        urg_flag_cnt

No weights

Variable Importance: NUM_NODES:
    1.            "dst_ip" 2137.000000 ################
    2. "init_fwd_win_byts" 1924.000000 ##############
    3.          "src_port" 1706.000000 ############
    4.            "src_ip" 1420.000000 ##########
    5.          "dst_port" 1094.000000 ########
    6.      "flow_iat_min" 504.000000 ###
    7.     "flow_duration" 430.000000 ###
    8.       "fwd_iat_tot" 417.000000 ###
    9.       "fwd_iat_min" 401.000000 ##
   10.      "flow_iat_max" 369.000000 ##
   11.      "fwd_iat_mean" 360.000000 ##
   12.       "fwd_iat_max" 350.000000 ##
   13.        "fwd_pkts/s" 345.000000 ##
   14.    "fwd_header_len" 331.000000 ##
   15.     "flow_iat_mean" 330.000000 ##
   16.       "flow_pkts/s" 325.000000 ##
   17.      "flow_iat_std" 297.000000 ##
   18.      "ack_flag_cnt" 274.000000 ##
   19.         "timestamp" 241.000000 #
   20.  "subflow_fwd_byts" 220.000000 #
   21.       "fwd_iat_std" 212.000000 #
   22.          "idle_min" 203.000000 #
   23.   "totlen_fwd_pkts" 203.000000 #
   24.         "idle_mean" 175.000000 #
   25.          "idle_max" 169.000000 #
   26.      "tot_fwd_pkts" 160.000000 #
   27.  "fwd_pkt_len_mean" 157.000000 #
```

```
   28.  "subflow_fwd_pkts" 150.000000 #
   29.  "fwd_seg_size_avg" 143.000000 #
   30.   "fwd_pkt_len_max" 135.000000 #
   31. "fwd_act_data_pkts" 128.000000
   32.       "pkt_len_std" 124.000000
   33.        "bwd_pkts/s" 117.000000
   34.      "tot_bwd_pkts" 114.000000
   35.  "fwd_seg_size_min" 113.000000
   36.      "pkt_size_avg" 97.000000
   37.  "subflow_bwd_pkts" 97.000000
   38.       "pkt_len_var" 96.000000
   39. "init_bwd_win_byts" 89.000000
   40.      "psh_flag_cnt" 89.000000
   41.      "pkt_len_mean" 88.000000
   42.    "bwd_header_len" 87.000000
   43.       "flow_byts/s" 80.000000
   44.       "pkt_len_max" 78.000000
   45.   "fwd_pkt_len_std" 71.000000
   46.          "protocol" 70.000000
   47.   "bwd_pkt_len_std" 69.000000
   48.      "urg_flag_cnt" 60.000000
   49.  "bwd_pkt_len_mean" 54.000000
   50.  "bwd_seg_size_avg" 54.000000
   51.       "active_max" 49.000000
   52.       "active_min" 46.000000
   53.   "bwd_pkt_len_max" 46.000000
   54.      "bwd_iat_mean" 38.000000
   55.       "active_mean" 37.000000
   56.       "bwd_iat_min" 33.000000
   57.  "subflow_bwd_byts" 33.000000
   58.   "totlen_bwd_pkts" 31.000000
   59.       "bwd_iat_std" 28.000000
   60.       "bwd_iat_max" 24.000000
   61.       "bwd_iat_tot" 24.000000
   62.       "pkt_len_min" 22.000000
   63.      "ece_flag_cnt" 11.000000
   64.   "fwd_pkt_len_min" 11.000000
   65.     "down/up_ratio" 10.000000
   66.      "rst_flag_cnt" 10.000000
   67.          "idle_std"  9.000000
   68.   "bwd_pkt_len_min"  2.000000
   69.           "flow_id"  2.000000
   70.     "fwd_psh_flags"  1.000000

Variable Importance: NUM_AS_ROOT:
    1.   "totlen_fwd_pkts" 52.000000 ################
    2.            "dst_ip" 38.000000 ###########
    3.  "subflow_fwd_byts" 36.000000 ##########
```

```
 4.   "fwd_pkt_len_max" 28.000000 ########
 5.  "fwd_seg_size_avg" 22.000000 ######
 6.  "fwd_pkt_len_mean" 20.000000 #####
 7.        "fwd_pkts/s" 18.000000 #####
 8.      "flow_iat_max" 13.000000 ###
 9.       "flow_pkts/s" 13.000000 ###
10.     "flow_duration" 12.000000 ###
11.          "dst_port" 10.000000 ##
12.     "flow_iat_mean"  9.000000 ##
13.      "flow_iat_min"  7.000000 #
14.       "fwd_iat_min"  6.000000 #
15.            "src_ip"  4.000000
16.        "bwd_pkts/s"  2.000000
17.       "fwd_iat_max"  2.000000
18.   "bwd_pkt_len_std"  1.000000
19.  "bwd_seg_size_avg"  1.000000
20.       "flow_byts/s"  1.000000
21.   "fwd_pkt_len_std"  1.000000
22. "init_fwd_win_byts"  1.000000
23.       "pkt_len_min"  1.000000
24.       "pkt_len_std"  1.000000
25.       "pkt_len_var"  1.000000

Variable Importance: SUM_SCORE:
 1.            "dst_ip" 58418253.203447 ################
 2.   "totlen_fwd_pkts" 37658585.280405 ##########
 3.  "subflow_fwd_byts" 27350424.756319 #######
 4.          "dst_port" 26253081.079194 #######
 5.      "flow_iat_max" 25568548.724911 #######
 6.   "fwd_pkt_len_max" 25367163.707673 ######
 7.  "fwd_pkt_len_mean" 24511117.910451 ######
 8.     "flow_duration" 21962165.421184 ######
 9.  "fwd_seg_size_avg" 18611214.422454 #####
10.        "fwd_pkts/s" 17403390.519783 ####
11.            "src_ip" 16718183.948190 ####
12.          "src_port" 14658840.738611 ####
13.       "flow_pkts/s" 13020428.693362 ###
14.     "flow_iat_mean" 9594783.898264 ##
15.       "fwd_iat_std" 8701210.826052 ##
16.      "flow_iat_min" 6609949.308666 #
17.       "fwd_iat_min" 6118297.151791 #
18.    "fwd_header_len" 6102065.106415 #
19.       "fwd_iat_tot" 5728295.329364 #
20. "init_fwd_win_byts" 5508980.458704 #
21.      "tot_fwd_pkts" 5419267.838008 #
22.  "subflow_fwd_pkts" 5146318.138159 #
23.      "flow_iat_std" 4919004.233550 #
24.   "fwd_pkt_len_std" 4067519.725596 #
```

```
 25.      "fwd_iat_mean" 4056095.937064 #
 26.   "bwd_pkt_len_std" 3486490.644881
 27.       "fwd_iat_max" 3194157.794822
 28.  "bwd_pkt_len_mean" 2703370.090755
 29.       "pkt_len_std" 2601224.374767
 30.  "bwd_seg_size_avg" 2485303.275225
 31.       "pkt_len_var" 2207489.578124
 32.    "bwd_header_len" 1630361.146017
 33.      "pkt_len_mean" 1494309.595876
 34.   "bwd_pkt_len_max" 1342674.175761
 35.      "ack_flag_cnt" 1314271.561025
 36.       "pkt_len_max" 1075111.279929
 37.       "flow_byts/s" 1042351.403669
 38.          "idle_min" 1024757.783981
 39.         "idle_mean" 1013903.756971
 40.   "totlen_bwd_pkts" 835860.790406
 41.      "pkt_size_avg" 689137.396187
 42.        "bwd_pkts/s" 651943.293294
 43.      "tot_bwd_pkts" 581553.360260
 44.  "subflow_bwd_byts" 565850.614341
 45. "init_bwd_win_byts" 478937.225708
 46.  "fwd_seg_size_min" 400621.393179
 47.       "bwd_iat_tot" 396789.022706
 48.        "active_max" 362403.524462
 49.          "idle_max" 359742.971171
 50.        "active_min" 339216.846628
 51.       "bwd_iat_std" 331268.599865
 52.       "active_mean" 291487.899870
 53. "fwd_act_data_pkts" 282957.930643
 54.  "subflow_bwd_pkts" 206655.627120
 55.      "psh_flag_cnt" 201160.049485
 56.       "pkt_len_min" 197851.901604
 57.      "bwd_iat_mean" 197213.980682
 58.          "protocol" 172479.812718
 59.          "idle_std" 166435.093180
 60.       "bwd_iat_min" 104101.725794
 61.           "flow_id" 39181.241673
 62.      "rst_flag_cnt" 38443.932622
 63.      "urg_flag_cnt" 37561.088255
 64.         "timestamp" 24023.981416
 65.      "ece_flag_cnt" 13743.876981
 66.       "bwd_iat_max" 9041.231045
 67.     "down/up_ratio" 8256.614299
 68.   "fwd_pkt_len_min" 8248.522245
 69.   "bwd_pkt_len_min" 234.387748
 70.     "fwd_psh_flags" 69.657275

Variable Importance: MEAN_MIN_DEPTH:
```

```
 1.        "active_std"  8.842275 ################
 2.  "bwd_blk_rate_avg"  8.842275 ################
 3.    "bwd_byts/b_avg"  8.842275 ################
 4.    "bwd_pkts/b_avg"  8.842275 ################
 5.     "bwd_psh_flags"  8.842275 ################
 6.     "bwd_urg_flags"  8.842275 ################
 7.    "cwe_flag_count"  8.842275 ################
 8.      "fin_flag_cnt"  8.842275 ################
 9.  "fwd_blk_rate_avg"  8.842275 ################
10.    "fwd_byts/b_avg"  8.842275 ################
11.    "fwd_pkts/b_avg"  8.842275 ################
12.     "fwd_urg_flags"  8.842275 ################
13.      "syn_flag_cnt"  8.842275 ################
14.           "__LABEL"  8.842275 ################
15.     "fwd_psh_flags"  8.841661 ###############
16.   "bwd_pkt_len_min"  8.839271 ###############
17.      "ece_flag_cnt"  8.838559 ###############
18.   "fwd_pkt_len_min"  8.827983 ###############
19.           "flow_id"  8.827609 ###############
20.     "down/up_ratio"  8.825543 ###############
21.       "bwd_iat_max"  8.823277 ###############
22.      "rst_flag_cnt"  8.811226 ###############
23.          "idle_std"  8.807857 ###############
24.   "totlen_bwd_pkts"  8.798095 ###############
25.       "pkt_len_min"  8.796450 ###############
26.       "bwd_iat_tot"  8.796232 ###############
27.       "bwd_iat_min"  8.794796 ###############
28.      "urg_flag_cnt"  8.771156 ###############
29.      "bwd_iat_mean"  8.769162 ###############
30.        "active_max"  8.762391 ###############
31.  "subflow_bwd_byts"  8.757677 ###############
32.       "active_mean"  8.755240 ###############
33.      "psh_flag_cnt"  8.751270 ###############
34.        "active_min"  8.735947 ###############
35. "fwd_act_data_pkts"  8.723533 ###############
36.       "bwd_iat_std"  8.714889 ###############
37.          "protocol"  8.710059 ###############
38.   "bwd_pkt_len_max"  8.695826 ###############
39.          "idle_max"  8.681836 ###############
40.       "pkt_len_max"  8.657966 ###############
41.      "tot_bwd_pkts"  8.648103 ###############
42.         "idle_mean"  8.647853 ###############
43.      "pkt_len_mean"  8.642594 ###############
44.  "subflow_bwd_pkts"  8.639830 ###############
45.  "fwd_seg_size_min"  8.619052 ###############
46.      "pkt_size_avg"  8.618724 ###############
47.       "flow_byts/s"  8.614086 ###############
48.  "bwd_seg_size_avg"  8.593510 ##############
```

```
49.  "bwd_pkt_len_mean"  8.593181 ##############
50. "init_bwd_win_byts"  8.592534 ##############
51.          "idle_min"  8.592383 ##############
52.    "bwd_header_len"  8.570238 ##############
53.         "timestamp"  8.563517 ##############
54.        "bwd_pkts/s"  8.555295 ##############
55.       "pkt_len_var"  8.512633 ##############
56.  "subflow_fwd_pkts"  8.451283 ##############
57.      "ack_flag_cnt"  8.417376 ##############
58.   "fwd_pkt_len_std"  8.403956 ##############
59.       "pkt_len_std"  8.378426 ##############
60.      "tot_fwd_pkts"  8.365388 #############
61.   "bwd_pkt_len_std"  8.324957 #############
62.       "fwd_iat_max"  8.080720 ############
63.    "fwd_header_len"  8.072816 ############
64.      "fwd_iat_mean"  8.049655 ############
65.       "fwd_iat_std"  8.024761 ############
66.      "flow_iat_std"  7.900815 ###########
67.       "fwd_iat_tot"  7.771343 ###########
68.       "fwd_iat_min"  7.684660 ###########
69.  "fwd_seg_size_avg"  7.644608 ##########
70.     "flow_iat_mean"  7.638222 ##########
71.       "flow_pkts/s"  7.524451 ##########
72.   "fwd_pkt_len_max"  7.386471 #########
73.  "fwd_pkt_len_mean"  7.320154 #########
74.      "flow_iat_min"  7.303737 #########
75.        "fwd_pkts/s"  7.280026 #########
76. "init_fwd_win_byts"  7.268278 #########
77.  "subflow_fwd_byts"  7.188470 ########
78.     "flow_duration"  6.822895 #######
79.   "totlen_fwd_pkts"  6.806144 #######
80.      "flow_iat_max"  6.755520 #######
81.            "src_ip"  6.751037 #######
82.          "src_port"  6.419851 #####
83.          "dst_port"  6.391851 #####
84.            "dst_ip"  5.111565
```

```
Winner take all: true
Out-of-bag evaluation: accuracy:0.999999 logloss:1.10132e-05
Number of trees: 300
Total number of nodes: 35148

Number of nodes by tree:
Count: 300 Average: 117.16 StdDev: 42.0187
Min: 39 Max: 243 Ignored: 0
----------------------------------------------
```

```
[  39,  49)  4   1.33%   1.33% #
[  49,  59) 11   3.67%   5.00% ###
[  59,  69) 16   5.33%  10.33% #####
[  69,  80) 35  11.67%  22.00% ##########
[  80,  90) 30  10.00%  32.00% #########
[  90, 100) 27   9.00%  41.00% ########
[ 100, 110) 21   7.00%  48.00% ######
[ 110, 121) 24   8.00%  56.00% #######
[ 121, 131) 34  11.33%  67.33% ##########
[ 131, 141) 15   5.00%  72.33% ####
[ 141, 151) 15   5.00%  77.33% ####
[ 151, 162) 16   5.33%  82.67% #####
[ 162, 172) 13   4.33%  87.00% ####
[ 172, 182) 18   6.00%  93.00% #####
[ 182, 192)  5   1.67%  94.67% #
[ 192, 203)  7   2.33%  97.00% ##
[ 203, 213)  4   1.33%  98.33% #
[ 213, 223)  2   0.67%  99.00% #
[ 223, 233)  1   0.33%  99.33%
[ 233, 243]  2   0.67% 100.00% #

Depth by leafs:
Count: 17724 Average: 8.99972 StdDev: 3.28637
Min: 1 Max: 15 Ignored: 0
------------------------------------------------
[  1,  2)   53   0.30%   0.30%
[  2,  3)  177   1.00%   1.30% #
[  3,  4)  611   3.45%   4.74% ###
[  4,  5) 1165   6.57%  11.32% ######
[  5,  6) 1150   6.49%  17.81% ######
[  6,  7) 1183   6.67%  24.48% ######
[  7,  8) 1460   8.24%  32.72% #######
[  8,  9) 1790  10.10%  42.82% #########
[  9, 10) 1970  11.11%  53.93% ##########
[ 10, 11) 1976  11.15%  65.08% ##########
[ 11, 12) 1728   9.75%  74.83% #########
[ 12, 13) 1618   9.13%  83.96% ########
[ 13, 14) 1229   6.93%  90.89% ######
[ 14, 15)  878   4.95%  95.85% ####
[ 15, 15]  736   4.15% 100.00% ####

Number of training obs by leaf:
Count: 17724 Average: 94199.6 StdDev: 474672
Min: 5 Max: 4022668 Ignored: 0
------------------------------------------------
[       5,  201138) 16659  93.99%  93.99% ##########
[  201138,  402271)   371   2.09%  96.08%
[  402271,  603404)    57   0.32%  96.41%
```

```
[  603404,  804537)   153   0.86%  97.27%
[  804537, 1005671)    97   0.55%  97.82%
[ 1005671, 1206804)    33   0.19%  98.00%
[ 1206804, 1407937)    11   0.06%  98.06%
[ 1407937, 1609070)    22   0.12%  98.19%
[ 1609070, 1810203)     6   0.03%  98.22%
[ 1810203, 2011337)     3   0.02%  98.24%
[ 2011337, 2212470)    16   0.09%  98.33%
[ 2212470, 2413603)    20   0.11%  98.44%
[ 2413603, 2614736)    13   0.07%  98.52%
[ 2614736, 2815869)    24   0.14%  98.65%
[ 2815869, 3017003)    22   0.12%  98.78%
[ 3017003, 3218136)    12   0.07%  98.84%
[ 3218136, 3419269)     4   0.02%  98.87%
[ 3419269, 3620402)    34   0.19%  99.06%
[ 3620402, 3821535)    16   0.09%  99.15%
[ 3821535, 4022668]   151   0.85% 100.00%

Attribute in nodes:
        2137 : dst_ip [CATEGORICAL]
        1924 : init_fwd_win_byts [NUMERICAL]
        1706 : src_port [NUMERICAL]
        1420 : src_ip [CATEGORICAL]
        1094 : dst_port [NUMERICAL]
        504 : flow_iat_min [NUMERICAL]
        430 : flow_duration [NUMERICAL]
        417 : fwd_iat_tot [NUMERICAL]
        401 : fwd_iat_min [NUMERICAL]
        369 : flow_iat_max [NUMERICAL]
        360 : fwd_iat_mean [NUMERICAL]
        350 : fwd_iat_max [NUMERICAL]
        345 : fwd_pkts/s [NUMERICAL]
        331 : fwd_header_len [NUMERICAL]
        330 : flow_iat_mean [NUMERICAL]
        325 : flow_pkts/s [NUMERICAL]
        297 : flow_iat_std [NUMERICAL]
        274 : ack_flag_cnt [NUMERICAL]
        241 : timestamp [CATEGORICAL]
        220 : subflow_fwd_byts [NUMERICAL]
        212 : fwd_iat_std [NUMERICAL]
        203 : totlen_fwd_pkts [NUMERICAL]
        203 : idle_min [NUMERICAL]
        175 : idle_mean [NUMERICAL]
        169 : idle_max [NUMERICAL]
        160 : tot_fwd_pkts [NUMERICAL]
        157 : fwd_pkt_len_mean [NUMERICAL]
        150 : subflow_fwd_pkts [NUMERICAL]
        143 : fwd_seg_size_avg [NUMERICAL]
```

```
        135 : fwd_pkt_len_max [NUMERICAL]
        128 : fwd_act_data_pkts [NUMERICAL]
        124 : pkt_len_std [NUMERICAL]
        117 : bwd_pkts/s [NUMERICAL]
        114 : tot_bwd_pkts [NUMERICAL]
        113 : fwd_seg_size_min [NUMERICAL]
        97 : subflow_bwd_pkts [NUMERICAL]
        97 : pkt_size_avg [NUMERICAL]
        96 : pkt_len_var [NUMERICAL]
        89 : psh_flag_cnt [NUMERICAL]
        89 : init_bwd_win_byts [NUMERICAL]
        88 : pkt_len_mean [NUMERICAL]
        87 : bwd_header_len [NUMERICAL]
        80 : flow_byts/s [NUMERICAL]
        78 : pkt_len_max [NUMERICAL]
        71 : fwd_pkt_len_std [NUMERICAL]
        70 : protocol [NUMERICAL]
        69 : bwd_pkt_len_std [NUMERICAL]
        60 : urg_flag_cnt [NUMERICAL]
        54 : bwd_seg_size_avg [NUMERICAL]
        54 : bwd_pkt_len_mean [NUMERICAL]
        49 : active_max [NUMERICAL]
        46 : bwd_pkt_len_max [NUMERICAL]
        46 : active_min [NUMERICAL]
        38 : bwd_iat_mean [NUMERICAL]
        37 : active_mean [NUMERICAL]
        33 : subflow_bwd_byts [NUMERICAL]
        33 : bwd_iat_min [NUMERICAL]
        31 : totlen_bwd_pkts [NUMERICAL]
        28 : bwd_iat_std [NUMERICAL]
        24 : bwd_iat_tot [NUMERICAL]
        24 : bwd_iat_max [NUMERICAL]
        22 : pkt_len_min [NUMERICAL]
        11 : fwd_pkt_len_min [NUMERICAL]
        11 : ece_flag_cnt [NUMERICAL]
        10 : rst_flag_cnt [NUMERICAL]
        10 : down/up_ratio [NUMERICAL]
        9 : idle_std [NUMERICAL]
        2 : flow_id [CATEGORICAL]
        2 : bwd_pkt_len_min [NUMERICAL]
        1 : fwd_psh_flags [NUMERICAL]

Attribute in nodes with depth <= 0:
        52 : totlen_fwd_pkts [NUMERICAL]
        38 : dst_ip [CATEGORICAL]
        36 : subflow_fwd_byts [NUMERICAL]
        28 : fwd_pkt_len_max [NUMERICAL]
        22 : fwd_seg_size_avg [NUMERICAL]
```

```
        20 : fwd_pkt_len_mean [NUMERICAL]
        18 : fwd_pkts/s [NUMERICAL]
        13 : flow_pkts/s [NUMERICAL]
        13 : flow_iat_max [NUMERICAL]
        12 : flow_duration [NUMERICAL]
        10 : dst_port [NUMERICAL]
        9 : flow_iat_mean [NUMERICAL]
        7 : flow_iat_min [NUMERICAL]
        6 : fwd_iat_min [NUMERICAL]
        4 : src_ip [CATEGORICAL]
        2 : fwd_iat_max [NUMERICAL]
        2 : bwd_pkts/s [NUMERICAL]
        1 : pkt_len_var [NUMERICAL]
        1 : pkt_len_std [NUMERICAL]
        1 : pkt_len_min [NUMERICAL]
        1 : init_fwd_win_byts [NUMERICAL]
        1 : fwd_pkt_len_std [NUMERICAL]
        1 : flow_byts/s [NUMERICAL]
        1 : bwd_seg_size_avg [NUMERICAL]
        1 : bwd_pkt_len_std [NUMERICAL]

Attribute in nodes with depth <= 1:
        82 : totlen_fwd_pkts [NUMERICAL]
        75 : subflow_fwd_byts [NUMERICAL]
        67 : dst_ip [CATEGORICAL]
        51 : fwd_pkt_len_max [NUMERICAL]
        49 : flow_iat_max [NUMERICAL]
        47 : fwd_pkt_len_mean [NUMERICAL]
        45 : flow_duration [NUMERICAL]
        35 : fwd_seg_size_avg [NUMERICAL]
        34 : fwd_pkts/s [NUMERICAL]
        32 : tot_fwd_pkts [NUMERICAL]
        30 : dst_port [NUMERICAL]
        27 : pkt_len_std [NUMERICAL]
        27 : flow_pkts/s [NUMERICAL]
        26 : subflow_fwd_pkts [NUMERICAL]
        25 : fwd_act_data_pkts [NUMERICAL]
        19 : fwd_header_len [NUMERICAL]
        19 : bwd_pkt_len_std [NUMERICAL]
        13 : flow_iat_mean [NUMERICAL]
        10 : src_port [NUMERICAL]
        10 : fwd_iat_tot [NUMERICAL]
        10 : bwd_seg_size_avg [NUMERICAL]
        9 : fwd_pkt_len_std [NUMERICAL]
        9 : fwd_iat_std [NUMERICAL]
        9 : flow_iat_min [NUMERICAL]
        8 : pkt_len_var [NUMERICAL]
        8 : bwd_pkt_len_mean [NUMERICAL]
```

```
        7 : src_ip [CATEGORICAL]
        7 : pkt_len_max [NUMERICAL]
        7 : fwd_iat_min [NUMERICAL]
        7 : bwd_pkt_len_max [NUMERICAL]
        5 : bwd_iat_std [NUMERICAL]
        5 : bwd_header_len [NUMERICAL]
        4 : init_fwd_win_byts [NUMERICAL]
        4 : bwd_pkts/s [NUMERICAL]
        3 : pkt_size_avg [NUMERICAL]
        3 : pkt_len_mean [NUMERICAL]
        3 : fwd_iat_mean [NUMERICAL]
        3 : fwd_iat_max [NUMERICAL]
        2 : totlen_bwd_pkts [NUMERICAL]
        2 : subflow_bwd_byts [NUMERICAL]
        2 : flow_iat_std [NUMERICAL]
        1 : tot_bwd_pkts [NUMERICAL]
        1 : rst_flag_cnt [NUMERICAL]
        1 : pkt_len_min [NUMERICAL]
        1 : flow_id [CATEGORICAL]
        1 : flow_byts/s [NUMERICAL]
        1 : down/up_ratio [NUMERICAL]
        1 : bwd_iat_tot [NUMERICAL]

Attribute in nodes with depth <= 2:
        127 : totlen_fwd_pkts [NUMERICAL]
        121 : subflow_fwd_byts [NUMERICAL]
        110 : dst_ip [CATEGORICAL]
        80 : flow_duration [NUMERICAL]
        76 : fwd_pkt_len_mean [NUMERICAL]
        74 : flow_iat_max [NUMERICAL]
        68 : fwd_act_data_pkts [NUMERICAL]
        65 : fwd_pkt_len_max [NUMERICAL]
        62 : fwd_seg_size_avg [NUMERICAL]
        59 : tot_fwd_pkts [NUMERICAL]
        57 : subflow_fwd_pkts [NUMERICAL]
        55 : pkt_len_std [NUMERICAL]
        51 : fwd_pkts/s [NUMERICAL]
        51 : dst_port [NUMERICAL]
        44 : fwd_header_len [NUMERICAL]
        41 : src_port [NUMERICAL]
        40 : flow_pkts/s [NUMERICAL]
        39 : fwd_iat_tot [NUMERICAL]
        38 : bwd_pkt_len_std [NUMERICAL]
        37 : src_ip [CATEGORICAL]
        37 : pkt_len_var [NUMERICAL]
        36 : flow_iat_mean [NUMERICAL]
        27 : fwd_iat_min [NUMERICAL]
        26 : flow_iat_min [NUMERICAL]
```

```
        24 : pkt_size_avg [NUMERICAL]
        24 : fwd_iat_mean [NUMERICAL]
        22 : pkt_len_max [NUMERICAL]
        22 : bwd_seg_size_avg [NUMERICAL]
        21 : bwd_pkt_len_mean [NUMERICAL]
        20 : pkt_len_mean [NUMERICAL]
        20 : fwd_iat_max [NUMERICAL]
        17 : fwd_pkt_len_std [NUMERICAL]
        17 : fwd_iat_std [NUMERICAL]
        17 : bwd_pkt_len_max [NUMERICAL]
        14 : bwd_pkts/s [NUMERICAL]
        11 : subflow_bwd_byts [NUMERICAL]
        11 : init_fwd_win_byts [NUMERICAL]
        10 : bwd_iat_std [NUMERICAL]
        10 : bwd_header_len [NUMERICAL]
        9 : flow_byts/s [NUMERICAL]
        8 : tot_bwd_pkts [NUMERICAL]
        8 : pkt_len_min [NUMERICAL]
        7 : totlen_bwd_pkts [NUMERICAL]
        7 : subflow_bwd_pkts [NUMERICAL]
        7 : flow_iat_std [NUMERICAL]
        5 : protocol [NUMERICAL]
        4 : fwd_seg_size_min [NUMERICAL]
        3 : idle_min [NUMERICAL]
        3 : bwd_iat_max [NUMERICAL]
        2 : rst_flag_cnt [NUMERICAL]
        2 : init_bwd_win_byts [NUMERICAL]
        2 : fwd_pkt_len_min [NUMERICAL]
        2 : down/up_ratio [NUMERICAL]
        2 : bwd_iat_tot [NUMERICAL]
        2 : active_max [NUMERICAL]
        1 : idle_std [NUMERICAL]
        1 : idle_mean [NUMERICAL]
        1 : idle_max [NUMERICAL]
        1 : flow_id [CATEGORICAL]
        1 : ece_flag_cnt [NUMERICAL]
        1 : bwd_iat_min [NUMERICAL]
        1 : bwd_iat_mean [NUMERICAL]
        1 : active_min [NUMERICAL]
        1 : active_mean [NUMERICAL]
        1 : ack_flag_cnt [NUMERICAL]

Attribute in nodes with depth <= 3:
        191 : dst_ip [CATEGORICAL]
        158 : subflow_fwd_byts [NUMERICAL]
        157 : totlen_fwd_pkts [NUMERICAL]
        118 : flow_duration [NUMERICAL]
        115 : flow_iat_max [NUMERICAL]
```

96 : fwd_pkt_len_mean [NUMERICAL]
95 : fwd_act_data_pkts [NUMERICAL]
95 : dst_port [NUMERICAL]
89 : fwd_pkt_len_max [NUMERICAL]
86 : src_port [NUMERICAL]
86 : fwd_iat_tot [NUMERICAL]
84 : subflow_fwd_pkts [NUMERICAL]
84 : pkt_len_std [NUMERICAL]
84 : fwd_seg_size_avg [NUMERICAL]
83 : tot_fwd_pkts [NUMERICAL]
79 : src_ip [CATEGORICAL]
79 : flow_iat_min [NUMERICAL]
68 : fwd_pkts/s [NUMERICAL]
64 : fwd_iat_min [NUMERICAL]
64 : fwd_header_len [NUMERICAL]
61 : fwd_iat_mean [NUMERICAL]
56 : flow_iat_mean [NUMERICAL]
55 : flow_pkts/s [NUMERICAL]
53 : bwd_pkt_len_std [NUMERICAL]
51 : pkt_len_var [NUMERICAL]
48 : fwd_iat_max [NUMERICAL]
47 : fwd_iat_std [NUMERICAL]
42 : pkt_size_avg [NUMERICAL]
42 : pkt_len_mean [NUMERICAL]
41 : init_fwd_win_byts [NUMERICAL]
39 : pkt_len_max [NUMERICAL]
39 : fwd_pkt_len_std [NUMERICAL]
39 : bwd_seg_size_avg [NUMERICAL]
39 : bwd_pkt_len_mean [NUMERICAL]
34 : flow_iat_std [NUMERICAL]
31 : bwd_pkt_len_max [NUMERICAL]
27 : bwd_pkts/s [NUMERICAL]
21 : flow_byts/s [NUMERICAL]
21 : bwd_header_len [NUMERICAL]
20 : subflow_bwd_pkts [NUMERICAL]
20 : subflow_bwd_byts [NUMERICAL]
18 : totlen_bwd_pkts [NUMERICAL]
17 : tot_bwd_pkts [NUMERICAL]
16 : bwd_iat_std [NUMERICAL]
13 : pkt_len_min [NUMERICAL]
12 : idle_min [NUMERICAL]
11 : protocol [NUMERICAL]
11 : ack_flag_cnt [NUMERICAL]
10 : init_bwd_win_byts [NUMERICAL]
10 : idle_max [NUMERICAL]
9 : idle_mean [NUMERICAL]
7 : fwd_seg_size_min [NUMERICAL]
7 : bwd_iat_tot [NUMERICAL]

```
        6 : bwd_iat_min [NUMERICAL]
        6 : bwd_iat_mean [NUMERICAL]
        5 : active_max [NUMERICAL]
        4 : bwd_iat_max [NUMERICAL]
        3 : rst_flag_cnt [NUMERICAL]
        3 : idle_std [NUMERICAL]
        3 : fwd_pkt_len_min [NUMERICAL]
        3 : ece_flag_cnt [NUMERICAL]
        3 : down/up_ratio [NUMERICAL]
        3 : active_mean [NUMERICAL]
        2 : timestamp [CATEGORICAL]
        2 : psh_flag_cnt [NUMERICAL]
        1 : flow_id [CATEGORICAL]
        1 : active_min [NUMERICAL]

Attribute in nodes with depth <= 5:
        457 : dst_ip [CATEGORICAL]
        271 : src_port [NUMERICAL]
        237 : dst_port [NUMERICAL]
        232 : src_ip [CATEGORICAL]
        193 : flow_duration [NUMERICAL]
        184 : init_fwd_win_byts [NUMERICAL]
        181 : subflow_fwd_byts [NUMERICAL]
        178 : fwd_iat_tot [NUMERICAL]
        178 : flow_iat_min [NUMERICAL]
        172 : totlen_fwd_pkts [NUMERICAL]
        170 : flow_iat_max [NUMERICAL]
        144 : fwd_iat_mean [NUMERICAL]
        139 : fwd_iat_min [NUMERICAL]
        133 : fwd_iat_std [NUMERICAL]
        131 : flow_iat_std [NUMERICAL]
        129 : fwd_header_len [NUMERICAL]
        128 : fwd_pkt_len_mean [NUMERICAL]
        125 : fwd_iat_max [NUMERICAL]
        125 : flow_iat_mean [NUMERICAL]
        122 : subflow_fwd_pkts [NUMERICAL]
        121 : tot_fwd_pkts [NUMERICAL]
        120 : fwd_act_data_pkts [NUMERICAL]
        117 : fwd_pkts/s [NUMERICAL]
        115 : fwd_pkt_len_max [NUMERICAL]
        109 : fwd_seg_size_avg [NUMERICAL]
        107 : flow_pkts/s [NUMERICAL]
        102 : pkt_len_std [NUMERICAL]
        72 : pkt_len_var [NUMERICAL]
        69 : pkt_size_avg [NUMERICAL]
        64 : bwd_pkt_len_std [NUMERICAL]
        64 : ack_flag_cnt [NUMERICAL]
        58 : pkt_len_max [NUMERICAL]
```

```
        57 : idle_min [NUMERICAL]
        54 : pkt_len_mean [NUMERICAL]
        54 : fwd_pkt_len_std [NUMERICAL]
        53 : bwd_pkts/s [NUMERICAL]
        50 : bwd_seg_size_avg [NUMERICAL]
        48 : idle_mean [NUMERICAL]
        48 : bwd_pkt_len_mean [NUMERICAL]
        47 : tot_bwd_pkts [NUMERICAL]
        44 : idle_max [NUMERICAL]
        43 : bwd_pkt_len_max [NUMERICAL]
        42 : subflow_bwd_pkts [NUMERICAL]
        42 : flow_byts/s [NUMERICAL]
        37 : bwd_header_len [NUMERICAL]
        30 : init_bwd_win_byts [NUMERICAL]
        26 : totlen_bwd_pkts [NUMERICAL]
        24 : protocol [NUMERICAL]
        23 : bwd_iat_std [NUMERICAL]
        22 : subflow_bwd_byts [NUMERICAL]
        22 : fwd_seg_size_min [NUMERICAL]
        21 : timestamp [CATEGORICAL]
        20 : pkt_len_min [NUMERICAL]
        14 : bwd_iat_min [NUMERICAL]
        14 : bwd_iat_mean [NUMERICAL]
        13 : active_mean [NUMERICAL]
        11 : bwd_iat_max [NUMERICAL]
        11 : active_min [NUMERICAL]
        10 : bwd_iat_tot [NUMERICAL]
        9 : psh_flag_cnt [NUMERICAL]
        9 : active_max [NUMERICAL]
        8 : rst_flag_cnt [NUMERICAL]
        7 : fwd_pkt_len_min [NUMERICAL]
        7 : ece_flag_cnt [NUMERICAL]
        6 : idle_std [NUMERICAL]
        4 : down/up_ratio [NUMERICAL]
        2 : flow_id [CATEGORICAL]
        1 : bwd_pkt_len_min [NUMERICAL]

Condition type in nodes:
        13624 : HigherCondition
        2405 : ContainsCondition
        1395 : ContainsBitmapCondition
Condition type in nodes with depth <= 0:
        258 : HigherCondition
        42 : ContainsBitmapCondition
Condition type in nodes with depth <= 1:
        772 : HigherCondition
        75 : ContainsBitmapCondition
Condition type in nodes with depth <= 2:
```

```
        1616 : HigherCondition
        147 : ContainsBitmapCondition
        1 : ContainsCondition
Condition type in nodes with depth <= 3:
        2714 : HigherCondition
        267 : ContainsBitmapCondition
        6 : ContainsCondition
Condition type in nodes with depth <= 5:
        4968 : HigherCondition
        658 : ContainsBitmapCondition
        54 : ContainsCondition
Node format: NOT_SET

Training OOB:
        trees: 1, Out-of-bag evaluation: accuracy:0.999989 logloss:0.000387675
        trees: 7, Out-of-bag evaluation: accuracy:0.999996 logloss:0.000110349
        trees: 12, Out-of-bag evaluation: accuracy:0.999996 logloss:4.4888e-05
        trees: 15, Out-of-bag evaluation: accuracy:0.999998 logloss:1.98903e-05
        trees: 20, Out-of-bag evaluation: accuracy:0.999999 logloss:1.79278e-05
        trees: 23, Out-of-bag evaluation: accuracy:0.999999 logloss:1.05264e-05
        trees: 26, Out-of-bag evaluation: accuracy:0.999999 logloss:1.0468e-05
        trees: 31, Out-of-bag evaluation: accuracy:0.999999 logloss:1.01551e-05
        trees: 35, Out-of-bag evaluation: accuracy:0.999999 logloss:9.40367e-06
        trees: 41, Out-of-bag evaluation: accuracy:0.999999 logloss:9.3936e-06
        trees: 47, Out-of-bag evaluation: accuracy:0.999999 logloss:9.44069e-06
        trees: 51, Out-of-bag evaluation: accuracy:0.999999 logloss:9.45451e-06
        trees: 56, Out-of-bag evaluation: accuracy:0.999999 logloss:9.70042e-06
        trees: 60, Out-of-bag evaluation: accuracy:0.999999 logloss:9.52045e-06
        trees: 63, Out-of-bag evaluation: accuracy:0.999999 logloss:9.39215e-06
        trees: 66, Out-of-bag evaluation: accuracy:0.999999 logloss:9.34759e-06
        trees: 70, Out-of-bag evaluation: accuracy:0.999999 logloss:9.37471e-06
        trees: 75, Out-of-bag evaluation: accuracy:0.999999 logloss:9.35624e-06
        trees: 81, Out-of-bag evaluation: accuracy:0.999999 logloss:9.48176e-06
        trees: 84, Out-of-bag evaluation: accuracy:0.999999 logloss:9.62356e-06
        trees: 88, Out-of-bag evaluation: accuracy:0.999999 logloss:9.66675e-06
        trees: 92, Out-of-bag evaluation: accuracy:0.999999 logloss:9.63805e-06
        trees: 97, Out-of-bag evaluation: accuracy:0.999999 logloss:9.49868e-06
        trees: 101, Out-of-bag evaluation: accuracy:0.999999 logloss:9.4608e-06
        trees: 104, Out-of-bag evaluation: accuracy:0.999999 logloss:9.46038e-06
        trees: 109, Out-of-bag evaluation: accuracy:0.999999 logloss:9.49427e-06
        trees: 112, Out-of-bag evaluation: accuracy:0.999999 logloss:9.41738e-06
        trees: 116, Out-of-bag evaluation: accuracy:0.999999 logloss:9.63863e-06
        trees: 120, Out-of-bag evaluation: accuracy:0.999999 logloss:9.57974e-06
        trees: 123, Out-of-bag evaluation: accuracy:0.999999 logloss:9.58727e-06
        trees: 127, Out-of-bag evaluation: accuracy:0.999999 logloss:9.62461e-06
        trees: 133, Out-of-bag evaluation: accuracy:0.999999 logloss:9.72517e-06
        trees: 139, Out-of-bag evaluation: accuracy:0.999999 logloss:9.83346e-06
        trees: 144, Out-of-bag evaluation: accuracy:0.999999 logloss:9.77996e-06
```

```
trees: 148, Out-of-bag evaluation: accuracy:0.999999 logloss:9.79225e-06
trees: 151, Out-of-bag evaluation: accuracy:0.999999 logloss:9.83586e-06
trees: 156, Out-of-bag evaluation: accuracy:0.999999 logloss:1.00301e-05
trees: 160, Out-of-bag evaluation: accuracy:0.999999 logloss:1.00214e-05
trees: 163, Out-of-bag evaluation: accuracy:0.999999 logloss:1.00815e-05
trees: 167, Out-of-bag evaluation: accuracy:0.999999 logloss:1.02347e-05
trees: 171, Out-of-bag evaluation: accuracy:0.999999 logloss:1.05445e-05
trees: 174, Out-of-bag evaluation: accuracy:0.999999 logloss:1.06056e-05
trees: 179, Out-of-bag evaluation: accuracy:0.999999 logloss:1.05279e-05
trees: 185, Out-of-bag evaluation: accuracy:0.999999 logloss:1.05152e-05
trees: 191, Out-of-bag evaluation: accuracy:0.999999 logloss:1.05195e-05
trees: 193, Out-of-bag evaluation: accuracy:0.999999 logloss:1.05138e-05
trees: 198, Out-of-bag evaluation: accuracy:0.999999 logloss:1.0463e-05
trees: 201, Out-of-bag evaluation: accuracy:0.999999 logloss:1.04812e-05
trees: 204, Out-of-bag evaluation: accuracy:0.999999 logloss:1.04716e-05
trees: 209, Out-of-bag evaluation: accuracy:0.999999 logloss:1.04763e-05
trees: 215, Out-of-bag evaluation: accuracy:0.999999 logloss:1.04089e-05
trees: 221, Out-of-bag evaluation: accuracy:0.999999 logloss:1.0499e-05
trees: 226, Out-of-bag evaluation: accuracy:0.999999 logloss:1.05068e-05
trees: 231, Out-of-bag evaluation: accuracy:0.999999 logloss:1.05698e-05
trees: 233, Out-of-bag evaluation: accuracy:0.999999 logloss:1.05411e-05
trees: 238, Out-of-bag evaluation: accuracy:0.999999 logloss:1.08798e-05
trees: 242, Out-of-bag evaluation: accuracy:0.999999 logloss:1.0928e-05
trees: 246, Out-of-bag evaluation: accuracy:0.999999 logloss:1.09242e-05
trees: 249, Out-of-bag evaluation: accuracy:0.999999 logloss:1.09359e-05
trees: 255, Out-of-bag evaluation: accuracy:0.999999 logloss:1.09759e-05
trees: 261, Out-of-bag evaluation: accuracy:0.999999 logloss:1.09999e-05
trees: 267, Out-of-bag evaluation: accuracy:0.999999 logloss:1.0965e-05
trees: 273, Out-of-bag evaluation: accuracy:0.999999 logloss:1.10039e-05
trees: 279, Out-of-bag evaluation: accuracy:0.999999 logloss:1.09377e-05
trees: 284, Out-of-bag evaluation: accuracy:0.999999 logloss:1.09686e-05
trees: 287, Out-of-bag evaluation: accuracy:0.999999 logloss:1.09746e-05
trees: 291, Out-of-bag evaluation: accuracy:0.999999 logloss:1.1007e-05
trees: 296, Out-of-bag evaluation: accuracy:0.999999 logloss:1.09636e-05
trees: 300, Out-of-bag evaluation: accuracy:0.999999 logloss:1.10132e-05
```

[13]:
```
# Erstellen der Feature Importance Kriterien aus Sicht des TensorFlow Modells
model.make_inspector().variable_importances()
```

[13]:
```
{'NUM_AS_ROOT': [("totlen_fwd_pkts" (1; #81), 52.0),
  ("dst_ip" (4; #24), 38.0),
  ("subflow_fwd_byts" (1; #74), 36.0),
  ("fwd_pkt_len_max" (1; #45), 28.0),
  ("fwd_seg_size_avg" (1; #52), 22.0),
  ("fwd_pkt_len_mean" (1; #46), 20.0),
  ("fwd_pkts/s" (1; #50), 18.0),
```

```
("flow_iat_max" (1; #30), 13.0),
("flow_pkts/s" (1; #35), 13.0),
("flow_duration" (1; #29), 12.0),
("dst_port" (1; #25), 10.0),
("flow_iat_mean" (1; #31), 9.0),
("flow_iat_min" (1; #32), 7.0),
("fwd_iat_min" (1; #42), 6.0),
("src_ip" (4; #70), 4.0),
("bwd_pkts/s" (1; #18), 2.0),
("fwd_iat_max" (1; #40), 2.0),
("flow_byts/s" (1; #28), 1.0),
("pkt_len_std" (1; #64), 1.0),
("bwd_pkt_len_std" (1; #16), 1.0),
("pkt_len_min" (1; #63), 1.0),
("fwd_pkt_len_std" (1; #48), 1.0),
("bwd_seg_size_avg" (1; #20), 1.0),
("init_fwd_win_byts" (1; #60), 1.0),
("pkt_len_var" (1; #65), 1.0)]}
```