```
!pip install pefile
```

```
Collecting pefile
  Downloading
     https://files.pythonhosted.org/packages/36/58/acf7f35859d541985f0a6ea3c34b |
     ████████████████████████████████| 71kB 2.1MB/s
Requirement already satisfied: future in /usr/local/lib/python3.6/dist-packages
(from pe
Building wheels for collected packages: pefile
  Building wheel for pefile (setup.py) ... done
Created wheel for pefile: filename=pefile-2019.4.18-cp36-none-any.whl size=60824 sha25
  Stored in directory:
/root/.cache/pip/wheels/1c/a1/95/4f33011a0c013c872fe6f0f364dc463a Successfully
built pefile
Installing collected packages: pefile
Successfully installed pefile-2019.4.18
```

```
import os
directoriesWithLabels = [("Samples/Benign",0), ("Samples/Malware",1)]
listOfSamples = []
labels = []
for datasetPath, label in
    directoriesWithLabels: samples = [f for f
    in os.listdir(datasetPath)] for file in
    samples:
        filePath = os.path.join(datasetPath, file)
        listOfSamples.append(filePath)
        labels.append(label)
```

```
#Train-Test data split
from sklearn.model_selection import train_test_split
samples_train, samples_test, labels_train, labels_test = train_test_split(listOfSamples,
labe
```

```
from google.colab import drive
drive.mount('/content/drive')
```

```
Go to this URL in a browser: https://accounts.google.com/o/oauth2/auth?
client_id=9473189

Enter your authorization code:
··········
Mounted at /content/drive
```

Download and install Ember:

```
!wget https://github.com/endgameinc/ember/archive/master.zip
!unzip master.zip
!rm master.zip
!cp -r ember-master/* .
```

```
!rm -r ember-master
!pip install -r requirements.txt
!python setup.py install
```

```
--2020-05-02 05:34:40--  https://github.com/endgameinc/ember/archive/master.zip
Resolving github.com (github.com)... 140.82.113.3
Connecting to github.com (github.com)|140.82.113.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/endgameinc/ember/zip/master [following]
--2020-05-02 05:34:40--  https://codeload.github.com/endgameinc/ember/zip/master
Resolving codeload.github.com (codeload.github.com)... 140.82.112.10
Connecting to codeload.github.com (codeload.github.com)|140.82.112.10|:443...
connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: ‘master.zip’

master.zip              [  <=>               ]  11.22M  16.1MB/s   in 0.7s

2020-05-02 05:34:41 (16.1 MB/s) - ‘master.zip’ saved [11769324]

Archive: master.zip
f9a018632ba108b4e25c33d6c3e2e7a7c4487f58
   creating: ember-master/
  inflating: ember-master/LICENSE.txt
  inflating: ember-master/README.md
   creating: ember-master/ember/
  inflating: ember-master/ember/__init__.py
  inflating: ember-master/ember/features.py
   creating: ember-master/licenses/
  inflating: ember-master/licenses/AGPL-LICENSE-3.0.txt
  inflating: ember-master/licenses/MIT-LICENSE.txt
   creating: ember-master/malconv/
  inflating: ember-master/malconv/README.md
  inflating: ember-master/malconv/malconv.h5
  inflating: ember-master/malconv/malconv.py
  inflating: ember-master/malconv/multi_gpu.py
  inflating: ember-master/requirements.txt
  inflating: ember-master/requirements_conda.txt
  inflating: ember-master/requirements_notebook.txt
   creating: ember-master/resources/
  inflating: ember-master/resources/ember-notebook.ipynb
  inflating: ember-master/resources/ember2018-notebook.ipynb
  inflating: ember-master/resources/logo.png
   creating: ember-master/scripts/
  inflating: ember-master/scripts/classify_binaries.py
  inflating: ember-master/scripts/train_ember.py
  inflating: ember-master/setup.py
Collecting lief>=0.9.0
  Downloading
     https://files.pythonhosted.org/packages/f7/38/e6bf942cf2ee073bf81fa3324bca |
     ████████████████████████████████| 3.5MB 2.8MB/s
Requirement already satisfied: tqdm>=4.31.0 in /usr/local/lib/python3.6/dist-
packages (f
Requirement already satisfied: numpy>=1.16.3 in /usr/local/lib/python3.6/dist-
packages (
Requirement already satisfied: pandas>=0.24.2 in /usr/local/lib/python3.6/dist-
packages
Requirement already satisfied: lightgbm>=2.2.3 in /usr/local/lib/python3.6/dist-
packages
Requirement already satisfied: scikit-learn>=0.20.3 in
/usr/local/lib/python3.6/dist-pac
Requirement already satisfied: python-dateutil>=2.6.1 in
/usr/local/lib/python3.6/dist-p
```

```
Requirement already satisfied: pytz>=2017.2 in /usr/local/lib/python3.6/dist-
packages (f
Requirement already satisfied: scipy in /usr/local/lib/python3.6/dist-packages (from
lig
Requirement already satisfied: joblib>=0.11 in /usr/local/lib/python3.6/dist-
packages (f
Requirement already satisfied: six>=1.5 in /usr/local/lib/python3.6/dist-
packages (from
Installing collected packages: lief
S       f ll   i   t ll d li f 0    0
```

```
Successfully installed lief-0.10.1
running install
running bdist_egg
running egg_info
creating ember.egg-info
writing ember.egg-info/PKG-INFO
writing dependency_links to
ember.egg-info/dependency_links.txt writing requirements
to ember.egg-info/requires.txt
writing top-level names to ember.egg-info/top_level.txt
writing manifest file 'ember.egg-info/SOURCES.txt'
reading manifest file 'ember.egg-info/SOURCES.txt'
writing manifest file 'ember.egg-info/SOURCES.txt'
installing library code to build/bdist.linux-x86_64/egg
running install_lib
running build_py
creating build
creating build/lib
creating build/lib/ember
copying ember/features.py -> build/lib/ember
copying ember/__init__.py -> build/lib/ember
creating build/bdist.linux-x86_64
creating build/bdist.linux-x86_64/egg
creating build/bdist.linux-x86_64/egg/ember
copying build/lib/ember/features.py ->
build/bdist.linux-x86_64/egg/ember copying
build/lib/ember/__init__.py -> build/bdist.linux-x86_64/egg/ember
byte-compiling         build/bdist.linux-x86_64/egg/ember/features.py         to
features.cpython-36.pyc                                                byte-compiling
build/bdist.linux-x86_64/egg/ember/__init__.py    to    __init__.cpython-36.pyc
creating build/bdist.linux-x86_64/egg/EGG-INFO
copying ember.egg-info/PKG-INFO -> build/bdist.linux-x86_64/egg/EGG-INFO
copying ember.egg-info/SOURCES.txt -> build/bdist.linux-x86_64/egg/EGG-INFO
copying ember.egg-info/dependency_links.txt -> build/bdist.linux-x86_64/egg/EGG-
INFO
copying ember.egg-info/requires.txt -> build/bdist.linux-x86_64/egg/EGG-INFO
copying ember.egg-info/top_level.txt -> build/bdist.linux-x86_64/egg/EGG-INFO
zip_safe flag not set; analyzing archive contents...
creating dist
creating 'dist/ember-0.1.0-py3.6.egg' and adding
'build/bdist.linux-x86_64/egg' to it removing 'build/bdist.linux-x86_64/egg'
(and everything under it) Processing ember-0.1.0-py3.6.egg
Copying ember-0.1.0-py3.6.egg to /usr/local/lib/python3.6/dist-
packages Adding ember 0.1.0 to easy-install.pth file

Installed /usr/local/lib/python3.6/dist-packages/ember-0.1.0-py3.6.egg
Processing dependencies for ember==0.1.0
Searching for scikit-learn==0.22.2.post1
Best match: scikit-learn 0.22.2.post1
Adding scikit-learn 0.22.2.post1 to easy-install.pth file

Using /usr/local/lib/python3.6/dist-packages Read vectorized
features from the data les.
Searching for lightgbm==2.2.3
Best match: lightgbm 2.2.3
Adding lightgbm 2.2.3 to easy-install.pth file
import ember
X_train, y_train, X_test, y_test = ember.read_vectorized_features("drive/My Drive/vMalConv1/" Using
/usr/local/lib/python3.6/dist-packages
metadata_dataframe = ember.read_metadata("drive/My Drive/vMalConv1/")
Searching for pandas==1.0.3
Best match: pandas 1.0.3
Adding pandas 1.0.3 to easy-install.pth file
```

```
Using /usr/local/lib/python3.6/dist-packages
```

```
Searching for numpy==1.18.3
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
Best match: numpy 1.18.3
WARNING: lief version 0.10.1-bfe5414 found instead. There may be slight inconsistencie Adding numpy 1.18.3 to easy-
install.pth file
WARNING:  in the feature calculations.
Installing f2py script to /usr/local/bin
/usr/local/lib/python3.6/dist-packages/numpy/lib/arraysetops.py:569: FutureWarning: elem Installing f2py3 script to
/usr/local/bin
  mask |= (ar1 == a)
Installing f2py3.6 script to /usr/local/bin

Using /usr/local/lib/python3.6/dist-packages
Searching for tqdm==4.38.0
#ClientPEBest.pymatcodeh: tqdm 4.38.0
importAddingboto3 tqdm 4.38.0 to easy-install.pth file
importInstallingnumpyas nptqdm script to /usr/local/bin
import argparse
     Using /usr/local/lib/python3.6/dist-packages import
ast
     Searching for lief==0.10.1
from sklearn.preprocessingBestmatch:lief0.10.1import RobustScaler
     Adding lief 0.10.1 to easy-install.pth file
### Change the following to the correct endpoint name ###
myEndpoUsintNameg/usr/loc='sagemakerl/lib/py-tensorflowhon3.6/dist-2020-
packages-05-02-04-36-51-919' def main():Searching for
scipy==1.4.1
     Best match: scipy 1.4.1
     Adding scipy 1.4.1 to easy-install.pth file
    import json
    import ember
     Using /usr/local/lib/python3.6/dist-packages
     Searching for joblib==0.14.1
    fromBestsklearn.preprocessingmatch:joblib0.14.1 import RobustScaler
    rsAdding=RobustScaler()joblib0.14.1 to easy-install.pth file

    parserUsing =/usargparse/local/lib/python3.ArgumentParser().6/dist-packages
      Searching for pytz==2018.9
    parser.add_argument("-v", "--featureversion", type=int, default=2, help="EMBER feature ve Best match: pytz
     2018.9
    parser.add_argument("binaries", metavar="BINARIES", type=str, nargs="+", help="PE files t Adding pytz
     2018.9 to easy-install.pth file
    args = parser.parse_args()
    #opening the downloaded PE file
     Using /usr/local/lib/python3.6/dist-packages
    testpe = open(args.binaries[0],'rb').read()
     Searching for python-dateutil==2.8.1
    #FeatureBstmatch:extractorpyhonclass-dteutilofthe2.8ember.1 project
    extractAdding =pythonember-.dateutilPEFeatureExtractor()2.8.1easy-install.pth
    file
    data = extract.feature_vector(testpe) #vectorizing the extracted features
    scaledUsing_data/usr/local/lib/python3=rs.fittransform([data]).6/ist-
    packages
      Searching for six==1.12.0
    Xdata = np.reshape(scaled_data,(1, 2381))
      Best match: six 1.12.0
    Xdata= Xdata.tolist()
     Adding six 1.12.0 to easy-install.pth file

    clientUsing =/usr/local/lib/python3.6/distboto3.client('runtime.sagemaker',-
    packages
          region_name='us-east-1',
     Finished processing dependencies for ember==0.1.0
                               #### Change the following to your AWS credentials ####
       aws_access_key_id='ASIAV72BNHYBIA4QZPCA',
       aws_secret_access_key='lmpi3DYqvwyw98TfVbCE8FmS6riEi89YH3BzAS6A',
       aws_session_token='FwoGZXIvYXdzEBYaDO9p8bs/
       YCcEIECEciLGAYEiASQ781BY8LJxaRpjqj5xsW2x6a

    response = client.invoke_endpoint(EndpointName=myEndpointName,
    Body=json.dumps(Xdata))
```

```
        response_body = response['Body']
        out = response_body.read()
        astr = out.decode("UTF-8")
        out = ast.literal_eval(astr)
        out = out['outputs']['score']['floatVal']
```

```
    if out[0] >0.5:
        print("Malicious")
    else:
        print("Benign")
```

Malicious Tests

```
!python clientPE.py
/content/Samples/Malware/VirusShare_2a53d20292b250b8fbba31d3d247cc26.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Malicious
```

```
!python clientPE.py
/content/Samples/Malware/VirusShare_2bca410519250ba329e1f04689299807.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Malicious
```

```
!python clientPE.py
/content/Samples/Malware/VirusShare_3deab418505d2d4d7d97c3ebc5ab66e5.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Malicious
```

```
!python clientPE.py
/content/Samples/Malware/VirusShare_4a0bf367c39e71c2342fca939325ddcd.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Malicious
```

```
!python clientPE.py
/content/Samples/Malware/VirusShare_4c87db0339f1ce57247d6c597773d0f8.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Malicious
```

```
!python clientPE.py
/content/Samples/Malware/VirusShare_5c62bacc1aaa80b56fd86a6acdead49a.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Malicious
```

```
!python clientPE.py
/content/Samples/Malware/VirusShare_6c6f9b3777d9152bbb6dafbaf0c57d52.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Malicious
```

```
!python clientPE.py
/content/Samples/Malware/VirusShare_7b6594becbf9803e85d33b72d7e7090e.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Malicious
```

```
!python clientPE.py
/content/Samples/Malware/VirusShare_8d8332c9da04cdaf4097ececf4871ccb.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Malicious
```

```
!python clientPE.py
/content/Samples/Malware/VirusShare_9a3eaa431c7232f6b7390c152b4e0f8e.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Malicious
```

```
!python clientPE.py
/content/Samples/Malware/VirusShare_9fbcb7c103313f32e2c418fd72aab1d4.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Malicious
```

Benign Tests

```
!python clientPE.py /content/Samples/Benign/printf.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Benign
```

```
!python clientPE.py /content/Samples/Benign/colorify.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Benign
```

```
! th   li  tPE   /   t  t/S   l  /B  i  / h  d
```

```
!python clientPE.py /content/Samples/Benign/chmod.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Benign
```

```
!python clientPE.py /content/Samples/Benign/color-to-alpha.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Benign
```

```
!python clientPE.py /content/Samples/Benign/antialias.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Benign
```

```
!python clientPE.py /content/Samples/Benign/LogCollector.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
lief error: This file is not a PE binary
Benign
```

```
!python clientPE.py /content/Samples/Benign/bsqldb.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Benign
```

```
!python clientPE.py /content/Samples/Benign/blur.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Benign
```

```
!python clientPE.py /content/Samples/Benign/aspnetca.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
lief error: This file is not a PE binary
```

```
Benign
```

```
!python clientPE.py /content/Samples/Benign/wc.exe
```

```
WARNING: EMBER feature version 2 were computed using lief version 0.9.0-
WARNING:  lief version 0.10.1-bfe5414 found instead. There may be slight
inconsistencie
WARNING:  in the feature calculations.
Benign
```