


# Save and Load Machine Learning Models in Python with scikit-learn

by **Jason Brownlee** on June 8, 2016 in **Python Machine Learning**



Finding an accurate machine learning model is not the end of the project.

In this post you will discover how to save and load your machine learning model in Python using scikit-learn.

This allows you to save your model to file and load it later in order to make predictions.

Let's get started.

- **Update Jan/2017**: Updated to reflec
- **Update March/2018**: Added alterna
  appears to have been taken down.

Save and Load Machine Learning Models in Python with scikit-learn
Photo by Christine, some rights reserved.



## Finalize Your Model wit

Pickle is the standard way of serializing

You can use the pickle operation to seria ne serialized format to a file.

Later you can load this file to deserialize

The example below demonstrates how y ma Indians onset of diabetes dataset, save the unseen test set (update: download fr

```
# Save Model Using Pickle
import pandas
from sklearn import model_selection
from sklearn.linear_model import LogisticRegression
import pickle
url = "https://raw.githubusercontent.com/jbrownlee/Datasets/master/pima-indians-di
names = ['preg', 'plas', 'pres', 'skin', 'test', 'mass', 'pedi', 'age', 'class']
dataframe = pandas.read_csv(url, names=names)
array = dataframe.values
X = array[:,0:8]
Y = array[:,8]
test_size = 0.33
seed = 7
X_train, X_test, Y_train, Y_test = model_selection.train_test_split(X, Y, test_siz
# Fit the model on 33%
model = LogisticRegression()
model.fit(X_train, Y_train)
# save the model to disk
filename = 'finalized_model.sav'
pickle.dump(model, open(filename, 'wb'))

# some time later...

# load the model from disk
loaded_model = pickle.load(open(filename, 'rb'))
result = loaded_model.score(X_test, Y_test)
print(result)
```

Running the example saves the model to **finalized_model.sav** in your local working directory. Load the saved model and evaluating it provides an estimate of accuracy of the model on unseen data.

```
0.755905511811
```

# Finalize Your Model with joblib

Joblib is part of the SciPy ecosystem an

It provides utilities for saving and loadin
structures, efficiently.

This can be useful for some machine lea
store the entire dataset (like K-Nearest N

The example below demonstrates how y
Indians onset of diabetes dataset, saves
predictions on the unseen test set.

```
# Save Model Using joblib
import pandas
from sklearn import model_selecti
from sklearn.linear_model import
from sklearn.externals import job
url = "https://raw.githubusercont
```

```
names = ['preg', 'plas', 'pres', 'skin', 'test', 'mass', 'pedi', 'age', 'class']
dataframe = pandas.read_csv(url, names=names)
array = dataframe.values
X = array[:,0:8]
Y = array[:,8]
test_size = 0.33
seed = 7
X_train, X_test, Y_train, Y_test = model_selection.train_test_split(X, Y, test_siz
# Fit the model on 33%
model = LogisticRegression()
model.fit(X_train, Y_train)
# save the model to disk
filename = 'finalized_model.sav'
joblib.dump(model, filename)

# some time later...

# load the model from disk
loaded_model = joblib.load(filename)
result = loaded_model.score(X_test, Y_test)
print(result)
```

Running the example saves the model to file as **finalized_model.sav** and also creates one file for each NumPy array in the model (four additional files). After the model is loaded an estimate of the accuracy of the model on unseen data is reported.

```
0.755905511811
```

## Tips for Finalizing Your Model

This section lists some important considerations when finalizing your machine learning models.

- **Python Version**. Take note of the p ame major (and maybe minor) version of r load it and deserialize it.
- **Library Versions**. The version of a project almost certainly need to be t is not limited to the version of NumPy
- **Manual Serialization**. You might lik ed model so that you can use them dir e. Often the algorithms used by machi ot simpler than those used to learn the custom code that you have control

Take note of the version so that you can cannot reload your model on another ma

## Summary

In this post you discovered how to persist your machine learning algorithms in Python with scikit-learn.

You learned two techniques that you can use:

- The pickle API for serializing standard Python objects.
- The joblib API for efficiently serializing Python objects with NumPy arrays.

Do you have any questions about saving and loading your machine learning algorithms or about this post? Ask your questions in the comments and I will do my best to answer them.



**About Jason Brownl**

Jason Brownlee, PhD is a
to get results with modern
View all posts by Jason Br

‹ Binary Classification Tutorial with the Keras De
Regr
non ›

## 146 Responses to *Save and Load Machine Learning Models in Python with scikit-learn*

**Kayode** October 18, 2016 at 6:15 pm #

REPLY

Thank you so much for this educative post.

**Jason Brownlee** October 19, 2016 at 9:17 am #

REPLY

You're welcome Kayode.

**TonyD** November 13, 2016 at 3:52 pm #

REPLY

Hi Jason,

I have two of your books and they are awesome. I took several machine learning courses before, however as you mentioned they are more geared towards theory than practicing. I devoured your Machine Learnign with Python book and 20x my skills compared to the courses I took.

I found this page by Googling a code snippet in chapter 17 in your book. The line:

loaded_model = pickle.load(open(filenar

throws the error:

runfile('C:/Users/Tony/Documents/Mass
/Tony/Documents')
File "C:/Users/Tony/Documents/MassDa
loaded_model = pickle.load(open(filenar
^
SyntaxError: invalid syntax

**Jason Brownlee** November 14, 2016 at 7:36 am #

REPLY

Thanks TonyD.

I wonder if there is a copy-paste error, like an extra space or something?

Does the code example (.py file) provided with the book for that chapter work for you?

**William** January 7, 2019 at 9:37 pm #

REPLY

As Jason already said, this is a copy paste problem. In your line specifically, the quotes are the problem.

```
loaded_model = pickle.load(open(filename, ‘rb’))
```

It should be

```
loaded_model = pickle.load(open(filename, 'rb'))
```

Try to understand the difference :).

**Jason Brownlee** January 8, 2019 at 6:49 am #

REPLY

Thanks.

This might help:
https://machinelearningmastery.com/faq/single-faq/how-do-i-copy-code-from-a-tutorial

**Konstantin** November 19, 2016 at 6:01 am #

REPLY

Hello, Jason

Where we can get X_test, Y_test “sometime later”? It is “garbag collected”!
X_test, Y_test not pickled In your example you pickle classifier only but you keep refer to x and y. Real applications is not single flow I found work around and get Y from clf.classes_ object.

What is correct solution? Should we pickle decorator class with X and Y or use pickled classifier to pull Ys values? I didn’t find legal information from documentation on KNeighborclassifier(my example) as well; how to pull Y values from classifier.

Can you advise?

**Jason Brownlee** November 19, 2016 at 8:51 am #

REPLY

Hi Konstantin,

I would not suggest saving the data. The idea is to show how to load the model and use it on new data – I use existing data just for demonstration purposes.

You can load new data from file in the future when you load your model and use that new data to make a prediction.

If you have the expected values also (y), you can compare the predictions to the expected values and see how well the model performed.

**Guangping Zhang** N

I’m newer Pythoner, yc
used windows 10.

**Jason Brownlee**

Thanks Guangping

The save file is in your curre
commandline.

If you’re using a notebook c

**Mohammed Alnemari** December 13, 2016 at 2:45 pm #

REPLY

Hi Jason ,
I am just wondering if can we use Yaml or Json with sklearn library . I tried to do it many times but I could not reach to an answer . I tried to do it as your lesson of Kares , but for some reason is not working . hopefully you can help me if it is possible

**Jason Brownlee** December 14, 2016 at 8:24 am #

REPLY

Hi Mohammed, I believe the serialization of models to yaml and json is specific to the Keras library.

sklearn serialization is focused on binary files like pickle.

**Normando Zubia** December 29, 2016 at 9:55 am #

REPLY

Hi, my name is Normando Zubia and I have been reading a lot of your material for my school lessons.

I'm currently working on a model to predict user behavoir in a production environment. Due to several situations I can not save the model in a pickle file. Do you know any way to save the model in a json file?

I have been playing a little with sklearn classes and I noticed that if I save some parameters for example: n_values_, feature_indices_ and active_features_ in a OneHotEncoding model I can reproduce the results. Could this be
each model's parameters to load each r

PS: Sorry for my bad english and thanks

**Jason Brownlee** Decembe

Hi Normando,

If you are using a simple model, you
then try and put them back in a new
algorithm yourself (very easy for mo

Let me know how you go.

**Samuel** February 6, 2017 at 3:14 pm #

REPLY

Hello Jason,

I am new to machine learning. I am your big fan and read a lot of your blog and books. Thank you very much for teaching us machine learning.

I tried to pickle my model but fail. My model is using VGG16 and replace the top layer for my classification solution. I further narrowed down the problem and find that it is the VGG16 model failed to pickle. Please find my simplified code below and error log below:

It will be highly appreciated if you can give me some direction on how to fix this error.

Thank you very much

———————————————————-

```
# Save Model Using Pickle
from keras.applications.vgg16 import VGG16
import pickle

model = VGG16(weights='imagenet', include_top=False)

filename = 'finalized_model.sav'
pickle.dump(model, open(filename, 'wb'))
```

———————————————————-

```
/Library/Frameworks/Python.framework/Versions/2.7/bin/python2.7 /Users/samueltin/Projects
/bitbucket/share-card-ml/pickle_test.py
Using TensorFlow backend.
Traceback (most recent call last):
File "/Users/samueltin/Projects/bitbucket/share-card-ml/pickle_test.py", line 8, in
pickle.dump(model, open(filename, 'wb'
File "/Library/Frameworks/Python.frame
in dump
Pickler(file, protocol).dump(obj)
File "/Library/Frameworks/Python.frame
dump
self.save(obj)
File "/Library/Frameworks/Python.frame
save
self.save_reduce(obj=obj, *rv)
File "/Library/Frameworks/Python.frame
save_reduce
save(state)
File "/Library/Frameworks/Python.frame
save
f(self, obj) # Call unbound method with
File "/Library/Frameworks/Python.frame
save_dict
```

self._batch_setitems(obj.iteritems())

File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 669, in _batch_setitems
save(v)
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 286, in save
f(self, obj) # Call unbound method with explicit self
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 606, in save_list
self._batch_appends(iter(obj))
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 621, in _batch_appends
save(x)
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 331, in save
self.save_reduce(obj=obj, *rv)
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 425, in save_reduce
save(state)
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 286, in save
f(self, obj) # Call unbound method with explicit self
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 655, in save_dict
self._batch_setitems(obj.iteritems())
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 669, in _batch_setitems
save(v)
File “/Library/Frameworks/Python.frame
save
f(self, obj) # Call unbound method with
File “/Library/Frameworks/Python.frame
save_list
self._batch_appends(iter(obj))
File “/Library/Frameworks/Python.frame
_batch_appends
save(x)
File “/Library/Frameworks/Python.frame
save
self.save_reduce(obj=obj, *rv)
File “/Library/Frameworks/Python.frame
save_reduce
save(state)
File “/Library/Frameworks/Python.frame

```
save
f(self, obj) # Call unbound method with explicit self
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 655, in
save_dict
self._batch_setitems(obj.iteritems())
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 669, in
_batch_setitems
save(v)
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 331, in
save
self.save_reduce(obj=obj, *rv)
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 425, in
save_reduce
save(state)
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 286, in
save
f(self, obj) # Call unbound method with explicit self
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 655, in
save_dict
self._batch_setitems(obj.iteritems())
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 669, in
_batch_setitems
save(v)
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 331, in
save
self.save_reduce(obj=obj, *rv)
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 425, in
save_reduce
save(state)
File “/Library/Frameworks/Python.frame
save
f(self, obj) # Call unbound method with
File “/Library/Frameworks/Python.frame
save_dict
self._batch_setitems(obj.iteritems())
File “/Library/Frameworks/Python.frame
_batch_setitems
save(v)
File “/Library/Frameworks/Python.frame
save
f(self, obj) # Call unbound method with
File “/Library/Frameworks/Python.frame
save_dict
self._batch_setitems(obj.iteritems())
File “/Library/Frameworks/Python.frame
```

```
_batch_setitems
save(v)
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 286, in
save
f(self, obj) # Call unbound method with explicit self
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 606, in
save_list
self._batch_appends(iter(obj))
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 621, in
_batch_appends
save(x)
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 331, in
save
self.save_reduce(obj=obj, *rv)
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 425, in
save_reduce
save(state)
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 286, in
save
f(self, obj) # Call unbound method with explicit self
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 655, in
save_dict
self._batch_setitems(obj.iteritems())
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 669, in
_batch_setitems
save(v)
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 331, in
save
self.save_reduce(obj=obj, *rv)
File “/Library/Frameworks/Python.frame
save_reduce
save(state)
File “/Library/Frameworks/Python.frame
save
f(self, obj) # Call unbound method with
File “/Library/Frameworks/Python.frame
save_dict
self._batch_setitems(obj.iteritems())
File “/Library/Frameworks/Python.frame
_batch_setitems
save(v)
File “/Library/Frameworks/Python.frame
save
self.save_reduce(obj=obj, *rv)
File “/Library/Frameworks/Python.frame
```

```
save_reduce
save(state)
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 286, in
save
f(self, obj) # Call unbound method with explicit self
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 655, in
save_dict
self._batch_setitems(obj.iteritems())
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 669, in
_batch_setitems
save(v)
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 286, in
save
f(self, obj) # Call unbound method with explicit self
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 606, in
save_list
self._batch_appends(iter(obj))
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 621, in
_batch_appends
save(x)
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 286, in
save
f(self, obj) # Call unbound method with explicit self
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 568, in
save_tuple
save(element)
File “/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/pickle.py”, line 286, in
save
f(self, obj) # Call unbound method with e
File “/Library/Frameworks/Python.frame
save_dict
self._batch_setitems(obj.iteritems())
File “/Library/Frameworks/Python.frame
_batch_setitems
save(v)
File “/Library/Frameworks/Python.frame
save
rv = reduce(self.proto)
File “/Library/Frameworks/Python.frame
in _reduce_ex
raise TypeError, “can’t pickle %s objects
TypeError: can’t pickle module objects

Process finished with exit code 1
```

**Jason Brownlee** February 7, 2017 at 10:11 am #

REPLY

Sorry Samuel, I have not tried to save a pre-trained model before. I don't have good advice for you.

Let me know how you go.

**huikang** September 21, 2018 at 11:50 am #

REPLY

Is there a more efficient method in machine learning than joblib.load(), storing the model directly in memory and using it again?

**Jason Brownlee** September 21, 2018 at 2:21 pm #

REPLY

Sure, you can make an in-memory copy. I think sklearn has a clone() function that you can use.

**Amy** March 8, 2017 at 7:03 am #

REPLY

I have trained a model using liblinearutils. The model could not be saved using pickle as it gives error that ctype module with pointers cannot be pickled. How can I save my model?

**Jason Brownlee** March 8,

Sorry Amy, I don't have an

Perhaps you can save the coefficier

**SHUBHAM BHARDWAJ** Apri

Thanks a lot, very useful

**Jason Brownlee** April 4, 20

REPLY

You're welcome!

**Benju** April 11, 2017 at 1:35 am #

REPLY

My saved modells are 500MB+ Big….is that normal?

**Jason Brownlee** April 11, 2017 at 9:34 am #

REPLY

Ouch, that does sound big.

If your model is large (lots of layers and neurons) then this may make sense.

**Anupam** April 13, 2017 at 2:32 am #

REPLY

How to use model file ("finalized_model.sav") to test unknown data. Like, if the model is for tagger , how this model will tag the text file data? Is there any example?

**Jason Brownlee** April 13, 2017 at 10:08 am #

REPLY

You can load the saved model and start making predictions (e.g. yhat = model.predict(X)).

See this post on finalizing models:
http://machinelearningmastery.com/

**Oss Mps** April 21, 2017 at 3:09 pm

Dear Sir, please advice on how

**Jason Brownlee** April 22, 2

I would suggest extracting
in your preferred format.

**Suhas** May 24, 2017 at 4:44 am #

REPLY

Hi I love your website; it's very useful!

Are there any examples showing how to save out the training of a model after say 100 epochs/iterations? It's not immediately clear from looking at joblib or scikit learn.

This is esp. useful when dealing with large datasets and/or computers or clusters which may be unreliable (e.g., subject to system reboots, etc.)

**Jason Brownlee** May 24, 2017 at 4:59 am #

REPLY

I'm not sure how to do this with sklearn. You may need to write something custom. Consider posting to stackoverflow.

**Viktor** May 30, 2017 at 8:52 am #

REPLY

Hey!
Is it possible to open my saved model and make a prediction on cloud server where is no sklearn installed?

**Jason Brownlee** June 2, 2017 at 12:31 pm #

REPLY

no.

You could save the coefficients from
prediction code.

**Clemence** June 8, 2017 at 6:55 pm

REPLY

Hello Jason and thank you very

Do you know if it's possible to load featu
I'm mostly thinking of categorical variabl

I'm using sklearn to do that, but I don't k
transformation with the ML model into th

#Encode categorical variable into nume
from sklearn.preprocessing import Labe

list_var = [‘country’, ‘city’]

encoder = LabelEncoder()
for i in list_var:
df[i] = encoder.fit_transform(df[i])

Then I fit the model on the training dataset…

And I need to save this transformation with the model. Do you know if that’s possible ?
Thank you!

REPLY

**Jason Brownlee** June 9, 2017 at 6:23 am #

I’m not sure I follow sorry.

You can transform your data for your model, and you can apply this same transform in the future when you load your model.

You can save the transform objects using pickle. Is that what you mean?

REPLY

**Bhavani Shanker** June 22, 2017 at 1:24 am #

Hi Jason,
Kindly accept my encomiums for the illustrative lecture that you have delivered on Machine Learning using Python.

**********

# save the model to disk
filename = ‘finalized_model.sav’
joblib.dump(model, filename)

# sometime later…

# load the model from disk
loaded_model = joblib.load(filename)
result = loaded_model.score(X_test, Y_
print(result)
**********

After saving the model ‘finalized_model.
session at later date?

I would appreciate if you can advice on



REPLY

**Jason Brownlee** June 22, 2017 at 6:11 am #

The code after “sometime later” would be in a new session.

**jinsh** June 28, 2017 at 8:57 pm #

REPLY

Hello sir,

The above code saves the model and later we can check the accuracy also
but what i have to do for making predicting the class of unknown data?
I mean which function have to be called ?

eg: 2,132,40,35,168,43.1,2.288,33

can you suggest how to get the class of above data through prediction ?

thank you

**Jason Brownlee** June 29, 2017 at 6:35 am #

REPLY

Pass in input data to the predict function and use the result.

```
1 yhat = model.predict(X)
```

**Ukesh Chawal** July 24, 2017 at 11:00 pm #

REPLY

Can we use “pickling” to save a
fit model to generate forecasts based on

When I tried to use it, it gave me followi

PicklingError: Can’t pickle : attribute lool

**Jason Brownlee** July 25, 2

No.

See this tutorial on how to save Ker
http://machinelearningmastery.com/

**Ukesh Chawal** July 25, 2017 at 11:59 pm #

REPLY

Great. It worked.

You are awesome Jason. Appreciated.

**Jason Brownlee** July 26, 2017 at 7:57 am #

REPLY

Glad to hear it.

**akatsuki** August 9, 2017 at 1:21 pm #

REPLY

tbh this is best of the sites on web. Great!
I love the email subscriptions of yours as a beginner they are quite helpful to me .

**Jason Brownlee** August 10, 2017 at 6:45 am #

REPLY

Thanks, I'm glad to hear that.

**vikash** August 10, 2017 at 9:32 pm #

REPLY

Hi @Jason Brownlee thanks fo
a problem where i would like to retrain t
keeping the previous learning intact. I h
it forgets the previous learning. Please s
Thanks

**Jason Brownlee** August 11

Sorry, I don't follow. Can y

**sassashi** August 28, 201

REPLY

Hi Jason, I believe @v
model with new examples after

searching for as well. I know it is possible to retrain a model in tensorflow with new examples but I am not sure if it's possible with sklearn.

to expand the question some more: 1-you train a model with sklearn 2-save it with pickle or joblib
3-then you get your hands on some new examples that were not available at the time of initial training "step 1" 4-you load the previous model 5-and now you try to train the model again using the new data without losing the previous knowledge… is step 5 possible with sklearn?

**Jason Brownlee** August 28, 2017 at 6:52 am #

REPLY

I have not updated a model in sklearn, but I would expect you can.

Here is an example of updating a model in Keras which may help in general principle:
https://machinelearningmastery.com/update-lstm-networks-training-time-series-forecasting/

**Navdeep Singh** August 22, 2017 at 8:30 pm #

REPLY

Hi Json,

I need your guidance on Updation of saved pickle files with new data coming in for training

I recall 3 methods, Online Learning which is train one every new observation coming in and in this case model would always be biased

Second is, Whenever some set of n obs
do retraining again from scratch, that i d
time

Third is Mini batch learning, i know som
method and do same but I have other a
logistic regression. I wana ask can i upc

I am doing it in text classification, I read
take new features of new data ( made u
help.

Also as domain is same, and If client(Pr
sharing old data with new client (new pr
update it with training in new client data

**Jason Brownlee** August 23, 2017 at 6:48 am #

REPLY

Great question.

This is a challenging problem to solve. Really, the solution must be specific to your project requirements.

A flexible approach may be to build-in capacity into your encodings to allow for new words in the future.

The simplest approach is to ignore new words.

These, and other strategies are testable. See how performance degrades under both schemes with out-of-band test data.

**Merari** September 11, 2017 at 7:59 am #

REPLY

Gracias por compartir,
Existe alguna forma en la que pueda realizar predicciones con nuevos datos solo con el modelo guardado? llamando este modelo desde un archivo nuevo? lo he intentado con la instruccion final:

```
# load the model from disk
loaded_model = pickle.load(open(filename, 'rb'))
result = loaded_model.score(X_test, Y_test)
print(result)
```

pero no lo he logrado

373/5000
Thanks for sharing,
Is there any way I can make predictions
model from a new file? I have tried with

```
# load the model from disk
loaded_model = pickle.load (open (filen
result = loaded_model.score (X_test, Y_
print (result)
```

but I have not achieved it

**Jason Brownlee** September 11, 2017 at 12:11 pm #

REPLY

That is exactly what we do in this tutorial.

What is the problem exactly?

**AP** September 29, 2017 at 6:36 am #

REPLY

Hi Jason, I learn a lot reading your python books and blogs. Thank you for everything.

I'm having an issue when I work on text data with loaded model in a different session. I fit and transform training data with countvectorizer and tfidf. Then I only transform the test data with the fitted instances as usual. But, when work on loaded pretrained model in a different session, I am having problem in feature extraction. I can't just transform the test data as it asks for fitted instance which is not present in the current session. If I fit and transform on test data only, model prediction performance drastically decreases. I believe that is wrong way of doing machine learning. So, how can I do the feature extraction using countvectorizer, tfidf or other cases while working with previously trained model?

I'm using spark ML but I think it would be the same for scikit-learn as well.

**Jason Brownlee** September 30, 2017 at 7:31 am #

REPLY

Perhaps you can pickle your data transform objects as well. and re-use them in the second session?

**Bhavya Chugh** October 29, 2017

Hi Jason,

I trained a random forest model and sav
then copied that pickle file to my remote
giving incorrect predictions. I am using p
however the version of scikit-learn are s

**Jason Brownlee** October 2

REPLY

No idea, perhaps see if the

or different machines with the same version of Python?

**Berkin Albert Antony** November 10, 2017 at 5:45 pm #

REPLY

Hi Jason Brownlee,

I have a LogisticRegression model for binary classification. I wish to find a similar data points in a trained model for a given test data points. So that I can show these are similar data points predicted with these same class.

Could you please suggest your thoughts for the same. I am using scikit learn logistic regression

Thanks

**Jason Brownlee** November 11, 2017 at 9:18 am #

REPLY

Perhaps you could find data points with a low Euclidean distance from each other?

**James** November 16, 2017 at 8:47 am #

REPLY

Hi Jason –

If you pickle a model trained on a subse
loading the pickled model in a different f
You train the model on a,c,e. Is it possib
see the model was trained on a,c,e?

Thanks,
James

**Jason Brownlee** Novembe

Yes, you can save your mo
on new data.

**Mrinal Mitra** November 22, 2017 a

REPLY

Hi Jason,

Thanks for explaining it so nicely. I am new to this and will be needing your guidance. I have data using which I have trained the model. Now I want this model to predict an untested data set. However, my requirement is an output which will have the data and corresponding prediction by the model. For example, record 1 – type a, record 2 – type a, record 3 – type c and so on. Could you please guide me on this?

**Jason Brownlee** November 22, 2017 at 11:16 am #

REPLY

You can provide predictions one at a time or in a group to the model and the predictions will be in the same order as the inputs.

Does that help?

**Niranjan** December 3, 2017 at 3:22 pm #

REPLY

Hi,

I am using chunks functionality in the read csv method in pandas and trying to build the model iteratively and save it. But it always saves the model that is being built in the last chunk and not the entire model. Can you help me with it

clf_SGD = SGDClassifier(loss='modified_huber', penalty='l2', alpha=1e-3, max_iter=500, random_state=42)
pd.read_csv("file_name",chunksize = 1000):
""
data preparation and cleaning
""
hashing = hv.fit_transform(X_train['desc
clf_SGD.partial_fit(hashing, y_train, clas

joblib.dump(clf_SGD, source_folder + o

**Jason Brownlee** Decembe

Sorry, I'm not sure I follow,

**Shabbir** December 8, 2017 at 8:50

REPLY

Hi Jason,
This is extremely helpful and saved me quite a bit of processing time.

I was training a Random Forest Classifier on a 250MB data which took 40 min to train everytime but results were accurate as required. The joblib method created a 4GB model file but the time was cut down to 7 Minutes to load. That was helpful but the results got inaccurate or atleast varied quite a bit from the original results. I use average of 2 Decision Tree and 1 Random Forest for the model. Decision Tree Models have kept there consistency loading vs training but RF hasn't. Any ideas?

**Nilanka** December 19, 2017 at 9:10 pm #

REPLY

Thank you very useful!!

**Jason Brownlee** December 20, 2017 at 5:43 am #

REPLY

You're welcome.

**Gokhan** December 28, 2017 at 2:55 pm #

REPLY

Hello, if i load model
loaded_model = joblib.load(filename)
result = loaded_model.score(X_test, Y_test)
print(result)

can i use this model for another testsets

**Jason Brownlee** Decembe

Sure.

**Vinay Boddula** January 20, 2018

REPLY

Hi Jason,

How do I generated new X_Test for pre
the passed parameters are same in the

Background: I am basically saving the model and predicting with new values from time to time. How do we check whether the new values have all the parameters and correct data type.

**Jason Brownlee** January 20, 2018 at 8:25 am #

REPLY

Visualization and statistics.

I have many posts on the topic, try the search box.

**Sekar** February 1, 2018 at 4:06 am #

REPLY

Jason. Very good article. As asked by others, in my case I am using DecisionTreeClassifier with text feature to int transformation. Eventhough, you mentioned that transformation map can also be picked and read back, is there any example available? Will it be stored in the same file or it will be another file?

**Jason Brownlee** February 1, 2018 at 7:24 am #

REPLY

In a separate file.

**Yousif** February 5, 2018 at 8:01 pm

Thank you so much professor we get more new knowledge

**Jason Brownlee** February

You're welcome. Also, I'm

**Adarsh C** February 8, 2018 at 12:29 pm #

REPLY

HI sir,
I would like to save predicted output as a CSV file. After doing ML variable I would like to save “y_predicted”. And I’m using python ide 3.5.x I have pandas,sklearn,tensorflow libraries

**Jason Brownlee** February 9, 2018 at 8:58 am #

REPLY

You can save the numpy array as a csv.
https://docs.scipy.org/doc/numpy-1.13.0/reference/generated/numpy.savetxt.html

**Atul** March 11, 2018 at 6:45 am #

REPLY

Hi Jason,

I would like to save predicted output as a CSV file. After doing ML variable I would like to save “y_predicted”. How I can save Naive Bayes, SVM, RF and DT Classification for final predictions for all samples saved as a .csv with three columns namely Sample, Actual value, Prediction
values

**Jason Brownlee** March 12, 2018 at 6:24 am #

REPLY

Perhaps create a datafram
dataframe directly via to_csv():
https://pandas.pydata.org/pandas-d

**Tommy** March 22, 2018 at 11:14 pm

I have a list of regression coeff
coefficients into the sklearn logistic regr
Thanks!
Tommy

**Jason Brownlee** March 23

REPLY

No model is needed, use each coefficient to weight the inputs on the data, the weighted sum is the prediction.

**Vincent** April 10, 2018 at 10:25 am #

REPLY

Hi,all
I am using scikit 0.19.1
I generated a training model using random forest and saved the model. These were done on ubuntu 16.01 x86_64.
I copied the model to a windows 10 64 bit machine and wanted to reuse the saved model. But unfortunately i get the following
Traceback (most recent call last):
File “C:\Users\PC\Documents\Vincent\nicholas\feverwizard.py.py”, line 19, in
rfmodel=joblib.load(modelfile)
File “C:\Python27\lib\site-packages\sklearn\externals\joblib\numpy_pickle.py”, line 578, in load
obj = _unpickle(fobj, filename, mmap_mode)
File “C:\Python27\lib\site-packages\sklearn\externals\joblib\numpy_pickle.py”, line 508, in
_unpickle
obj = unpickler.load()
File “C:\Python27\lib\pickle.py”, line 864, in load
dispatchkey
File “C:\Python27\lib\pickle.py”, line 1139, in load_reduce
value = func(*args)
File “sklearn\tree_tree.pyx”, line 601, in sklearn.tree._tree.Tree.cinit
ValueError: Buffer dtype mismatch, expected ‘SIZE_t’ but got ‘long long’

What could be happening? Is it because
able to reuse the model in my ubuntu.

**Jason Brownlee** April 11, 2

Perhaps the pickle file is n

**Pramod** April 17, 2018 at 9:03 pm #

Can we load model trained on

**Jason Brownlee** April 18, 2

REPLY

I'm skeptical that it would work. Try it and see. Let me know how you go.

**Arnaud** April 17, 2018 at 9:29 pm #

REPLY

Dear Jason :

Thank you for 'le cours' which is very comprehensive.

I have a maybe tricky but 'could be very usefull' question about my newly created standard Python object.

Is it possible to integrate a call to my Python object in a Fortran program ?

Basically I have a deterministic model in which I would like to make recursive calls to my Python object at every time step.

Do I need some specific libraries ?

Thank you
Best regards

**Jason Brownlee** April 18, 2018 at 8:06 am #

REPLY

You're welcome.

I suspect it is possible. It's all just code at the end of the day. You might need some kind of Python-FORTRAN bridge software. I have not done this, sorry.

**Pratip** April 23, 2018 at 4:32 pm #

Hi Sir ,
I wanted to know if its possible to combi
datasets to get more training data to get
loaded dataset and then save model usi
Which method will be correct ?
Please help .

**Jason Brownlee** April 24, 2018 at 6:20 am #

REPLY

Sure, you can, but it may only make sense if the data was collected in the same way from the same domain.

**Ishit Gandhi** May 4, 2018 at 6:00 pm #

REPLY

Hii Jason,

Can you put example of how to store and load Pipeline models?

eg.

clf = Pipeline([(“rbm”,rbm),(“logistic”,logistic)])
clf.fit(trainX,trainY)

**Jason Brownlee** May 5, 2018 at 6:18 am #

REPLY

Perhaps use pickle? This might help:
https://machinelearningmastery.com/save-load-machine-learning-models-python-scikit-learn/

**Akash** May 14, 2018 at 4:15 pm #

REPLY

Hi jason,
My name is Akash Joshi.I am trying to t
out of memory.Is there a way where I ca
pickle?

**Jason Brownlee** May 15, 2

Perhaps try running on a m

Perhaps try using a sample of your

Perhaps use a generator to progres



**Samarth** May 14, 2018 at 4:54 pm

REPLY

Hi Jason

I want to know how can presist a minmax transjformation? There are ways to persist the final model but to persist the transformations?

Thanks

**Jason Brownlee** May 15, 2018 at 7:51 am #

REPLY

Save the min and max values for each variable.

Or save the whole object.

**SOORAJ T S** May 16, 2018 at 12:30 am #

REPLY

thank you the post, it is very informative but i have a doubt about the labels or names of the dataset can specify each.

**Jason Brownlee** May 16, 2018 at 6:05 am #

REPLY

What do you mean exactly?

**SOORAJ T S** May 16, 2018 at 4:1

names = [‘preg’, ‘plas’, ‘pres’, ‘s

in the above code what are these “preg’

**Jason Brownlee** May 17, 2

You can learn about these

https://github.com/jbrownlee/Datase

**SOORAJ T S** May 17, 2018 at 4:23 pm #

REPLY

thank you sir…

**Aniko** June 7, 2018 at 12:13 am #

REPLY

HI Jason!

I created a machine learning (GBM) model to predict house prices and a Django application to usability. This model has more than 1000 n_estimators and it takes more than 1 minutes to load before getting the prediction in every request.
I would like to load joblib dump file just once and store the model in memory, avoiding loading the model in every get requests.

What is your best practice for this?

Thanks

**Jason Brownlee** June 7, 2018 at 6:31 am #

REPLY

This sounds like a web application software engineering question rather than a machine learning question.

Perhaps you can host the model behind a web service?

**Aniko** June 7, 2018 at 6:5

thank you, meanwhile
documentation, this perhaps so

**Jason Brownlee**

Glad to hear it.

**LamaOS223** June 9, 2018 at 2:00

REPLY

okay what if i had 2 datasets fo

the first dataset has a Loan_Status attribute
and the second one does not have a Loan_Status attribute
if i trained the model on the first dataset and i want to predict the Loan_Status for the second dataset, how to do that? please make it simple for me i'm beginner

**Jason Brownlee** June 10, 2018 at 5:58 am #

REPLY

This process will how you how to work through a predictive model systematically:
https://machinelearningmastery.com/start-here/#process

**Imti** July 12, 2018 at 4:55 pm #

REPLY

Hey Jason, I am working on a model to classify text files. I am using the CountVectorizer, TfidfTransformer and SGDClassifier in the same sequence on a set of data files. I am saving the SGDClassifier object via the joblib.dump method you have mentioned in this article.

Do I also need to save the vectorizer and transformer objects/models ? Since when i take a new file for classification I will need to go through these steps again.

**Jason Brownlee** July 13, 2018 at 7:33 am #

REPLY

Yes, they are needed to pr

**Dennis Faucher** July 28, 2018 a

Just what I needed today. Thar

**Jason Brownlee** July 28, 2

I'm happy to hear that Den

**Tejaswini** July 30, 2018 at 9:01 am

REPLY

Hi Jason,

Appreciate for the article. when i am saving the model and loading it in different page.Then it is showing different accuracy.

Problem trying to solve: I am using oneclasssvm model and detecting outliers in sentences.

REPLY

**Jason Brownlee** July 30, 2018 at 2:15 pm #

I have not seen that, are you sure you are evaluating the model on exactly the same data?

REPLY

**Tejaswini** August 2, 2018 at 2:10 pm #

Yes Jason i am using gensim word2vec to convert text into feature vectors and then performing classification task.after saving model and reloading in another session its giving different results.

REPLY

**Jason Brownlee** August 2, 2018 at 2:11 pm #

That is odd. I have not seen this.

Perhaps report a fault/bug?

REPLY

**EvapStudent** August 7, 2018 at 1

Hi Jason,

I am training a neural network using ML
different geometries of heat exchangers
low MRE, but I can't figure out how to u
call again, I am getting an error when u
about bringing in new data for the netwo

REPLY

**Jason Brownlee** August 7,

I don't recommend using p
your model.

Once you find a config that works for your problem, perhaps switch from the sklearn wrappers to the Keras API directly.

**EvapStudent** August 7, 2018 at 11:13 pm #

REPLY

Hi Jason,

Thanks for the recommendation. Is there no easy way to save a model and call from it to use in scikit learn? I have been getting good results with the model I have made on there, I just don't know how to get it to the point where I can actually use the network (i.e. put in a geometry and get it's predictions).

If using Keras API to save/load is the best option, how do I go about doing that?

**Jason Brownlee** August 8, 2018 at 6:21 am #

REPLY

There may be, but I don't have an example, sorry.

**Golnoush** August 21, 2018 at 1:38 am #

REPLY

Hello Jason,

Thank you for your nice tutorial! Does pickle.dump(model, open(filename, 'wb')) only save the neural network model or it also save the parameters and weights of the model?
Does the back propagation and training
What I would like to do is that I aim to sa
during training and use the same trained
thankful if you could assist me in this wa

**Jason Brownlee** August 21

I believe you cannot use pi

**Somo** August 29, 2018 at 3:05 pm #

REPLY

Hi Jason,

I am trying to save my model using jobli

another .py file model = joblib.load('model.pkl') but then the accuracy dropped and each time I run it the accuracy differs a lot. I coefficient and the intercept and the same for both models. Any ideas why this might happen. Thanks in advance.

**Jason Brownlee** August 30, 2018 at 6:26 am #

REPLY

Perhaps this will help:
https://machinelearningmastery.com/faq/single-faq/why-do-i-get-different-results-each-time-i-run-the-code

**Dhrumil** September 1, 2018 at 3:11 pm #

REPLY

Hey man I am facing a trouble with pickle, when I try to load my .pkl model I am getting following error :

UnicodeDecodeError: 'ascii' codec can't decode byte 0xbe in position 3: ordinal not in range(128)

Can you please tell me something since I have tried all fixes I could find..

**Jason Brownlee** September 2, 2018 at 5:30 am #

REPLY

Perhaps post your error on stackoverflow?

**Aakash Aggarwal** September 8

I want to develop to train my m
onwards, when i want to train the model
append mode that reduces the time of t
model.

Any helps would be greatly appreciated

**Jason Brownlee** September 8, 2018 at 6:17 am #

REPLY

This post shows how:
https://machinelearningmastery.com/save-load-machine-learning-models-python-scikit-learn/

**Aakash Aggarwal** October 2, 2018 at 12:45 am #

REPLY

This article shows how to save a model that is built from scratch. But I am looking to train the model by including additional data so as to achieve high prediction performance and accuracy for unseen data. Is there any leads or approach you can think?

**Jason Brownlee** October 2, 2018 at 6:26 am #

REPLY

I don't understand, sorry. Training a model and saving it are separate tasks.

**My3** October 15, 2018 at 10:11 pm #

REPLY

Hi Jason,

I have some requirement to integrate py

I have a ML model which is trained as s
to load this one time using java and ther
python. So my workflow is like:

1. Read Randomforestclassifier.pkl file (
2. Send this model as input to function c
for each request
3. python_file.py has prediction code an
code
Please provide suggestions for this worl
to execute python_file.py and everythin
activity.

Can you help me with some client serve
time model loading?

**Jason Brownlee** October 16, 2018 at 6:37 am #

REPLY

I recommend treating it like any other engineering project, gather requirements, review options, minimize risk.

**Rahul** October 18, 2018 at 6:10 pm #

REPLY

Hi Jason,My3,

I have a similar requirement to integrate java with python as my model is in python and in my project we are using java.

Could you please help here.

**Jason Brownlee** October 19, 2018 at 6:01 am #

REPLY

Thanks for the suggestion.

**Theekshana** October 30, 2018 at 12:35 am #

REPLY

Hi Jason,

I have trained my model and evaluated the accuracy using cross-validation score

After evaluating the model, should I trai
new trained model for new future data. (
accuracy around mean accuracy from c

Thank you for your tutorials and instant

**Jason Brownlee** October 3

Yes, see this post:
https://machinelearningmastery.com

**Gagan** December 11, 2018 at 5:56 pm #

REPLY

Jason, thanks so much for value add.

**Jason Brownlee** December 12, 2018 at 5:50 am #

REPLY

You're welcome.

**Roger** January 1, 2019 at 5:55 am #

REPLY

That helped me a lot. Thank you

**Jason Brownlee** January 1, 2019 at 6:29 am #

REPLY

I'm happy to hear that.

**Kiril Kirov** January 4, 2019 at 3:19 am #

REPLY

How would you go about saving and loading a scikit-learn pipeline that uses a custom function created using FunctionTransformer?

**Jason Brownlee** January 4

Perhaps pickle?

**Shubham** January 4, 2019 at 8:37

Hey Jason,

I have a very basic question, let's say I
6 months I feel to retrain it on new data.
to have target for my new data and nee
obviously don't have the target and ther

**Jason Brownlee** January 4, 2019 at 11:01 am #

REPLY

You have many options, e.g. develop a new model, update the old model, some mixture of the two with an ensemble.

**Rajesh Mahajan** January 18, 2019 at 7:44 am #

REPLY

Hi Jason,

I am new to this.. So pardon, if I am asking something incorrect…

I have two stages. Build model and predict.

For Build model:
I am using vectorizer.fit_transform(data) and building the logistic model. My data is a bunch of comments and the target is a set of categories. In order for me to use that model for predicting categories for new comments, I am using the vector created earlier during building of model to predict

So, when I do the save model joblib.dump(log_model, “model.sav”)

Foe Predict:
When I try to re-run the model (saved) at a later point of time, I don’t have the original vectorizer anymore with the original data set

log_model = joblib.load(“model.sav”)
inputfeatures_nd = vectorizer.transform(newComment);
pred = log_model.predict(inputfeatures_nd)

I get this error – sklearn.exceptions.Not
fitted.

What do you suggest I should do ? Sho

**Jason Brownlee** January 1

You must use the same ve
it along with your model.

**Rajesh Mahajan** January 18, 2019 at 1:17 pm #

REPLY

Thanks Jason! Yes it worked after I save and reload.

**Jason Brownlee** January 19, 2019 at 5:32 am #

REPLY

I'm happy to hear that.

## Leave a Reply

Name (required)

Email (will not be published) (required)

Website

SUBMIT COMMENT

**Welcome to Machine Learning Mastery!**

Hi, I'm Jason Brownlee, P
I write tutorials to help de

Read More

POPULAR


**So, You are Working on a Machine Learning Problem…**
APRIL 4, 2018


**How to Develop LSTM Models for Multi-Step Time Series Forecasting of Household Power Consumption**
OCTOBER 10, 2018


**11 Classical Time Series Forecasti**
AUGUST 6, 2018


**How to Make Predictions with Kera**
APRIL 9, 2018


**You're Doing it Wrong. Why Machi**
MARCH 28, 2018


**How to Develop LSTM Models for T**
NOVEMBER 14, 2018


**How to Make Predictions with sciki**
APRIL 6, 2018

**You might also like…**

- How to Install Python for Machine Learning
- Your First Machine Learning Project in Python
- Your First Neural Network in Python
- Your First Classifier in Weka
- Your First Time Series Forecasting Project