Python 3.7 Error: Unsupported Pickle Protocol 5

Asked 3 years, 1 month ago Modified 1 year, 2 months ago Viewed 175k times

91

I'm trying to restore a pickled config file from RLLib (json didn't work as shown in this post), and getting the following error:

```
config = pickle.load(open(f"{path}/params.pkl", "rb"))

---------------------------------------------------------------------------
ValueError                                Traceback (most recent call last)
<ipython-input-28-c964561b863c> in <module>
----> 1 config = pickle.load(open(f"{path}/params.pkl", "rb"))

ValueError: unsupported pickle protocol: 5
```

Python Version = 3.7.0

How can I open this file in 3.7?

python pickle

Share Improve this question Follow

asked Aug 9, 2020 at 18:03
hubbs5
1,235 1 12 22

2 Do you know in which version this file was saved? – Banana Aug 9, 2020 at 18:04

1 Unfortunately, I don't. Trying to track that down though. – hubbs5 Aug 9, 2020 at 18:06

117

For pandas users who saved a dataframe to a pickle file with protocol 5 in python 3.8 and need to load it into python 3.6 which only supports protocol 4 (I'm looking at you **google colab**):

```
!pip3 install pickle5
import pickle5 as pickle
with open(path_to_protocol5, "rb") as fh:
  data = pickle.load(fh)
```

Could also save into a protocol-4 pickle from python 3.6

```
data.to_pickle(path_to_protocol4)
```

Update: If facing this when loading a model from stable-baselines3:

```
!pip install --upgrade --quiet cloudpickle pickle5
from stable_baselines3 import PPO
# restart kernel if in jupyter notebook

# Might not need this dict in all cases
custom_objects = {
    "lr_schedule": lambda x: .003,
    "clip_range": lambda x: .02
}
model = PPO.load("path/to/model.zip", custom_objects=custom_objects)
```

Tested on 2021-05-31 with env:

```
cloudpickle: 1.6.0
pickle5: 0.0.11
stable-baselines3: 1.0
```

Reference: https://brainsteam.co.uk/2021/01/14/pickle-5-madness-with-mlflow/

Share Improve this answer Follow

edited May 31, 2021 at 10:09

answered Dec 16, 2020 at 7:18

Shadi
9,762 4 43 65

65

Use [pickle5](https://pypi.org/project/pickle5/) or load it into python 3.8+ and then serialize it to a lower version of it using the protocol parameter.

Share Improve this answer Follow

answered Aug 9, 2020 at 18:08

hd1
34k 5 80 91

3 Didn't know about pickle5! I was in the process of setting up a 3.8 virtual env and installing, all the dependencies, but this is much easier. Thanks! – hubbs5 Aug 9, 2020 at 18:23

1 I just found it myself. PyPi needs to be better at advertising itself. – hd1 Aug 9, 2020 at 19:24

2 ModuleNotFoundError: No module named 'pickle5' though I import it. – Fatemeh Asgarinejad Jan 13, 2021 at 5:49

1 Is it installed in your venv? – hd1 Jan 13, 2021 at 6:03

4 A concrete example of serializing to a lower version with pandas data frame: df.to_pickle('filename.pkl', protocol=4) – Nir Feb 25, 2021 at 0:18

0

In the event that you cannot load pickle5 because of its dependencies (mainly Visual Building c++), another solution could be that you change the Python interpreter you're using (to the old one, before the error occured). For me, I was getting this error after I ran a program in IDLE that I had been running in Spyder. When I ran it again within Spyder, it dropped this error.

```
Python Error: Unsupported Pickle Protocol 5
```

To resolve this, within Spyder I changed my Python interpreter to the Python I was using with IDLE (Tools -> Preferences). Once I rebooted Spyder, I had to install the necessary dependencies with command prompt so that within Spyder the console could be used:

```
pip install spyder-kernels
```

Naturally, this may introduce some irregularities within Spyder (namely, packages it's supposed to come with are no longer there because of the different interpreter). These should easily be sussed out when debugging, and resolved using standard pip installs.

Once you recover your (thought to be lost) files, it might be wise to think about reverting back to Spyder's Python interpreter, and updating code to elegantly handle this problem (I would love if somebody could suggest in comments how to do this that didn't require pickle5!)

Share Improve this answer Follow

answered Feb 22, 2021 at 16:13
ntk4
1,247 1 13 18

0

If this error is due to **heroku deployment** then check your python version of local setup and heroku setup. If both are different then it might lead you to this error.
Solution:

- Create a runtime.txt file in your application's base directory

```
python-3.9.2
```

Share Improve this answer

Follow

edited Apr 10, 2021 at 11:12

answered Apr 3, 2021 at 14:17

sauravjoshi23

837 11 9