**Save The Model**

Project Name: statistical machine learning TEAM ID: PNT2022TMID04163 approaches to liver disease prediction

 machine learning, while working with scikit learn library, we need to save the trained models in a file and restore them in order to reuse them to compare the model with other models, and to test the model on new data. **The saving of data is called Serialization, while restoring the data is called Deserialization**.

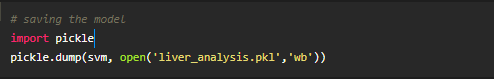
Save the model with Pickle  
  
To save the ML model using Pickle all we need to do is **pass the model object into the dump() function of Pickle**. This will serialize the object and convert it into a “byte stream” that we can save as a file called model.

The pickle module **keeps track of the objects it has already serialized, so that later references to the same object won't be serialized again**, thus allowing for faster execution time. Allows saving model in very little time.

After building the model we have to save the model.

Pickle is used for serializing and de-serializing Python object structures, also called marshalling or flattening. Serialization refers to the process of converting an object in memory to a byte stream that can be stored on disk or sent over a network. Later on, this character stream can then be retrieved and de-serialized back to a Python object.

This is done by the below code



Here, svm is our Support Vector Machine Classification class, saving as liver\_analysis.pkl file. Wb is the write binary in bytes.

Pickle is one of the most popular ways to serialize objects in Python; You can use Pickle to serialize your trained machine learning model and save it to a file. At a later time or in another script, you can deserialize the file to access the trained model and use it to make predictions.

Here’s a utility function I created to save the model pipeline — I’ll also demonstrate its functionality in the training pipeline:

|  |
| --- |
| import pickle |
|  |  |
|  | def save\_pipeline(\*, pipeline\_to\_persist: Pipeline) -> None: |
|  | """Persist the pipeline. |
|  | Saves the versioned model, and overwrites any previous |
|  | saved models. This ensures that when the package is |
|  | published, there is only one trained model that can be |
|  | called, and we know exactly how it was built. |
|  | """ |
|  |  |
|  | # Prepare versioned save file name |
|  | save\_file\_name = f"{config.app\_config.pipeline\_save\_file}{\_version}.pkl" |
|  | save\_path = TRAINED\_MODEL\_DIR / save\_file\_name |
|  |  |
|  | remove\_old\_pipelines(files\_to\_keep=[save\_file\_name]) |
|  | pickle.dump(pipeline\_to\_persist, save\_path) |

To save a pickle, **use pickle.** **dump** . A convention is to name pickle files \*. pickle , but you can name it whatever you want.