Pickling

Pickling is a process of converting a class object into a byte stream so that it can be stored into a file. This is also called as object serialization.

We use *pickle* module to perform pickling and unpickling.

Function

dump( ) – This function is used to perform the pickling. It returns the pickled representation of the object as a bytes object, instead of writing it to a file.

This method belongs to pickle module.

Syntax:-

```
import pickle
pickle.dump(object, file)
```

Unpickling

Unpickling is a process whereby byte stream is converted back into a class object. It is inverse operation of pickling. This is also called as de-serialization.

Pickling and unpickling should be done using binary files since they support byte streams.

We use *pickle* module to perform pickling and unpickling.

Warning: The pickle module is not secure against erroneous or maliciously constructed data. Never unpickle data received from an untrusted or unauthenticated source.

Function

load( ) – This function is used to read an pickled object from a binary file and returns it into object. This method belongs to pickle module.

Syntax:-

```
import pickle
pickle.load(file)
```

Why do we need Pickling and Unpickling

When we store some structured data in the file and want to perform calculation that time we need pickling and unpickling.