The Pickle Module

- We know that Python considers everything as an object. So, all data types including list, tuple, dictionary, etc. are also considered as objects. During execution of a program, we may require to store current state of variables so that we can retrieve them later to its present state. Suppose you are playing a video game, and after some time, you want to close it. So, the program should be able to store the current state of the game, including current level/stage, your score, etc. as a Python object. Likewise, you may like to store a Python dictionary as an object, to be able to retrieve later. To save any object structure along with data, Python provides a module called Pickle. The module Pickle is used for serializing and de-serializing any Python object structure. Pickling is a method of preserving food items by placing them in some solution, which increases the shelf life. In other words, it is a method to store food items for later consumption.

- Serialization is the process of transforming data or an object in memory (RAM) to a stream of bytes called byte streams. These byte streams in a binary file can then be stored in a disk or in a database or sent through a network. Serialization process is also called pickling.

- De-serialization or unpickling is the inverse of pickling process where a byte stream is converted back to Python object. The pickle module deals with binary files. Here, data are not written but dumped and similarly, data are not read but loaded. The Pickle Module must be imported to load and dump data. The pickle module provides two methods - dump() and load() to work with binary files for pickling and unpickling, respectively.

The dump() method:

This method is used to convert (pickling) Python objects for writing data in a binary file. The file in which data are to be dumped, needs to be opened in binary write mode (wb).

Syntax of dump() is as follows:

dump(data_object, file_object)

where data_object is the object that has to be dumped to the file with the file handle named file_object.

The load() method:

This method is used to load (unpickling) data from a binary file. The file to be loaded is opened in binary read (rb) mode.

Syntax of load() is as follows:

Store_object = load(file_object)

Here, the pickled Python object is loaded from the file having a file handle named file_object and is stored in a new file handle called store_object.