**How does os.walk() work in python ?**

OS.walk() generate the file names in a directory tree by walking the tree either top-down or bottom-up. For each directory in the tree rooted at directory top (including top itself), it yields a 3-tuple (dirpath, dirnames, filenames).

* **root :** Prints out directories only from what you specified.
* **dirs :** Prints out sub-directories from root.
* **files :** Prints out all files from root and directories.
* **PICKLING AND UNPICKLING**
* The pickle module implements a fundamental, but powerful algorithm for serializing and de-serializing a Python object structure.
* **Pickling -** is the process whereby a Python object hierarchy is converted into a byte stream, and **Unpickling -** is the inverse operation, whereby a byte stream is converted back into an object hierarchy.
* Pickling (and unpickling) is alternatively known as **serialization**, **marshalling**, or **flattening**

Python Pickle

Python Pickle is used to serialize and deserialize a python object structure. Any object on python can be pickled so that it can be saved on disk.

At first Python pickle serialize the object and then converts the object into a character stream so that this character stream contains all the information necessary to reconstruct the object in another python script.

Note that the pickle module is not secure against erroneous or maliciously constructed data according to the documentation. So, never unpickle data received from an untrusted or unauthenticated source.

Python Pickle dump

In this section, we are going to learn, how to store data using Python pickle. To do so, we have to import the pickle module first.

Then use pickle.dump() function to store the object data to the file. pickle.dump() function takes 3 arguments. The first argument is the object that you want to store. The second argument is the file object you get by opening the desired file in write-binary (wb) mode. And the third argument is the key-value argument. This argument defines the protocol. There are two type of protocol – pickle.HIGHEST\_PROTOCOL and pickle.DEFAULT\_PROTOCOL. See the sample code to know how to dump data using pickle.

Python Pickle load

To retrieve pickled data, the steps are quite simple. You have to use pickle.load() function to do that. The primary argument of pickle load function is the file object that you get by opening the file in read-binary (rb) mode.

**Important Notes on Python Pickle**

Few important points about python pickle module are:

1. The pickle protocol is specific to Python – it’s not guaranteed to be cross-language compatible. This means you most likely can’t transfer the information to make it useful in other programming languages.
2. There is also no guarantee of compatibility between different versions of Python because not every Python data structure can be serialized by the module.
3. The latest version of the pickle protocol is used by default unless you manually change it.
4. Last but not least, the pickle module is not secure against erroneous or maliciously constructed data according to the documentation.

.