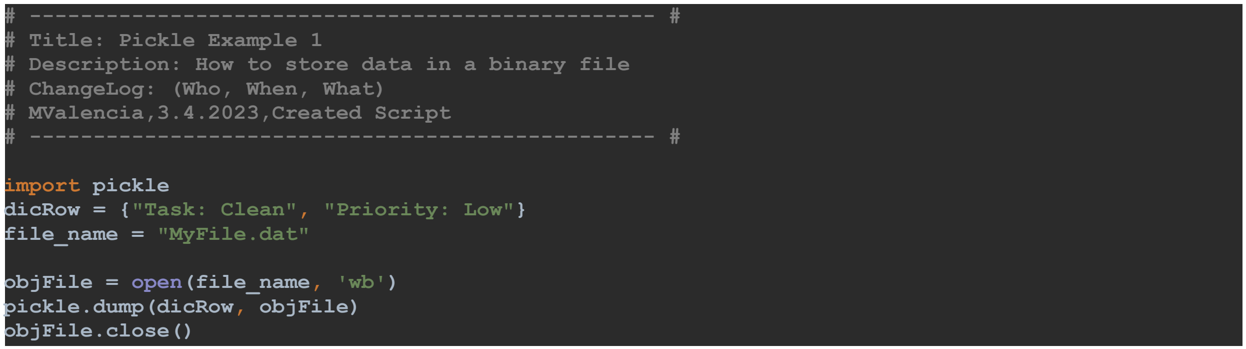
Maggie Valencia
March 4, 2023
IT FDN 110 A
Assignment07 Part II

Assignment 07 - Pickling in Python

Pickle is a module that is specific to Python used for binary serialization and deserialization of Python Objects (that means that it is converting objects into 0s and 1s). Things that can be pickled include integers, strings, lists, functions and many more. In Python, pickling objects are serialized into a non-human readable format. Use cases for pickling include are: storing into byte streams in files, databases and for moving data across the network. It is key to understand that Pickled objects are not inherently secure or encrypted, users should be aware that malicious data can be constructed to be executed during the unpickling process. This means users should only unplickle trusted data sources.

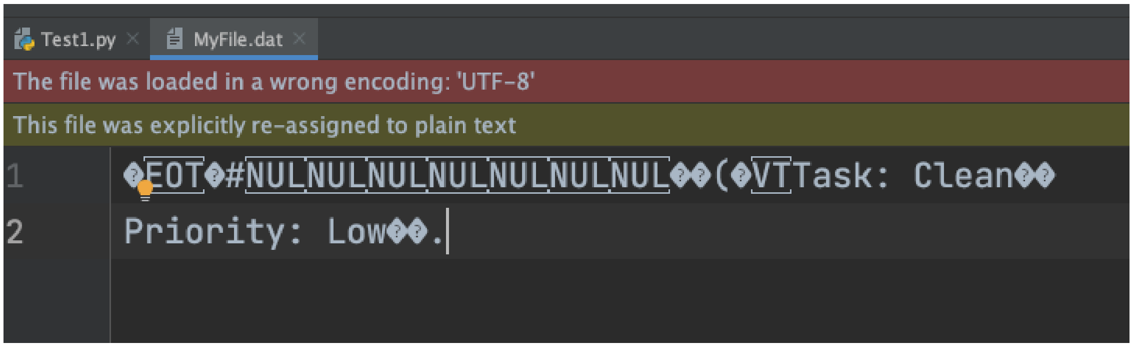
How to pickle in Python

To pickle in Python, first thing to do is use the “import pickle” to import the module. We can then use pickle.dump and ‘wb’ to save binary data to a file object, in the example in figure 1, we are saving this to a binary. From figure 2, we can see what a binary file looks like, its representation cannot be interpreted by humans but computers have no problem understanding 0s and 1s.



```
# ------------------------------------------------- #
# Title: Pickle Example 1
# Description: How to store data in a binary file
# ChangeLog: (Who, When, What)
# MValencia,3.4.2023,Created Script
# ------------------------------------------------- #

import pickle
dicRow = {"Task: Clean", "Priority: Low"}
file_name = "MyFile.dat"

objFile = open(file_name, 'wb')
pickle.dump(dicRow, objFile)
objFile.close()
```

Figure 1 - Pickle to File



The file was loaded in a wrong encoding: 'UTF-8'

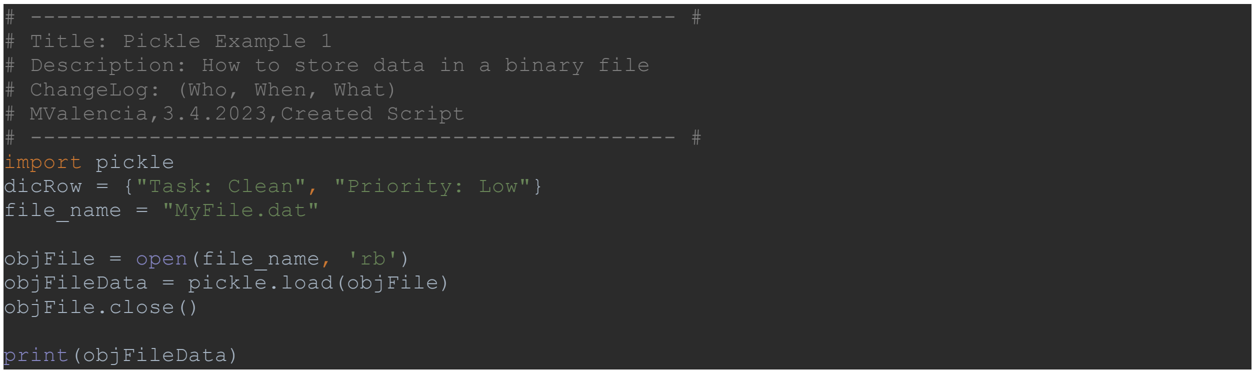
This file was explicitly re-assigned to plain text

```
�EOT�#NULNULNULNULNULNULNUL��(�VTTask: Clean��
Priority: Low��.
```

Figure 2 - Saved Binary FIle

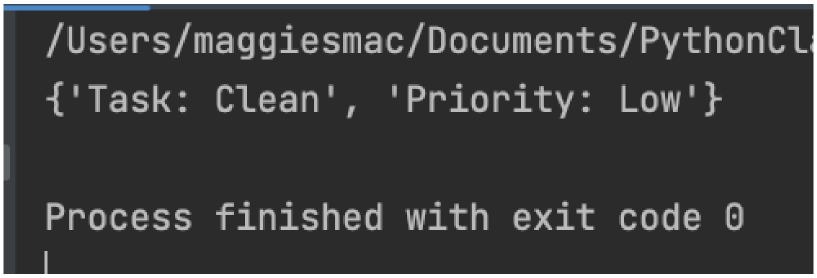
Unpickle Data from a file

To unpickle data, in other words to make it human readable we can use the ‘pickle.load’ and ‘rb’ module to read the picked object from the file object, in the example below in figure 2 we are reading from a binary file. Figure 2 we can see that we now can understand the objects saved in the binary file by unpickling:



```
# ------------------------------------------------- #
# Title: Pickle Example 1
# Description: How to store data in a binary file
# ChangeLog: (Who, When, What)
# MValencia,3.4.2023,Created Script
# ------------------------------------------------- #
import pickle
dicRow = {"Task: Clean", "Priority: Low"}
file_name = "MyFile.dat"

objFile = open(file_name, 'rb')
objFileData = pickle.load(objFile)
objFile.close()

print(objFileData)
```

Figure 2 - Unpickle from a file

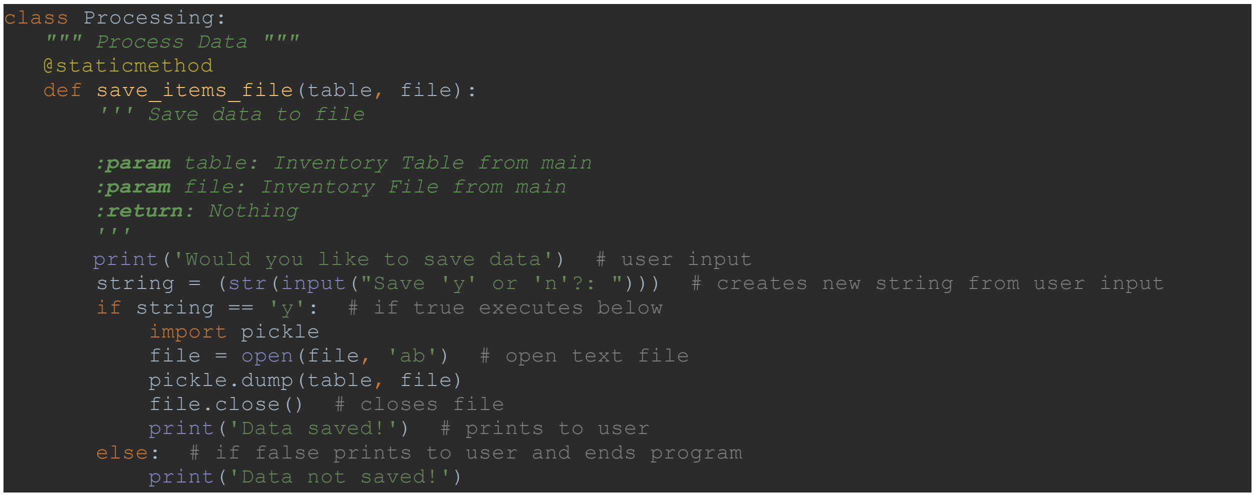


```
/Users/maggiesmac/Documents/PythonCl
{'Task: Clean', 'Priority: Low'}

Process finished with exit code 0
```

Figure 3 - Unpickled Data

Pickle a List in a Function

A more complex example in figure 4, we are pickling within a function with pickle.dump module and ‘ab’ to save to binary. As you can see, this works just the same way it would if this was outside a function. In this example, we are saving a lists and all the items in that lists are saved with the pickle module:

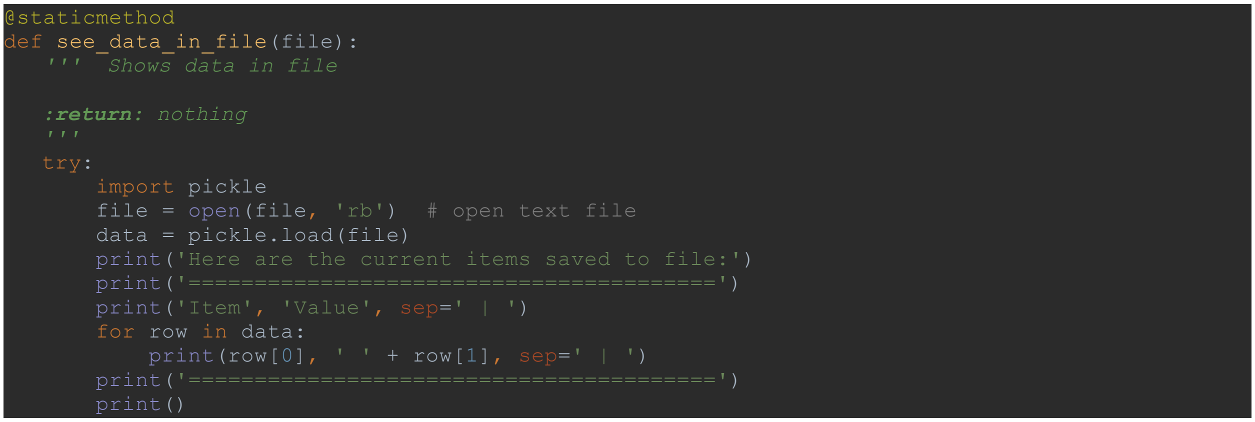


```python
class Processing:
    """ Process Data """
    @staticmethod
    def save_items_file(table, file):
        ''' Save data to file

        :param table: Inventory Table from main
        :param file: Inventory File from main
        :return: Nothing
        '''
        print('Would you like to save data')  # user input
        string = (str(input("Save 'y' or 'n'?: ")))  # creates new string from user input
        if string == 'y':  # if true executes below
            import pickle
            file = open(file, 'ab')  # open text file
            pickle.dump(table, file)
            file.close()  # closes file
            print('Data saved!')  # prints to user
        else:  # if false prints to user and ends program
            print('Data not saved!')
```

Figure 4 - Pickle Save to File in Function

Unpickle in a function

In just the same way, in figure 5, we can unpickle all the items in the list we created by using the pickle.load module. Once the data is extracted from the binary file can easily print out the data and do anything else with it.



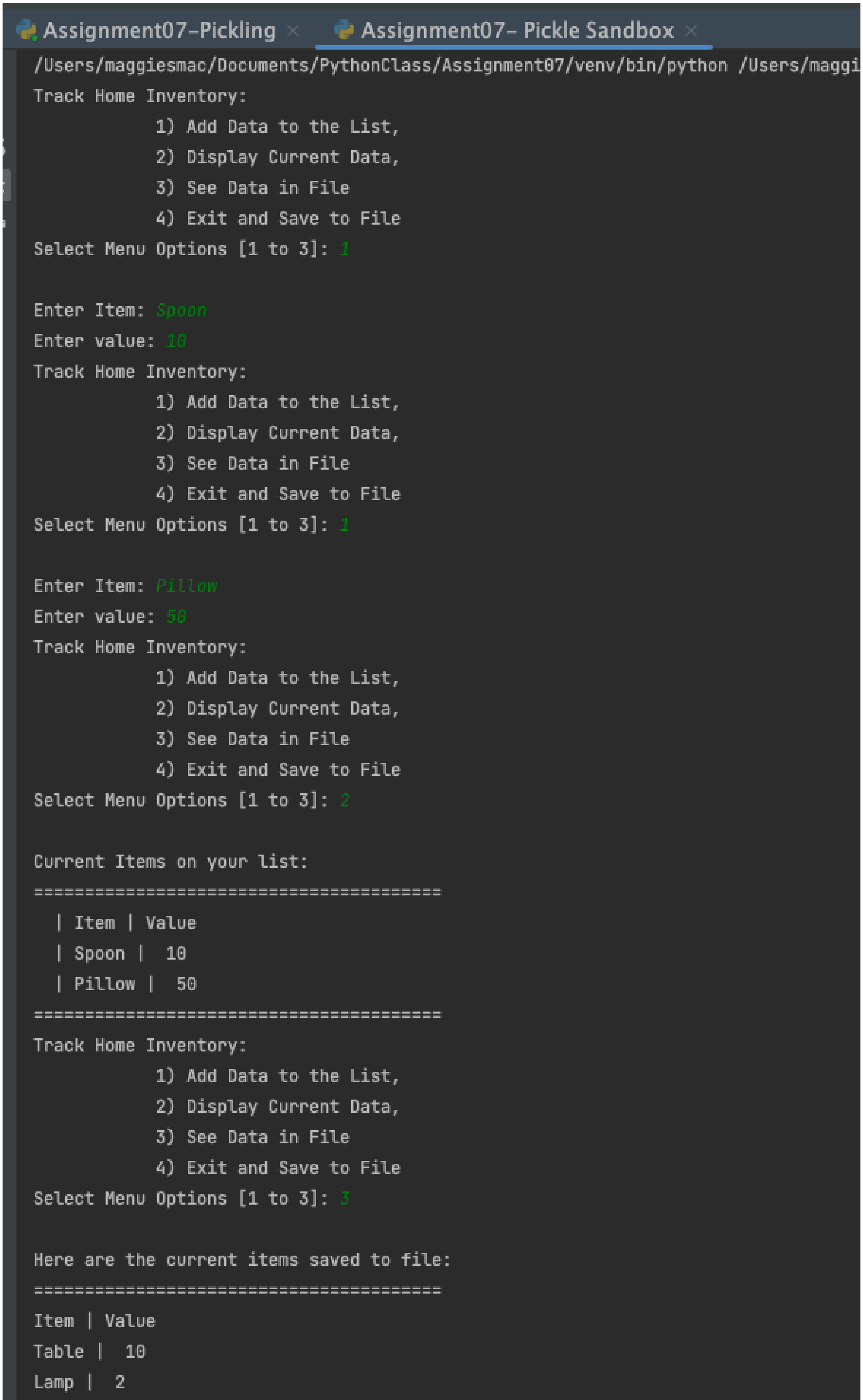
```python
@staticmethod
def see_data_in_file(file):
    '''  Shows data in file

    :return: nothing
    '''
    try:
        import pickle
        file = open(file, 'rb')  # open text file
        data = pickle.load(file)
        print('Here are the current items saved to file:')
        print('========================================')
        print('Item', 'Value', sep=' | ')
        for row in data:
            print(row[0], ' ' + row[1], sep=' | ')
        print('========================================')
        print()
    except:
        print('==============================================')
        print('File does not exist, try another option [1-4]')
        print('==============================================')
        print()
```

Figure 5 - Pickle Read from FIle in a Function

Summary

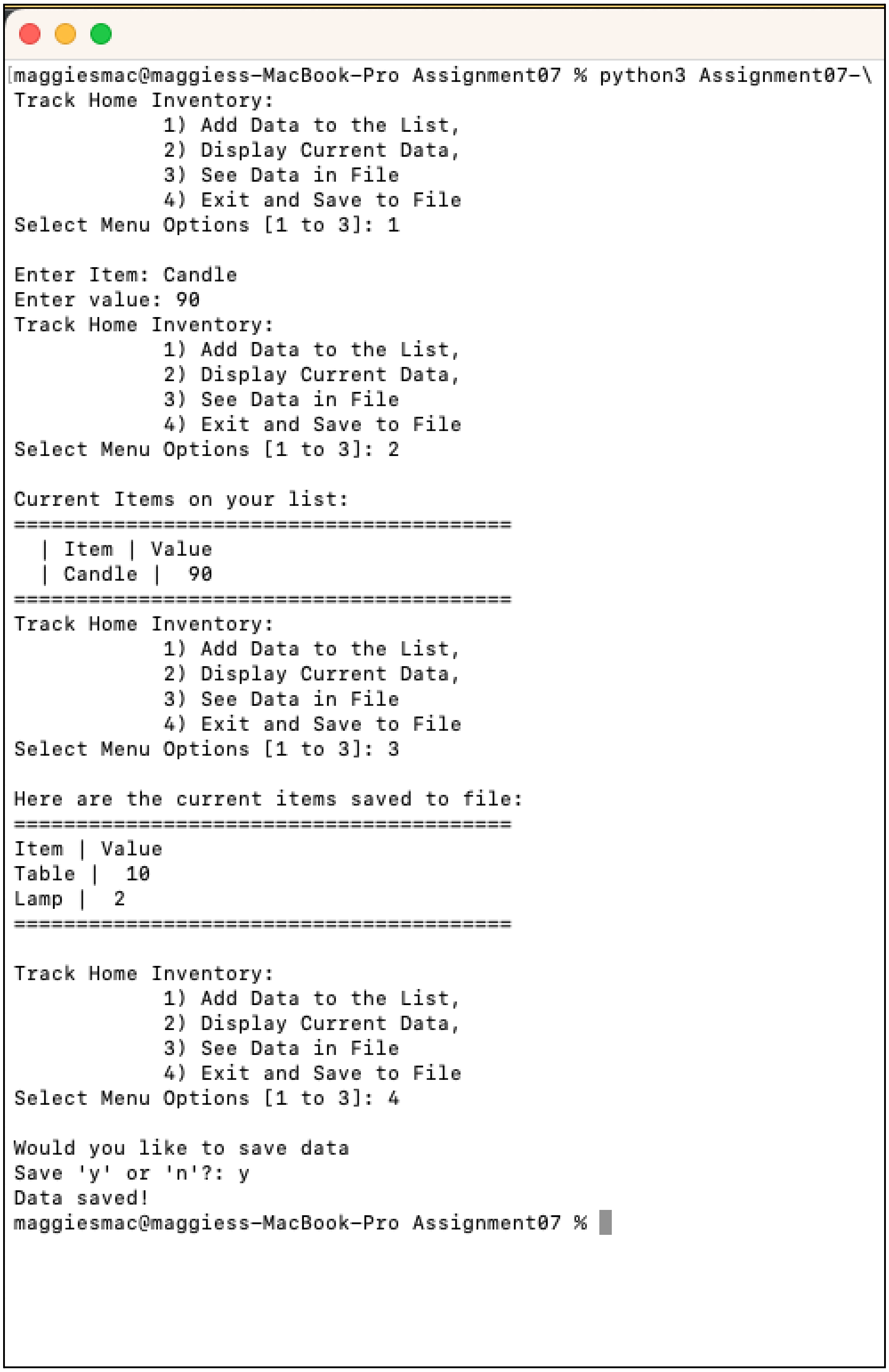
This document demonstrated how pickling works to save objects into binary files and back. It is important to understand that while pickling is a way to compress data that is faster to process, it is an inherently insecure way of doing this. Programmers should know that this data is not encrypted and when unpickling, it is very important to do this with a trusted binary file to protect against malicious code being executed in your program.

Running in PC



```
/Users/maggiesmac/Documents/PythonClass/Assignment07/venv/bin/python /Users/maggi
Track Home Inventory:
            1) Add Data to the List,
            2) Display Current Data,
            3) See Data in File
            4) Exit and Save to File
Select Menu Options [1 to 3]: 1

Enter Item: Spoon
Enter value: 10
Track Home Inventory:
            1) Add Data to the List,
            2) Display Current Data,
            3) See Data in File
            4) Exit and Save to File
Select Menu Options [1 to 3]: 1

Enter Item: Pillow
Enter value: 50
Track Home Inventory:
            1) Add Data to the List,
            2) Display Current Data,
            3) See Data in File
            4) Exit and Save to File
Select Menu Options [1 to 3]: 2

Current Items on your list:
========================================
  | Item | Value
  | Spoon |  10
  | Pillow |  50
========================================
Track Home Inventory:
            1) Add Data to the List,
            2) Display Current Data,
            3) See Data in File
            4) Exit and Save to File
Select Menu Options [1 to 3]: 3

Here are the current items saved to file:
========================================
Item | Value
Table |  10
Lamp |  2
```

Figure 6 - Running in PC



```
[maggiesmac@maggiess-MacBook-Pro Assignment07 % python3 Assignment07-\
Track Home Inventory:
            1) Add Data to the List,
            2) Display Current Data,
            3) See Data in File
            4) Exit and Save to File
Select Menu Options [1 to 3]: 1

Enter Item: Candle
Enter value: 90
Track Home Inventory:
            1) Add Data to the List,
            2) Display Current Data,
            3) See Data in File
            4) Exit and Save to File
Select Menu Options [1 to 3]: 2

Current Items on your list:
========================================
  | Item | Value
  | Candle |  90
========================================
Track Home Inventory:
            1) Add Data to the List,
            2) Display Current Data,
            3) See Data in File
            4) Exit and Save to File
Select Menu Options [1 to 3]: 3

Here are the current items saved to file:
========================================
Item | Value
Table |  10
Lamp |  2
========================================

Track Home Inventory:
            1) Add Data to the List,
            2) Display Current Data,
            3) See Data in File
            4) Exit and Save to File
Select Menu Options [1 to 3]: 4

Would you like to save data
Save 'y' or 'n'?: y
Data saved!
maggiesmac@maggiess-MacBook-Pro Assignment07 %
```

Figure 7 - Running in Terminal

Pickle Sources:

- https://docs.python.org/3/library/pickle.html#data-stream-format
- https://pythonbasics.org/pickle/
- https://codefather.tech/blog/python-pickle/
- https://pythonprogramming.net/python-pickle-module-save-objects-serialization/
- https://stackoverflow.com/questions/18963949/error-pickling-in-python-io-unsupportedoperation-read
- https://docs.python.org/3/library/pickle.html#what-can-be-pickled-and-unpickled
- https://www.synopsys.com/blogs/software-security/python-pickling/#:~:text=Pickle%20in%20Python%20is%20primarily,transport%20data%20over%20the%20network.