Packaging, Serving & Unit Testing - Q&A Summary

Thanks to: Omar Abbas

1. What is suitable for `pickle`?

Answer:

- Used to save objects in Python.
- Common for serializing models or data.
- **Hint:** Example – `model.save('model.pkl', 'wb')` where `'wb'` means *write binary*.

---

2. What are `torch` and `tensorflow` suitable for?

Answer:

- Used to save computation graphs.
- Stores nodes and their connections (model structure).

---

3. What are `ONNX` and `PMML` suitable for?

Answer:

- Suitable for model interchange between libraries like scikit-learn, TensorFlow, and PyTorch.
- **ONNX:** *Open Neural Network Exchange*
- **PMML:** *Predictive Model Markup Language* (better support for scikit-learn than ONNX)

---

4. Why do we need to separate research and production repositories?

Answer:

- Research is more experimental (like notebooks or drafts).
- Production is more structured and involves larger systems.
- Research usually involves smaller or single models; production involves scalable solutions.

---

5. What is `Poetry`?

Answer:

- A Python dependency management tool.
- Ensures consistent dependency versions using hashes.
- Prevents interference between research and production environments.
- **Example:** Useful for managing libraries like `pytest` (commonly used in production only).

---

6. What is `setup.py` used for?

Answer:

- Used for packaging Python projects.
- Allows installation via `pip`, e.g., `pip install ITI` (which may include packages like numpy, scikit-learn, etc.).

---

7. When to use `mlflow serve`?

Answer:

- For serving models **internally** (within the organization or team).

---

8. Why do we use logging?

Answer:

- For monitoring code behavior and tracking issues.
- Helps in debugging and auditing.
- Acts like an advanced version of `print` statements.

---

9. What is a unit test?

Answer:

- Tests individual units like functions or components in a model.
- Verifies success, failure, and exception cases.
- **Hint:** Related to *Test-Driven Development (TDD)* – writing tests before implementing code.

Original Text (for reference):

1 - what is suitable for pickle ?

ans : can save objects

2 - what is torch and tensorflow suitable for ?

ans : they save graph files ex nodes and connection between them

3 - what is onnx and pmml suitable for ?

(hint) onnx:open neural network exchange

(hint) pmml:predictive model markup language (better at sklearn than onnx)

ans : can unite many libs as sklearn and tenserflow and pytorch

(hint) model.save('model.pkl' , 'wb') wb= write binary

4 - why do we need to seperate research repository and production repository?

ans: because in the research is more as a draft or notebook not as production and in research you are more likely to work on a small model or single model not as production that you are a part of a big model

5 - what is poetry

ans: it stores the hash for your dependencies and synchronize them so they don't interfer together specially in researching and production as pytest library(only used for production)

6 - what is setup.py made for?

ans : for packaging like pip install ITI(composed of numpy , sklearn , etc..)

7 - when to use mlflow serve ?

ans : to use it internally

8 - why we use logging ?

ans : to check up on the code and updates and see where the problem happens and to get back to any incident happend (a little bit like print)

9 - what is unit test ?

ans : test the failure , success , exceptions for unit whether function or code or parts in model

(Hint) TDD : test driven development