

# Packaging and serving models

The importance of record keeping

# What is a model package?

- Everything relating to your model
  - The code used to make your model
  - The trained model
  - Training artifacts (e.g. fit imputation object, fit categorical encoding object)
  - Logs
  - Random seeds
  - Metadata
    - Logged hyperparameters
    - Logged metrics
    - What data version was used
    - Tags
    - Experiment description
    - Date and time of running
    - Length of run
    - Execution environment information

# Why is this important?

- Seeing what has happened in the past
  - Think of a scientific notebook
  - Best to have a single source of truth
- Reproducibility
  - If done right, a model package can be reused at any point in the future
  - Random seeds
- Making decisions for the future
  - All past experiments in one location
  - Easier to decide next steps
- Serving inference
  - Guarantees storage of everything needed for inference
  - Forces consistent interface for inference between model runs

# Inference first mentality

- Normally the last step of workflow
- Normally tied to training code
  - Data is split at beginning of code
  - Variables saved in training, used in inference
  - Heavily coupled
- Ideally decoupled
  - Training process and inference process are not tied together
  - Seperate functions
  - Focus on eliminating possibility of data leakage