



BitWith Bite

AI & MACHINE LEARNING WORKSHEET



Saving and Loading Models

Chapter: AI & Machine Learning • Level ★★★ •
Time: 30 min

SCORE

___ / 20

Name _____ Class _____ Date _____

AFTER THIS WORKSHEET YOU CAN

✓ Persist models with joblib ✓ Load and reuse ✓ Version model files ✓ Ship pipeline + model together



Section A • Concept Check

• BEGINNER

4 × 1 = 4

- 1 Sklearn models are commonly saved with:
☐ A. joblib.dump ☐ B. print() ☐ C. csv.save
☐ D. zip only
- 3 Best artifact to save is the:
☐ A. whole pipeline ☐ B. weights screenshot
☐ C. dataset ☐ D. notebook

- 2 Reload with:
☐ A. joblib.load ☐ B. import model
☐ C. open().read ☐ D. np.load only
- 4 Loading a model in an API lets you:
☐ A. serve predictions without retraining
☐ B. retrain nightly only ☐ C. edit data
☐ D. skip preprocessing wrongly



Section B • Problem Solving

• INTERMEDIATE

2 + 3 × 3 = 11

- 5 `joblib.dump(pipe, 'model.....')`
- 6 Never load pickles from sources.
- 7 Code: save and reload a pipeline.

- 8 Why save pipeline not just model?

- 9 Security note on pickle files?



Section C • Challenge

• CHALLENGE

5

- 10 What metadata should ship with a model file?

Reflection — the most useful thing I learned: _____

A ___/4 B ___/11 C ___/5 Total ___/20

Teacher's Signature

Parent's Signature

✂ ANSWER KEY — FOLD OR CUT BEFORE HANDING OUT

1-A 2-A 3-A 4-A | 5 `joblib/pkl` 6 untrusted 7 = `joblib.dump(pipe, 'm.joblib');`
`pipe2=joblib.load('m.joblib')` 8 = Inputs must be transformed the exact same way at serve time 9 =

They can execute code - only load trusted files | 10 = Version, training date, metrics, feature list