How to save models for Explainability?

Explainability module needs model object as input for this trial/community version, as the model may be created in any environment it needs to be saved it in format described below. For the Enterprise version of ML Works, the model object form the pipeline can be directly used as input for the XAI library,

Model objects can be both models and pipelines if the model or pipeline implements a predict or predict_proba function that conforms to the Scikit convention. If case of an incompatible model, user can wrap the model's prediction function into a wrapper function that transforms the output into the format that is supported by predict or predict_proba of Scikit.

The ultimate criteria for uploading any pair of data and model object should be that the model is directly able to consume the data provided to give predictions.

One must ensure that the transformed data is uploaded, and the saved model object can consume it directly for generating predictions.

Scikit-learn based models

Let's consider below code for model fitting and making predictions:

```
>>> from sklearn.datasets import load_iris

>>> from sklearn.linear_model import LogisticRegression

>>> X, y = load_iris(return_X_y=True)

>>> clf = LogisticRegression(random_state=0).fit(X, y)

>>> clf.predict(X[:2, :])

array([0, 0])

>>> clf.predict_proba(X[:2, :])

array([[9.8...e-01, 1.8...e-02, 1.4...e-08],

[9.7...e-01, 2.8...e-02, ...e-08]])

>>> clf.score(X, y)
```

```
0.97...
```

To pickle the model object:

```
>>> import pickle as pkl

>>> with open('filename.pkl', 'wb') as f:

>>> # Pickle the 'clf' model using the highest protocol available.

>>> pkl.dump(clf, f, pkl.HIGHEST_PROTOCOL)
```

The model is expected to be uploaded as “filename.pkl” file