Paper Title: DeepSniffer: A DNN Model Extraction Framework Based on Learning Architectural Hints
Code Link: https://github.com/xinghu7788/DeepSniffer

Software Requirements

Environment Setup

Orig Source Code:	*git clone https://github.com/xinghu7788/DeepSniffer.git*
Data & Model Checkpoints: (here)	*https://drive.google.com/drive/folders/1JrTkT9C0klWFMK4x-KSMqvvPJ7k3TL6U*

Use the Patch file provided for some modifications to the original code.

#To test Model Extraction using DeepSniffer Install

Python Version	3.6.v
Conda	>= 3. v
Tensorflow	pip install tensorflow==2.0.0

#To test Adversarial Attack with DeepSniffer, install

1. **Dependencies and Library:**

Python Version	3.6.v
Conda	>= 3. v
Tensorflow	>= 1.4 (pip install tensorflow==2.0.0)
Pytorch	1.8.0 (Strictly Recommended)
Cuda + GPU (Recommended)	>= 10.2
To Install Pytorch use this command:	conda install pytorch==1.8.0 torchvision==0.9.0 torchaudio==0.8.0 cudatoolkit=10.2 -c pytorch
Pytorch Installation (Refer to this)	https://pytorch.org/get-started/previous-versions/
scipy	Pip install scipy

Note: Model will fail to work if Pytorch version is above 1.9.0 (torch-library zero_gradients() API is not supported beyond this)

2. **Setup**

Extract the data and model checkpoint to the file path mentioned in the README.md file.
Unzip the files in the "models" to the directory of DeepSniffer/AdversarialAttack/

Unzip the files in ''data_100'' under the directory of DeepSniffer/AdversarialAttack/data_100

Now refer to the README.md file.