

PySyft Cheat Sheet

PySyft (<https://github.com/OpenMined/PySyft>) is an extension for PyTorch that implements algorithms for secure and private deep learning.

Loading PySyft

```
# loading PyTorch before PySyft!  
import torch
```

```
# loading PySyft  
import syft as sf
```

```
# hooking into Keras (if necessary)  
hook = sf.KerasHook(torch)
```

```
# hooking into PyTorch  
hook = sf.TorchHook(torch)
```

Workers

```
# using virtual workers  
worker = sf.VirtualWorker(hook, id="ID")
```

```
# print objects assigned to a worker  
print(worker._objects)
```

```
# moving a (PyTorch) tensor to a worker  
tensor_at_worker = tensor.send(worker)
```

```
# getting a tensor from a worker  
tensor_back = tensor_at_worker.get()
```

```
# moving a tensor from one worker to another  
tensor_at_w2 = tensor_at_worker.move(w2)
```

Federated learning

```
# loading a dataset  
loader = sf.FederatedDataLoader(  
    dataset.federated(  
        (tuple_of_workers)),  
    batch_size,  
    shuffle,  
    **kwargs)
```

```
# train function (additional lines of code  
# compared to a standard PyTorch train function)  
def train(...):  
    ...  
    for idx, (data,target) in enumerate(loader):  
        model.send(data.location)  
        ...  
        model.get()
```

©Simon Wenkel (<https://www.simonwenkel.com>)
This pdf is licensed under the CC BY-SA 4.0 license.