🚀 Quick Start - IDS Pipeline

⚡ TL;DR - Run the Pipeline NOW

```
# 1. Navigate to pipeline directory
cd /home/sujay/Programming/IDS/dpdk_suricata_ml_pipeline

# 2. Start Kafka
./scripts/02_setup_kafka.sh

# 3. Wait 30 seconds for Kafka to start
sleep 30

# 4. Start ML Consumer (in a new terminal)
source ../venv/bin/activate
python src/ml_kafka_consumer.py --config config/pipeline.conf

# 5. Generate Traffic (in another terminal)
./scripts/05_replay_traffic.sh
```

That's it! 🎉

📊 What's Happening?

```
PCAP Replay → Suricata → Kafka → ML Engine → Predictions
```

1. **Kafka** receives network flow events
2. **ML Engine** extracts 65 CICIDS2017 features from each flow
3. **Random Forest model** classifies traffic as BENIGN or ATTACK
4. **Predictions** are published to `ml-predictions` topic

PROF

🔍 Monitor the Pipeline

Check Status

```
./scripts/status_check.sh
```

Watch ML Predictions

```
kafka-console-consumer.sh \
    --bootstrap-server localhost:9092 \
    --topic ml-predictions \
    --from-beginning
```

View ML Consumer Logs

```
tail -f logs/ml/ml_consumer.log
```

🐛 Common Issues

Issue: Kafka won't start

```
pkill -9 -f kafka
./scripts/02_setup_kafka.sh
```

Issue: ML Consumer can't connect

```
# Check Kafka is running
netstat -tuln | grep 9092

# Reinstall packages
./install_missing_packages.sh
```

PROF

Issue: No traffic flowing

```
# Generate test traffic
ping -c 100 8.8.8.8 &
curl http://example.com
```

🛑 Stop Everything

```
./scripts/stop_all.sh
```

📚 Full Documentation

- **RUNTIME_GUIDE.md** - Complete step-by-step guide
- **SETUP_GUIDE.md** - Installation instructions
- **README.md** - Architecture and components

✅ Success Indicators

You know it's working when you see:

1. ✅ Kafka running on port 9092
2. ✅ ML Consumer logs: "✅ Connected to Kafka"
3. ✅ ML Consumer logs: "Processed flow from..."
4. ✅ Predictions appearing in `ml-predictions` topic

🎯 Test Commands

```bash
# Test 1: Check all packages installed
source ../venv/bin/activate
python -c "import kafka, sklearn, joblib, lightgbm; print('✅ All OK')"

# Test 2: Check ML model loads
python -c "import joblib; m=joblib.load('../ML Models/random_forest_model_2017.joblib'); print('✅ Model OK')"

# Test 3: Check Kafka topics
kafka-topics.sh --list --bootstrap-server localhost:9092

# Test 4: Generate benign traffic
python tests/test_benign_traffic.py

# Test 5: Generate attack traffic
python tests/test_attack_generator.py
```

PROF

Need help? Check `RUNTIME_GUIDE.md` for detailed troubleshooting.