**Installations**

* Install Ubuntu
* Install [Anaconda](https://www.anaconda.com/products/individual), for python

**Download Dataset, Pre processing and Training a Malware Detector**

* Download the [AndroZoo](https://androzoo.uni.lu/) dataset, containing benign and malware APKs.
  + APKs can be downloaded from an API by providing an APK SHA256 hash by using the following [script](https://colab.research.google.com/drive/1mUMG6ko3F0vJQRKato9lp8iO5q2k1zUg).(Downloading\_APKs.ipynb) Both API and APK’s SHA256 are given by AndroZoo.
* Extracting androidmanfestfiles.xml and classes.dex file from an APK by using [Androguard](https://github.com/androguard/androguard)
* Converting an APK to an image (fileName:APK\_to\_images(Androguard\_and\_preDefined\_Values)\_Version\_2.ipynb).
  + [Extract](https://colab.research.google.com/drive/1gtez9rhFDJ6uatJC4YPeEL8YGXzKC_Xr#scrollTo=ZoROhhkmHmTt&line=4&uniqifier=1) different properties from all these extracted files.
  + [Converting](https://colab.research.google.com/drive/1gtez9rhFDJ6uatJC4YPeEL8YGXzKC_Xr#scrollTo=OHbKpSTnHmTT&line=1&uniqifier=1) those properties to an integer values ([predefined](https://colab.research.google.com/drive/1jMSQvCSsR3GS-b717Od1_rjRjc8CPWjh#scrollTo=vGo-d_8EHmT1) + calculation)
  + Can select custom APKs based on publishing date, number of vt\_detection (detected by # of softwares in VirusTotal) etc.
  + [Place](https://colab.research.google.com/drive/1gtez9rhFDJ6uatJC4YPeEL8YGXzKC_Xr#scrollTo=KS1uKyqvHmTe&line=2&uniqifier=1) different properties on different channels.
  + [Interpolate](https://colab.research.google.com/drive/1gtez9rhFDJ6uatJC4YPeEL8YGXzKC_Xr#scrollTo=ms1Ilk6NHmTN&line=3&uniqifier=1) all channels to a fixed size.
  + [Merge](https://colab.research.google.com/drive/1gtez9rhFDJ6uatJC4YPeEL8YGXzKC_Xr#scrollTo=KS1uKyqvHmTe&line=2&uniqifier=1) all channels to make an image.
* Training a Deep Learning Model
  + [Converting](https://colab.research.google.com/drive/1gtez9rhFDJ6uatJC4YPeEL8YGXzKC_Xr#scrollTo=W9gEf-dQRchM&line=1&uniqifier=1) APKs images to .npy file for [training](https://colab.research.google.com/drive/10yqstpOiSvN_nlXNWyVo4nERBPNKL8gh) a model.
  + Load .npy file to train model
  + Make labels, ‘0’ for benign and ‘1’ for malware.

**Implementing DroidDetector (**[**P1**](https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7399288)**)**

* DroidDetector based on binary vectors
  + First extract different properties from an APK to file using [script](https://colab.research.google.com/drive/19RW4N5YaP1JLhkcMrv8vxCuQq9pCsmPf)
  + Convert those properties to a binary vector (Preprocessing for DroidDetector). ([APK2Vector](https://colab.research.google.com/drive/1GjM-O_NnVuTEWHRGuPIyODK9muxvgDMB))
  + Train DNN model on binary vector using following [script](https://colab.research.google.com/drive/1l6n9yUcF4bVQaMOiDpYBfNuHEvj-sAQ6)

**Implementing Malware Detection Based on CNN (**[**P9**](https://dl.acm.org/doi/pdf/10.1145/3199478.3199492)**)**

* Malware Detection Based on CNN
  + First extract different properties from an APK to file using [script](https://colab.research.google.com/drive/1bTUBEZ256BtGMU5RqG0wP5rdL23VMOK6)
  + [Pre processing](https://colab.research.google.com/drive/1qp4HPqykI2KbTpATKcE0cGHh10miNGRS)
  + [Train](https://colab.research.google.com/drive/1s-BBRbjl4XHkTf7Drdu5kFnqMohTT2BK) a CNN model

**Generating Adversarial Examples**

* Generating Adversarial Examples with [Pre defined benign properties](https://colab.research.google.com/drive/1edAJEGc_hxFl2afTCjpUdB_eqwWXD5no) (Attack1:-FileName: Generating\_Random\_benign)
  + [Convert](https://colab.research.google.com/drive/1edAJEGc_hxFl2afTCjpUdB_eqwWXD5no#scrollTo=XJxK3_M6I-AF&line=1&uniqifier=1) an APK to image.
  + [Append](https://colab.research.google.com/drive/1edAJEGc_hxFl2afTCjpUdB_eqwWXD5no#scrollTo=80jRB8YYI9__&line=1&uniqifier=1) benign properties.
* Generating bening APKs using GANs (Attack2)
  + Generating benign APKs using [DCGAN](https://colab.research.google.com/drive/1jrSbQ7n2hTP_WcH96bqCFgzXIaVCBDX1)
  + Generating benign APKs using [WGAN](https://colab.research.google.com/drive/1qgEshUupH4eEG0h14y_w3YlXlV3q17DI)
  + Generating benign APKs using [LSGAN](https://colab.research.google.com/drive/10KjycCVYMJCo9N6qzDbP1Ob1Misor_Fq)

**Attacks on Models**

* Attacks on own model, P1 and P9 Detectors
  + Attack via Attack1
    - [Own Detector](https://colab.research.google.com/drive/1edAJEGc_hxFl2afTCjpUdB_eqwWXD5no)
    - [P1](https://colab.research.google.com/drive/1GjM-O_NnVuTEWHRGuPIyODK9muxvgDMB" \l "scrollTo=3uHVBeh3DmG8)
    - [P9](https://colab.research.google.com/drive/1qp4HPqykI2KbTpATKcE0cGHh10miNGRS#scrollTo=JSCDd9gYJ1UR)
  + Attack via Attack2
    - [Own Detector](https://colab.research.google.com/drive/1edAJEGc_hxFl2afTCjpUdB_eqwWXD5no)
    - [P1](https://colab.research.google.com/drive/1GjM-O_NnVuTEWHRGuPIyODK9muxvgDMB#scrollTo=RT-T1hWNFXD8)
    - [P9](https://colab.research.google.com/drive/1qp4HPqykI2KbTpATKcE0cGHh10miNGRS#scrollTo=ugJbJWy1J9yF)