**Instalação e configuração do ambiente:**

Para quem está lendo isso e deseja fazer também, seguem abaixo as instruções para emular o ambiente, em Windows.

Antes de começarmos vale destacar que, durante o processo, eu perdi acesso as máquinas virtuais do virtual box, pois houve conflito com o WSL. Com isso, tive que optar pela opção de download do genymotion sem virtual box, pois nenhuma virtualização minha estava funcionando mais, para evitar futuros conflitos, optei pela opção do genymotion “without virtualbox”

1) Genymotion:

- Genymotion: basta iniciar o download no link abaixo. <without virtualbox>

https://www.genymotion.com/

2) Android Studio:

Optei pela opção do Android Studio devido as dificuldades citadas anteriormente, após o passo 4 eu mostro um problema com a utilização do JADX via Android Studio.

- ADB: É uma utilidade usada pra interagir com um dispositivo android, que eu usei na aula anterior pra abrir uma shell dentro do smartphone. Vocês podem instalar ela de duas formas:

    - De forma avulsa, se você usa algum sistema Linux que tem isso disponibilizado (é o meu caso com Arch). Talvez seja possível fazer isso com o Windows usando o WSL, mas eu não saberia auxiliar vocês nisso

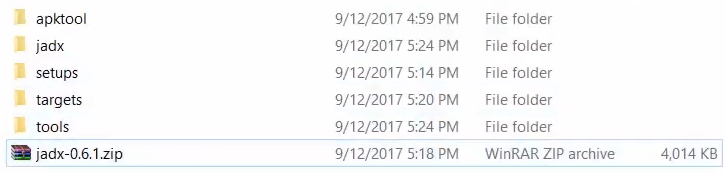
    - Baixando o Android Studio, que com ele vem outras utilidades, incluindo o ADB

3) JADX:

Optei pelo jadx

3.1)baixei o arquivo em .zip <https://github.com/skylot/jadx>, extrai o arquivo

3.2) extrair os arquivos



3.3) jadx --> bin --> jadx-gui.bat

- JADX ou APKTOOL: Duas ferramentas de análise estática, qualquer uma delas vai servir. Na aula eu vou usar o JADX porque é o que eu estou acostumado, mas se quiserem usar algo diferente, sintam-se à vontade (<https://github.com/skylot/jadx> ou <https://ibotpeaches.github.io/Apktool/>)

4) Frida:

A instalação via pip não deveria ter grandes dificuldades, entretanto, foi necessário adicionar o path do python para executar o comando “pip”.

- Frida: Ferramenta de análise dinâmica feita em Python e distribuida via PIP. Um pip install frida-tools deve resolver tudo, mas segue o site pra referência (https://frida.re/docs/installation/)

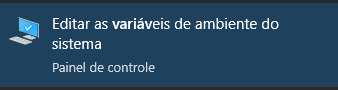
Dois problemas, uma solução:

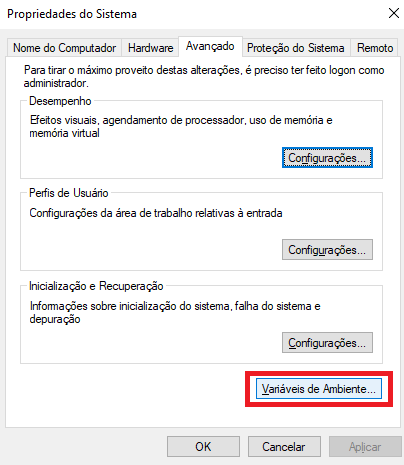
O JADX e o python precisavam ser adicionados ao PATH do Windows, segue abaixo o passo a passo de como fazer.

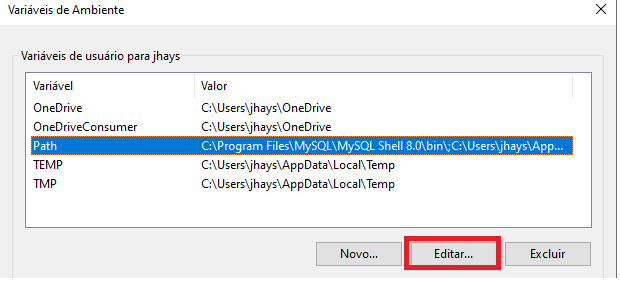
Passo 1:

Adicionar o caminho do python nas variáveis de ambiente

Pesquisar por variáveis de ambiente



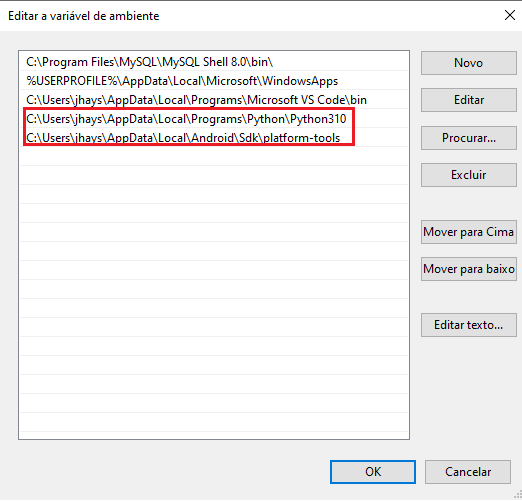




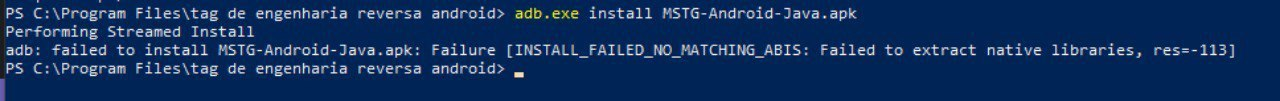
Passo 2:

-Adicionar o path.

O path é relativo de acordo com o local de instalação, mas se o seu caso foi o default na instalação do python e Android Studio, provavelmente estará nos mesmos diretórios abaixo, mudando apenas o User.



**Correção de erro:**

Problema --> eu estava tentando instalar um aplicativo que não tem suportes arquitetura do meu PC, pois, alguns apps que só possuem suporte para ARM

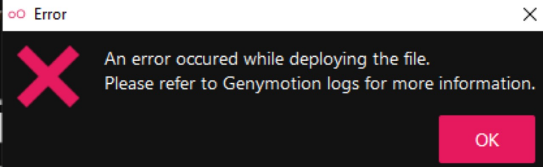
Solução --> baixar o “tradutor” .zip de ARM, de acordo com a versão do android instalado no genymotion

no link para download: <https://github.com/m9rco/Genymotion_ARM_Translation> dentro da pasta packages

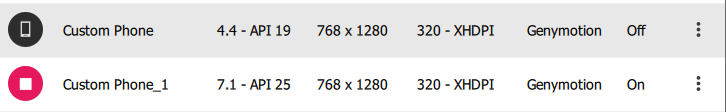
dentre os arquivos .zip disponíveis, temos 6 opções:

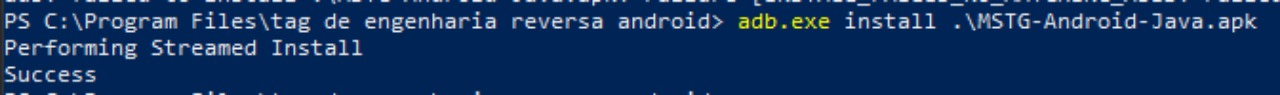


Tentei a opção 4.4 mas não obtive sucesso:



Segui as mesmas instruções, mas utilizando um android 7.1, ao invés do 4.4:

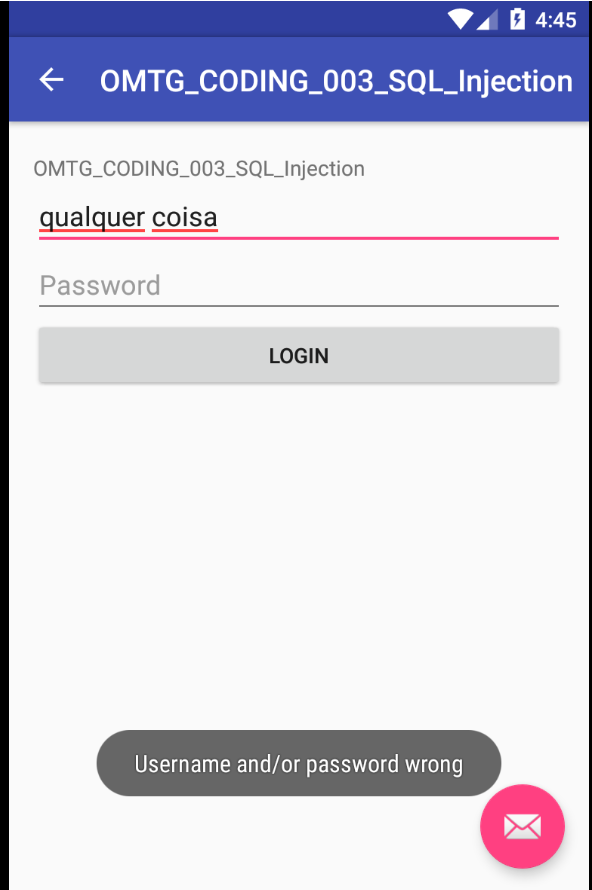


Obtive sucesso: 

**Sql injection, Exercício 1:**

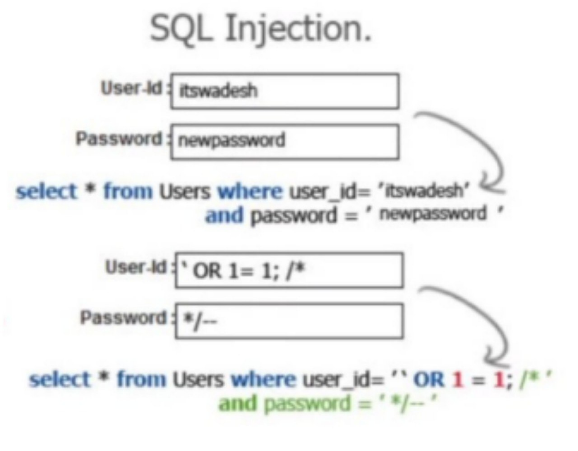
Análise dinâmica:

- testei a login e senha “admin” para ver como funcionava a execução

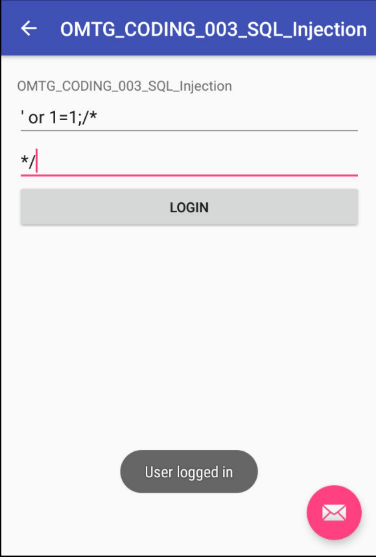


Seguindo as dicas dadas no get de web1/web2:

Passamos para o login um fecha aspas e a sentença or 1=1 (sempre verdadeira) e comentamos a requisição de senha



Conseguimos acesso com sucesso:



Vale destacar que a forma que eu acessei não foi a mais correta,

**Forma que eu fiz (não ideal):**

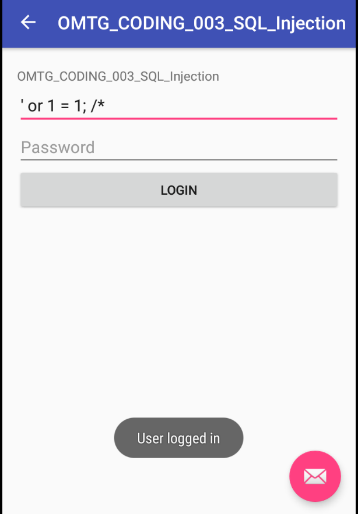
Note que ficou uma aspa solta no fim do comando



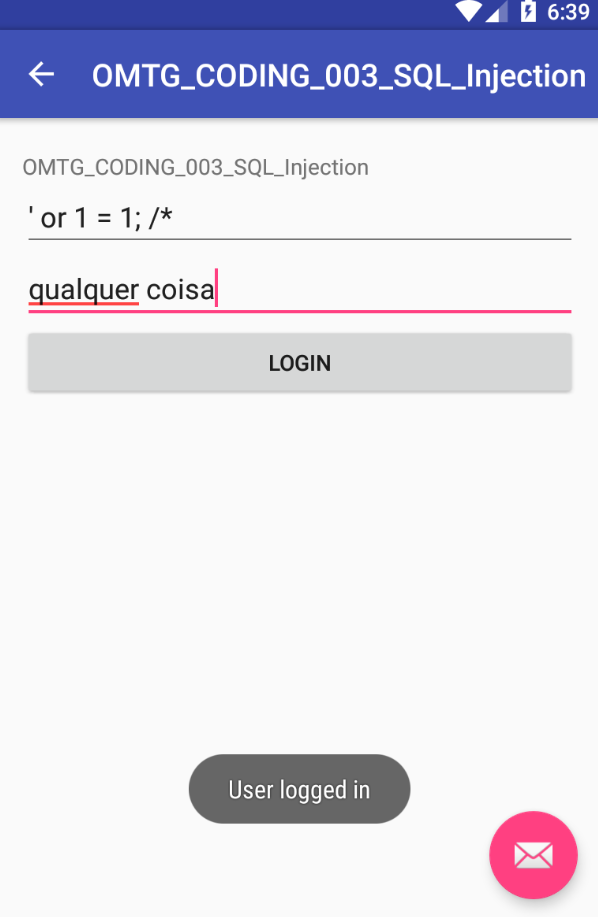
**Forma ideal:**

Note que a requisição da senha ficou comentada, de tal forma que não será necessário envia-la





Em alguns casos há verificação se o campo password foi preenchido ou não. Neste caso seria necessário preencher o campo password com qualquer palavra. Segue o exemplo abaixo:



Logging, exercicio 2:



Login em hexa 🡪 0x7f07005b

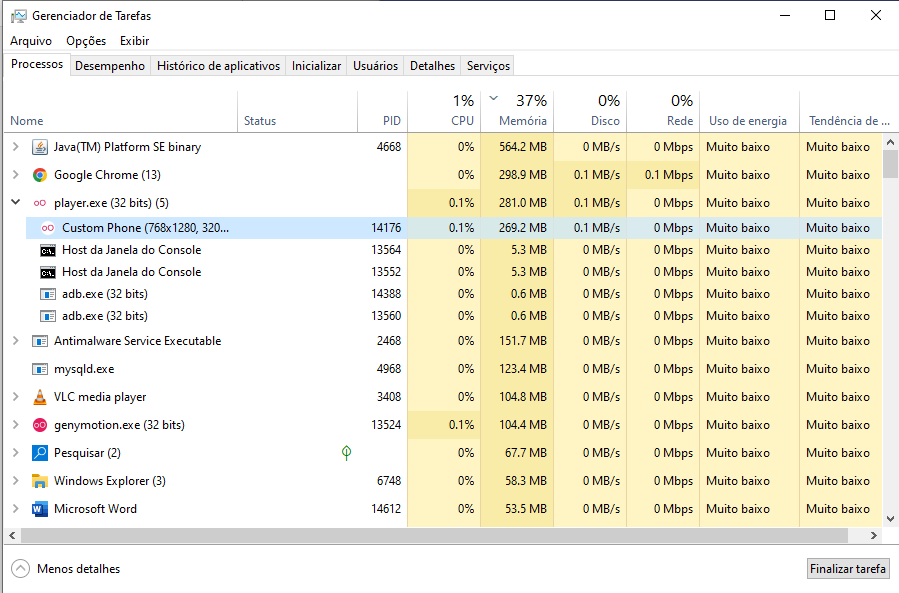
Login em decimal 🡪 2131165275

Password em hexa: 0x7f070059

Password em decimal 🡪 2131165273

Identificando o pid no gerenciador de tarefas:

Aprofundamento em --> <https://support.kaspersky.com/common/windows/6325#block2>



Pid 14176

Usando o adb logcat:

Limpei os logs antigos para facilitar identificação

