LTx Security

INTERCEPTANDO TRÁFEGO NO ANDROID

Sumário

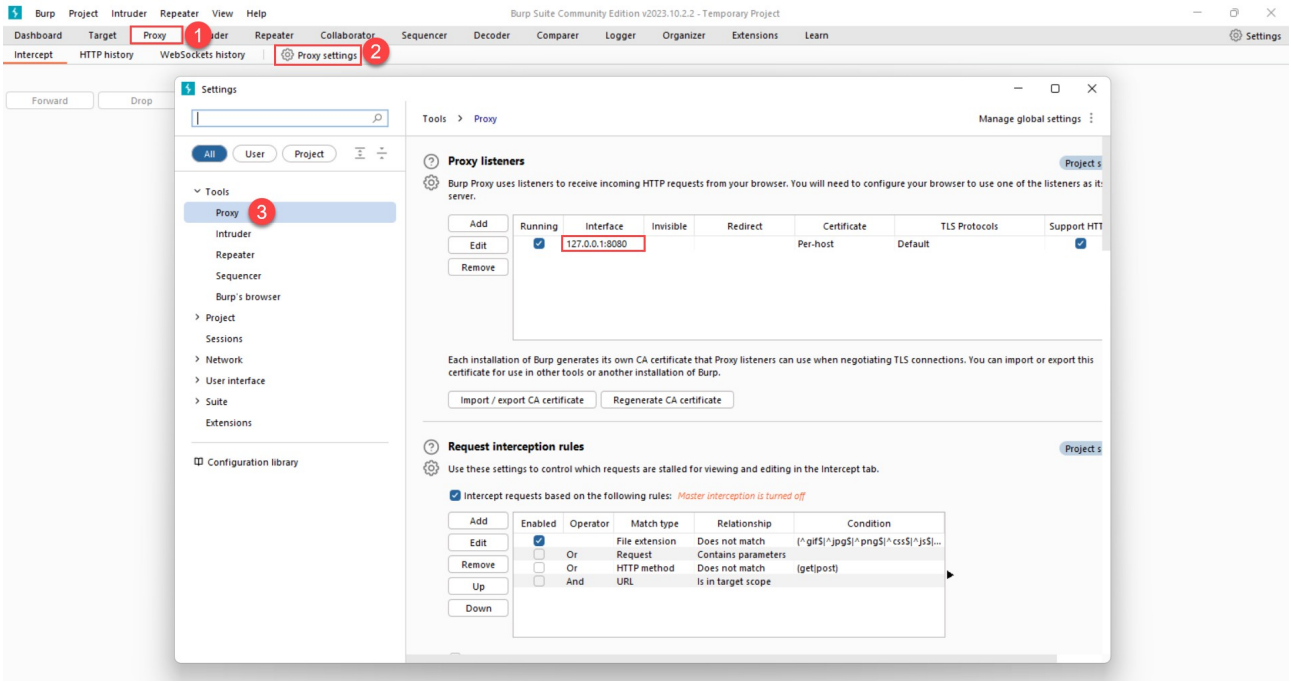
Introdução

Quando falamos de testes em aplicativos mobile, conseguir interceptar o tráfego do app com a API / Backend é fundamental para o sucesso da exploração. Nesse post vou mostrar uma das maneiras possíveis de se fazer isso.

Configurando o proxy

No burp

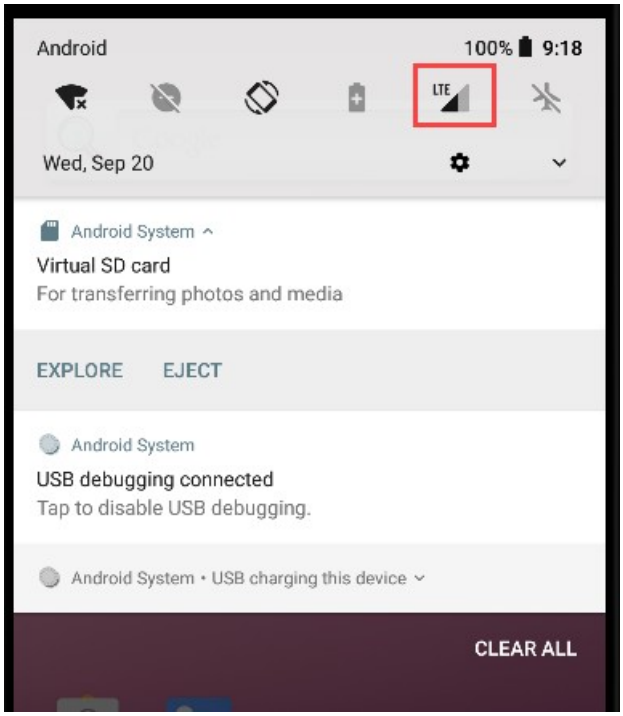
Antes de tudo, é necessário se certificar que o burp está utilizando o endereço “127.0.0.1:8080”. Então abra o burp e vá em Proxy -> Proxy settings -> Proxy para confirmar essa informação.



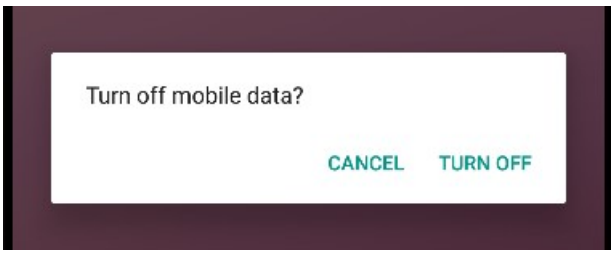
No dispositivo

O proxy será configurado através da rede Wi-Fi do dispositivo e durante o teste algumas coisas podem acabar barrando essa comunicação, como, por exemplo, uma proteção presente no app ou qualquer outro problema de conexão. Quando isso acontece, o sistema operacional Android entende que aquela rede Wi-Fi não possui conexão com a internet e começa a rotear os seus pacotes através dos dados móveis, o que faz com que não consigamos mais interceptar seu tráfego, para evitar que isso aconteça é necessário desabilitar os dados móveis no aparelho.

Para isso, basta arrastar a barra superior para baixo e clicar no ícone do LTE.



Após isso é só confirmar o desligamento dos dados móveis.



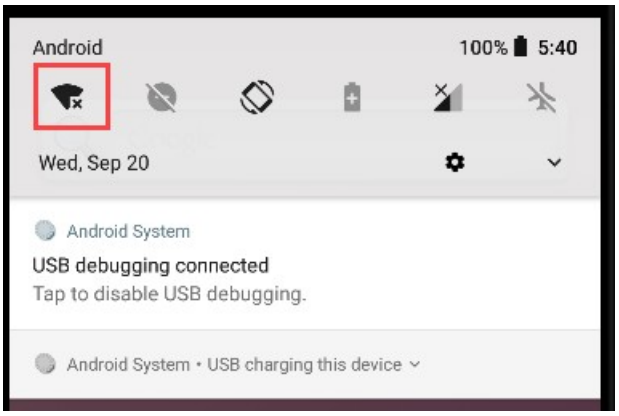
Com os dados móveis desligados, vamos realizar um port forwarding para criar um túnel que redireciona todo o tráfego do dispositivo para a máquina local na porta 8080.

Para isso, basta executar o seguinte comando do adb:

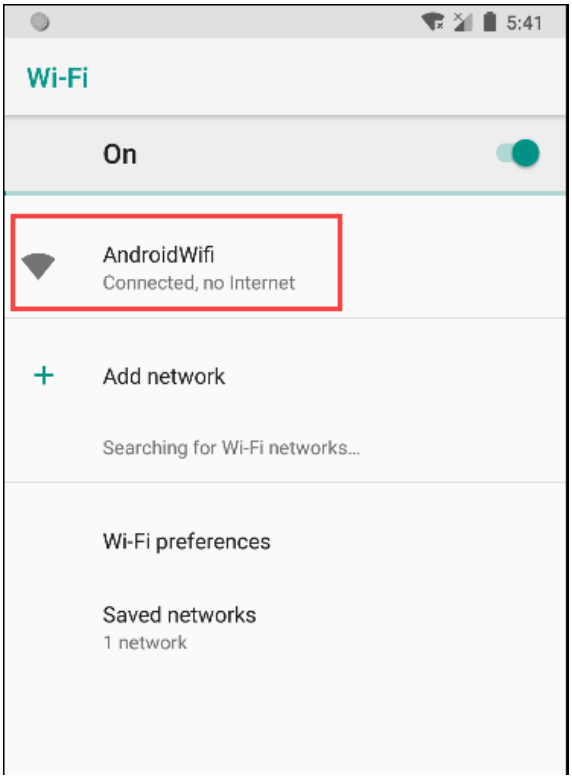
adb reverse tcp:8080 tcp:8080

Após a criação do túnel, chegou a hora de configurar o proxy no aparelho.

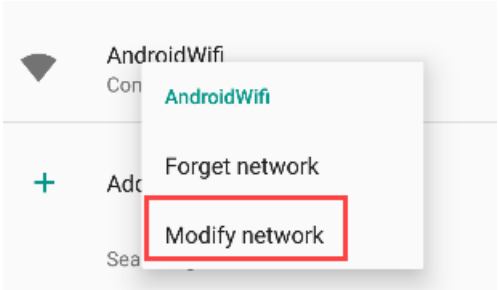
Novamente arraste a barra superior para baixo, então clique e segure o símbolo do Wi-Fi.



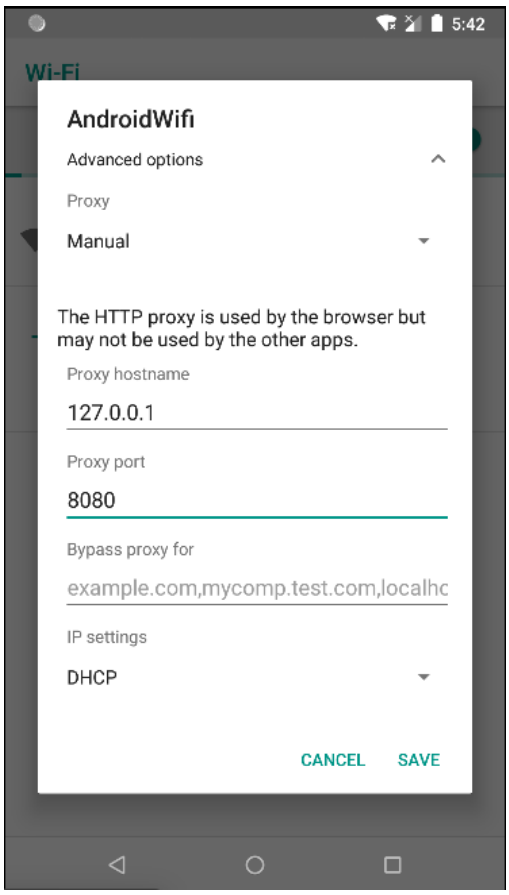
Então, aparecerá as redes disponíveis para o dispositivo, novamente clique e segure na rede “AndroidWifi”.



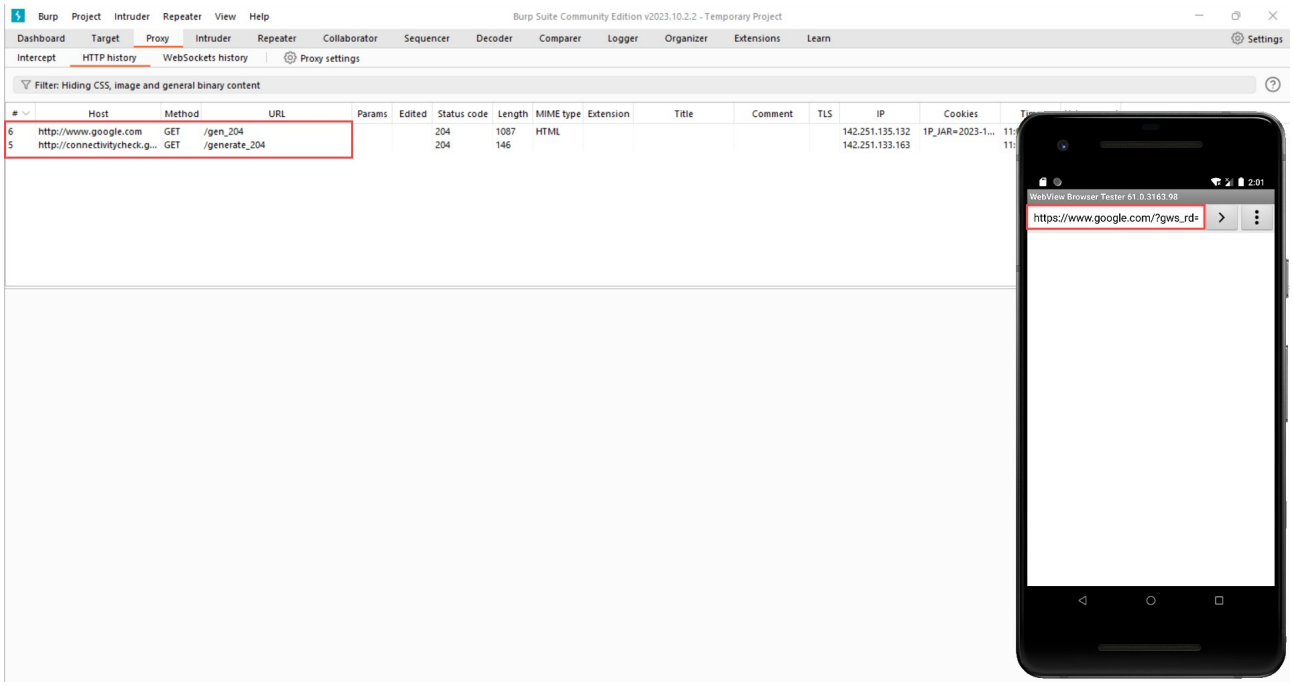
Nas opções que irão aparecer vá em “Modify network”.



Então altere o proxy para manual e coloque as informações do burp:



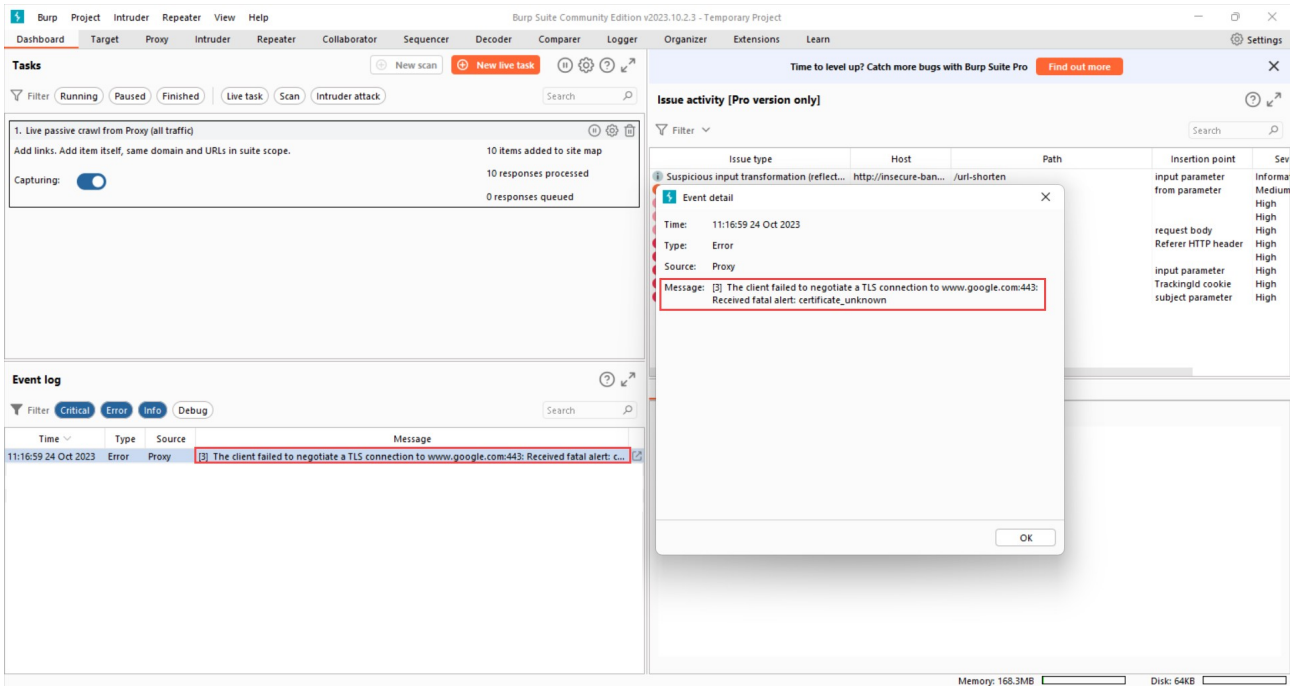
Com isso já é possível visualizar o tráfego do dispositivo através do burp.



LTx Security

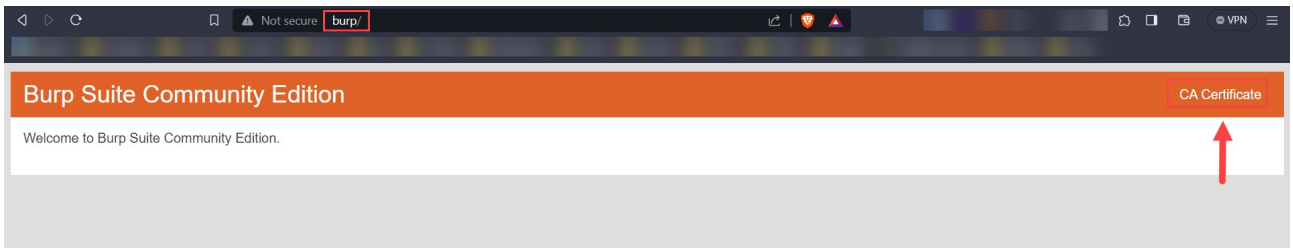
Instalando o certificado no Android

Como pode ser visto no exemplo acima, apesar de o tráfego estar sendo interceptado, não foi possível acessar o site do Google. Analisando os logs do burp é possível identificar o problema.



O erro foi causado pelo certificado, o que faz com que o cliente não consiga acessar sites que utilizem o TLS. Para resolver esse problema é necessário instalar o certificado do burp no dispositivo Android.

Para realizar o download do certificado, acesse o endereço “http://burp” do navegador da sua máquina.



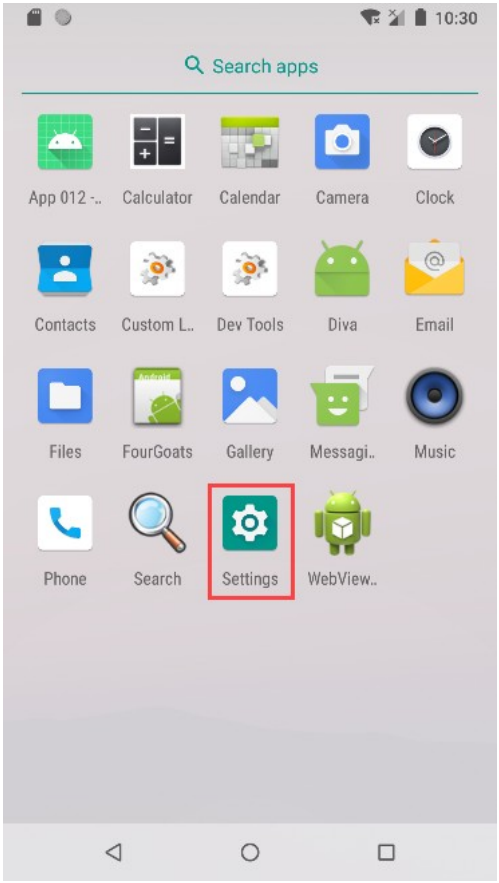
O certificado baixado possui o nome “cacert.der”, para realizar a instalação no dispositivo, é necessário alterar a sua extensão para “.cer”.

```
mv cacert.der cacert.cer
```

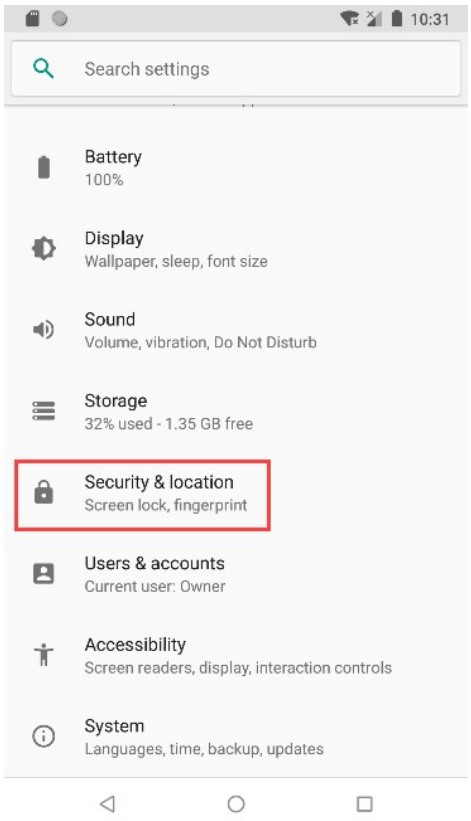
Após isso, envie o arquivo do certificado para o dispositivo Android.

```
adb push cacert.cer /sdcard/Download/cacert.cer
```

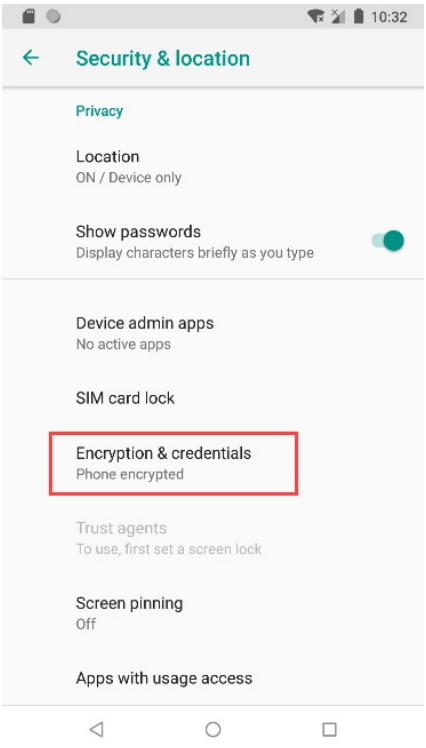
Agora, no dispositivo vá em “Settings”.



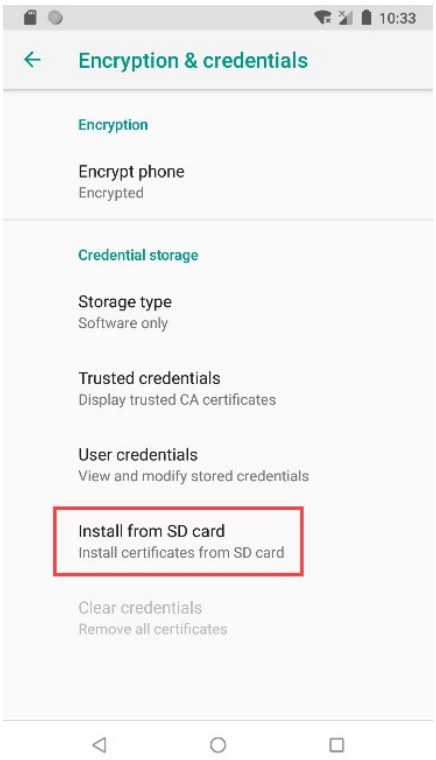
Depois em “Security & location”.



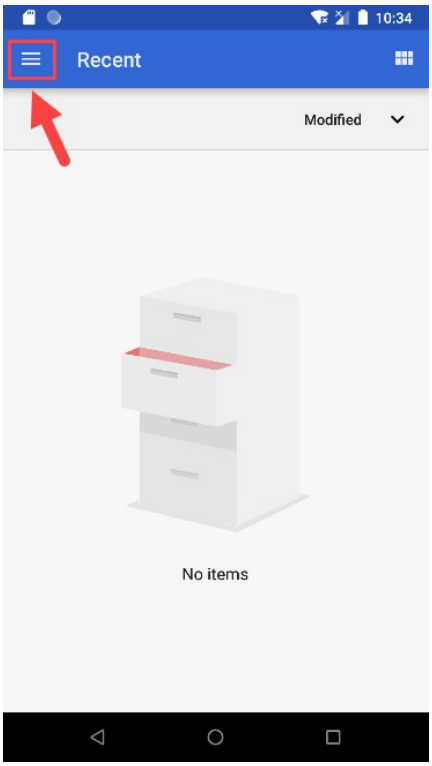
Depois em “Encryption & credentials”.

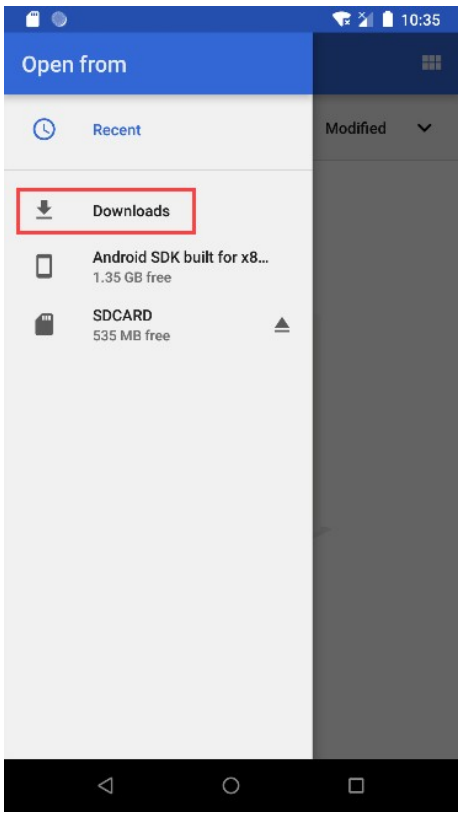


E por fim em “Install from SD card”.

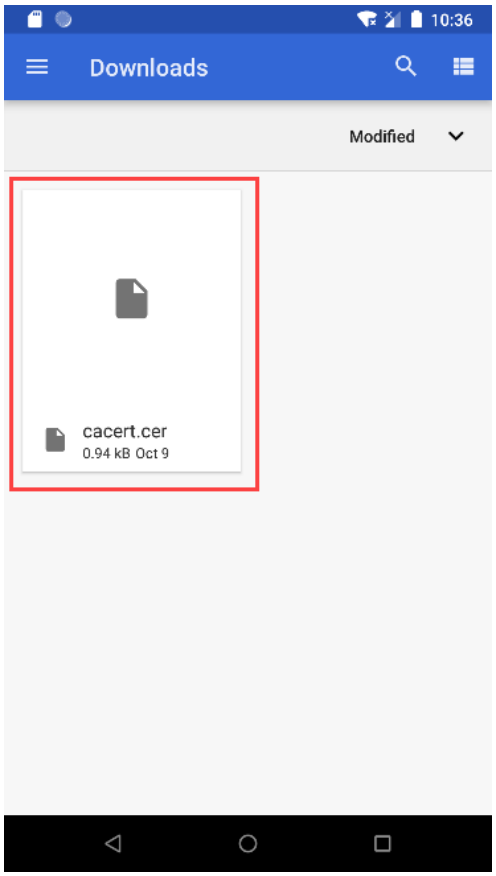


Ao abrir essa opção, vá no menu presente no canto superior esquerdo e em seguida abra a pasta de Downloads.

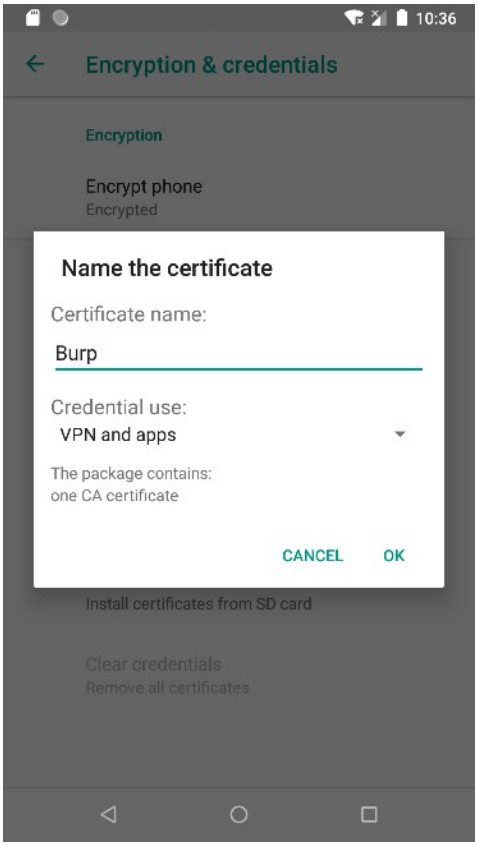




Pronto, ai está o certificado.

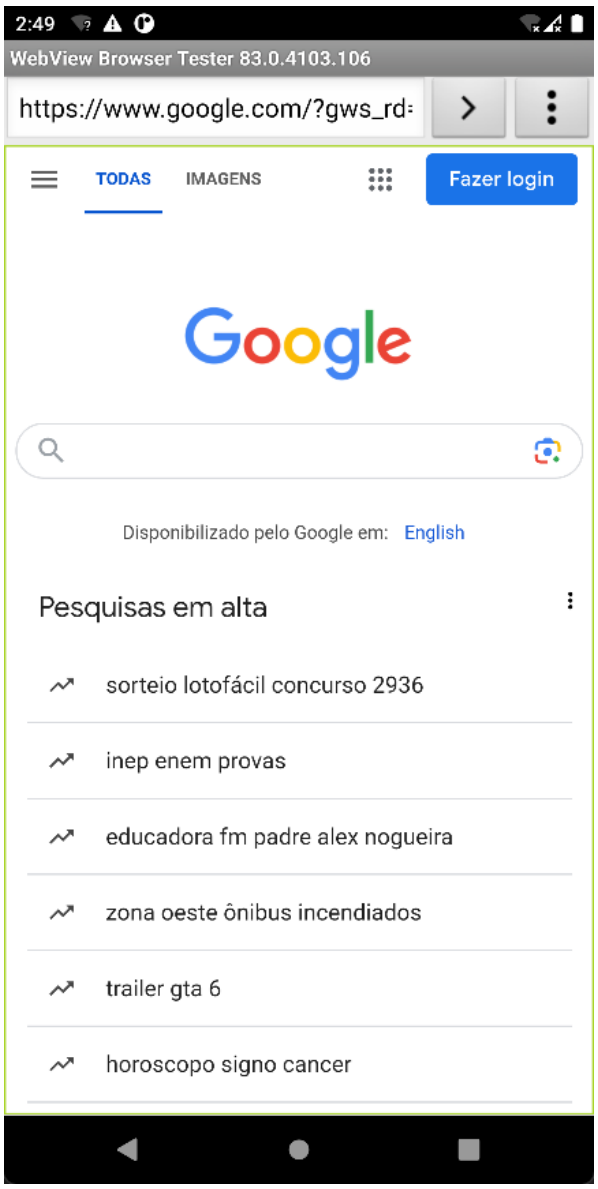


Agora basta clicar no arquivo, escolher o nome do certificado e realizar a instalação.



*** Nesse momento, pode ser que o aparelho peça para você configurar uma senha para o dispositivo, esse é um mecanismo de segurança padrão do Android e basta seguir o passo a passo.*

Pronto, agora já é possível acessar os sites utilizando o https.


2:49
WebView Browser Tester 83.0.4103.106
https://www.google.com/?gws_rd=
TODAS
IMAGENS
Fazer login
Google
Disponibilizado pelo Google em: English
Pesquisas em alta
sorteio lotofácil concurso 2936
inep enem provas
educadora fm padre alex nogueira
zona oeste ônibus incendiados
trailer gta 6
horoscopo signo cancer

LTx Security

Segurança Ofensiva