11 Are All Androids Polyglots or Only C-3PO?

by Philippe Teuwen

```
$ pm install /sdcard/pocorgtfo12.pdf
```

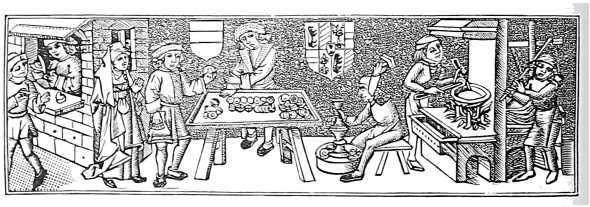
That's all it takes to install this polyglot as an Android application. So what's the Jedi mind trick?

Basically, we merged the content of an Android application with the ZIP feelies. (Please excuse the cruft you'll find in the feelies!)

Now I won't teach you anything if I tell you that an APK is just a ZIP. It is, of course, a ZIP, but not just, if we also want it to be an Android app; we need the application itself, for one thing, and then some.

The Android OS requires all applications to be signed in order to be installed, so our polyglot needs to be signed by our Pastor, which is actually not a bad practice. Beyond this, Android doesn't really care about what else the ZIP could be (e.g., it can be a PDF, as is the glorious PoC||GTFO tradition), but the trick is that *all* of the archive contents must be signed. In particular, this must include all the original feelies, as you can observe in `META-INF/MANIFEST.MF`.

The resulting polyglot can be installed directly if dropped on `/sdcard/`, as well as locally, by using the Android Package Manager as shown above.



But I expect most readers—well, only those crazy enough to give execute permission to the Pastor on their terminals—to install it via the Android Debug Bridge tool `adb`. This method expects the application package filename to end in `.apk`, so let's humor it:

```
$ ln -s pocorgtfo12.pdf pocorgtfo12.apk
$ adb install pocorgtfo12.apk
```

But what does this application do? Not much, really. It copies itself (the installed APK) to `/sdcard/pocorgtfo12.pdf` and opens the copy with your preferred PDF reader.

Note: Imperial security is improving and on the latest versions of the OS, even if this 'droid polyglot gets installed, it may fail in `dex2oat`. You may need to develop your own Jedi tricks to tell them these are not the droids they are looking for—and if you do, please send them to us![55]

And you, my friend, are *you* a polyglot? Let's celebrate this fine Québécoise release with a classic *charade*!

[55] This has been finally solved in time for this electronic release. Use the Force to unravel its secrets... You may even propagate it neighbourly by Near Force Communication, in which case Padawans have first to accept apks from *unknown sources*.

Charade des temps modernes

Mon premier est le nombre de Messier de la Galaxie d'Andromède.
Mon second est la somme de quatre nombres premiers consécutifs commençant par 41.
Mon troisième est le nombre atomique de l'Unennquadium.
Mon quatrième est le nombre modèle qui succéda au Sinclair ZX80.

Mon tout lève tous les obstacles sur le chemin de la Science.