

Notes.

Forensics and Stego.

Summary:

1. Android
2. Encoding and Decoding:
3. Web
4. Stego and File Formatting

Android:

apktool

Use debug mode to decode the apl file:

```
apktool d an_android_app.apk
```

dex2jar

Unpack the apk file, and run dex2jar on classes.dex file:

```
d2j-dex2jar an_android_app/classes.dex
```

jadx-gui

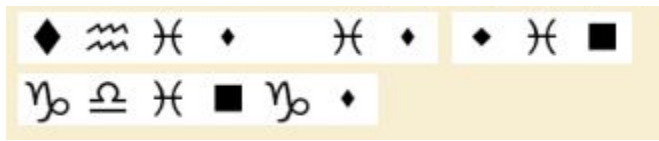
View the source of the classes:

- Import the apk

Encoding and Decoding:

Wingdings:

Sample:

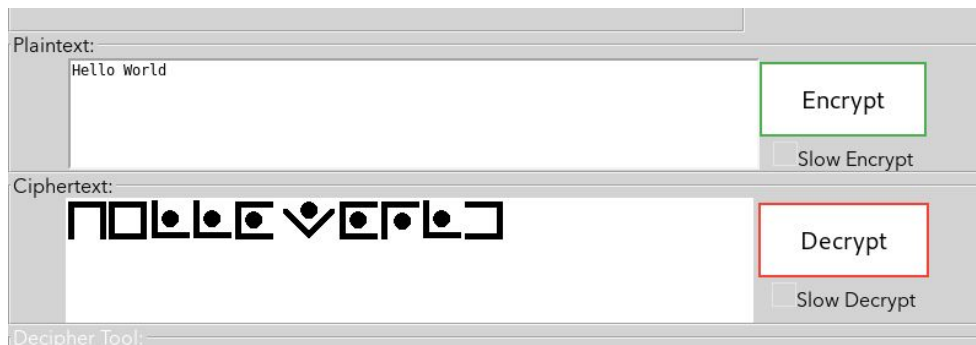


Decoding tool:

<https://www.dcode.fr/wingdings-font>

PigPen:

Sample:

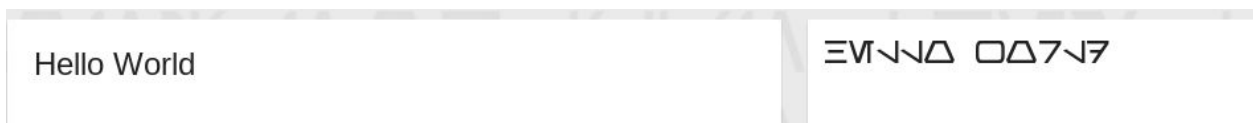


Encoding and Decoding tool:

<https://crypto.interactive-maths.com/pigpen-cipher.html>

Aurebesh Translator:

Sample:



Encoding Tool:

<https://lingoam.com/AurebeshTranslator>

CyberChef: Swiss Army Knife Encoding and Decoding Tool

Supported Functions:

1. base64, base32, etc.

2. Caesar Cipher
3. ROT13, ROT47
4. XOR, Morse, Vignere, Atbash, Bacon Cipher, etc.

Allows user to apply multiple functions sequentially

Link: <https://gchq.github.io/CyberChef/>

Hidden Binary Cipher:

Sample:

The chicken crossed The road
the chicken Crossed the road
the chicken crossed The road
The chicken crossed the Road
the chicken Crossed the road
The chicken crossed The Road

Decoding:

Capitals are 1s, and lowercase are 0s

The chicken crossed The road	10010	18	S
the chicken Crossed the road	00100	4	E
the chicken crossed The road	00010	2	C
The chicken crossed the Road	10001	17	R
the chicken Crossed the road	00100	4	E
The chicken crossed The Road	10011	19	T

BrainF*ck:

Sample: Hello World

```
+[-[<<[+[->>]-[<<<]]]>>>-]>.-.-.->.,>.<<<<.-<+,>>>>>>>.>.<<.<.-
```

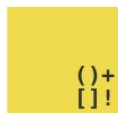
Interpreter:

Page 10 of 10

Web:

JSF*ck:

Sample: Hello World



JSFuck

JSFuck is an esoteric and educational programming style based on the atomic parts of JavaScript. It uses only six different characters to write and execute code.

It does not depend on a browser, so you can even run it on Node.js.

Use the form below to convert your own script. Uncheck "eval source" to get back a plain string.

[illegible]

Wiki:

<https://esolangs.org/wiki/JSFuck>

Interpreter:

<https://enkhee-osiris.github.io/Decoder-JSFuck/>

Stego & File Formatting:

- List of File Signatures: https://en.wikipedia.org/wiki/List_of_file_signatures
- Stego Tools: steghide, binwalk, exiftool ...
- GIMP: Change exposure to reveal things hidden in the image.
- Use sonic visualiser to reveal patterns in the sound waves

List all the file types in a folder:

```
for i in $(ls); do file "$i"; done > file_typepest.txt
```