Summary

Super Summary

1. Perform activity

2. Trigger a HEAP dump of process

3. Copy out dump file and execute ‘strings’ command against it

Reference

<https://github.com/ronaldyho/hacking_android/wiki/Android-Memory-(-Heap---threads>-)

Example App

Fleksy Keyboard

1. Data Preparation

Here is the activity that we have performed

# Launch Termux and “use” Fleksy keyboard on the app

This created the data that we can use

2. Capture the dump file

Forensics tool “mem” is used to capture the dump file. In a nutshell, here is what we did

# adb shell

# cd /data/local/tmp

# ps | grep fleksy

# mem <PID> output.hprof

3. Copy out the dump file for processing

ADB is your good friend

# adb pull /data/local/tmp/output.hprof .

Once in the local machine, the “strings” command is used to extract “readable” strings.

# strings output.hprof > output\_hprof.txt

Towards the end of the file, we see the words being typed into Termux app:

8vCT

V7s|

oP>?C

**help**

**grep**

Bs$

op(wC

~Bs@