Cheat sheet

Basic commands

Command	Example	Comment
re re re wr		Read the registers Write to registers
b	b 0x00000076cb964ed0 b libc.so`sendto breakpoint set -s libc.so -n send	setting up a breakpoint
watchpoint	`w s e -s 1 -w read_write -- $x0&0x0000FFFFFFFFFFF`	hardware breakpoint, ignoring memory tags
image lookup -r -n <symbol>	image lookup -r -n fopen image lookup -r -n send libc.so	regex lookup function name
image lookup -a <address>	(lldb) image lookup -a `((int ***)$x0)[0][6]` Address: libart.so[0x00000000003900c0] ... FindClass(_JNIEnv*, char const*) (lldb) image lookup -a 0x000000787952b0c0 Address: libart.so[0x00000000003900c0] ... FindClass(_JNIEnv*, char const*)	translate address to symbol, in example - parsing JNIEnv * object
memory region <ADDRESS>	(lldb) mem reg 0x0000007c23b510f8 [0x0000007c23b47000-0x0000007c23b52000) r-- /data/app/XXX/YYY/base.apk	shows the region of the specified address
memory read --outfile <PATH> --binary --force <START_ADDR> <END_ADDR>	(lldb) memory read --outfile C:\temp\dump.bin --binary --force 0x0000007872124000 0x000000787219a000 483328 bytes written to 'C:\temp\dump.bin'	dump binary memory

Revision #9
Created 13 August 2024 07:15:02 by Ariel
Updated 6 January 2025 15:53:21 by Ariel