* Android IPC
  - Intent -> AIDL -> Binder
  - cat /sys/kernel/debug/binder ????????
  - Parcel????
  - binder ??shared memory ?service
  - ??service??binder ????

* Android debuggerd
  - Android ??process segmentation fault signal??????????socket??debuggerd
  - debuggerd?logcat????address??????address
  - lr -> register for storing return address in ARM
  - ????crash log?/proc/pid/maps
  - ???https://wiki.linaro.org/WorkingGroup...nwindDebuggerd

* Dynamic linker/program interpreter
  - ls-linux.so.2 (Linux?)
  - ???
  - ??? root file system ????????? ELF interpreter
  - Android???????/system/bin/linker?address????
    + ???????performance??
  - X86
    + Entry: libc_start_main
    + library: libc
    + linker: ls-linux.so.2 (????)
  - Android
    + Entry: __libc_init
    + library: bionic
    + linker: /system/bin/linker
      - ?????? stack & calling convention???? SegFault

* bionic
  - __init_libc?static?dynamic ????
  - init process (pid 1 ??)?static????malloc
  - ????????AOSP?????(????)
  - adbd ?static (?)
  - ?interpreter??
  - objdump -s -j .interp filename

* memory map of a process
  - cat /proc/pid/maps
    + ????:
      - address
      - perms
        + r = read

```
        + w = write
        + x = execute
        + s = shared
        + p = private (copy on write)
      - offset
      - dev
      - inode
      - pathname
  - ???path????????text/data???
adb shell cat /proc/18696/maps (?????)
00008000-00009000 r-xp 00000000 b3:02 8959       /data/local/hello
00009000-0000a000 rwxp 00001000 b3:02 8959       /data/local/hello
b0001000-b0009000 r-xp 00001000 b3:01 128        /system/bin/linker
b0009000-b000a000 rwxp 00009000 b3:01 128        /system/bin/linker
b000a000-b0015000 rwxp 00000000 00:00 0
beb07000-beb28000 rw-p 00000000 00:00 0          [stack]
ffff0000-ffff1000 r-xp 00000000 00:00 0          [vectors
  - heap??address?????
  - stack??address?????
  - ????????trace??
```

* ABI

```
  - readelf?????
$ readelf -h ../libs/armeabi/a
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           ARM
  Version:                           0x1
  Entry point address:               0x8540
  Start of program headers:          52 (bytes into file)
  Start of section headers:          7592 (bytes into file)
  Flags:                             0x5000002, has entry point, Version5 EABI
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         7
  Size of section headers:           40 (bytes)
  Number of section headers:         22
  Section header string table index: 21
```

- eabi/oabi: e for embedded, o for old
- ???ABI (??ABI??)??data type?size???????
  + sizeof (char)
    - EABI: 1
    - OABI: 4
  + sizeof (struct empty_struct{};)
    - EABI: 1
- x86??ABI?????
- Embedded?ABI????????
  + ??
  + ????????????????
  + ??
  + ref: http://wiki.debian.org/ArmEabiPort
- ARM EABI ????????

* Start a process
  - create a process
  - load executable file
  - setup runtime
  - page valid (?)

* Before Hello World..
  - UID/GID
  - Signal
  - load ld.so
  - mmap
  - random
  - load libstdc++.so
  - ...

* Android GDB
  - adb forward tcp:port tcp:port
  - symbol ???
  - ${PWD}/out/target/product/product_name/symbols/system/bin

* LD debug
  - export LD_DEBUG=files
  - LD_DEBUG=help /lib/ld-2.13.so

* Hear Say/??????
  - BUILD_ID
    + Issue tracking
      - ?????ELF??AOSP/Cyanogenmod
  - NDK?????Android SDK?????
  - mm -b => make clean; make

- ??elf?????main????
  + pypy
- 2010???ELF??build ID
- abort()
- ptrace
- addr2line -e [file]
- Android???libc/linker?size????????????
- libunwind
- ELF section?offset??????/proc/pid/maps?????????????
- ANR
  + Android Not Responding
  + ????????????? Service ?
- Android????mix????flinger
  + Surface flinger
  + service flinger
  + ...