Android ????

记录安卓相关技术

apk 4??????????

apk 4□□□□□□□□□

apk 4字节对齐及重新签名

4k ??

简介:

- 需求，对于 **Android30** 版本以上需要对 **apk** 安装包进行 **4k**对齐 **.**

命令:

- **zipalign -v -p 4 d:\test\app1.apk d:\test\app1_zipa.apk**

apk 4字节对齐及重新签名

apk ????

命令:

```
 apksigner sign --ks .\test.jks --ks-key-alias testalias  --out ./unsigned_lab9.apk
.\lab9_task_4.apk
```

说明:

1. unsigned_lab9.apk 为签名后的 apk

??native

□□ Android native □□□ so

调试native

????

1. 下载ida-pro 7.5
2. 打开命令行窗口，执行

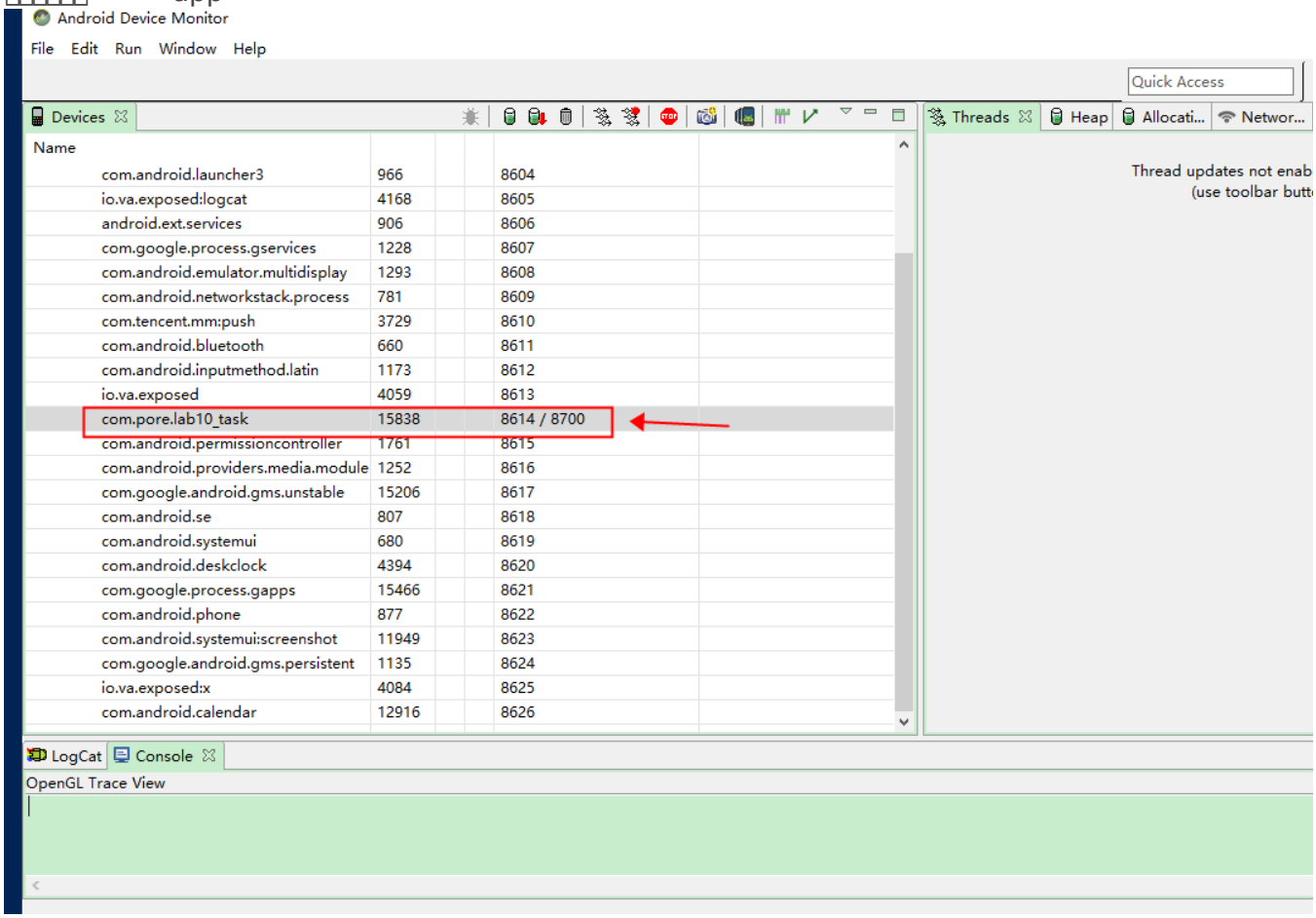
   ```
   adb shell


   su
   ```

3. 再把ida目录下的dbgsrv的目录下的android_server(先看下手机是32位还是64位，32位选择32位的android_server，64位选择64位的android_server)复制到/data/user/0/server下（没有目录先创建目录）

4.
   ```
   # 以x86为例
   chomod +x android_x86_server
   # 修改名称
   move android_x86_server asd
   # 执行
   ./asd
   ```

5. 打开ddms

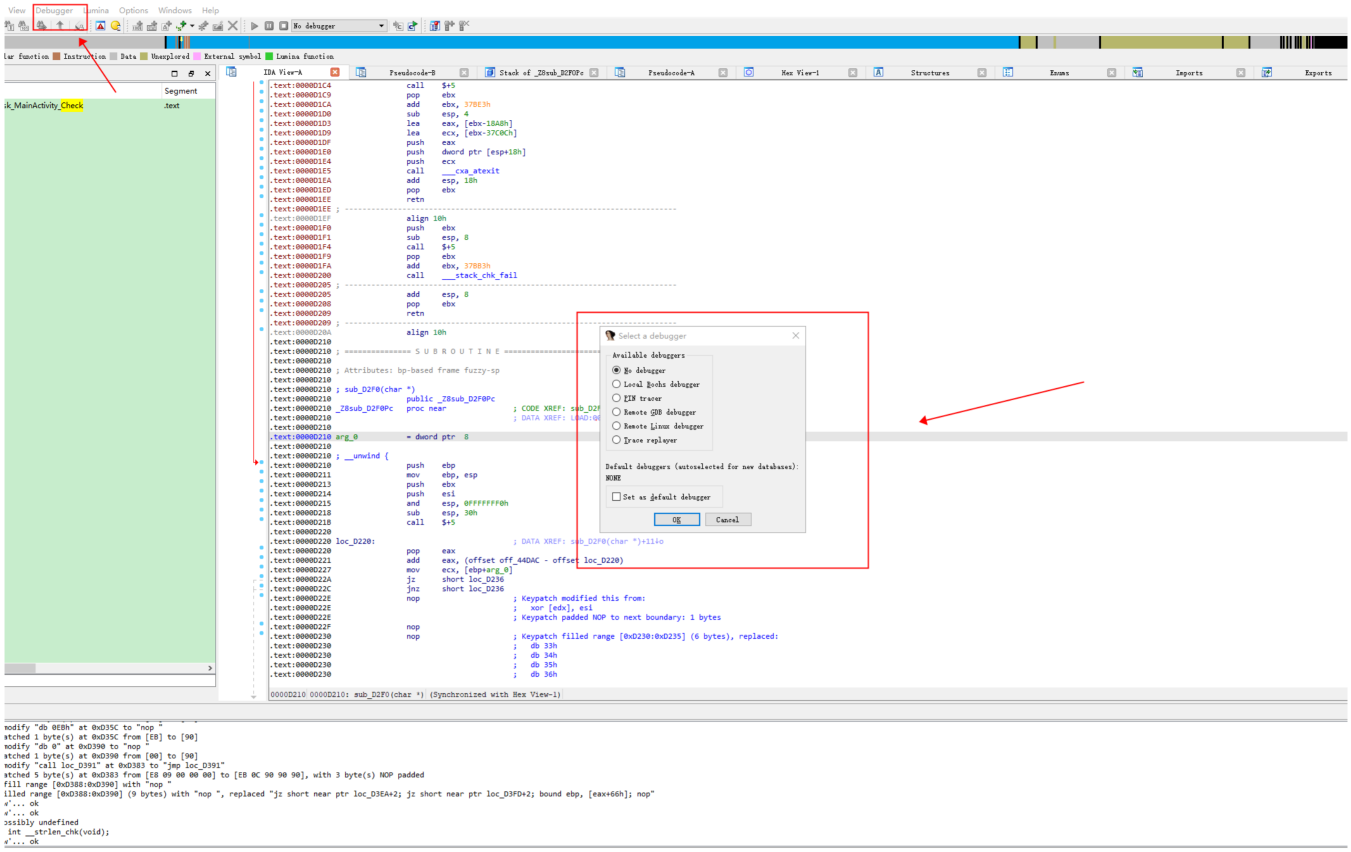
6. □□□□□□ app



7. jdb -connect com.sun.jdi.SocketAttach:hostname=127.0.0.1,port=8614□ jdk□□ 1.8□ port □□□□□ 8614□
8. □□□□□□

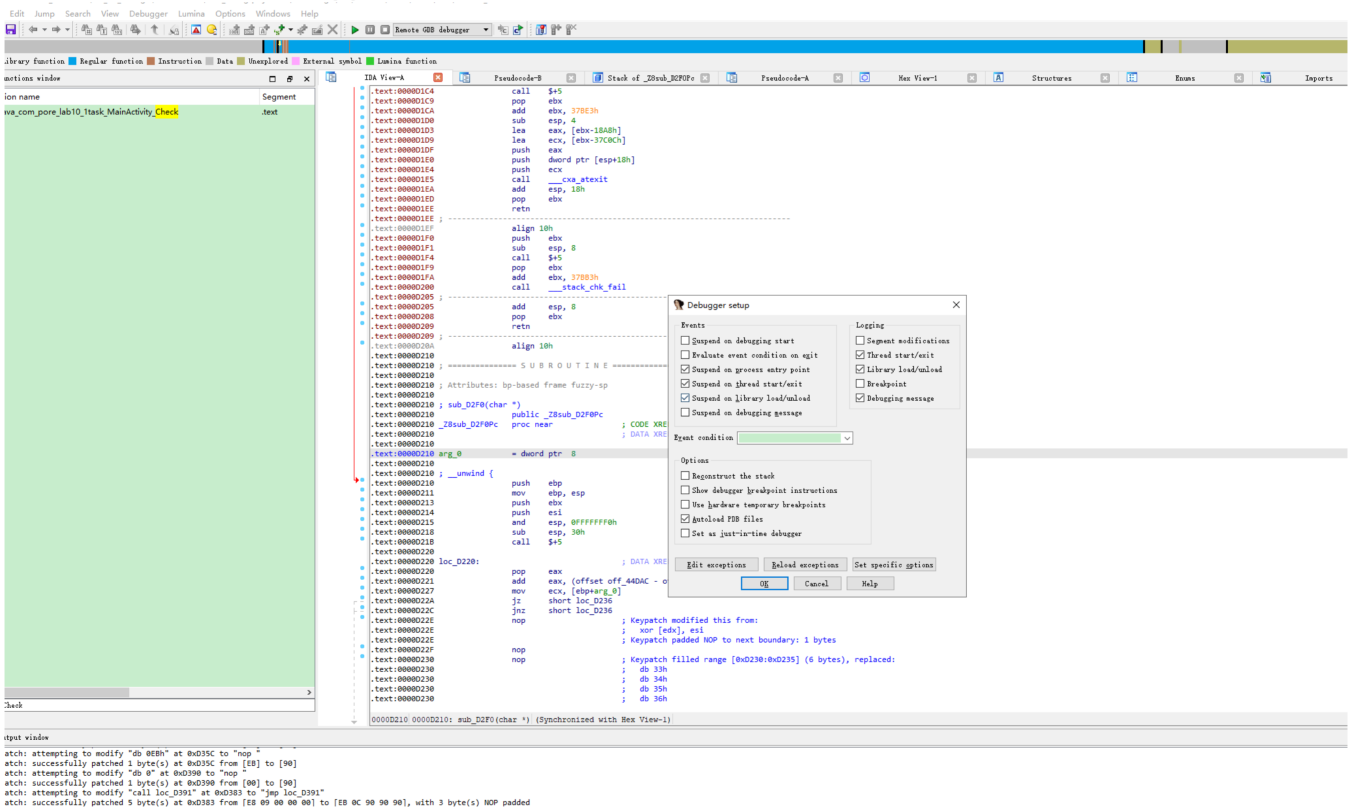
```
adb forward tcp:23946 tcp:23946
```

9. 打开 ida-pro



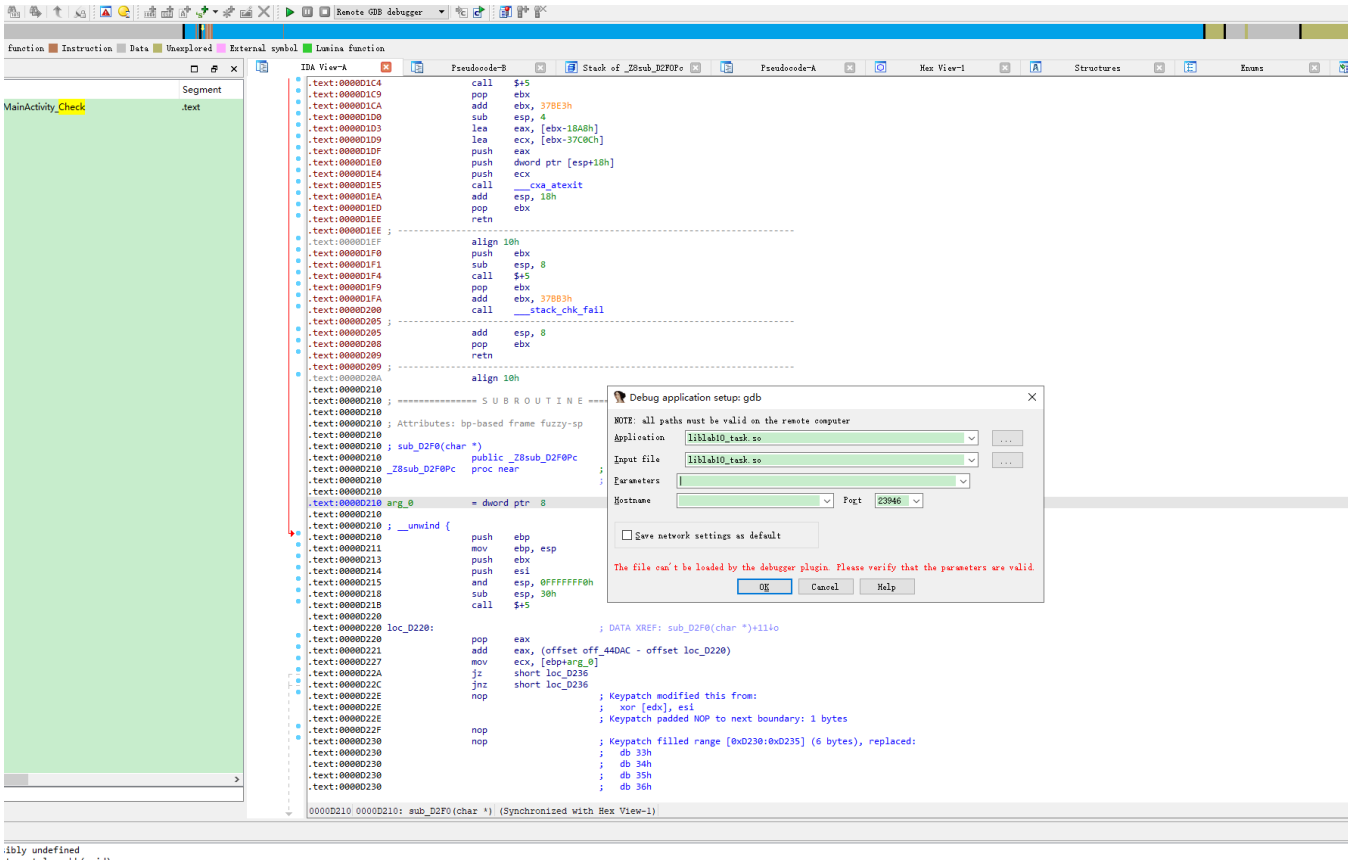
10. 选择 remote Linux debugger

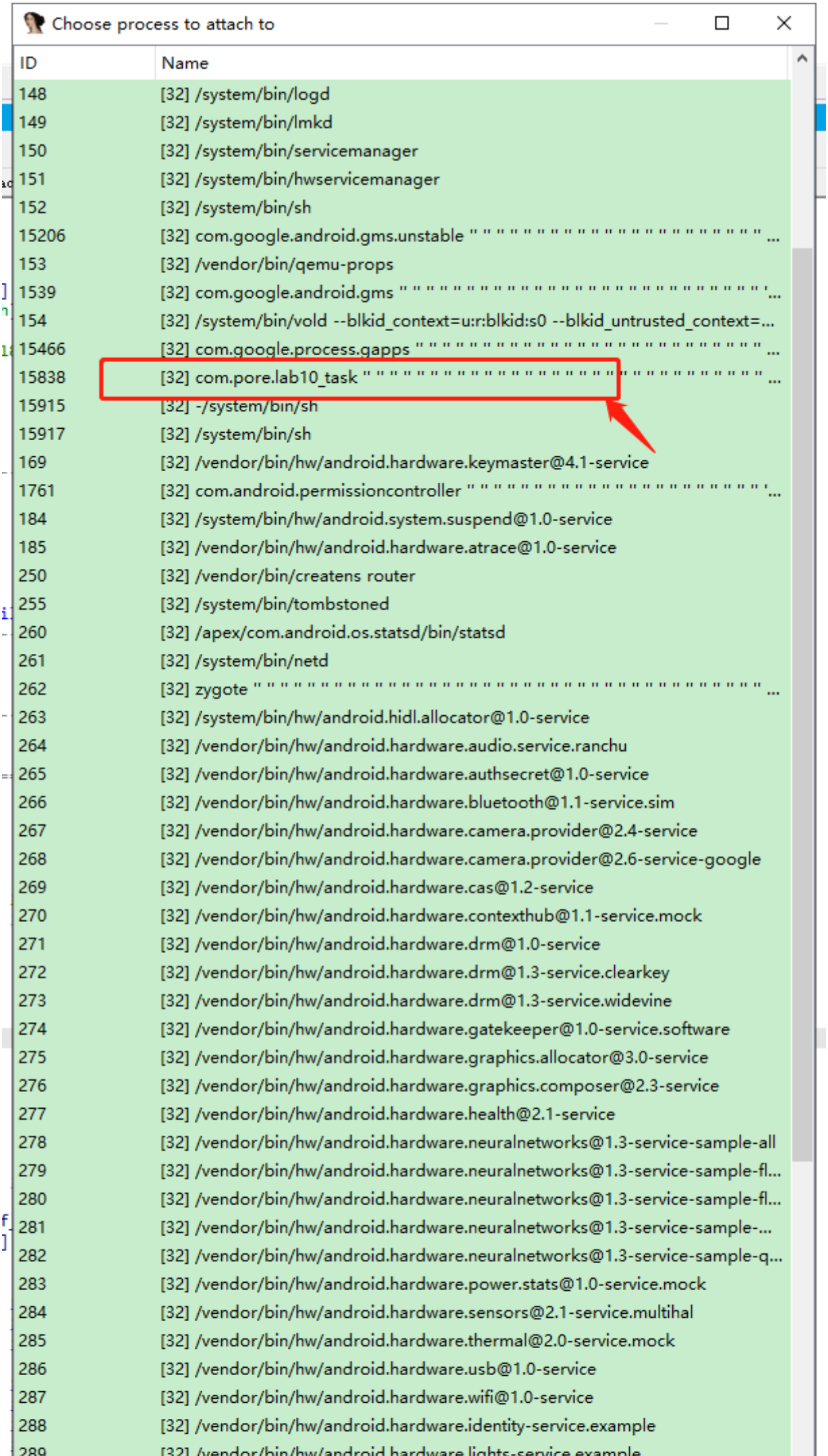
11.



12. 选中 3项

13. 在 hostname 中填写 127.0.0.1 port 填写 23946 (与端口转发的要一致)


Remote GDB debugger
function Instruction Data Unexplored External symbol Lumina function
Segment
MainActivity_Check
.text
IDA View-A
Pseudocode-B
Stack of _Z8sub_D2F0Pc
Pseudocode-A
Hex View-1
Structures
Enums
.text:0000D1C4 call $+5
.text:0000D1C9 pop ebx
.text:0000D1CA add ebx, 37BE3h
.text:0000D1D0 sub esp, 4
.text:0000D1D3 lea eax, [ebx-18A8h]
.text:0000D1D9 lea ecx, [ebx-37C0Ch]
.text:0000D1DF push eax
.text:0000D1E0 push dword ptr [esp+18h]
.text:0000D1E4 push ecx
.text:0000D1E5 call ___cxa_atexit
.text:0000D1EA add esp, 18h
.text:0000D1ED pop ebx
.text:0000D1EE retn
.text:0000D1EF align 10h
.text:0000D1F0 push ebx
.text:0000D1F1 sub esp, 8
.text:0000D1F4 call $+5
.text:0000D1F9 pop ebx
.text:0000D1FA add ebx, 37BB3h
.text:0000D200 call ___stack_chk_fail
.text:0000D205 add esp, 8
.text:0000D208 pop ebx
.text:0000D209 retn
.text:0000D20A align 10h
.text:0000D210 ; Attributes: bp-based frame fuzzy-sp
.text:0000D210 ; sub_D2F0(char *)
.text:0000D210 public _Z8sub_D2F0Pc
.text:0000D210 _Z8sub_D2F0Pc proc near
.text:0000D210 arg_0 = dword ptr 8
.text:0000D210 ; __unwind {
.text:0000D210 push ebp
.text:0000D211 mov ebp, esp
.text:0000D213 push ebx
.text:0000D214 push esi
.text:0000D215 and esp, 0FFFFFFF0h
.text:0000D218 sub esp, 30h
.text:0000D21B call $+5
.text:0000D220 loc_D220: ; DATA XREF: sub_D2F0(char *)+11↓o
.text:0000D220 pop eax
.text:0000D221 add eax, (offset off_44DAC - offset loc_D220)
.text:0000D227 mov ecx, [ebp+arg_0]
.text:0000D22A jz short loc_D236
.text:0000D22C jnz short loc_D236
.text:0000D22E nop ; Keypatch modified this from:
.text:0000D22E ; xor [edx], esi
.text:0000D22E ; Keypatch padded NOP to next boundary: 1 bytes
.text:0000D22F nop
.text:0000D230 nop ; Keypatch filled range [0xD230:0xD235] (6 bytes), replaced:
.text:0000D230 ; db 33h
.text:0000D230 ; db 34h
.text:0000D230 ; db 35h
.text:0000D230 ; db 36h
0000D210 0000D210: sub_D2F0(char *) (Synchronized with Hex View-1)
Debug application setup: gdb
NOTE: all paths must be valid on the remote computer
Application libiabl0_task.so
Input file libiabl0_task.so
Parameters
Hostname
Port 23946
Save network settings as default
The file can't be loaded by the debugger plugin. Please verify that the parameters are valid.
OK
Cancel
Help
ibly undefined


Choose process to attach to
ID
Name
148 [32] /system/bin/logd
149 [32] /system/bin/lmkd
150 [32] /system/bin/servicemanager
151 [32] /system/bin/hwservicemanager
152 [32] /system/bin/sh
15206 [32] com.google.android.gms.unstable
153 [32] /vendor/bin/qemu-props
1539 [32] com.google.android.gms
154 [32] /system/bin/vold --blkid_context=u:r:blkid:s0 --blkid_untrusted_context=...
15466 [32] com.google.process.gapps
15838 [32] com.pore.lab10_task
15915 [32] -/system/bin/sh
15917 [32] /system/bin/sh
169 [32] /vendor/bin/hw/android.hardware.keymaster@4.1-service
1761 [32] com.android.permissioncontroller
184 [32] /system/bin/hw/android.system.suspend@1.0-service
185 [32] /vendor/bin/hw/android.hardware.atrace@1.0-service
250 [32] /vendor/bin/createns router
255 [32] /system/bin/tombstoned
260 [32] /apex/com.android.os.statsd/bin/statsd
261 [32] /system/bin/netd
262 [32] zygote
263 [32] /system/bin/hw/android.hidl.allocator@1.0-service
264 [32] /vendor/bin/hw/android.hardware.audio.service.ranchu
265 [32] /vendor/bin/hw/android.hardware.authsecret@1.0-service
266 [32] /vendor/bin/hw/android.hardware.bluetooth@1.1-service.sim
267 [32] /vendor/bin/hw/android.hardware.camera.provider@2.4-service
268 [32] /vendor/bin/hw/android.hardware.camera.provider@2.6-service-google
269 [32] /vendor/bin/hw/android.hardware.cas@1.2-service
270 [32] /vendor/bin/hw/android.hardware.contexthub@1.1-service.mock
271 [32] /vendor/bin/hw/android.hardware.drm@1.0-service
272 [32] /vendor/bin/hw/android.hardware.drm@1.3-service.clearkey
273 [32] /vendor/bin/hw/android.hardware.drm@1.3-service.widevine
274 [32] /vendor/bin/hw/android.hardware.gatekeeper@1.0-service.software
275 [32] /vendor/bin/hw/android.hardware.graphics.allocator@3.0-service
276 [32] /vendor/bin/hw/android.hardware.graphics.composer@2.3-service
277 [32] /vendor/bin/hw/android.hardware.health@2.1-service
278 [32] /vendor/bin/hw/android.hardware.neuralnetworks@1.3-service-sample-all
279 [32] /vendor/bin/hw/android.hardware.neuralnetworks@1.3-service-sample-fl...
280 [32] /vendor/bin/hw/android.hardware.neuralnetworks@1.3-service-sample-fl...
281 [32] /vendor/bin/hw/android.hardware.neuralnetworks@1.3-service-sample-...
282 [32] /vendor/bin/hw/android.hardware.neuralnetworks@1.3-service-sample-q...
283 [32] /vendor/bin/hw/android.hardware.power.stats@1.0-service.mock
284 [32] /vendor/bin/hw/android.hardware.sensors@2.1-service.multihal
285 [32] /vendor/bin/hw/android.hardware.thermal@2.0-service.mock
286 [32] /vendor/bin/hw/android.hardware.usb@1.0-service
287 [32] /vendor/bin/hw/android.hardware.wifi@1.0-service
288 [32] /vendor/bin/hw/android.hardware.identity-service.example
289 [32] /vendor/bin/hw/android.hardware.lights-service.example