

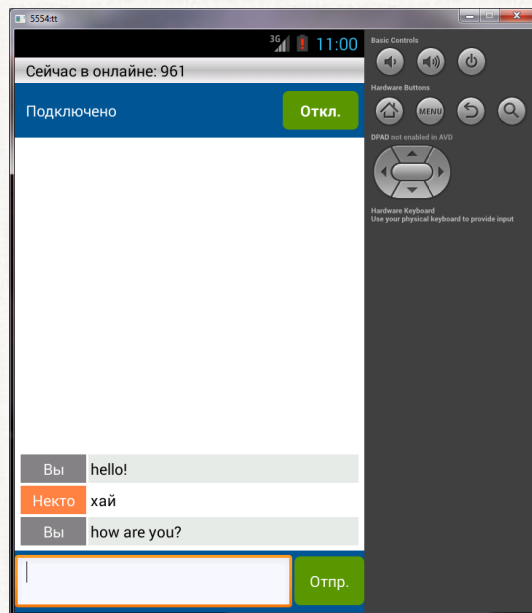
Динамический анализ и обратная отладка мобильных приложений

Н.И. Фурсова
П.М. Довгалюк
И.А. Васильев
М.А. Климушенкова
В.А. Макаров



Постановка задачи

- ❖ Приложения, работающие в реальном времени
- ❖ Недетерминированные приложения



Подходы к обратной отладке

- ◆ Детерминированное воспроизведение
- ◆ Трассировка

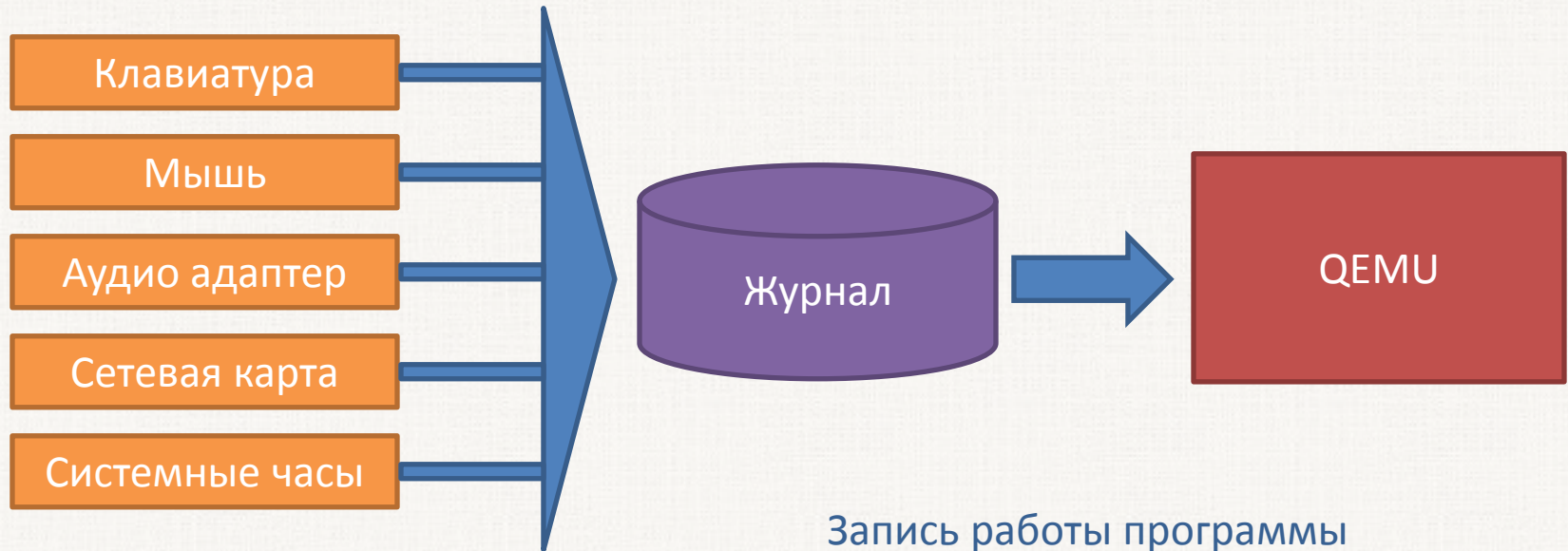
UndoDBG

- ◆ Двухнаправленный отладчик
- ◆ Поддержка нативных приложений под Android

Ограничения:

- ◆ Работает только с отдельными приложениями
- ◆ Работает только под ОС Linux

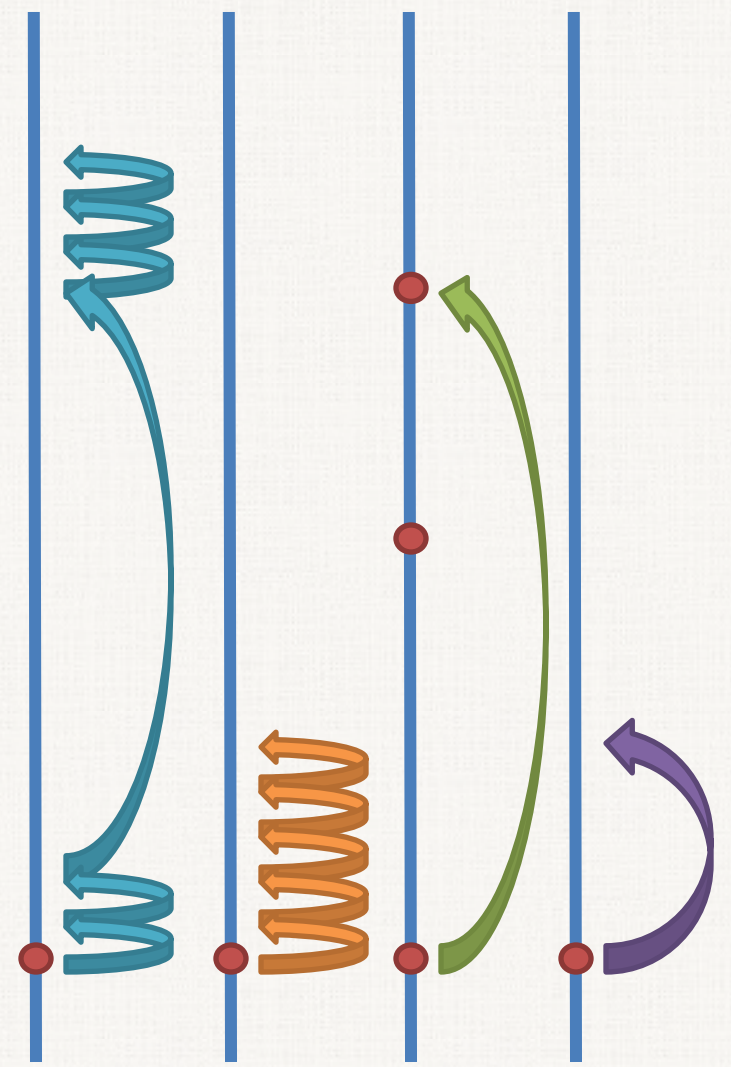
ДВ в QEMU



Обратная отладка с помощью gdb

- ◆ **reverse-stepi**
- ◆ **reverse-nexti**
- ◆ **reverse-continue**
- ◆ **reverse-finish**

```
func3 ()  
{  
    ...  
    ...  
    ...  
}  
  
func2 ()  
{  
    ...  
    ...  
}  
  
func1 ()  
{  
    ...  
    ...  
    func2 ();  
    func3 ();  
    ...  
}
```



Трассировка

136A0D88

Регистры

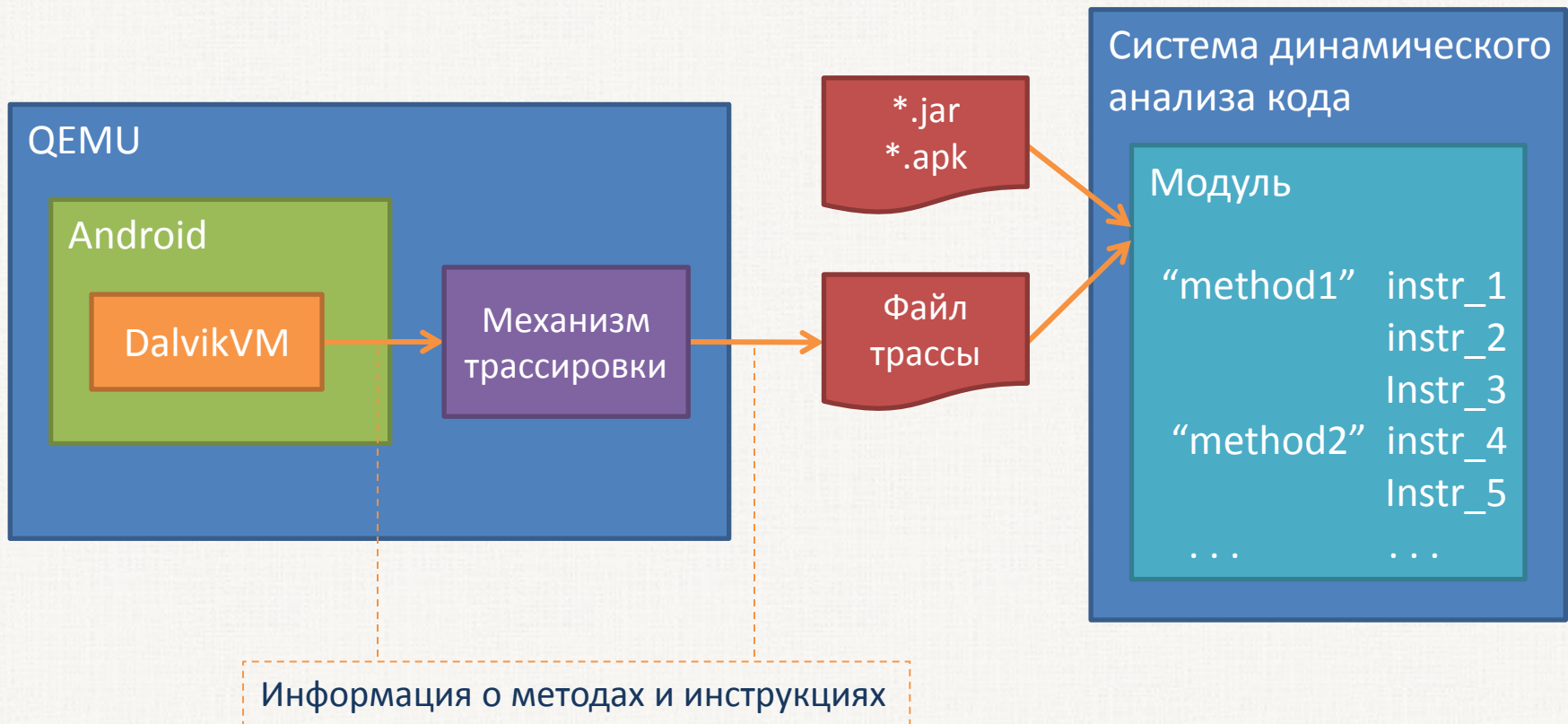
GPR SR CP15 EXT ???

pc = c0022e94 r0 = 001214e0 r1 = 00000007 r2 = 00000002 r3 = 0000000c r4 = 40512818 r5 = 0000abe0
 r6 = 001214e0 r7 = 00000014 r8 = 20000010 r9 = 4214cb50 r10 = 4214cb38 r11 = 00000000 r12 = 00093177
 r13 = beff1f98 r14 = ad34d47b r13_svc = e7daffb0 r14_svc = afd0b5ac r13_abt = c02d0b0c r14_abt = c0022b20 r13_und = c02d0b18
 r14_und = 00000000 r13_irq = c02d0b00 r14_irq = c0022b80 cpsr = 20000013 spsr_svc = 20000010 spsr_abt = 40000193 spsr_und = 00000000
 spsr_irq = 60000193 cpacr = 00000000 nsacr = 00000000 hcptr = 00000000 fcseidr = 00000000 contextidr = 00000000 tpidrprw = 00000000
 fpexc = 00000000 tid = 0000000000000127 pid = 0000000000000127 zid = 0000000000000000

АА

Адрес	Модуль	ИСК	KCK	Опкод	Инструкция, Ссылки, Комментарий
136A0D87		C0022E90	0xC0022E90	13F021E3	MSR CPSR c, 0x00000013
136A0D88		C0022E94	0xC0022E94	AD96A0E1	MOV R9, R13_SVC, LSR #13
136A0D89		C0022E98	0xC0022E98	8996A0E1	MOV R9, R9, LSL #13
136A0D8A		C0022E9C	0xC0022E9C	80808FE2	ADD R8, PC, 0x00000080
136A0D8B		C0022EA0	0xC0022EA0	00C099E5	LDR R12, [R9] ; [E7DAE000]
136A0D8C		C0022EA4	0xC0022EA4	30002DE9	STMDB R13_SVC!, {R4, R5}
136A0D8D		C0022EA8	0xC0022EA8	010C1CE3	TST R12, 0x00000100
136A0D8E		C0022EAC	0xC0022EAC	0800001A	BNE 0xC0022ED4
136A0D8F		C0022EB0	0xC0022EB0	5B0F57E3	CMP R7, 0x0000016C
136A0D90		C0022EB4	0xC0022EB4	47EF4FE2	SUB R14_SVC, PC, 0x0000011C
136A0D91		C0022EB8	0xC0022EB8	07F19837	LDRCC PC, [R8, R7, LSL #2] ; [C0022F74]
136A0D92		C00444F0	0xC00444F0	0DC0A0E1	MOV R12, R13_SVC
136A0D93		C00444F4	0xC00444F4	00D82DE9	STMDB R13_SVC!, {R11, R12, R14_SVC, PC}
136A0D94		C00444F8	0xC00444F8	04B04CE2	SUB R11, R12, 0x00000004
136A0D95		C00444FC	0xC00444FC	0D20A0E1	MOV R2, R13_SVC
136A0D96		C0044500	0xC0044500	7F3DC2E3	BIC R3, R2, 0x00001FC0
136A0D97		C0044504	0xC0044504	3F30C3E3	BIC R3, R3, 0x0000003F
136A0D98		C0044508	0xC0044508	0C3093E5	LDR R3, [R3, 0x0000000C] ; [E7DAE00C]
136A0D99		C004450C	0xC004450C	0C3293E5	LDR R3, [R3, 0x0000020C] ; [E7D7DE0C]
136A0D9A		C0044510	0xC0044510	280293E5	LDR R0, [R3, 0x00000228] ; [E7D7DE28]
136A0D9B		C0044514	0xC0044514	7E1D00EB	BL 0xC004BB14 ; -> C004BB14
136A0D9C		C004BB14	0xC004BB14	0DC0A0E1	MOV R12, R13_SVC
136A0D9D		C004BB18	0xC004BB18	00D82DE9	STMDB R13_SVC!, {R11, R12, R14_SVC, PC}
136A0D9E		C004BB1C	0xC004BB1C	04B04CE2	SUB R11, R12, 0x00000004
136A0D9F		C004BB20	0xC004BB20	0D20A0E1	MOV R2, R13_SVC
136A0DA0		C004BB24	0xC004BB24	7F3DC2E3	BIC R3, R2, 0x00001FC0
136A0DA1		C004BB28	0xC004BB28	3F30C3E3	BIC R3, R3, 0x0000003F
136A0DA2		C004BB2C	0xC004BB2C	0C3093E5	LDR R3, [R3, 0x0000000C] ; [E7DAE00C]
136A0DA3		C004BB30	0xC004BB30	000050E3	CMP R0, 0x00000000
136A0DA4		C004BB34	0xC004BB34	183393E5	LDR R3, [R3, 0x00000318] ; [E7D7DF18]
136A0DA5		C004BB38	0xC004BB38	103093E5	LDR R3, [R3, 0x00000010] ; [C02B64C0]
136A0DA6		C004BB3C	0xC004BB3C	0800000A	BEQ 0xC004BB64
136A0DA7		C004BB40	0xC004BB40	182093E5	LDR R2, [R3, 0x00000018] ; [C02B63B0]
136A0DA8		C004BB44	0xC004BB44	041090E5	LDR R1, [R0, 0x00000004] ; [EAB31124]
136A0DA9		C004BB48	0xC004BB48	010052E1	CMP R2, R1
136A0DAA		C004BB4C	0xC004BB4C	0400008A	BHI 0xC004BB64

Трассировка Java-приложений



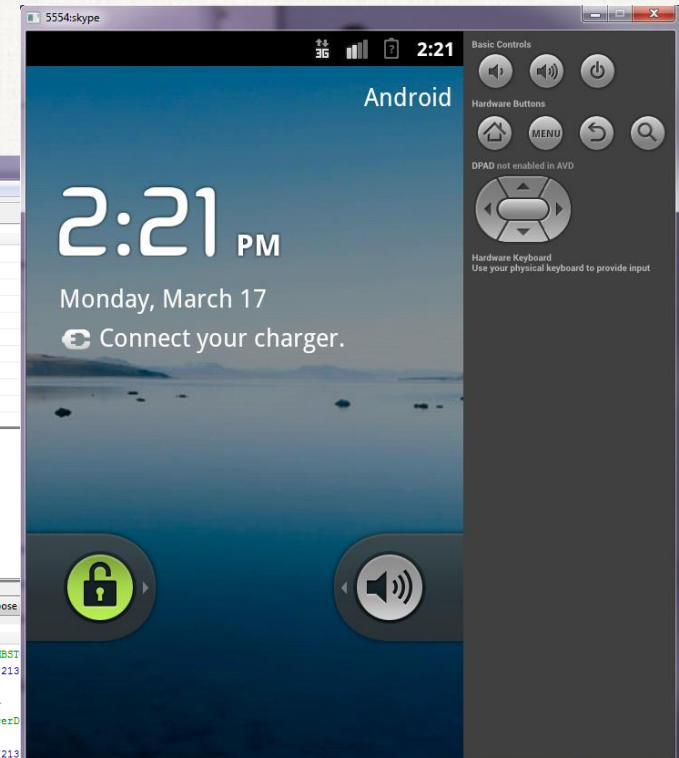
Dalvik Debug Monitor Server

The screenshot shows the Dalvik Debug Monitor (DDMS) interface. The top part displays a list of processes running on the emulator. Below that, there is a table of threads with columns for ID, Tid, Status, utime, stime, and Name. The bottom part shows a log of messages with columns for L, Time, PID, TID, Application, Tag, and Text.

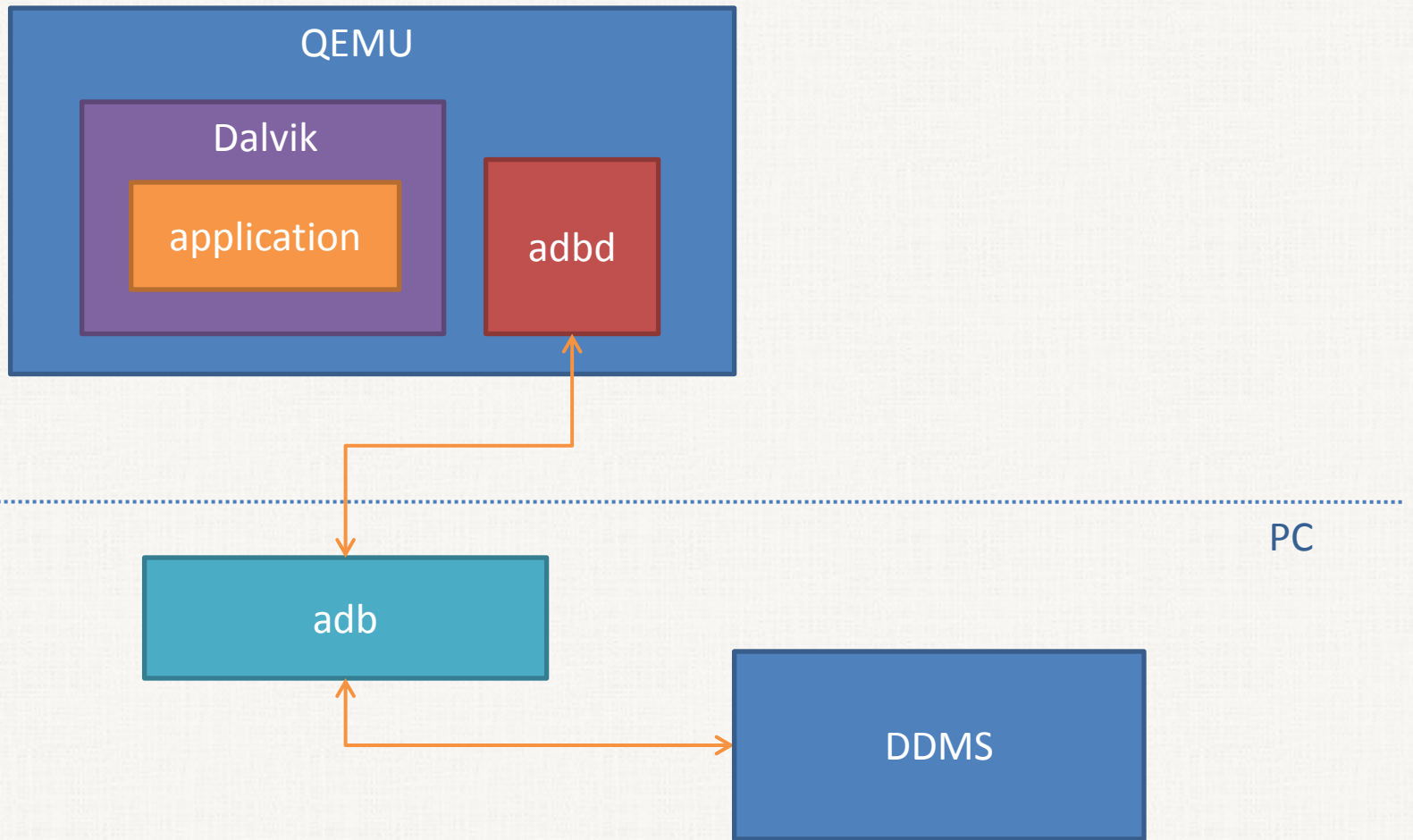
Name	Online	skype [2.3.3, d...]
emulator-5554	Online	skype [2.3.3, d...]
system_process	74	8600
jp.co.omronsoft.openwmn	123	8601 / 8700
com.android.phone	131	8602
com.android.systemui	134	8603
com.android.launcher	139	8604
com.android.settings	174	8605
android.process.acore	194	8606
android.process.media	206	8607
com.android.mms	221	8608
com.android.deskclock	242	8609

ID	Tid	Status	utime	stime	Name
1	123	Native	83	20	main
*2	125	VmWait	4	13	HeapWorker
*3	128	VmWait	33	5	GC
*4	142	VmWait	0	0	Signal Catcher
*5	143	Runnable	0	5	JDWP
*6	144	VmWait	4	4	Compiler
7	148	Native	0	0	Binder Thread #1
8	150	Native	0	0	Binder Thread #2

L...	Time	PID	TID	Application	Tag	Text
I	03-17 14:20:5...	74	205	system_process	BootReceiver	Copying /data/tombstones/tombstone_00 to DropBox (SYSTEM_TOMBST
D	03-17 14:20:5...	32	32	system_process	dalvikvm	GC_EXPLICIT freed <1K, 53% free 2538K/5379K, external 1625K/213
I	03-17 14:20:5...	194	194	android.process...	ActivityTh...	Pub call_log: com.android.providers.contacts.CallLogProvider
I	03-17 14:20:5...	194	194	android.process...	ActivityTh...	Pub user_dictionary: com.android.providers.userdictionary.UserD
D	03-17 14:20:5...	32	32	system_process	dalvikvm	GC_EXPLICIT freed <1K, 53% free 2538K/5379K, external 1625K/213
D	03-17 14:20:5...	74	205	system_process	dalvikvm	GC_FOR_MALLOC freed 904K, 53% free 4270K/8967K, external 4373K/5461
D	03-17 14:20:5...	221	224	com.android.mms	dalvikvm	GC_CONCURRENT freed 410K, 54% free 2635K/5639K, external 1625K/2137
I	03-17 14:20:5...	221	221	com.android.mms	ActivityTh...	Pub com.android.mms.SuggestionsProvider: com.android.mms.Suggestion
D	03-17 14:20:5...	74	102	system_process	dalvikvm	GC_EXPLICIT freed 398K, 54% free 4143K/8967K, external 4373K/5461K,
I	03-17 14:20:5...	74	81	system_process	ActivityMa...	Start proc com.android.deskclock for broadcast com.android.deskclock



Симулятор + DDMS



ДВ + DDMS

- ❖ Запись: сохраняется единственный сценарий работы с отладчиком
- ❖ Воспроизведение: отладчик не может получить ответ от системы

Идея

- ◆ Детерминированное воспроизведение
- ◆ DDMS
- ◆ Модуль сбора данных
- ◆ Среда динамического анализа кода



Аналоги

◆ Crosscut

- Выделение работы приложений при воспроизведении

◆ DroidScope

- Интроспекция Java-приложений для платформы Android

Результаты

- ❖ Реализовано детерминированное воспроизведение работы мобильных приложений
- ❖ Обратная отладка нативных приложений
- ❖ Трассировка нативных приложений
- ❖ Предложен метод трассировки и отладки java-приложений

Дальнейшие планы

- ❖ Трассировка java-приложений
- ❖ Отладка java-приложений
- ❖ Исследование интроспекции и реализация без внедрения модулей в DalvikVM