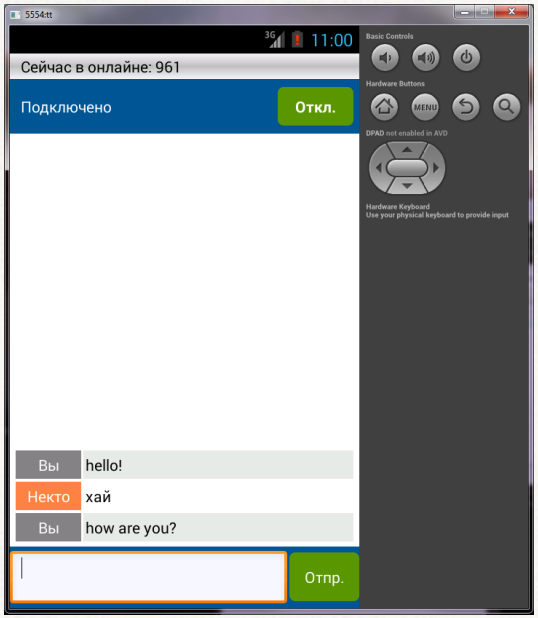
Новгородский Государственный Университет им. Ярослава Мудрого

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

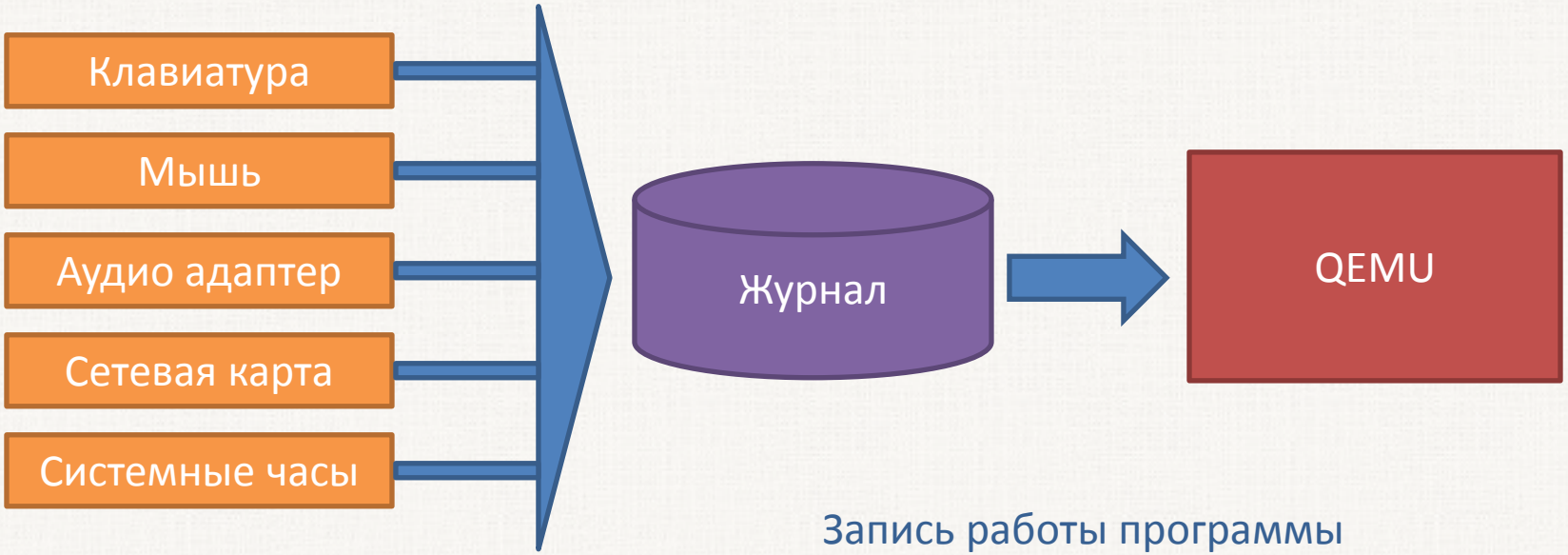
UndoDBG

- Двунаправленный отладчик
- Поддержка нативных приложений под Android

Ограничения:

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

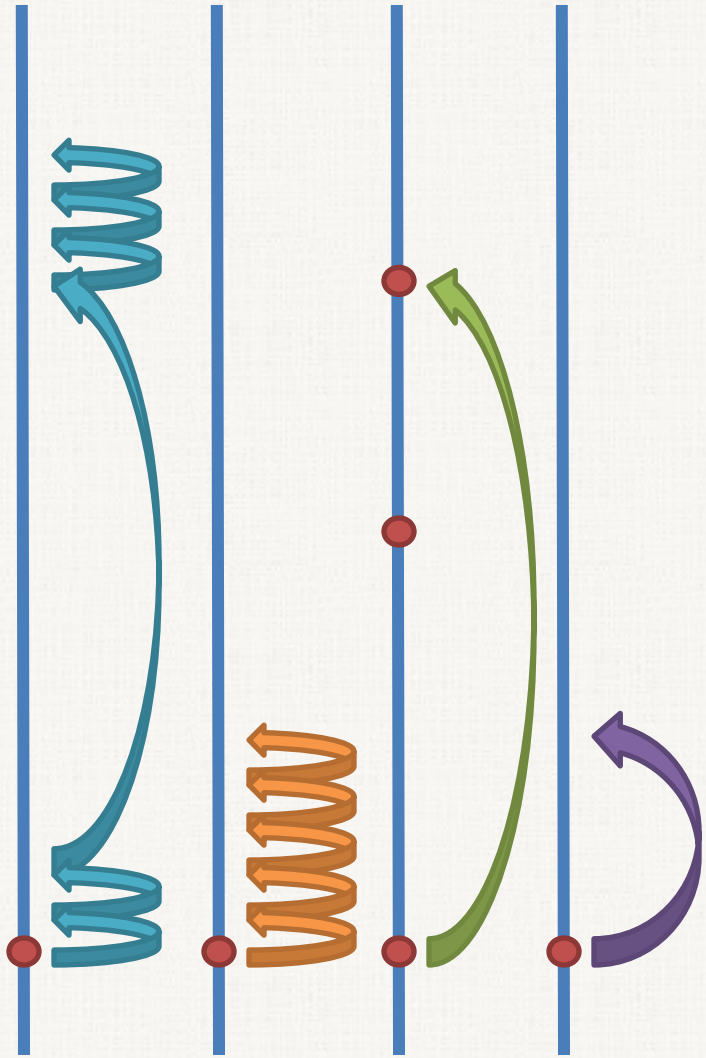
ДВ в QEMU


Клавиатура
Мышь
Аудио адаптер
Сетевая карта
Системные часы
Журнал
QEMU
Запись работы программы
Воспроизведение работы программы
Журнал
QEMU
Инструменты анализа

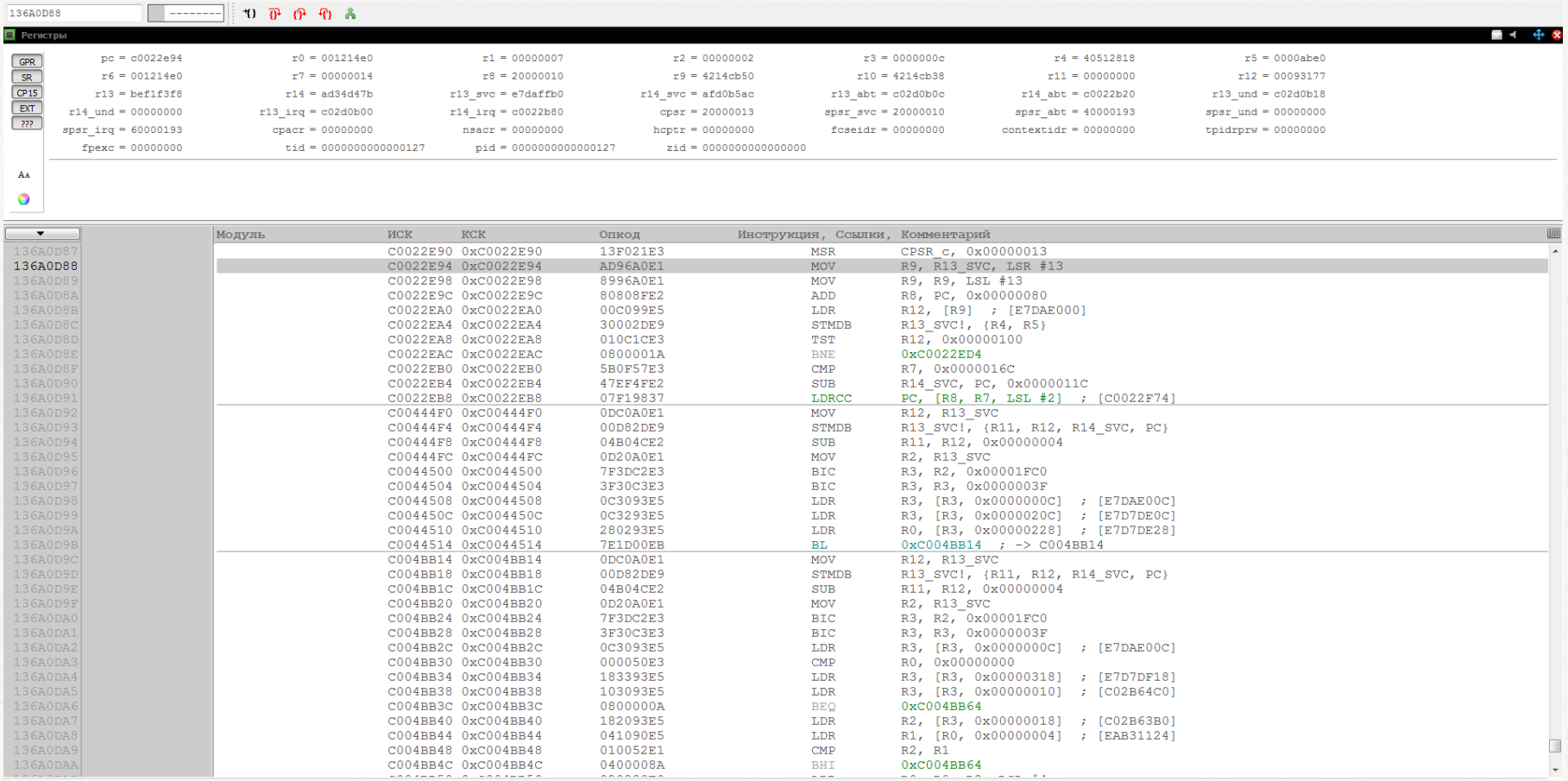
Обратная отладка с помощью gdb

- reverse-stepi
- reverse-nexti
- reverse-continue
- reverse-finish

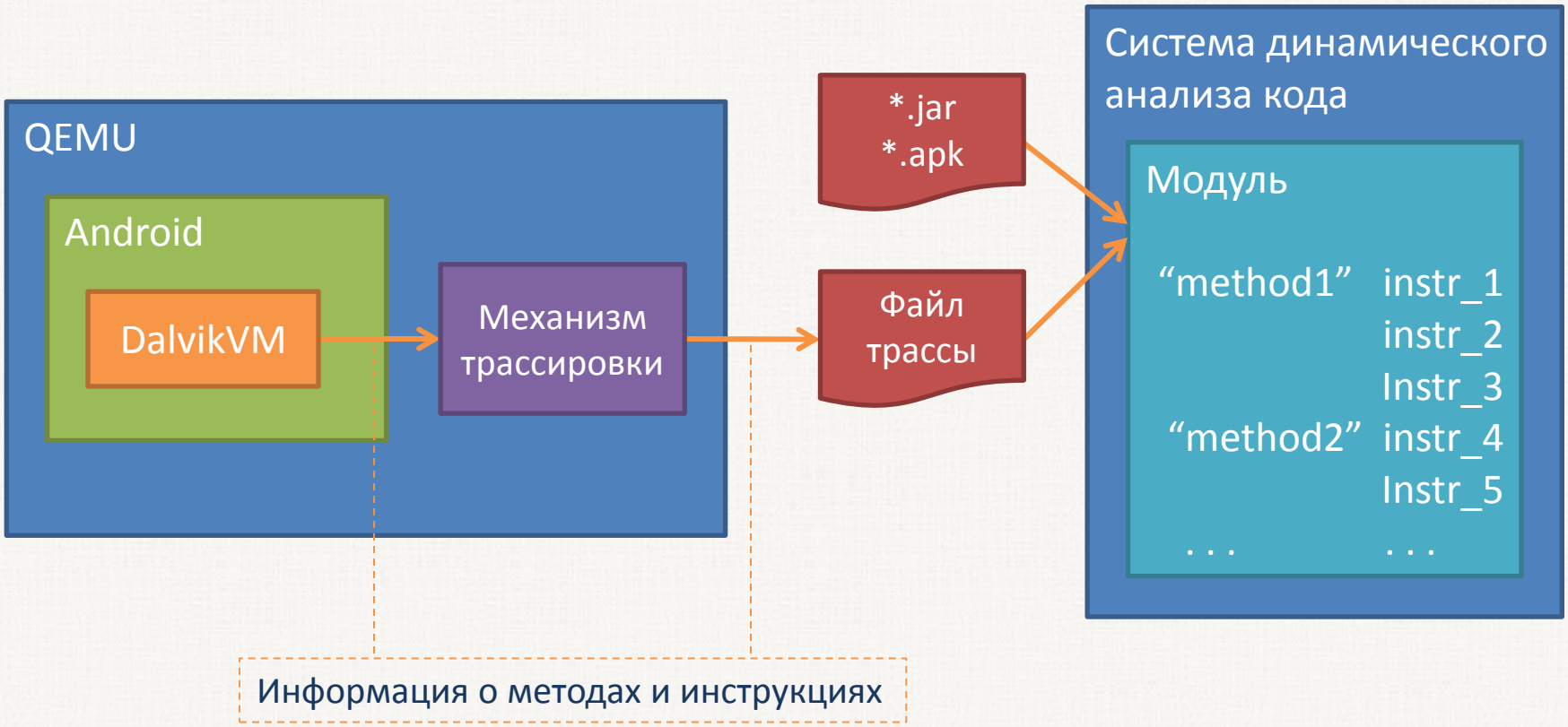
```
func3()
{
    ...
    ...
    ...
}

func2()
{
    ...
    ...
}

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



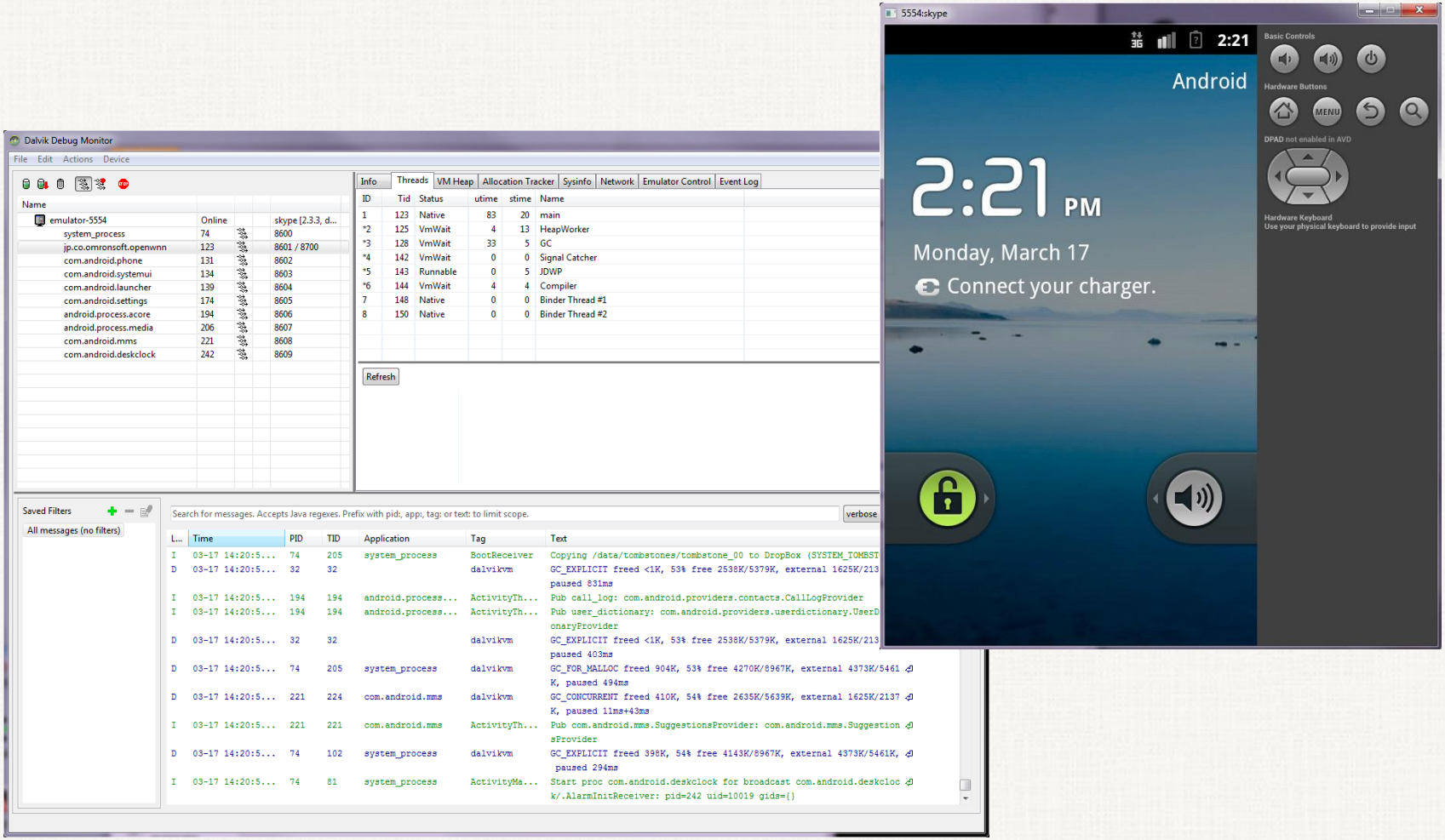
Трассировка



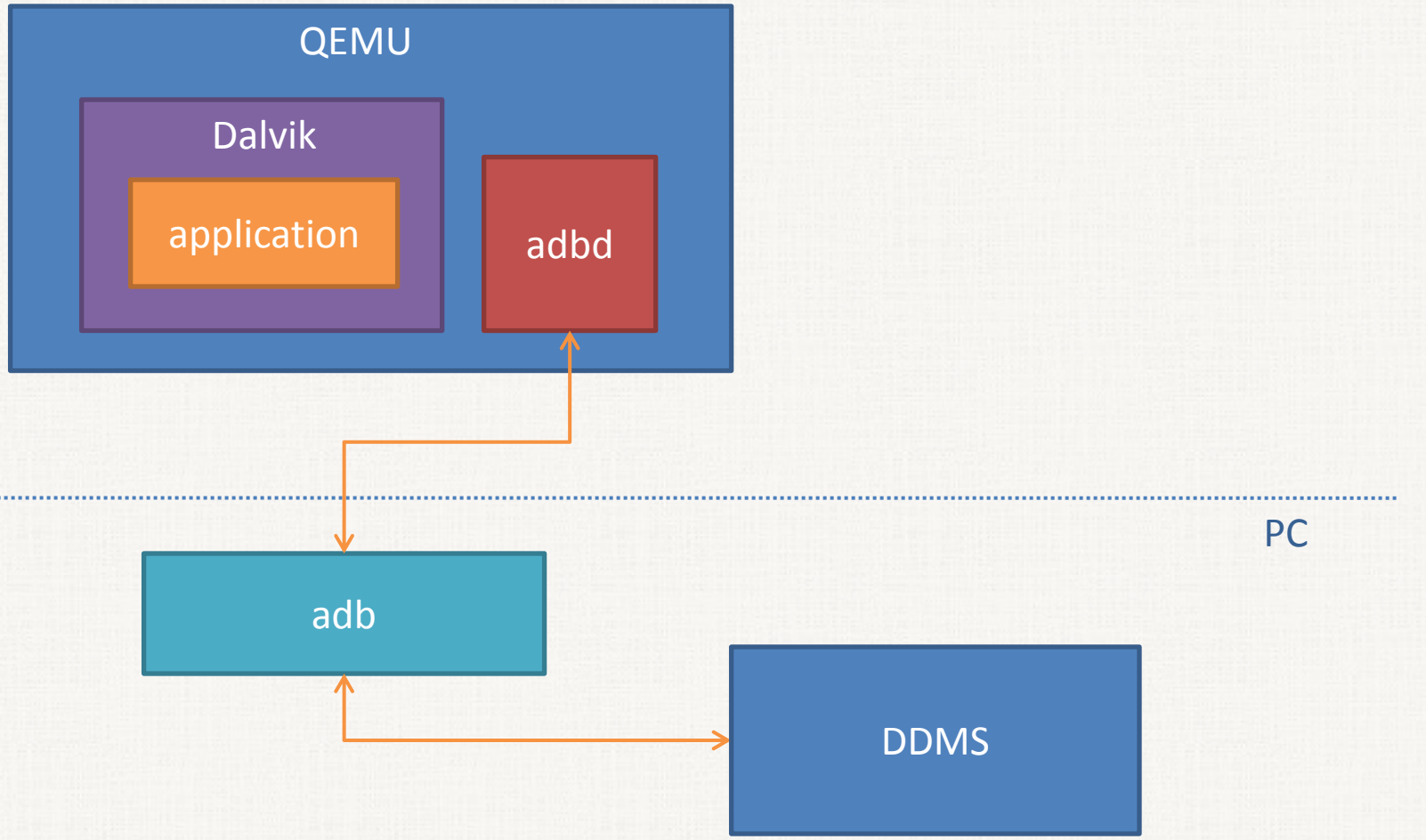
Трассировка Java-приложений



Dalvik Debug Monitor Server



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