Снятие образа Android с помощью агента

Автор: Лысенко Юлия
Научный руководитель: ст. преп. Губанов Ю.А.
Рецензент: ст. преп. Луцив Д.В.

Санкт-Петербургский Государственный Университет

14 июня 2018 г.

Введение

Обзор:

- Цифровая криминалистика занимается сбором доказательств с мобильных устройств
- Android — составляет 74% рынка мобильных устройств
- Извлечение данных без прав суперпользователя
- Метод агентов — на устройство устанавливается приложение для сбора данных:
  - Не зависит от модели телефона
  - Не требует прав суперпользователя
  - Доступна большая часть данных

Цели и задачи

Цель — разработка программного средства для извлечения данных с мобильных устройств без прав суперпользователя с операционной системой Android 7.0 и выше.
Интересующие данные: список контактов, звонков, SMS-сообщений, список установленных приложений, мультимедиа и информация из календаря.
Поставленные задачи:

- Разработать приложение-агент для сбора требуемых данных на устройстве
- Разработать клиент-приложение для управления агентом
- Настроить связь между клиентом и агентом
- Провести апробацию

Android Debug Bridge

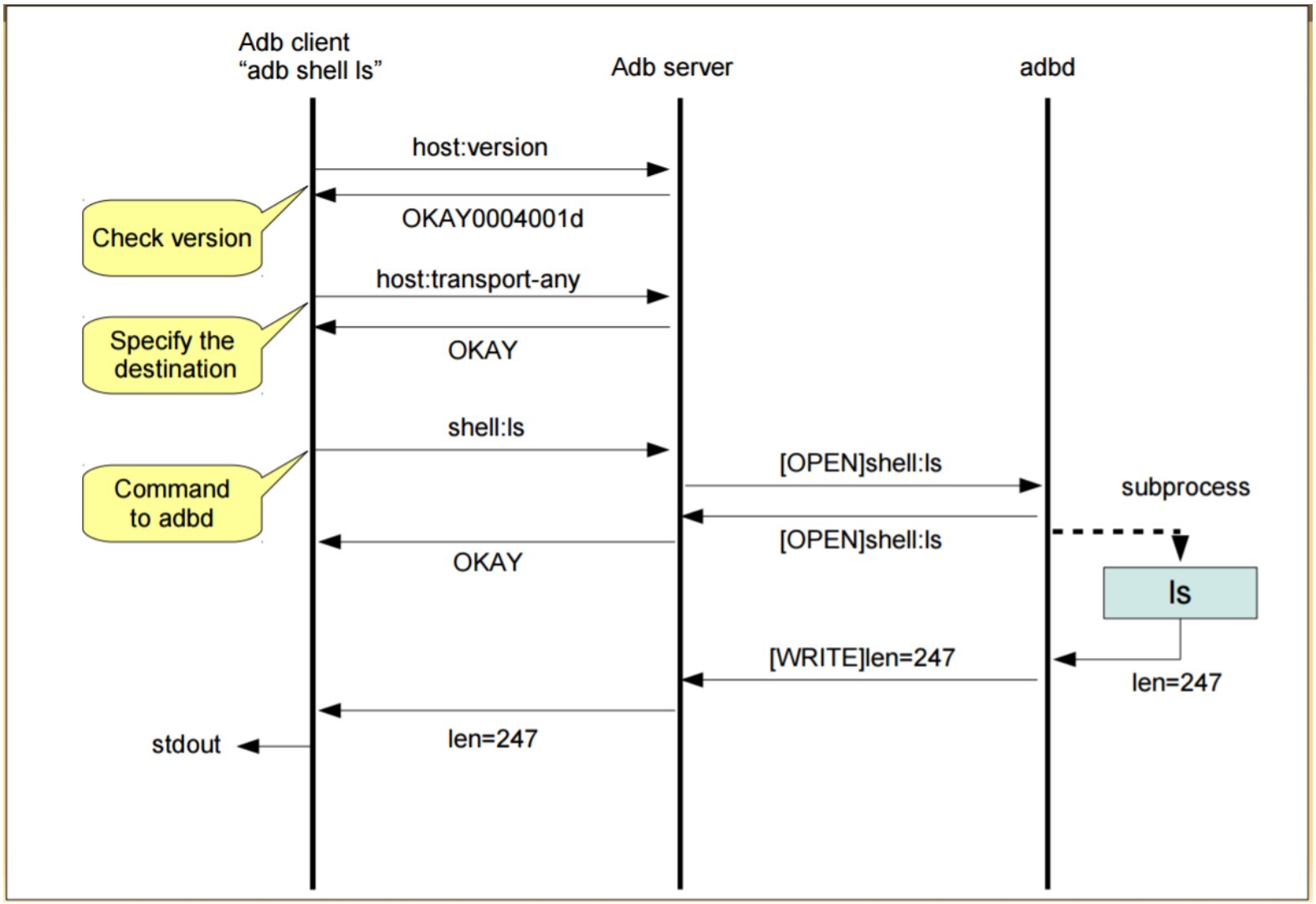
Определение

Android Debug Bridge (ADB) — это инструмент командной строки, который обеспечивает обмен данными между устройством Android и персональным компьютером.

ADB состоит из:

- Клиента — выполняет команды на ПК
- Демона (ADBD) — выполняет команды на устройстве
- Сервера — регулирует связь между клиентом и демоном. Работает как фоновый процесс на ПК

Схема работы ADB



https://www.slideshare.net/tetsu.koba/adbandroid-debug-bridge-how-it-works

ADB / работа с консолью

Недостатки работы с ADB непосредственно через консоль:

- У ADB нет доступа к нужным данным без root-доступа
- Даже при наличии агента его установка и управление будут затруднены
  - ADB не позволяет полноценно поддерживать двустороннюю связь и обрабатывать ответы от команд ADB-сервера
  - Некому принимать данные

ADB / работа с консолью

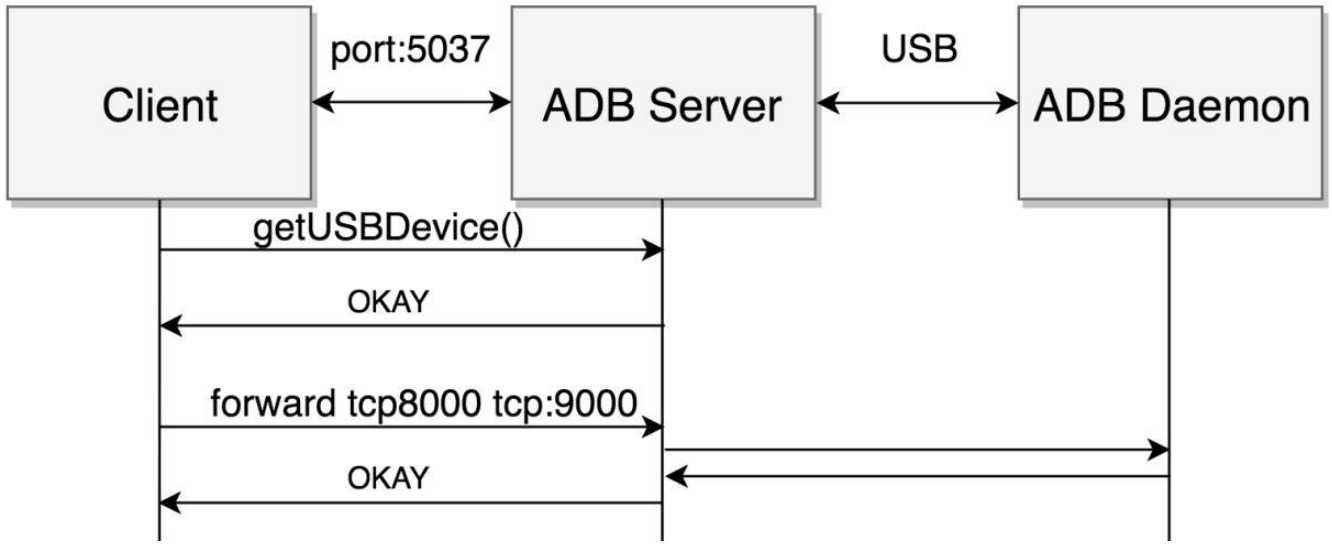
Недостатки работы с ADB непосредственно через консоль:

- У ADB нет доступа к нужным данным без root-доступа
- Даже при наличии агента его установка и управление будут затруднены
  - ADB не позволяет полноценно поддерживать двустороннюю связь и обрабатывать ответы от команд ADB-сервера
  - Некому принимать данные

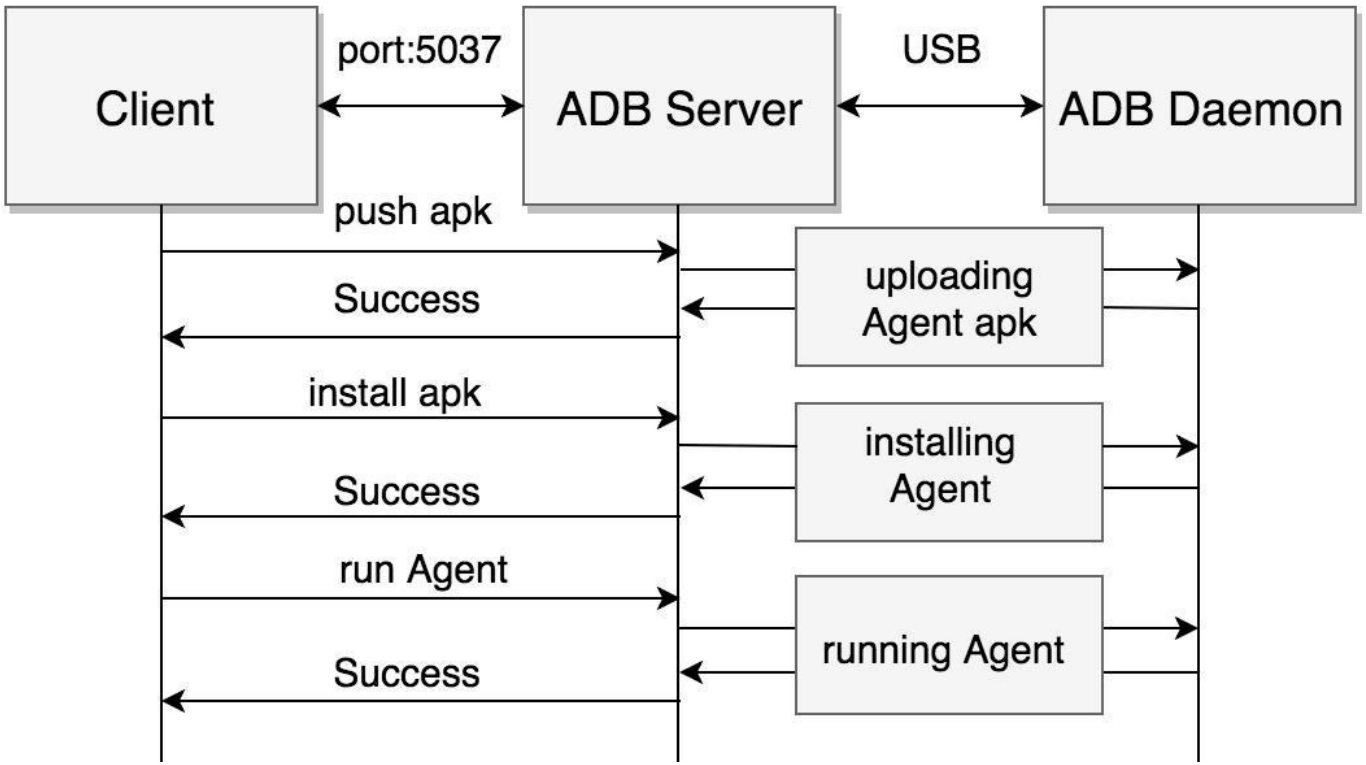
Таким образом, нам необходимы все три компоненты:

- Агент, который будет выкачивать данные
- Программа-клиент, которая будет управлять агентом
- ADB-сервер, который будет устанавливать связь между клиентом и агентом

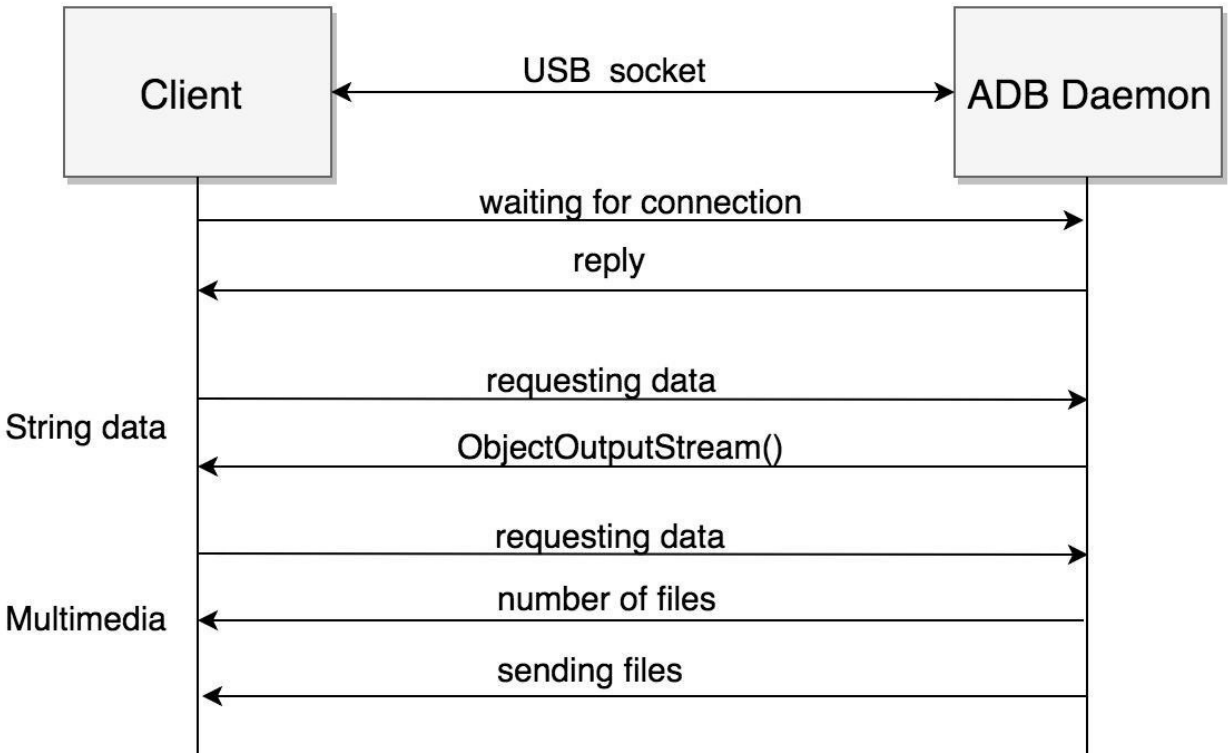
Клиент / работа с сервером / соединение



Клиент / работа с сервером / установка агента



Клиент / работа с агентом



Агент / работа с данными

- ADB позволяет устанавливать приложения с выданными разрешениями из манифеста
- Для сбора данных использовался Android API

Агент / работа с клиентом

- Ожидает запрос на сбор данных
- Обрабатывает запрос
- Собирает данные
  - Для работы с мультимедиа сохраняются списки путей к файлам
  - Остальная информация извлекается как списки строк данных
- Отправляет данные клиенту
  - Мультимедиа отправляется клиенту побитово передается клиенту
  - Остальные данные передаются через *ObjectOutputStream*()

Результаты

- Реализовано приложение-агент для сбора требуемых данных с устройства
- Реализовано клиент-приложение для управления агентом
- Реализована связь между агентом и клиентом
- Проведена апробация на физических устройствах Android 6.0 — 8.0