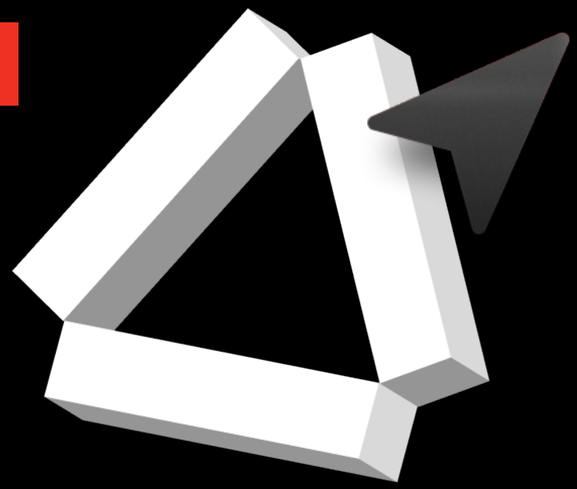
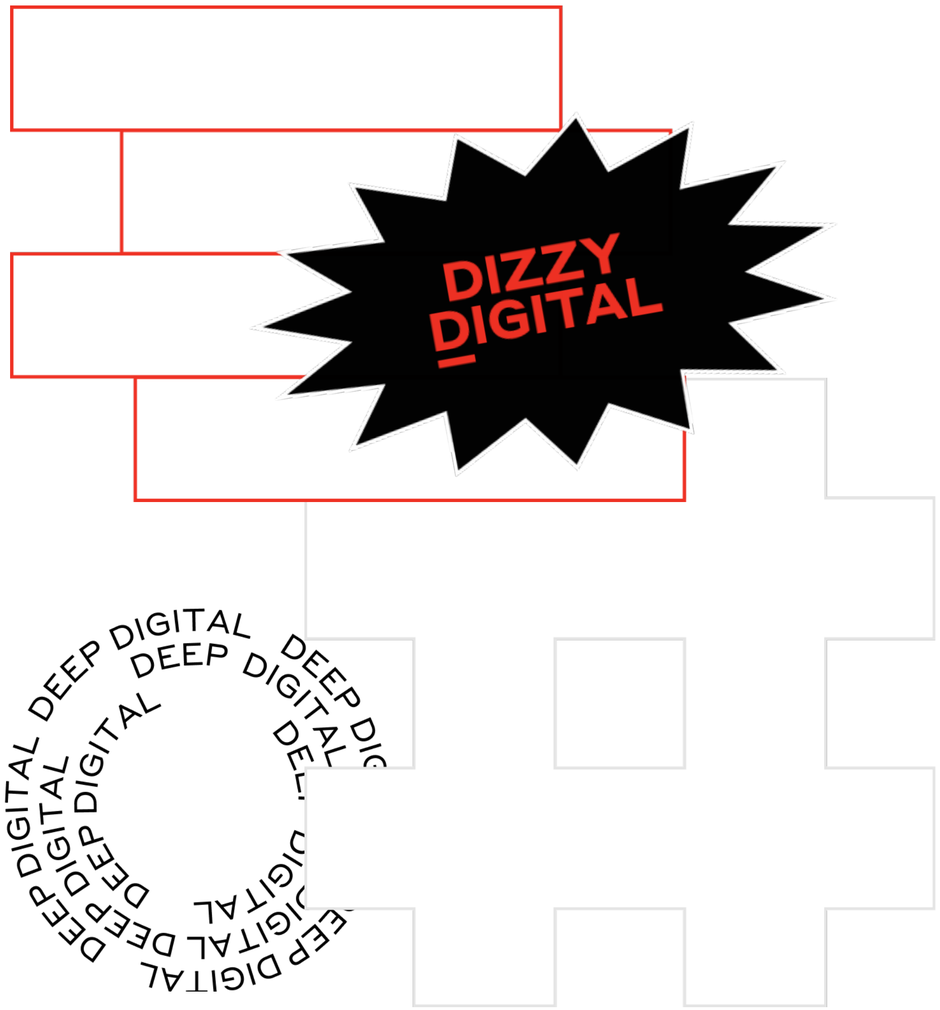
A Digital

Как приручить iPhone. Или общаемся с телефоном по проводу



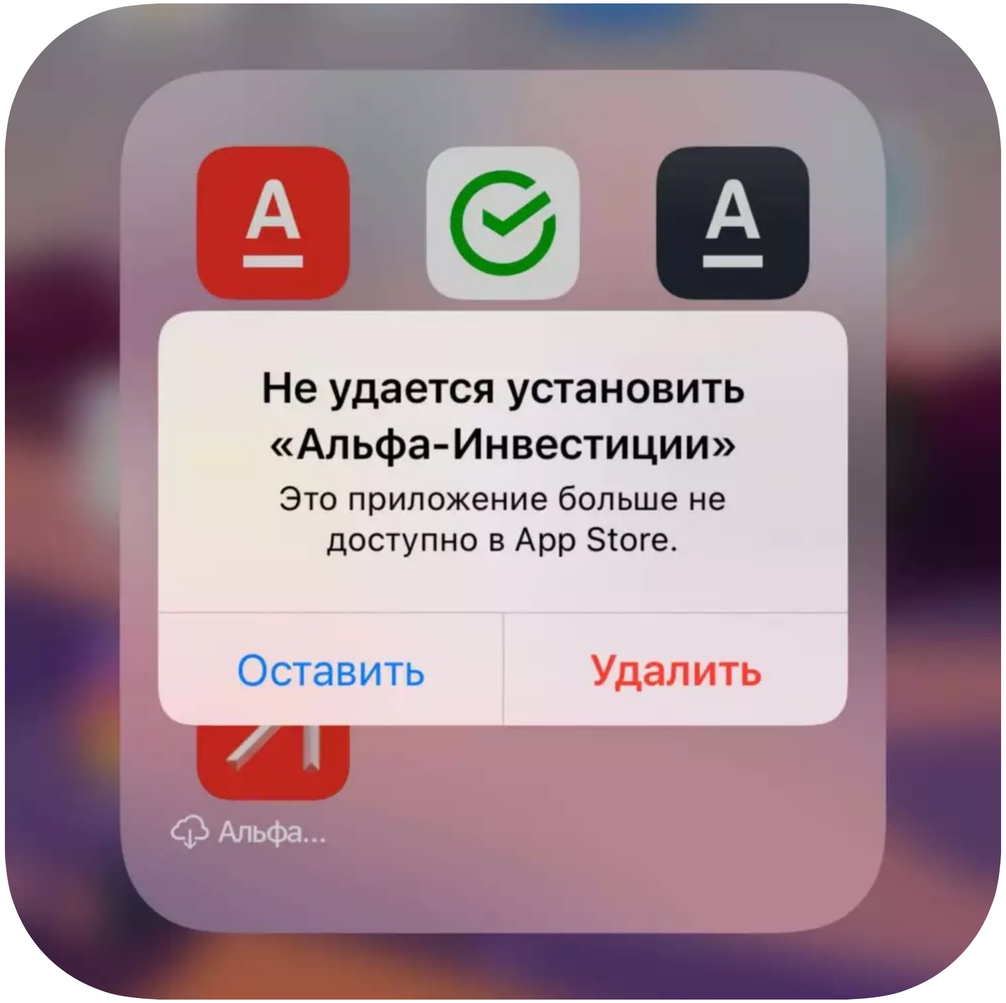
Евгений Онуфрейчик Альфа-Банк

План доклада



- Как пришла идея доклада
- Процесс взаимодействия телефона с ноутбуком
- MobileDevice framework
- Набор библиотек Libimobiledevice
- PeerTalk

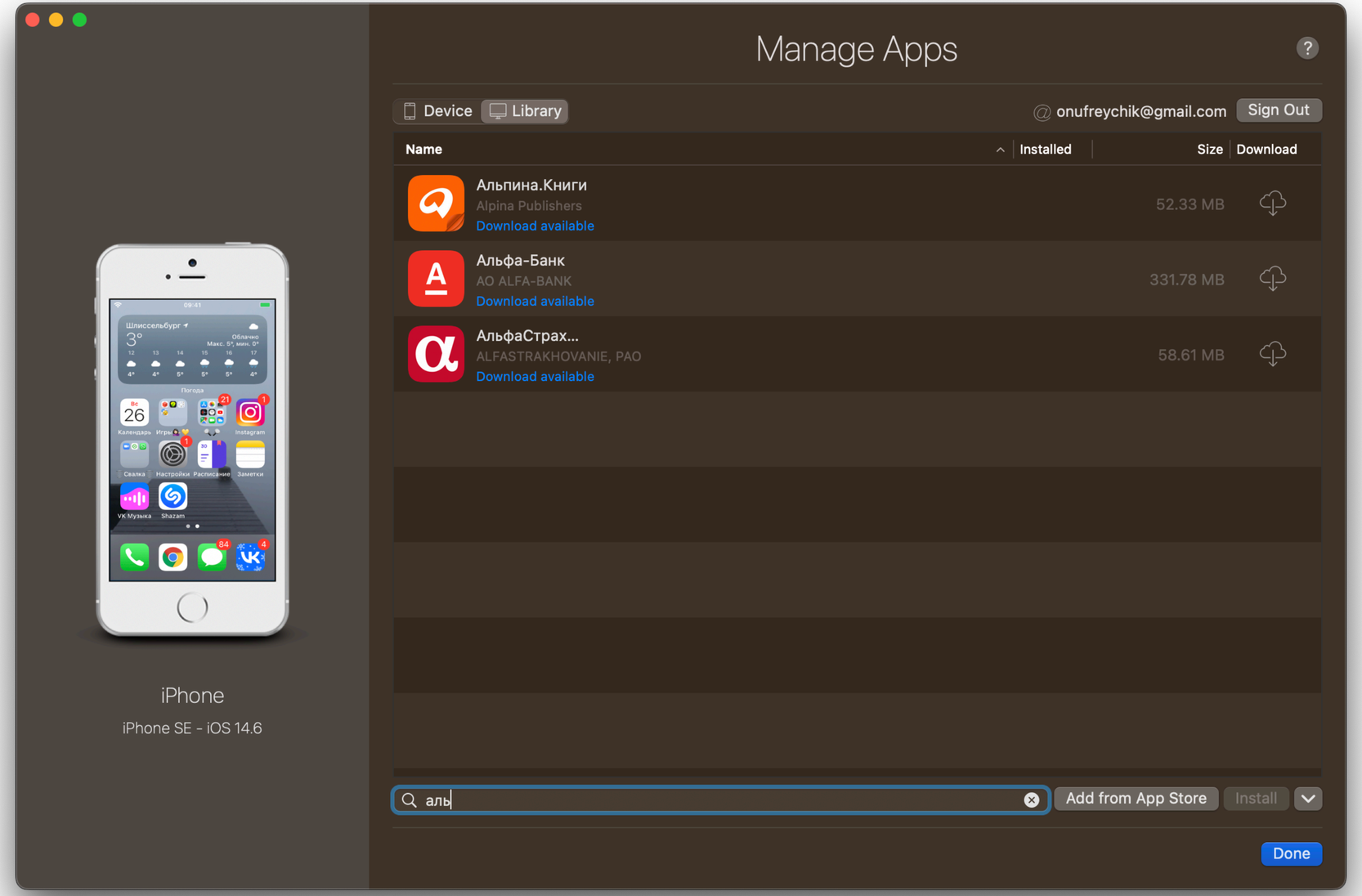
Идея доклада



Идея доклада

Схема подключения

iMazing


Manage Apps
Device
Library
onufreychik@gmail.com
Sign Out
Name
Installed
Size
Download
Альпина.Книги
Alpina Publishers
Download available
52.33 MB
Альфа-Банк
АО ALFA-BANK
Download available
331.78 MB
АльфаСтрах...
ALFASTRAKHOVANIE, PAO
Download available
58.61 MB
iPhone
iPhone SE - iOS 14.6
аль
Add from App Store
Install
Done

iMazing

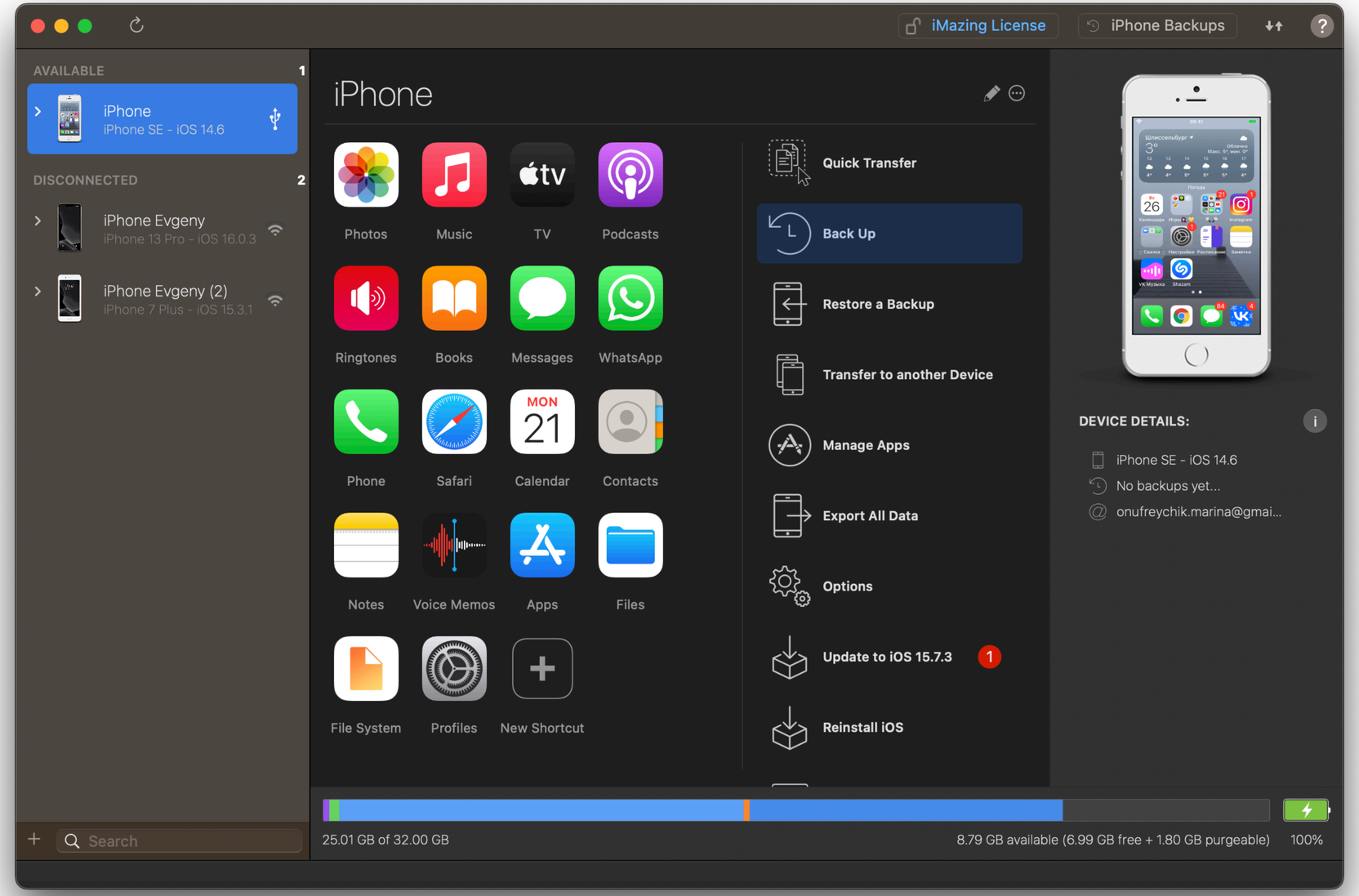
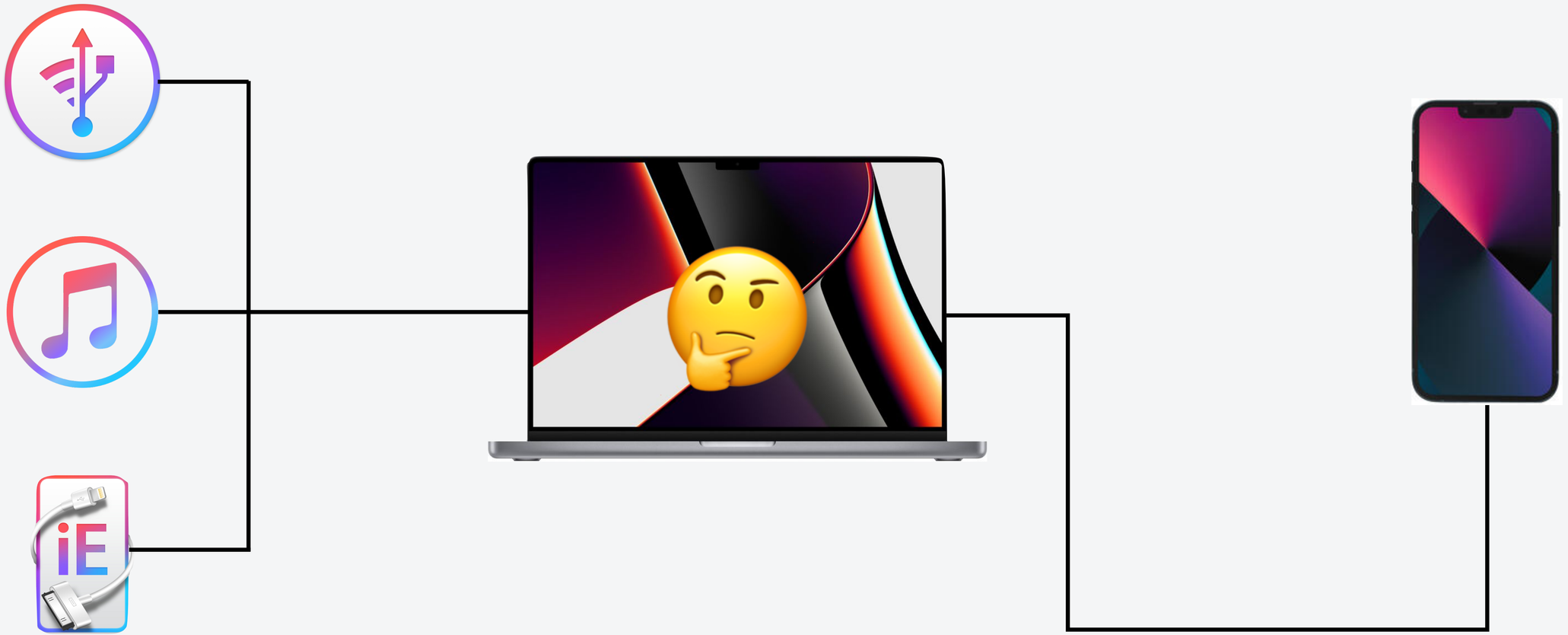

iMazing License
iPhone Backups
AVAILABLE 1
iPhone
iPhone SE - iOS 14.6
DISCONNECTED 2
iPhone Evgeny
iPhone 13 Pro - iOS 16.0.3
iPhone Evgeny (2)
iPhone 7 Plus - iOS 15.3.1
iPhone
Photos
Music
TV
Podcasts
Ringtones
Books
Messages
WhatsApp
Phone
Safari
MON
21
Calendar
Contacts
Notes
Voice Memos
Apps
Files
File System
Profiles
New Shortcut
Quick Transfer
Back Up
Restore a Backup
Transfer to another Device
Manage Apps
Export All Data
Options
Update to iOS 15.7.3
1
Reinstall iOS
DEVICE DETAILS:
iPhone SE - iOS 14.6
No backups yet...
onufreychik.marina@gmai...
Search
25.01 GB of 32.00 GB
8.79 GB available (6.99 GB free + 1.80 GB purgeable)
100%

Схема подключения



Небольшое отступление

https://github.com/majd/ipatool

usbmuxd

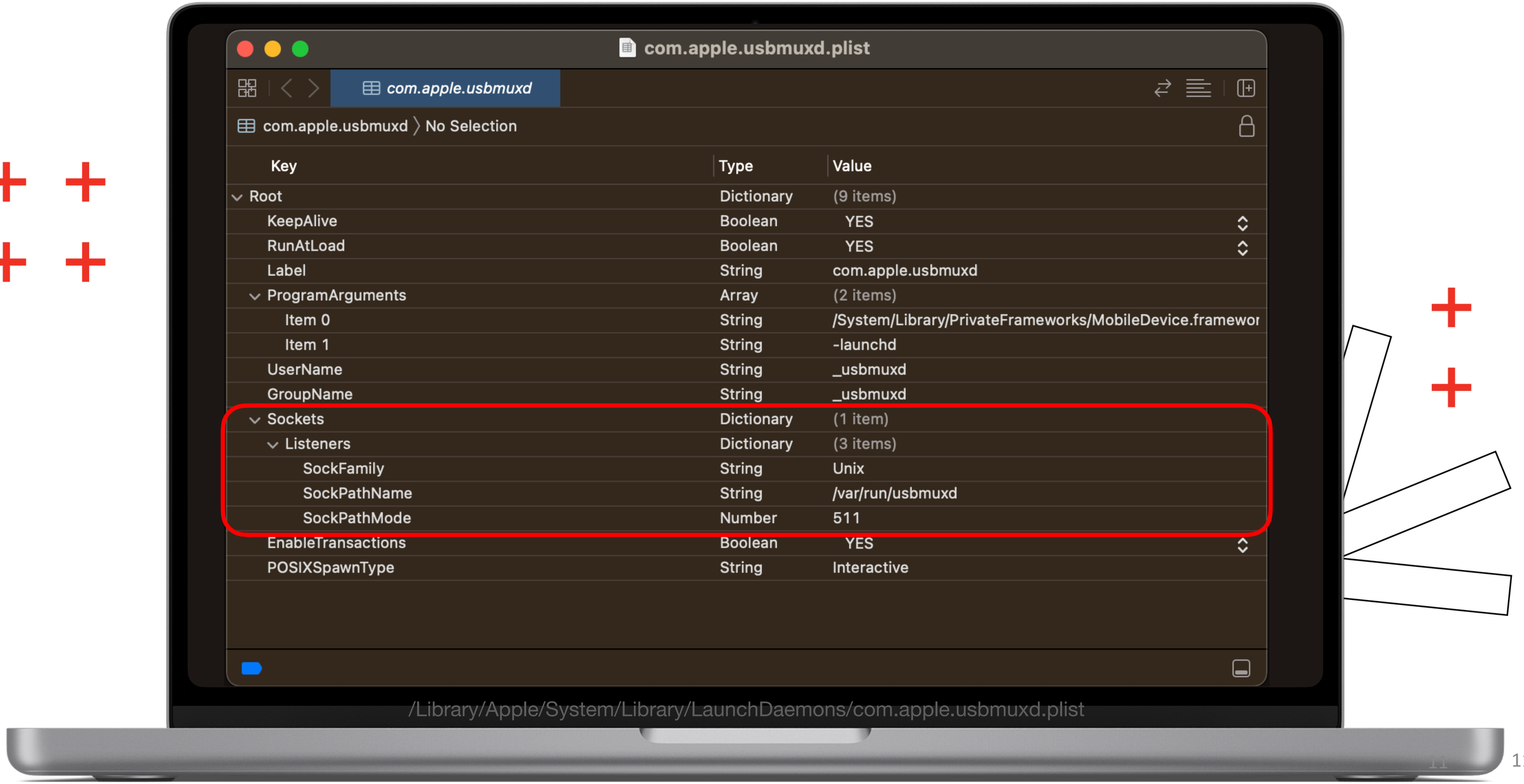
usb-multiplexer — система мультиплексирования нескольких соединений iPhone по одному USB-каналу

usbmuxd

- Поставляется Apple для работы iTunes, Xcode, etc

- В MacOS можно найти тут: /System/Library/PrivateFrameworks/MobileDevice.framework/Resources/usbmuxd

usbmuxd


com.apple.usbmuxd.plist
com.apple.usbmuxd
com.apple.usbmuxd 〉 No Selection
Key
Type
Value
Root
Dictionary
(9 items)
KeepAlive
Boolean
YES
RunAtLoad
Boolean
YES
Label
String
com.apple.usbmuxd
ProgramArguments
Array
(2 items)
Item 0
String
/System/Library/PrivateFrameworks/MobileDevice.framewor
Item 1
String
-launchd
UserName
String
_usbmuxd
GroupName
String
_usbmuxd
Sockets
Dictionary
(1 item)
Listeners
Dictionary
(3 items)
SockFamily
String
Unix
SockPathName
String
/var/run/usbmuxd
SockPathMode
Number
511
EnableTransactions
Boolean
YES
POSIXSpawnType
String
Interactive
/Library/Apple/System/Library/LaunchDaemons/com.apple.usbmuxd.plist

UNIX-сокеты

- Средство межпроцессного взаимодействия
- “Клиент-серверное” взаимодействие
- Поддерживается всеми основными ОС

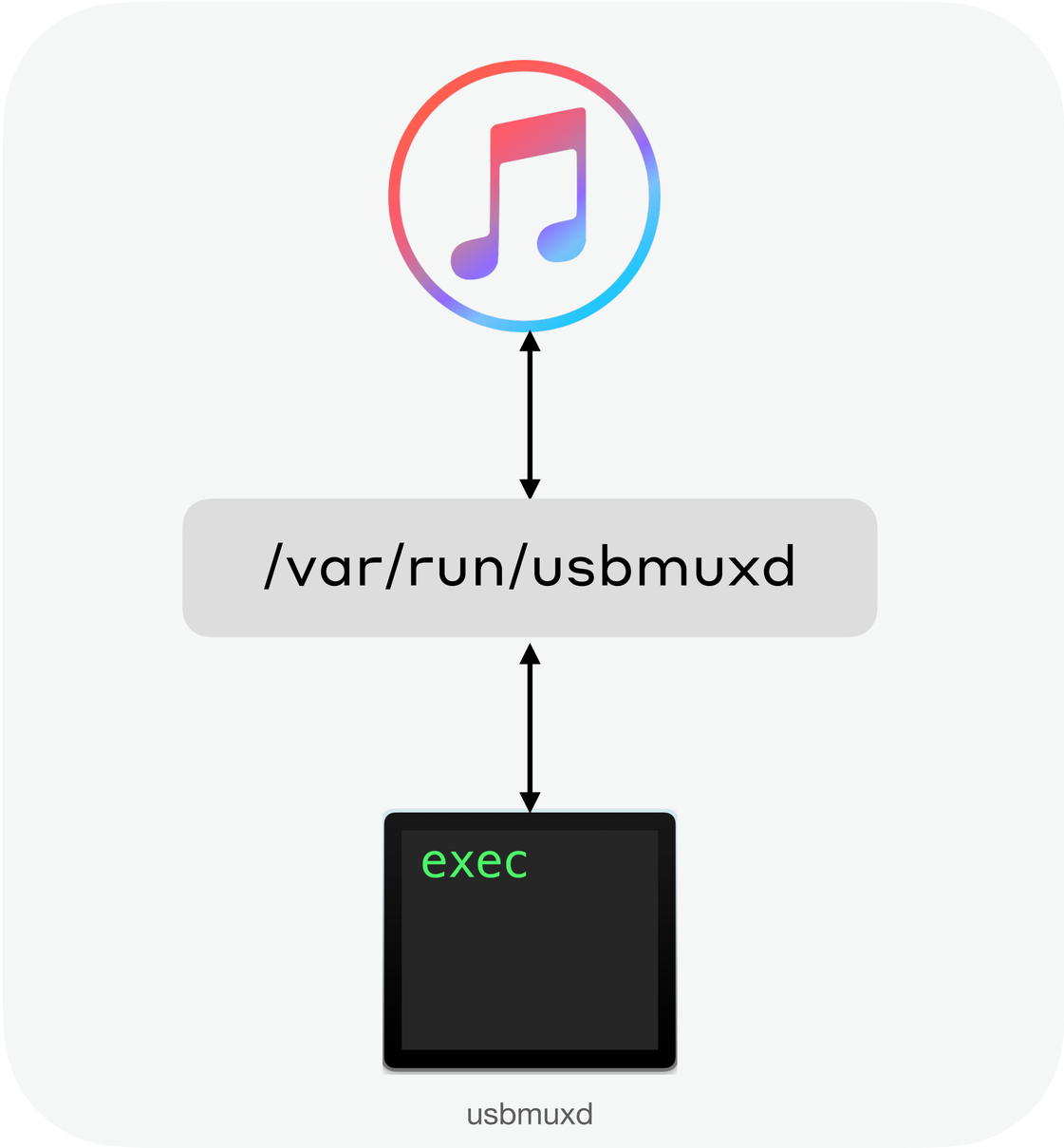


Схема подключения

socat

socat

- Ретранслятор, который может использоваться для передачи данных в обоих направлениях между двумя независимыми каналами.

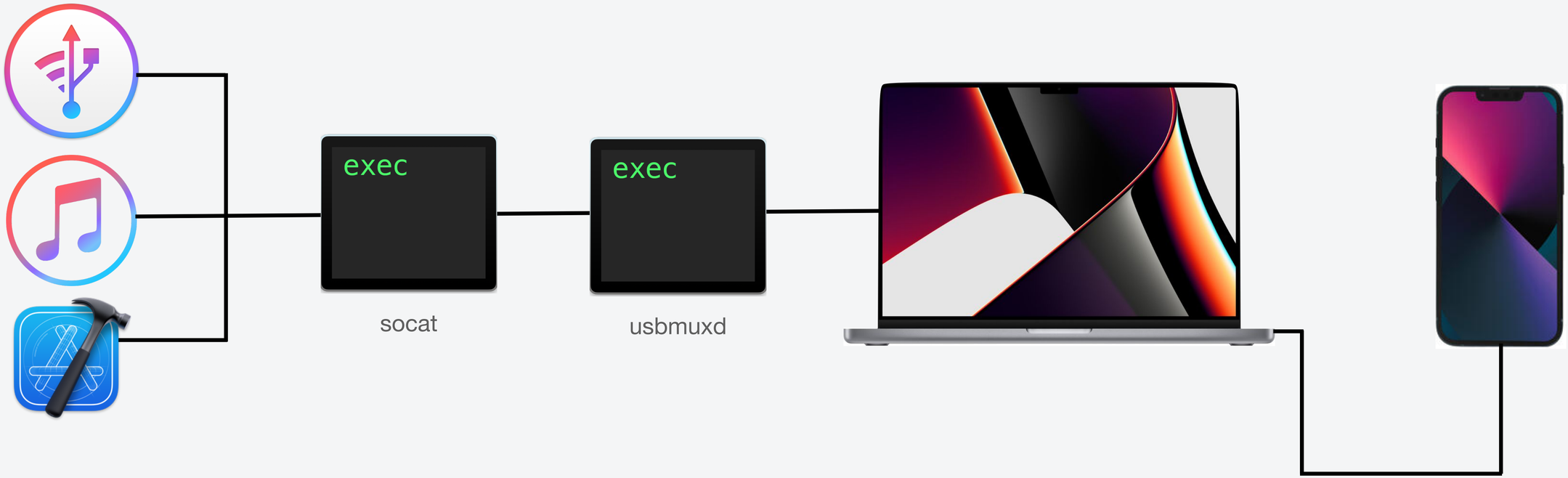
- Каналы данных могут быть представлены в виде файла, канала, устройства, сокета (UNIX, IP4, IP6 (raw), UDP, TCP), сокета SSL, файлового дескриптора (например, stdin), программы или нескольких программ.

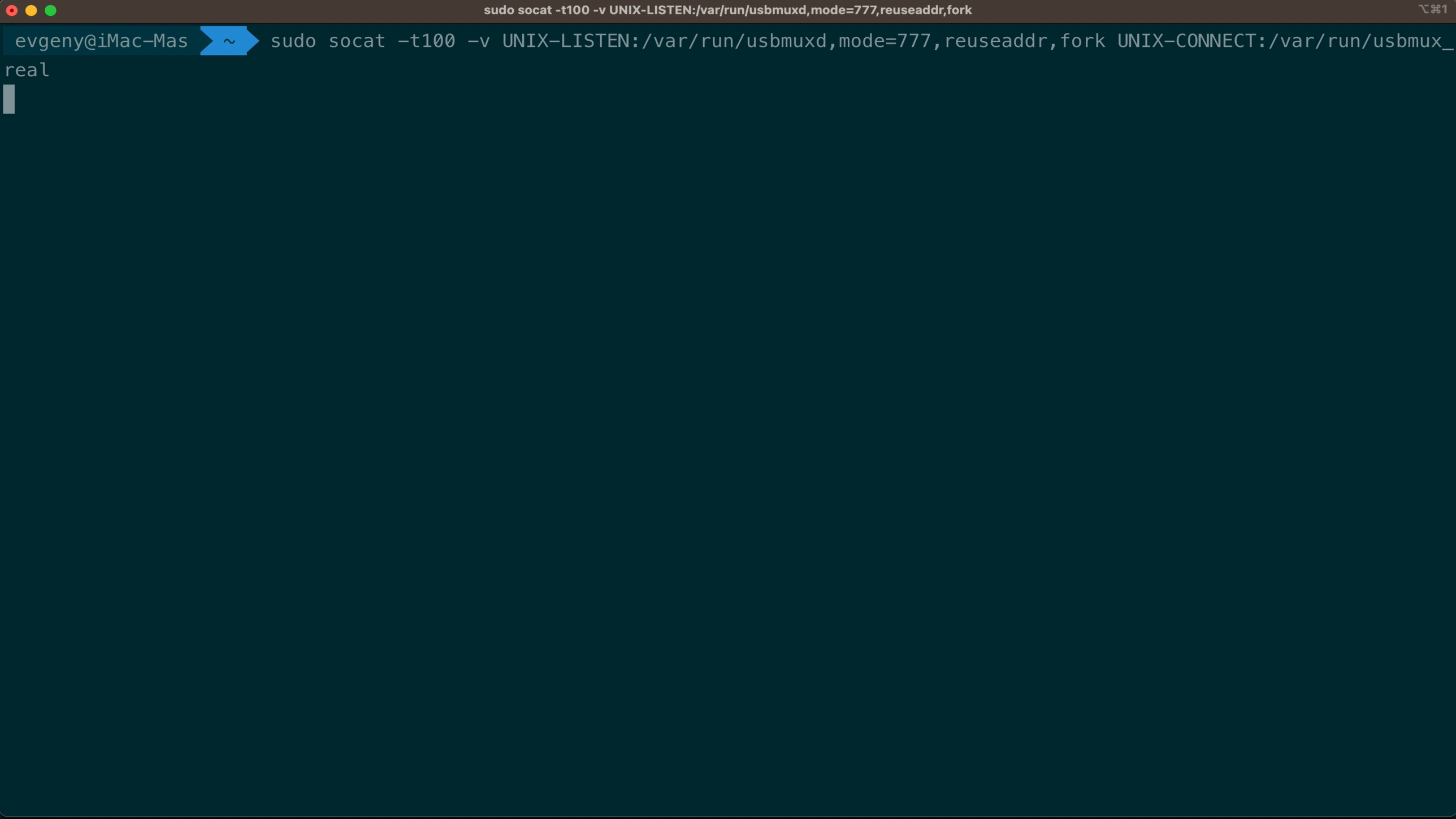
Перехват сообщений

```
$ sudo mv /var/run/usbmuxd /var/run/usbmux_real

$ sudo socat -t100 -x -v
UNIX-LISTEN:/var/run/usbmuxd,mode=777,reuseaddr,fork
UNIX-CONNECT:/var/run/usbmux_real
```

Схема подключения




sudo socat -t100 -v UNIX-LISTEN:/var/run/usbmuxd,mode=777,reuseaddr,fork
⌥⌘1
evgeny@iMac-Mas ~ sudo socat -t100 -v UNIX-LISTEN:/var/run/usbmuxd,mode=777,reuseaddr,fork UNIX-CONNECT:/var/run/usbmux_
real

Connect

Первый запрос отправляемый процессом usbmuxd

connect.plist

- **REQ:**
  ClientVersionString: **usbmuxd-423**
  DeviceID: **4**
  MessageType: **Connect**
  PortNumber: **32498** */* htonl 62078 */*
  ProgName: **usbmuxd**

- **RES:**
  MessageType: **Result**
  Number: **0**

Порядок запросов

usbmuxd и lockdownd

MacOS:
/var/db/lockdown/

iOS:
/var/root/Library/Lockdown/
pair_records/
/var/root/Library/Lockdown/
escrow_records/

udid-of-the-device.plist

MacOS plist:
DeviceCertificate
EscrowBag
HostCertificate
HostID
HostPrivateKey
RootCertificate
RootPrivateKey
SystemBUID
WiFiMACAddress

iOS plist:
DeviceCertificate
HostCertificate
HostID
RootCertificate
SystemBUID
escrow_records

Порядок запросов

usbmuxd

REQ: StartSessionfor Host ID

RES: EnableSessionSSL with Session ID

REQ: Connect

RES: Result 0

REQ: QueryType

RES: com.apple.mobile.lockdown

REQ: GetValue ProductVersion

RES: the iOS version number e.g. 16.4.1

Lockdown Service

iOS:
/usr/libexec/lockdownd

lockdownd

- *com.apple.mobile.lockdown.plist:*
  SockFamily: **Unix**
  SockPathName: **/var/run/lockdown.sock**
  SockPathMode: **511**

  SockFamily: **IPv4**
  SockServiceName: **62078**

- */System/Library/Lockdown/Services.plist:*
  com.apple.mobile.house_arrest
  com.apple.mobile.installation_proxy
  com.apple.debugserver
  com.apple.mobile.screenshotr
  com.apple.mobilesync
  com.apple.afc
  ...

Пример подключения

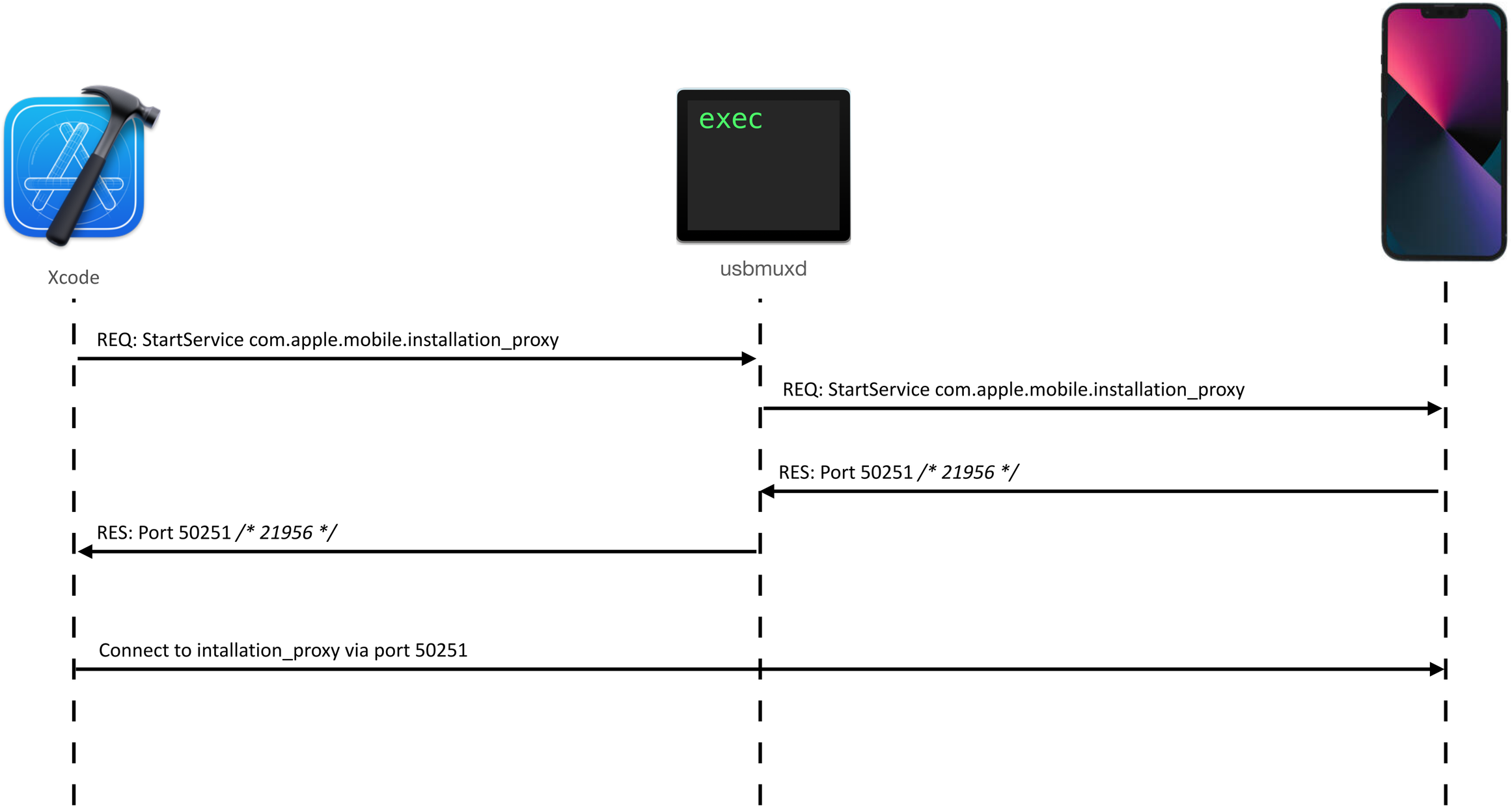
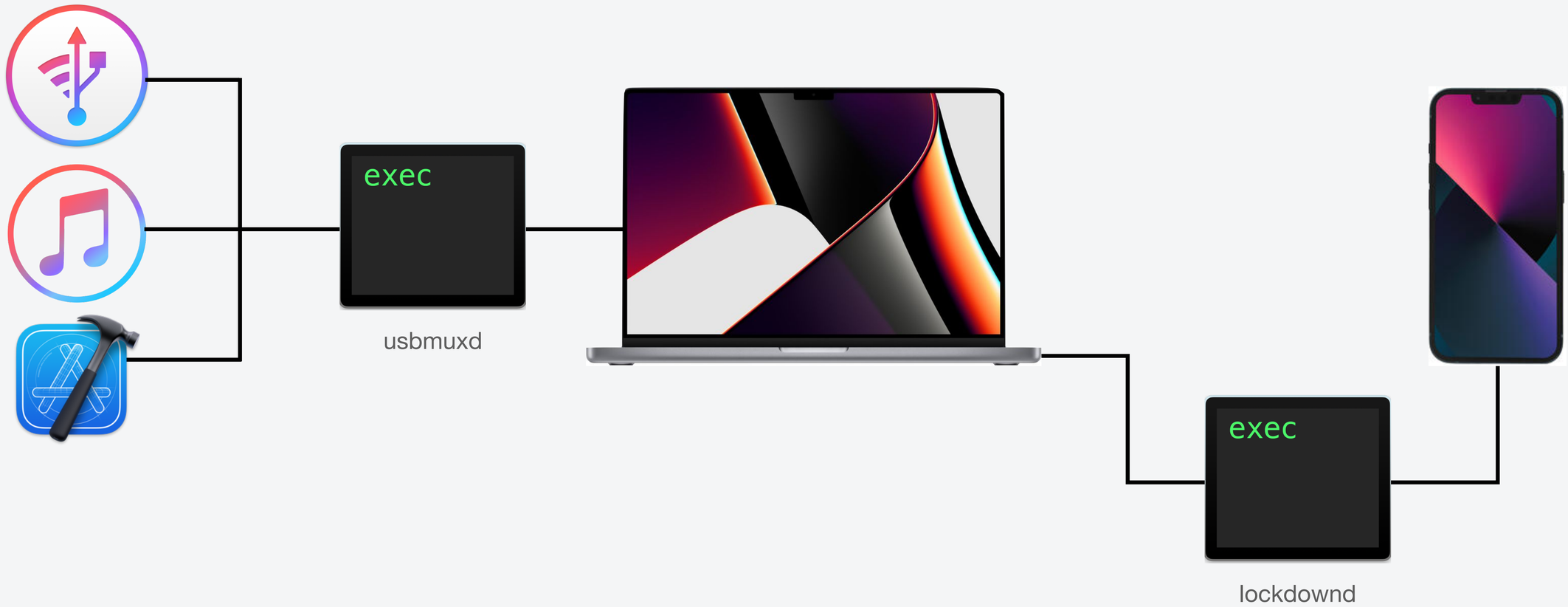


Схема подключения



MobileDevice

https://github.com/imkira/mobiledevice

- Взаимодействует с Mobile Device Framework
- Предоставляет CLI-интерфейс
- Позволяет автоматизировать задачи по установке и удалению приложений

Libimobiledevice

https://github.com/libimobiledevice

- Набор утилит, которые предоставляют полный набор утилит для взаимодействия с телефоном
- Включает в себя собственную версию usbmuxd
- Позволяет подключиться к основным сервисам lockdown
- Работает на всех основных ОС MacOS, Windows, Android

Open-source usbmuxd

https://github.com/
libimobiledevice/usbmuxd

usbmuxd

- Open Source проект симулирующий usbmuxd от Apple
- Позволяет посмотреть размеры пакетов, адреса и т.д.

Open-source usbmuxd

```
static const char *socket_path = "/var/run/usbmuxd"; // 1
static const char *lockfile = "/var/run/usbmuxd.pid";
...
listenfd = socket(AF_UNIX, SOCK_STREAM, 0); // 2
...
if (bind(listenfd, (struct sockaddr*)&bind_addr, sizeof(bind_addr)) != 0) {  //3
    usbmuxd_log(LL_FATAL, "bind() failed: %s", strerror(errno));
    return -1;
}
// Start listening
if (listen(listenfd, 5) != 0)  { // 4
    usbmuxd_log(LL_FATAL, "listen() failed: %s", strerror(errno));  return -1;
}
chmod(socket_path, 0666); // 5
```

ideviceinfo

https://github.com/
libimobiledevice/ideviceinstaller

- Выводит информацию о подключенном устройстве
- Содержит в себе как базовую информацию (имя устройства, тип устройства и т.д), так и дополнительную информацию (оператор, MAC-адреса bluetooth, wi-fi и т.д)

ideviceinstaller

https://github.com/
libimobiledevice/ideviceinstaller

- $ ideviceinstaller -l
  Выводит список ipa-файлов установленных на устройстве

- $ ideviceinstaller -i path-to-ipa
  Устанавливает на устройство ipa-файл

idevicecrashreport

https://github.com/
libimobiledevice/ideviceinstaller

- $ idevicecrashreport path-to-dir
  Перемещает все crashlog
  с устройства в папку

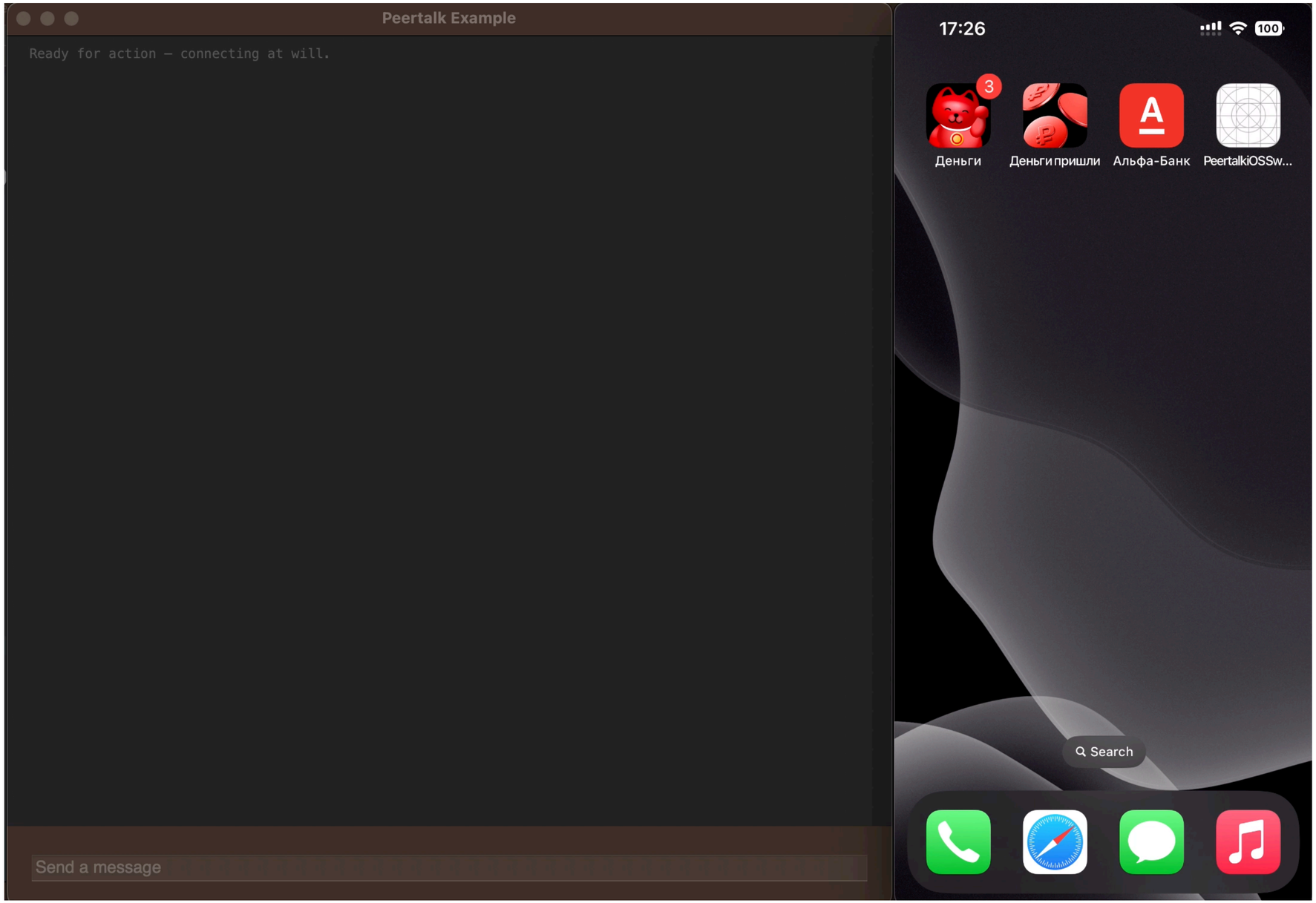
- Использует для
  взаимодействия сервис
  com.apple.crashreportmover

PeerTalk

https://github.com/rsms/peertalk

- Пример использования прямого подключения к открытому сокету на девайсе iOS
- В iOS приложении создаем socket сервер на свободном порту
- На MacOS отправляем Connect через usbmuxd на свободный порт iOS
- Обмениваемся сообщениями

PeerTalk


Peertalk Example
Ready for action — connecting at will.
Send a message
17:26
100
3
Деньги
Деньги пришли
Альфа-Банк
PeertalkiOSSw...
Search

Выводы

01 Не то что кажется

Удалось разобраться в том каким образом телефон получает информацию по проводу, хотя изначально казалось, что подобные вещи должны быть реализованы низкоуровнево и выстроиться туда будет сложно.

02 Возможно применить

Есть много наработок в OpenSource, которые легко встроить в свои процессы, не погружаясь слишком глубоко.

03 Место для творчества

Понимание того, как процессы работают, дают возможность применять технологию правильным образом. А так же находить нетривиальное применение.

СПА
СИ
Б*!

Евгений Онуфрейчик

Альфа-Банк

Alfa Digital

digital.alfabank.ru

Рассказываем о работе в IT и Digital в Альфа-Банке,
делимся интересными вакансиями, новостями
и полезными советами, иногда шутим