

О том, как ВКонтакте собирает информацию о нас

Владислав Велюга (vlad805) • July 29, 2017

Перейти ко второй части.

Сегодня, ковыряя отснифеный трафик официального приложения ВКонтакте под Android, пытаюсь найти особенности, по которым API отсеивает официальные приложения для получения музыки, я наткнулся на запросы довольно интересного содержания...

Disclaimer

Сразу хочу отметить, что я **снимаю** с себя любую ответственность за возможный ущерб, который Вы можете причинить себе/своим устройствам или другим/чужим устройствам, выполняя действия, которые здесь описаны. Также я **не призываю** заниматься подобной деятельностью на своих сетях. Информация **предоставлена исключительно в ознакомительных целях** и крайне **не рекомендуется к воспроизведению/повтору** на личных устройствах, сетях, а также **строго не рекомендуются эксплуатации на пользователей**, поскольку снифинг чужих данных - дело незаконное, а свое устройство я промониторить в праве.

И да, для любителей найти рекламу там, где её нет: этот пост/статья -- не является рекламой. Упомянутые ниже приложения приводятся в качестве примеров, не более.

Update 6

А еще давайте сразу, вот что ответил (где-то) Андрей Rogozov про данную информацию.



Андрей Rogozov Надеюсь, что до такого бреда не дойдет. Но раз дошло, тогда давайте рассмотрим всё по порядку.

> Через Роскомнадзор они пролоббировали запрет собирать данные о пользователях ВКонтакте.

Запрет на сбор и обработку персональных данных пользователей без их на то согласия прописан в законах и отдельно в правилах использования ВК (6.3.9 и 6.3.11 vk.com/terms). И это то, что напрямую защищает интересы любого пользователя сети. В то же время, мы скорее будем изобретать более эффективные технические средства борьбы с подобными нарушениями, чем что-то там лоббировать.

> При этом ВКонтакте только что поймали на бесцеремонной слежке - они, оказываются, тайком фиксируют следующие данные.

Любая социальная сеть, имеющая рекламную сеть или движок рекомендаций, фиксирует и анализирует огромное количество данных, чтобы постоянно улучшать персональную выдачу контента. У каждого собираемого типа данных есть своя понятная и конкретная задача.

Например, о местоположении. В рекламе и рекомендациях существует геотаргетинг. Надеюсь, тут не нужно объяснять каким образом он может влиять на качество выдачи. При этом пользователь сам выбирает разрешать ли ему доступ к этим данным или нет. Это ограничение может быть выставлено на уровне устройства. В то же время был вопрос, почему ВК запрашивает геолокацию при работе с аудиозаписями. Потому что не всю музыку, защищенную правами, можно слушать за пределами зоны действия контрактов.

Анализ приложений на устройстве производится для того, чтобы не рекомендовать пользователям устанавливать те приложения, которые у него и так уже установлены. Эта возможность предоставлена операционной системой Android, т.е. доступна любому приложению на платформе. При этом в ВК существует настройка, которая позволяет отключать передачу этих данных на сервер.

Или возьмем тот же сервис Viko, который используется для мониторинга доставки видеоконтента. Благодаря этому сервису мы повышаем эффективность маршрутизации трафика в регионы и другие страны. При этом там вообще не идет никакой речи о передаче персональных данных сторонней компании. Еще один безосновательный наброс.

Подобная аналитика непрофессиональная и крайне поверхностная. Для всех интересующихся в ближайшее время выпустим статью в техническом блоге, где подробно распишем какие данные анализируются и для чего. Чтобы не пропустить, можете подписаться на сообщество vk.com/tech. И в свободное время рекомендую поизучать какие данные о вас собирает FB или Twitter.

Предисловие

Года два назад я тоже снифил трафик с помощью *Shark for Root*, отправляемый ВКонтакте с телефона. Ничего странного я тогда не видел. Сейчас же, когда нас окружают “умные” (именно в кавычках, ибо они идиотские) ленты, машинное обучение и прочее, техника стала, мягко говоря, следить. С одной стороны, это хорошо (мы даем пищу для машин, чтобы они обучались), с другой - плохо (данные о нас сохраняются на серверах).

Результаты

Проснифив только авторизацию, аудиозаписи и вообще первые минуты после авторизации в приложении, уже можно поймать все эти странные запросы. Итак:

```
1 POST /method/stats.trackInstalledApps HTTP/1.1
2 X-Get-Processing-Time: 1
3 User-Agent: VKAndroidApp/4.12.1-1172 (Android 5.1.1; SDK 22; armeabi-v7a; Sony Xperia L; en)
4 Content-Type: application/x-www-form-urlencoded
5 Content-Length: 4205
6 Host: api.vk.com
7 Connection: Keep-Alive
8 Accept-Encoding: gzip
9 Cookie: remixlang=0
10
11 v=5.68&lang=en&https=1&apps=%5B%7B%22package%22%3A%22ru.loyaltyplant.partner.chainayalozhka%22%2C%22installed%22%3A1484822421%2C%22updated%22%3A1484822421%2C%22version%22%3A%2212.97%22%7D%2C%7B%22package%22%3A%22com.sony.playmemories.mobile%22%2C%22installed%22%3A1456649970%2C%22updated%22%3A1491114919%2C%22version%22%3A%225.8.0%22%7D%2C%7B%22package%22%3A%22com.vkontakte.android%22%2C%22installed%22%3A1501318615%2C%22updated%22%3A1501318615%2C%22version%22%3A%224.12.1%22%7D%2C%7B%22package%22%3A%22org.mozilla.fennec%22%2C%22installed%22%3A1482668713%2C%22updated%22%3A1500874880%2C%22version%22%3A%2256.0a1%22%7D%2C%7B%22package%22%3A%22org.telegram.messenger%22%2C%22installed%22%3A1496422893%2C%22updated%22%3A1496422893%2C%22version%22%3A%224.0.1%22%7D%2C%7B%22package%22%3A%22org.documentfoundation.libreoffice%22%2C%22installed%22%3A1495148537%2C%22updated%22%3A1495148537%2C%22version%22%3A%225.3.0.0%22%7D%2C%7B%22package%22%3A%22com.exploreinc.timelapse%22%2C%22installed%22%3A1477806265%2C%22updated%22%3A1477806265%2C%22version%22%3A%221.2%22%7D%2C%7B%22package%22%3A%22com.andcreate.app.trafficmonitor%22%2C%22installed%22%3A1477986249%2C%22updated%22%3A1477986249%2C%22version%22%3A%221.10.1138%22%7D%2C%7B%22package%22%3A%22com.foxit.mobile.pdf.rms%22%2C%22installed%22%3A1473931927%2C%22updated%22%3A1473931927%2C%22version%22%3A%223.8.0.0407%22%7D%2C%7B%22package%22%3A%22ru.vlad805.mapsharedpoints%22%2C%22installed%22%3A1489869398%2C%22updated%22%3A1495148594%2C%22version%22%3A%221.0%22%7D%2C%7B%22package%22%3A%22com.azxiker.mod.omni%22%2C%22installed%22%3A1476643721%2C%22updated%22%3A1476643721%2C%22version%22%3A%227.6.4.a2.01.0.8%22%7D%2C%7B%22package%22%3A%22com.teamviewer.teamviewer.market.mobile%22%2C%22installed%22%3A1490244238%2C%22updated%22%3A1495148633%2C%22version%22%3A%2211.16.990%22%7D%2C%7B%22package%22%3A%22com.google.android.youtube%22%2C%22installed%22%3A1479677832%2C%22updated%22%3A1479851015%2C%22version%22%3A%223.2.0%22%7D%2C%7B%22package%22%3A%22ru.yandex.yandexbus%22%2C%22installed%22%3A1482529757%2C%22updated%22%3A1495084285%2C%22version%22%3A%224.30%22%7D%2C%7B%22package%22%3A%22ru.yandex.weatherplugin%22%2C%22installed%22%3A1457046412%2C%22updated%22%3A1463264425%2C%22version%22%3A%224.2.1%22%7D%2C%7B%22package%22%3A%22com.perm.kate.pro%22%2C%22installed%22%3A1456271068%2C%22updated%22%3A1485781513%2C%22version%22%3A%2237%22%7D%2C%7B%22package%22%3A%22ru.dublgis.dgismobile%22%2C%22installed%22%3A1495794353%2C%22updated%22%3A1500052713%2C%22version%22%3A%224.1.19.1753%22%7D%2C%7B%22package%22%3A%22com.google.android.inputmethod.latin%22%2C%22installed%22%3A1456476927%2C%22updated%22%3A1463379043%2C%22version%22%3A%224.1.23%22%7D%2C%7B%22package%22%3A%22ru.vlad805.mapsharedpoints%22%2C%22installed%22%3A1489869398%2C%22updated%22%3A1495148594%2C%22version%22%3A%221.0%22%7D%2C%7B%22package%22%3A%22com.azxiker.mod.omni%22%2C%22installed%22%3A1476643721%2C%22updated%22%3A1476643721%2C%22version%22%3A%227.6.4.a2.01.0.8%22%7D%2C%7B%22package%22%3A%22com.teamviewer.teamviewer.market.mobile%22%2C%22installed%22%3A1490244238%2C%22updated%22%3A1495148633%2C%22version%22%3A%2211.16.990%22%7D%2C%7B%22package%22%3A%22com.google.android.youtube%22%2C%22installed%22%3A1479677832%2C%22updated%22%3A1479851015%2C%22version%22%3A%223.2.0%22%7D%2C%7B%22package%22%3A%22ru.yandex.yandexbus%22%2C%22installed%22%3A1482529757%2C%22updated%22%3A1495084285%2C%22version%22%3A%224.30%22%7D%2C%7B%22package%22%3A%22ru.yandex.weatherplugin%22%2C%22installed%22%3A1457046412%2C%22updated%22%3A1463264425%2C%22version%22%3A%224.2.1%22%7D%2C%7B%22package%22%3A%22com.perm.kate.pro%22%2C%22installed%22%3A1456271068%2C%22updated%22%3A1485781513%2C%22version%22%3A%2237%22%7D%2C%7B%22package%22%3A%22ru.dublgis.dgismobile%22%2C%22installed%22%3A1495794353%2C%22updated%22%3A1500052713%2C%22version%22%3A%224.1.19.1753%22%7D%2C%7B%22package%22%3A%22com.google.android.inputmethod.latin%22%2C%22installed%22%3A1456476927%2C%22updated%22%3A1463379043%2C%22version%22%3A%224.1.23%22%7D%2C%7B%22package%22%3A%22ru.vlad805.mapsharedpoints%22%2C%22installed%22%3A1489869398%2C%22updated%22%3A1495148594%2C%22version%22%3A%221.0%22%7D%2C%7B%22package%22%3A%22com.azxiker.mod.omni%22%2C%22installed%22%3A1476643721%2C%22updated%22%3A1476643721%2C%22version%22%3A%227.6.4.a2.01.0.8%22%7D%2C%7B%22package%22%3A%22com.teamviewer.teamviewer.market.mobile%22%2C%22installed%22%3A1490244238%2C%22updated%22%3A1495148633%2C%22version%22%3A%2211.16.990%22%7D%2C%7B%22package%22%3A%22com.google.android.youtube%22%2C%22installed%22%3A1479677832%2C%22updated%22%3A1479851015%2C%22version%22%3A%223.2.0%22%7D%2C%7B%22package%22%3A%22ru.yandex.yandexbus%22%2C%22installed%22%3A1482529757%2C%22updated%22%3A1495084285%2C%22version%22%3A%224.30%22%7D%2C%7B%22package%22%3A%22ru.yandex.weatherplugin%22%2C%22installed%22%3A1457046412%2C%22updated%22%3A1463264425%2C%22version%22%3A%224.2.1%22%7D%2C%7B%22package%22%3A%22com.perm.kate.pro%22%2C%22installed%22%3A1456271068%2C%22updated%22%3A1485781513%2C%22version%22%3A%2237%22%7D%2C%7B%22package%22%3A%22ru.dublgis.dgismobile%22%2C%22installed%22%3A1495794353%2C%22updated%22%3A1500052713%2C%22version%22%3A%224.1.19.1753%22%7D%2C%7B%22package%22%3A%22com.google.android.inputmethod.latin%22%2C%22installed%22%3A1456476927%2C%22updated%22%3A1463379043%2C%22version%22%3A%224.1.23%22%7D%2C%7B%22package%22%3A%22ru.vlad805.mapsharedpoints%22%2C%22installed%22%3A1489869398%2C%22updated%22%3A1495148594%2C%22version%22%3A%221.0%22%7D%2C%7B%22package%22%3A%22com.azxiker.mod.omni%22%2C%22installed%22%3A1476643721%2C%22updated%22%3A1476643721%2C%22version%22%3A%227.6.4.a2.01.0.8%22%7D%2C%7B%22package%22%3A%22com.teamviewer.teamviewer.market.mobile%22%2C%22installed%22%3A1490244238%2C%22updated%22%3A1495148633%2C%22version%22%3A%2211.16.990%22%7D%2C%7B%22package%22%3A%22com.google.android.youtube%22%2C%22installed%22%3A1479677832%2C%22updated%22%3A1479851015%2C%22version%22%3A%223.2.0%22%7D%2C%7B%22package%22%3A%22ru.yandex.yandexbus%22%2C%22installed%22%3A1482529757%2C%22updated%22%3A1495084285%2C%22version%22%3A%224.30%22%7D%2C%7B%22package%22%3A%22ru.yandex.weatherplugin%22%2C%22installed%22%3A1457046412%2C%22updated%22%3A1463264425%2C%22version%22%3A%224.2.1%22%7D%2C%7B%22package%22%3A%22com.perm.kate.pro%22%2C%22installed%22%3A1456271068%2C%22updated%22%3A1485781513%2C%22version%22%3A%2237%22%7D%2C%7B%22package%22%3A%22ru.dublgis.dgismobile%22%2C%22installed%22%3A1495794353%2C%22updated%22%3A1500052713%2C%22version%22%3A%224.1.19.1753%22%7D%2C%7B%22package%22%3A%22com.google.android.inputmethod.latin%22%2C%22installed%22%3A1456476927%2C%22updated%22%3A1463379043%2C%22version%22%3A%224.1.23%22%7D%2C%7B%22package%22%3A%22ru.vlad805.mapsharedpoints%22%2C%22installed%22%3A1489869398%2C%22updated%22%3A1495148594%2C%22version%22%3A%221.0%22%7D%2C%7B%22package%22%3A%22com.azxiker.mod.omni%22%2C%22installed%22%3A1476643721%2C%22updated%22%3A1476643721%2C%22version%22%3A%227.6.4.a2.01.0.8%22%7D%2C%7B%22package%22%3A%22com.teamviewer.teamviewer.market.mobile%22%2C%22installed%22%3A1490244238%2C%22updated%22%3A1495148633%2C%22version%22%3A%2211.16.990%22%7D%2C%7B%22package%22%3A%22com.google.android.youtube%22%2C%22installed%22%3A1479677832%2C%22updated%22%3A1479851015%2C%22version%22%3A%223.2.0%22%7D%2C%7B%22package%22%3A%22ru.yandex.yandexbus%22%2C%22installed%22%3A1482529757%2C%22updated%22%3A1495084285%2C%22version%22%3A%224.30%22%7D%2C%7B%22package%22%3A%22ru.yandex.weatherplugin%22%2C%22installed%22%3A1457046412%2C%22updated%22%3A1463264425%2C%22version%22%3A%224.2.1%22%7D%2C%7B%22package%22%3A%22com.perm.kate.pro%22%2C%22installed%22%3A1456271068%2C%22updated%22%3A1485781513%2C%22version%22%3A%2237%22%7D%2C%7B%22package%22%3A%22ru.dublgis.dgismobile%22%2C%22installed%22%3A1495794353%2C%22updated%22%3A1500052713%2C%22version%22%3A%224.1.19.1753%22%7D%2C%7B%22package%22%3A%22com.google.android.inputmethod.latin%22%2C%22installed%22%3A1456476927%2C%22updated%22%3A1463379043%2C%22version%22%3A%224.1.23%22%7D%2C%7B%22package%22%3A%22ru.vlad805.mapsharedpoints%22%2C%22installed%22%3A1489869398%2C%22updated%22%3A1495148594%2C%22version%22%3A%221.0%22%7D%2C%7B%22package%22%3A%22com.azxiker.mod.omni%22%2C%22installed%22%3A1476643721%2C%22updated%22%3A1476643721%2C%22version%22%3A%227.6.4.a2.01.0.8%22%7D%2C%7B%22package%22%3A%22com.teamviewer.teamviewer.market.mobile%22%2C%22installed%22%3A1490244238%2C%22updated%22%3A1495148633%2C%22version%22%3A%2211.16.990%22%7D%2C%7B%22package%22%3A%22com.google.android.youtube%22%2C%22installed%22%3A1479677832%2C%22updated%22%3A1479851015%2C%22version%22%3A%223.2.0%22%7D%2C%7B%22package%22%3A%22ru.yandex.yandexbus%22%2C%22installed%22%3A1482529757%2C%22updated%22%3A1495084285%2C%22version%22%3A%224.30%22%7D%2C%7B%22package%22%3A%22ru.yandex.weatherplugin%22%2C%22installed%22%3A1457046412%2C%22updated%22%3A1463264425%2C%22version%22%3A%224.2.1%22%7D%2C%7B%22package%22%3A%22com.perm.kate.pro%22%2C%22installed%22%3A1456271068%2C%22updated%22%3A1485781513%2C%22version%22%3A%2237%22%7D%2C%7B%22package%22%3A%22ru.dublgis.dgismobile%22%2C%22installed%22%3A1495794353%2C%22updated%22%3A1500052713%2C%22version%22%3A%224.1.19.1753%22%7D%2C%7B%22package%22%3A%22com.google.android.inputmethod.latin%22%2C%22installed%22%3A1456476927%2C%22updated%22%3A1463379043%2C%22version%22%3A%224.1.23%22%7D%2C%7B%22package%22%3A%22ru.vlad805.mapsharedpoints%22%2C%22installed%22%3A1489869398%2C%22updated%22%3A1495148594%2C%22version%22%3A%221.0%22%7D%2C%7B%22package%22%3A%22com.azxiker.mod.omni%22%2C%22installed%22%3A1476643721%2C%22updated%22%3A1476643721%2C%22version%22%3A%227.6.4.a2.01.0.8%22%7D%2C%7B%22package%22%3A%22com.teamviewer.teamviewer.market.mobile%22%2C%22installed%22%3A1490244238%2C%22updated%22%3A1495148633%2C%22version%22%3A%2211.16.990%22%7D%2C%7B%22package%22%3A%22com.google.android.youtube%22%2C%22installed%22%3A1479677832%2C%22updated%22%3A1479851015%2C%22version%22%3A%223.2.0%22%7D%2C%7B%22package%22%3A%22ru.yandex.yandexbus%22%2C%22installed%22%3A1482529757%2C%22updated%22%3A1495084285%2C%22version%22%3A%224.30%22%7D%2C%7B%22package%22%3A%22ru.yandex.weatherplugin%22%2C%22installed%22%3A1457046412%2C%22updated%22%3A1463264425%2C%22version%22%3A%224.2.1%22%7D%2C%7B%22package%22%3A%22com.perm.kate.pro%22%2C%22installed%22%3A1456271068%2C%22updated%22%3A1485781513%2C%22version%22%3A%2237%22%7D%2C%7B%22package%22%3A%22ru.dublgis.dgismobile%22%2C%22installed%22%3A1495794353%2C%22updated%22%3A1500052713%2C%22version%22%3A%224.1.19.1753%22%7D%2C%7B%22package%22%3A%22com.google.android.inputmethod.latin%22%2C%22installed%22%3A1456476927%2C%22updated%22%3A1463379043%2C%22version%22%3A%224.1.23%22%7D%2C%7B%22package%22%3A%22ru.vlad805.mapsharedpoints%22%2C%22installed%22%3A1489869398%2C%22updated%22%3A1495148594%2C%22version%22%3A%221.0%22%7D%2C%7B%22package%22%3A%22com.azxiker.mod.omni%22%2C%22installed%22%3A1476643721%2C%22updated%22%3A1476643721%2C%22version%22%3A%227.6.4.a2.01.0.8%22%7D%2C%7B%22package%22%3A%22com.teamviewer.teamviewer.market.mobile%22%2C%22installed%22%3A1490244238%2C%22updated%22%3A1495148633%2C%22version%22%3A%2211.16.990%22%7D%2C%7B%22package%22%3A%22com.google.android.youtube%22%2C%22installed%22%3A1479677832%2C%22updated%22%3A1479851015%2C%22version%22%3A%223.2.0%22%7D%2C%7B%22package%22%3A%22ru.yandex.yandexbus%22%2C%22installed%22%3A1482529757%2C%22updated%22%3A1495084285%2C%22version%22%3A%224.30%22%7D%2C%7B%22package%22%3A%22ru.yandex.weatherplugin%22%2C%22installed%22%3A1457046412%2C%22updated%22%3A1463264425%2C%22version%22%3A%224.2.1%22%7D%2C%7B%22package%22%3A%22com.perm.kate.pro%22%2C%22installed%22%3A1456271068%2C%22updated%22%3A1485781513%2C%22version%22%3A%2237%22%7D%2C%7B%22package%22%3A%22ru.dublgis.dgismobile%22%2C%22installed%22%3A1495794353%2C%22updated%22%3A1500052713%2C%22version%22%3A%224.1.19.1753%22%7D%2C%7B%22package%22%3A%22com.google.android.inputmethod.latin%22%2C%22installed%22%3A1456476927%2C%22updated%22%3A1463379043%2C%22version%22%3A%224.1.23%22%7D%2C%7B%22package%22%3A%22ru.vlad805.mapsharedpoints%22%2C%22installed%22%3A1489869398%2C%22updated%22%3A1495148594%2C%22version%22%3A%221.0%22%7D%2C%7B%22package%22%3A%22com.azxiker.mod.omni%22%2C%22installed%22%3A1476643721%2C%22updated%22%3A1476643721%2C%22version%22%3A%227.6.4.a2.01.0.8%22%7D%2C%7B%22package%22%3A%22com.teamviewer.teamviewer.market.mobile%22%2C%22installed%22%3A1490244238%2C%22updated%22%3A1495148633%2C%22version%22%3A%2211.16.990%22%7D%2C%7B%22package%22%3A%22com.google.android.youtube%22%2C%22installed%22%3A1479677832%2C%22updated%22%3A1479851015%2C%22version%22%3A%223.2.0%22%7D%2C%7B%22package%22%3A%22ru.yandex.yandexbus%22%2C%22installed%22%3A1482529757%2C%22updated%22%3A1495084285%2C%22version%22%3A%224.30%22%7D%2C%7B%22package%22%3A%22ru.yandex.weatherplugin%22%2C%22installed%22%3A1457046412%2C%22updated%22%3A1463264425%2C%22version%22%3A%224.2.1%22%7D%2C%7B%22package%22%3A%22com.perm.kate.pro%22%2C%22installed%22%3A1456271068%2C%22updated%22%3A1485781513%2C%22version%22%3A%2237%22%7D%2C%7B%22package%22%3A%22ru.dublgis.dgismobile%22%2C%22installed%22%3A1495794353%2C%22updated%22%3A1500052713%2C%22version%22%3A%224.1.19.1753%22%7D%2C%7B%22package%22%3A%22com.google.android.inputmethod.latin%22%2C%22installed%22%3A1456476927%2C%22updated%22%3A1463379043%2C%22version%22%3A%224.1.23%22%7D%2C%7B%22package%22%3A%22ru.vlad805.mapsharedpoints%22%2C%22installed%22%3A1489869398%2C%22updated%22%3A1495148594%2C%22version%22%3A%221.0%22%7D%2C%7B%22package%22%3A%22com.azxiker.mod.omni%22%2C%22installed%22%3A1476643721%2C%22updated%22%3A1476643721%2C%22version%22%3A%227.6.4.a2.01.0.8%22%7D%2C%7B%22package%22%3A%22com.teamviewer.teamviewer.market.mobile%22%2C%22installed%22%3A1490244238%2C%22updated%22%3A1495148633%2C%22version%22%3A%2211.16.990%22%7D%2C%7B%22package%22%3A%22com.google.android.youtube%22%2C%22installed%22%3A1479677832%2C%22updated%22%3A1479851015%2C%22version%22%3A%223.2.0%22%7D%2C%7B%22package%22%3A%22ru.yandex.yandexbus%22%2C%22installed%22%3A1482529757%2C%22updated%22%3A1495084285%2C%22version%22%3A%224.30%22%7D%2C%7B%22package%22%3A%22ru.yandex.weatherplugin%22%2C%22installed%22%3A1457046412%2C%22updated%22%3A1463264425%2C%22version%22%3A%224.2.1%22%7D%2C%7B%22package%22%3A%22com.perm.kate.pro%22%2C%22installed%22%3A1456271068%2C%22updated%22%3A1485781513%2C%22version%22%3A%2237%22%7D%2C%7B%22package%22%3A%22ru.dublgis.dgismobile%22%2C%22installed%22%3A1495794353%2C%22updated%22%3A1500052713%2C%22version%22%3A%224.1.19.1753%22%7D%2C%7B%22package%22%3A%22com.google.android.inputmethod.latin%22%2C%22installed%22%3A1456476927%2C%22updated%22%3A1463379043%2C%22version%22%3A%224.1.23%22%7D%2C%7B%22package%22%3A%22ru.vlad805.mapsharedpoints%22%2C%22installed%22%3A1489869398%2C%22updated%22%3A1495148594%2C%22version%22%3A%221.0%22%7D%2C%7B%22package%22%3A%22com.azxiker.mod.omni%22%2C%22installed%22%3A1476643721%2C%22updated%22%3A1476643721%2C%22version%22%3A%227.6.4.a2.01.0.8%22%7D%2C%7B%22package%22%3A%22com.teamviewer.teamviewer.market.mobile%22%2C%22installed%22%3A1490244238%2C%22updated%22%3A1495148633%2C%22version%22%3A%2211.16.990%22%7D%2C%7B%22package%22%3A%22com.google.android.youtube%22%2C%22installed%22%3A1479677832%2C%22updated%22%3A1479851015%2C%22version%
```



```
1 GET /uxzoom/2/notify?svcid=5d18&cid=d1d6b884d5e8c23de2bf056d64f38317&
api=ftl5ZrzetxL-hrDCEEhUn8IdIBN5yXjHqn7emMcizNkH1aMbJtmTfayBtc3tNv9Tm
27tCP5xYI0sL1Yin2qiT0qX4cSwupJTrmOxC_whKJ-J4Qp_Z8AB6FNU3_FZg0Kkzuwb3W
6675A_LMF3stITIKB0a4KtEYuYye7soqjQb1bL0dWXIprNj0I0Qsj0UyPG3XMsP6L3Kwi
y8k0v3xabwxSVBlVpj3McKjRJJos9ezS90y_nej35F0cUJW6nL09t11vASnk_gparckEPf
nQITh0KU9PMSuMd-I0bzHS9yWZD7PPamj6Ys9ZhFE2VHv_2Dr0G032soIb1sY5KG3esTo
jf7votu7LWREXxdXWFrR1a9B2dZERFg-zKz1JRstBsK-ZtmQpp-F2s1ykHRDyKQl8gR2Z
8p0aePEbJ9UGc-Devcu2au2DyCzeAaG_sRAqhLLl0SjjC-YQHhKTCyV22VwQ8PoxA7Ly6
qUVYwJU22z9TtRHnR5wCb0FUUrytRJ32SZ72WrJ9eK4-vGblrZoKjMKA HTTP/1.1
2 User-Agent: VKAndroidApp/4.12.1-1172 (Android 5.1.1; SDK 22;
armeabi-v7a; Sony Xperia L; en)
3 Host: api.vigo.ru
4 Connection: Keep-Alive
5 Accept-Encoding: gzip
6
7 HTTP/1.1 204 No Content
8 Server: nginx/1.10.0 (Ubuntu)
9 Date: Sat, 29 Jul 2017 09:02:16 GMT
10 Connection: close
11
12
```

Довольно часто промелькивали запросы к некоему сервису vigo.ru. Сервис позиционирует себя как аналитика в передаче, поиска ошибок, проблем и обработке видео. Но странно, ведь я всего лишь авторизовался, перешел в аудио и пролистал свою стену, где не было ни единого видеоролика (которые должны были автоматически проигрываться?), а запросов скопилось около 5-7 штук. Помимо notify еще был network_status.

```
1 POST /method/execute.wallGetWrapNew HTTP/1.1
2 X-Get-Processing-Time: 1
3 User-Agent: VKAndroidApp/4.12.1-1172 (Android 5.1.1; SDK 22;
armeabi-v7a; Sony Xperia L; en)
4 Content-Type: application/x-www-form-urlencoded
5 Content-Length: 817
6 Host: api.vk.com
7 Connection: Keep-Alive
8 Accept-Encoding: gzip
9 Cookie: remixlang=0
10
11 v=5.68&lang=en&https=1&photo_sizes=1&owner_id=
96&count=20&extend
ed=1&fields=photo_100%2Cphoto_50%2Csex%2Cfirst_name_dat%2Clast_name_d
at%2Cvideo_files&filters=ads_app%2Cads_site%2Cads_post%2Cads_app_slid
er&connection_type=wifi&connection_subtype=unknown&user_options=%7B%2
2autoplay_video%22%3A%7B%22value%22%3A%22always%22%7D%2C%22autoplay_g
if%22%3A%7B%22value%22%3A%22always%22%7D%7D&device_info=%7B%22app_v
ersion%22%3A%224.12.1%22%2C%22system_name%22%3A%22Android%22%2C%22syste
m_version%22%3A%225.1.1%22%2C%22manufacturer%22%3A%22Sony%22%2C%22dev
ice_model%22%3A%22Xperia%20L%22%2C%22ads_device_id%22%3A%22
b579f306%22%2C%22ads_android_id%22%3A%22E
79f306%22%7D&access_t
oken=
&sig=2edc9d892317423589865ec4520e40d5HTTP/1.1
200 OK
12
ys"},"autoplay_gif"-- Sublime Text
{"autoplay_video":{"value":"always"},"autoplay_gif
1 {"autoplay_video":{"value":"always"},"autoplay_gif":{"value":"always"
}}&device_info={"app_version":"4.12.1","system_name":"Android","syste
m_version":"5.1.1","manufacturer":"Sony","device_model":"Xperia L","a
ds_device_id":"5:
b579f306","ads_android_id":"53
b579f306"]
```

Вот опять. wallGetWrapNew - по названию понятно, что это запрос на получение чьей-то стены (пользователя или сообщества). Зачем тут передавать информацию о устройстве? Максимум, что приходит на ум - для статистики. Хорошо, а зачем данные о типе сети? Еще, что не относится к сливу информации: довольно раздражает то, что везде пытаются всунуть рекламу - лишь посмотреть на параметр fields.

```
1 POST /method/execute HTTP/1.1
2 X-Get-Processing-Time: 1
3 User-Agent: VKAndroidApp/4.12.1-1172 (Android 5.1.1; SDK 22;
armeabi-v7a; Sony Xperia L; en)
4 Content-Type: application/x-www-form-urlencoded
5 Content-Length: 792
6 Host: api.vk.com
7 Connection: Keep-Alive
8 Accept-Encoding: gzip
9 Cookie: remixlang=0
10
11 v=5.68&lang=en&https=1&code=API.account.setOnline%28%7Bpush_count%3A%
200%7D%22%3BAPI.stats.trackEvents%28%7Bevents%3A%22%5B%7B%5C%22e%5C%2
2%3A%5C%22user_action%5C%22%2C%5C%22action_type%5C%22%3A%5C%22menu_cl
ick%5C%22%2C%5C%22action_param%5C%22%3A%5C%22audio%5C%22%7D%2C%7B%5C%
22e%5C%22%3A%5C%22geo_data%5C%22%2C%5C%22no_data_reason%5C%22%3A%2C%
5C%22cell_id%5C%22%3A11700070%2C%5C%22cell_type%5C%22%3A%5C%22gsm%5C%
22%7D%2C%7B%5C%22e%5C%22%3A%5C%22view_post_time%5C%22%2C%5C%22views%5
C%22%3A%5B%7B%5C%22ref%5C%22%3A%5C%22feed_top%5C%22%2C%5C%22post_id%5
C%22%3A%5C%22-72495085_747138%5C%22%2C%5C%22times%5C%22%3A%5C%22%5B94
06%5D%5C%22%7D%5D%7D%5D%22%7D%29%3B&access_token=
&sig
=b3d9ec0cbf79c48e0457c1d14d36b20 HTTP/1.1 200 OK
API.stats.trackEvents({events:[{"e":"\user_acti
API.stats.trackEvents({events:[{"e":"\user_action\", \"action_type\
\": \"menu_click\", \"action_param\": \"audio\"}, {\"e\": \"geo_data\", \"no
_data_reason\": 2, \"cell_id\": 11700070, \"cell_type\": \"gsm\"}, {\"e\": \"
view_post_time\", \"views\": [{\"ref\": \"feed_top\", \"post_id\": \"-724
95085_747138\", \"times\": \"[9406]\"}]}]);&access_token=
&sig=b3d9ec0cbf79c48e0457c1d14d36b203
```

Приложение отправляет все действия пользователя: перешел через меню в раздел "аудио", "geo_data" - вероятно, отправлял бы примерное (или даже точное) местоположение устройства. Спрашивается, зачем, если пользователь не просит находить что-то по близости? Нет, облегчать пользователю жизнь, подсказывая релевантные данные в поиске, например - в этом ничего плохого нет, но зачем отправлять геоданные просто так, при открытии поста? Не понятно.

```
1 POST /method/stats.benchmark HTTP/1.1
2 X-Get-Processing-Time: 1
3 User-Agent: VKAndroidApp/4.12.1-1172 (Android 5.1.1; SDK 22;
armeabi-v7a; Sony Xperia L; en)
4 Content-Type: application/x-www-form-urlencoded
5 Content-Length: 200
6 Host: api.vk.com
7 Connection: Keep-Alive
8 Accept-Encoding: gzip
9 Cookie: remixlang=0
10
11 v=5.68&lang=en&https=1&api_response_time=477&image_load_time=322&acce
ss_token=
&sig=f9660047a23c326ba55bb3f1dfa1d997HTTP/1.
1 200 OK
12 Server: nginx
13 Date: Sat, 29 Jul 2017 09:02:03 GMT
14 Content-Type: application/json; charset=utf-8
15 Content-Length: 14
16 Connection: close
17 X-Powered-By: PHP/3.13286
18 Pragma: no-cache
19 Cache-control: no-store
20 X-Request-Processing-Time: 0.030
21
22 {"response":1}
```

Приложение делает бенчмарки и зачем-то передает время запроса к API и время загрузки изображений. Видимо, усредненные данные.

```
1 GET /counters.php HTTP/1.1
2 Host: m.vk.com
3 Connection: keep-alive
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; Xperia L Build/LMY492) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/39.0.0.0 Mobile Safari/537.36
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-GB,en-US;q=0.8
8 Cookie: remixlang=3
9 X-Requested-With: com.vkontakte.android
10
11 HTTP/1.1 200 OK
12 Server: nginx
13 Date: Sun, 30 Jul 2017 14:51:06 GMT
14 Content-Type: text/html; charset=windows-1251
15 Content-Length: 463
16 Connection: close
17 X-Powered-By: PHP/3.13290
18 Pragma: no-cache
19 Cache-control: no-cache
20 Strict-Transport-Security: max-age=0
21
22 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
23 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
24 <head>
25 <body>
26 
27 
28 </body>
29 </html>
```

Пока не понял когда, при каких условиях и зачем, в приложении подгружается невидимая WebView со страницей m.vk.com/counters.php. Ибо от нее же потом подгружаются две метрики-пикселя (внизу HTML-кода) и favicon. Накрутка статистики: упр: спустя еще пару минут отправился еще один запрос сюда же, уже с другими числами в тегах img - для того, чтобы тот самый пиксель не загрузился из кэша, а запрос к метрике все таки был реальным.

Update 3

Эдуард Безменов, разработчик модификации официального приложения VK Coffee, прокомментировал этот пост так:

«...сама настройка появилась далеееко не сразу, в сравнении от самого слива. Слив подобных данных лично для меня далеко не ново и в кофе давно отключено. ... Самый ад то, что libverify от мыла.ru собирает серийники sim-карт, а mytracker - lac и cid. Это вроде и показал Андрей. Серийники сим карт и т.п. Вот из-за этого и надо поднимать хайп.»

Update 4

Григорий Ключников, бывший разработчик этого самого приложения, как оказывается, был сам против включения сервисов Vigo в приложение:

«Vigo уже очень давно был, внедрял его я. Я был против с самого начала, но на моё мнение всем было известно как. И это вы там ещё до мейловского MyTracker не дошли, там самая мякотка.»

А вот, что на самом деле представляет Vigo по описанию Григория:

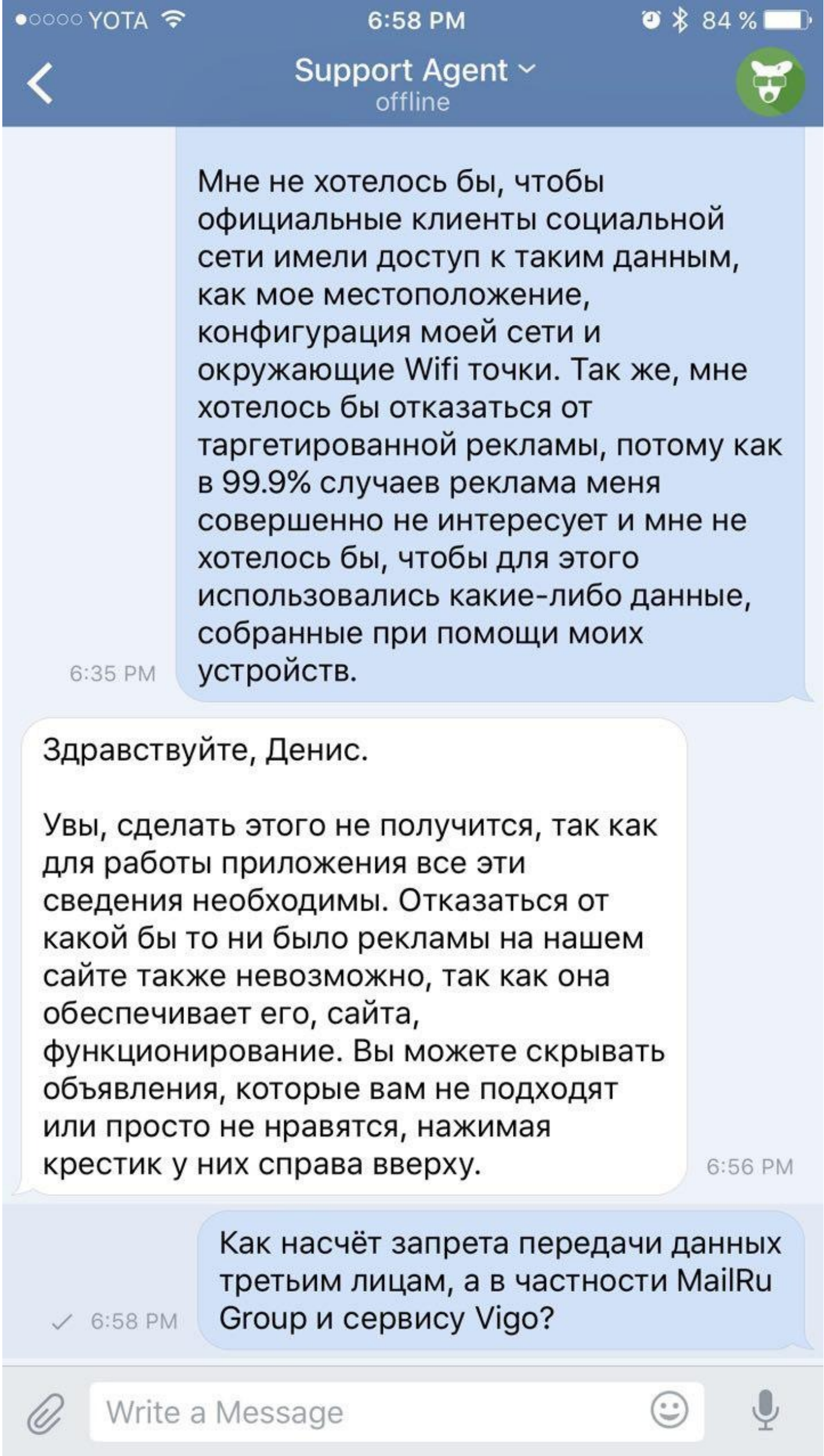
«По изначальному замыслу, точнее, как это мне все объясняли — "выбирать качество видео в зависимости от интернета". Естественно, я абсолютно не хотел сливать подобные данные ради этой никому не нужной мелочи. Хотели бы на самом деле сделать удобный просмотр видео с подстройкой качества под интернет — запилили бы DASH/HLS, как у настоящих видеохостингов. ...»

Отправка местоположения, как оказалось, производится только при просмотре отдельного поста. На аудиозаписи это не влияет, как некоторые стали считать, что в зависимости от региона некоторые треки "скрывается".

Update 5: Ответы от ВКонтакте

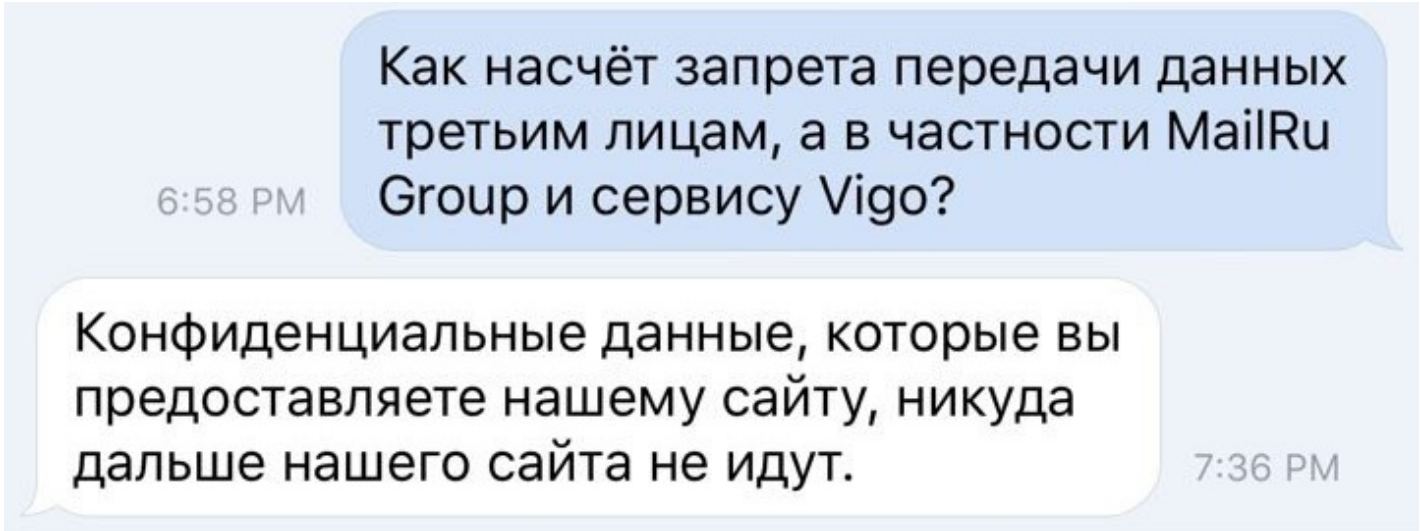
Мобильная техподдержка

Денис решил всё-таки добиться ответов на наши вопросы и задал их мобильной поддержке ВК (id333)



Оказывается, Ваше местоположение, данные для таргетинговой рекламы, список установленных приложений и сети Wi-Fi жизненно необходимы для приложения и сайта в целом.

В ответ на последний вопрос, поддержка решила отойти от темы.



О том, как это было получено

Подручные средства

У нас в распоряжении комп под Linux (Ubuntu 16.04 LTS), два телефона на Android 5.1 (Sony Xperia L) и 6.0.1 (Samsung *какой-то там*). У Sony выпилены Google Play Services. На обоих телефонах последняя версия приложения и стороннее приложение - Kate Mobile (версии 37 и 41 соответственно). Ну, и, естественно, единая локальная сеть, к которой подключен и комп, и два устройства.

Подготовка: создание сертификата SSL

Если просто начать sniffing, то мы получим лишь сырые данные, не поддающиеся обработке, поскольку они передаются по протоколу HTTPS - данные зашифрованы. Для того, чтобы получить данные такие, которые мы можем расшифровать, мы меняем сертификат на тот, который мы же и создали. Таким образом мы можем расшифровать этот трафик.

```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365
```

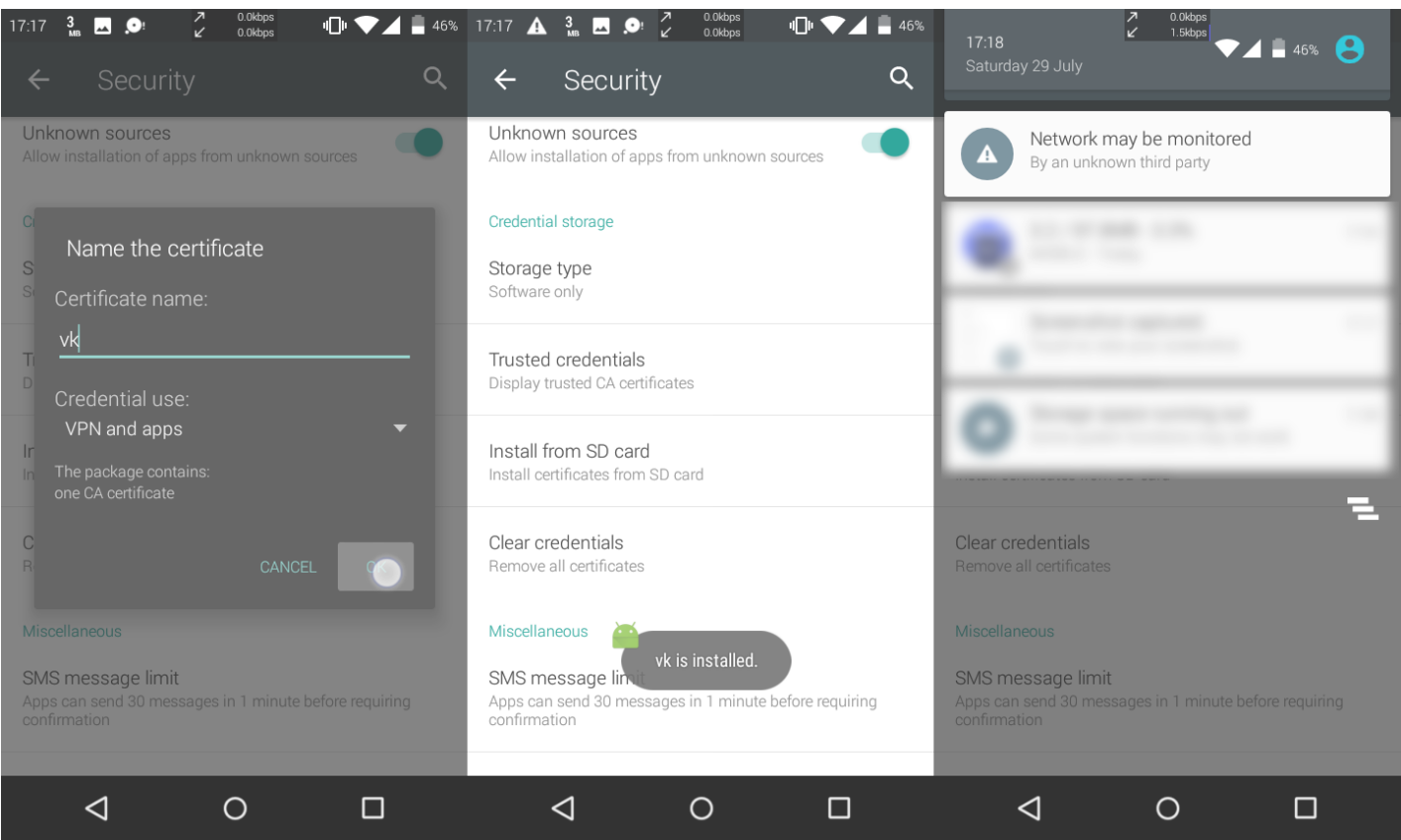
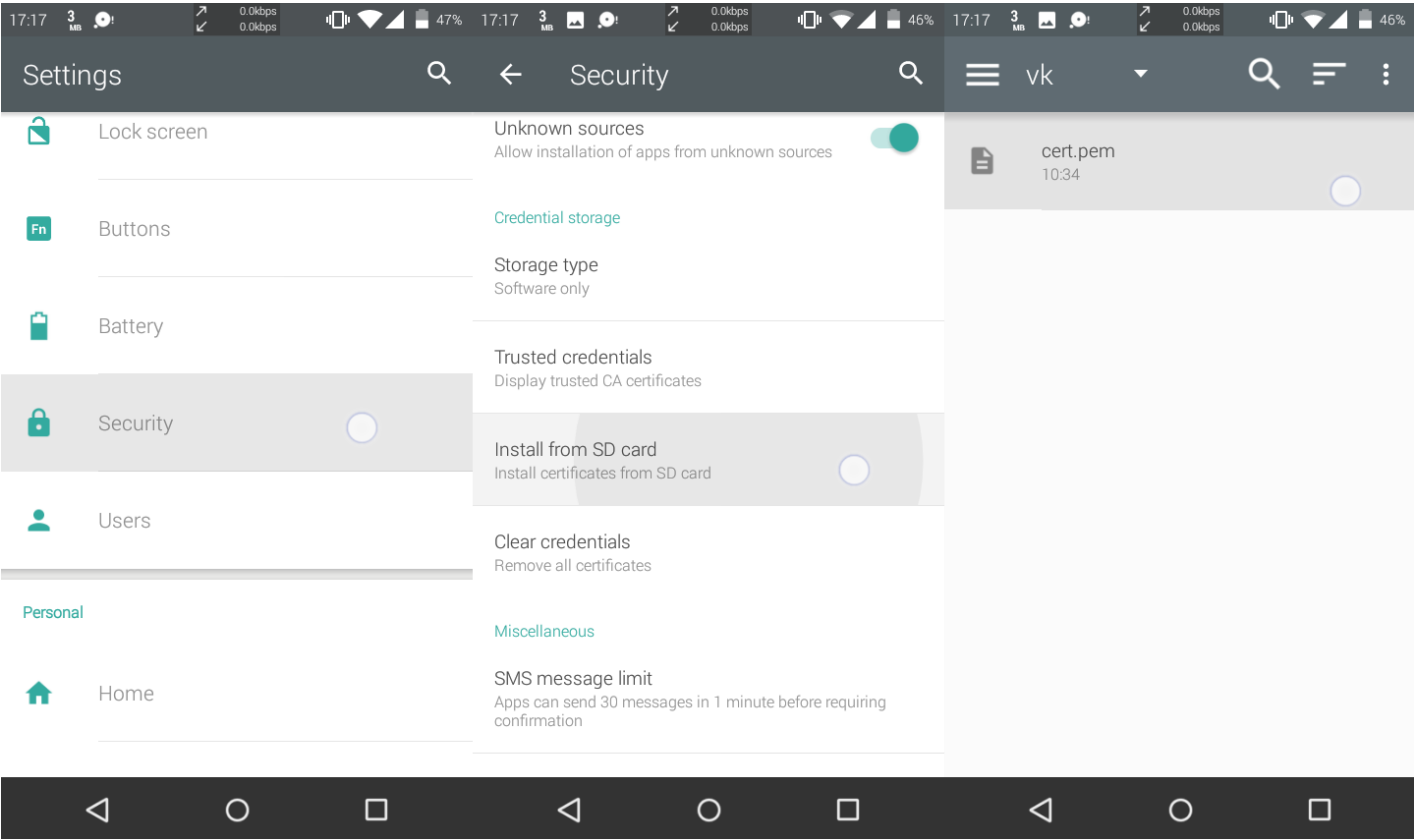
Этой командой создаем сертификат, где key.pem - файл ключа, cert.pem - сертификат.

В phrase key вводим что-то типа пароля. Он нам еще понадобится. Затем его еще раз повторить. Остальные поля можно оставить пустыми/не

вводить. По окончании в текущей директории будет создано два файла.

Подготовка: установка нашего сертификата на устройство

Передаем файл `cert.pem` на устройство и устанавливаем его в систему. Обращу внимание, что для установки сертификата необходимо, чтобы на телефоне была какая-нибудь защита на экране блокировки (графический ключ, пароль или PIN).



Пошаговая установка сертификата на Android 5.1

Сертификат установлен.

Подготовка: переброс портов

Возвращаемся на Linux, вбиваем в терминал:

```
sudo sysctl -w net.ipv4.ip_forward=1
sudo iptables -t nat -F
sudo iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-ports 8080
sudo iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-ports 8443
sudo iptables -t nat -A PREROUTING -p tcp --dport 587 -j REDIRECT --to-ports 8443
sudo iptables -t nat -A PREROUTING -p tcp --dport 465 -j REDIRECT --to-ports 8443
sudo iptables -t nat -A PREROUTING -p tcp --dport 993 -j REDIRECT --to-ports 8443
sudo iptables -t nat -A PREROUTING -p tcp --dport 5222 -j REDIRECT --to-ports 8080
```

Подготовка: Ettercap

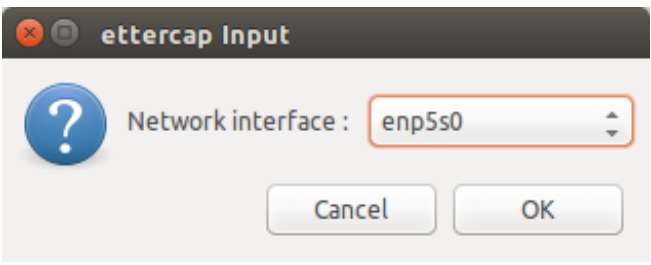
Устанавливаем Ettercap:

```
sudo apt-get -y install ettercap
```

После установки его запускаем.

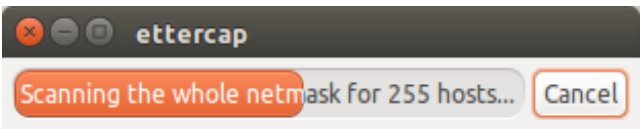
Сниффинг данных

Кликаем "Sniff" -> "Unified sniffing...". В окне выбора интерфейса обычно выбирается уже нужный (может быть `wlan0`, `wlp1s0`, `enp5s0`), если не тот - выбрать свой. "OK".



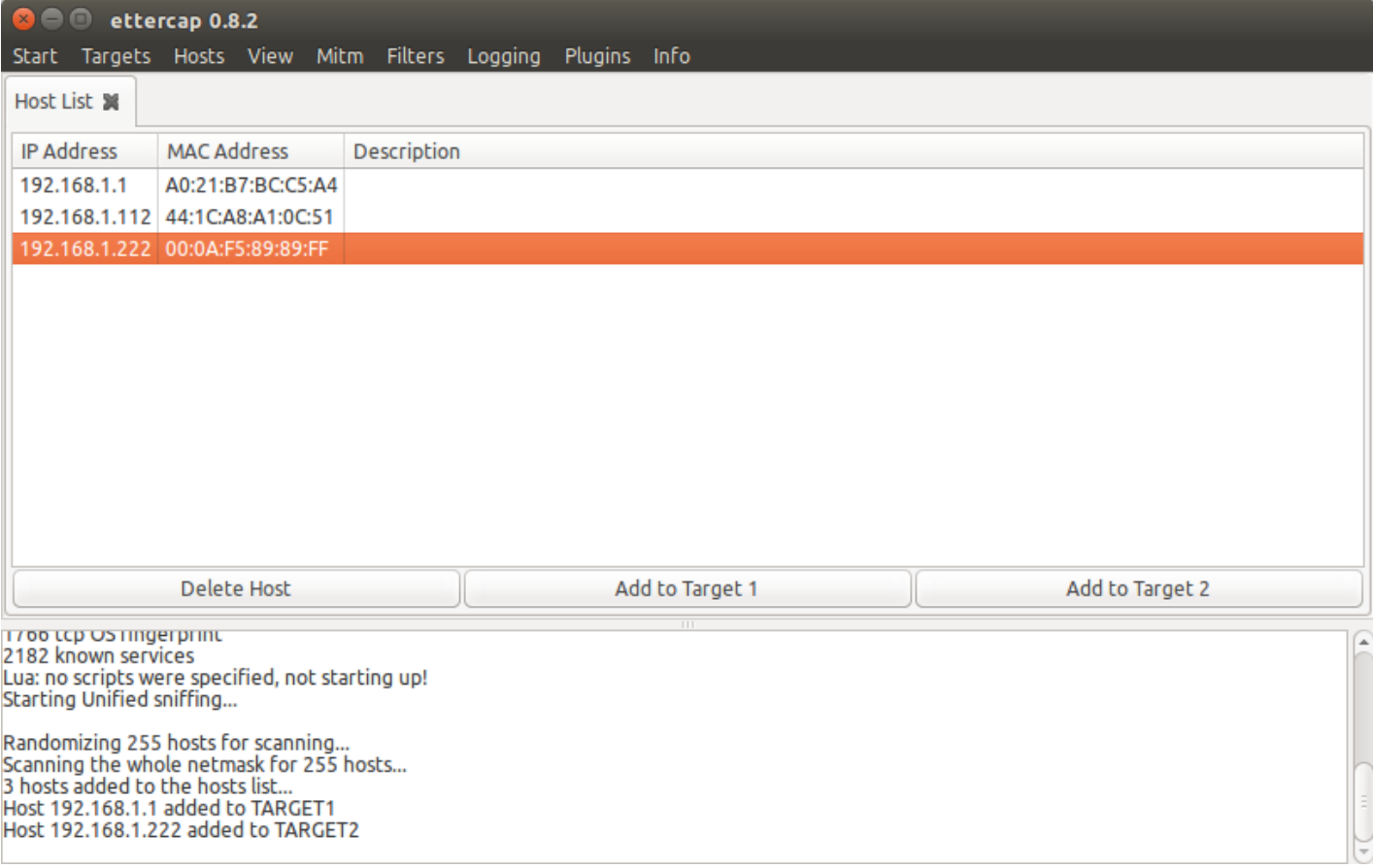
Выбор интерфейса

Далее: "Hosts" -> "Scan for hosts". Ожидаем сканирование хостов.



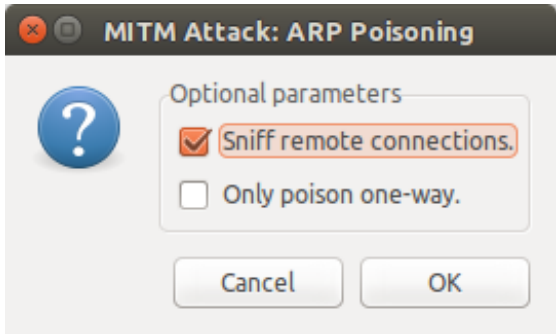
Сканирование хостов

Далее "Hosts" -> "Hosts list". В списке выбираем IP нашего роутера (у меня 192.168.1.1) и жмем "Add to target 1", затем выбираем IP устройства (у меня 192.168.1.222), затем "Add to target 2".



192.168.1.1 - роутер - target 1; 192.168.1.222 - телефон - target 2

Далее "Mitm" (Man in the Middle) -> "ARP Poisoning" -> ставим флаг "Sniff remote connections" -> "OK".



Далее "Start" -> "Start sniffing".

Конец подготовки: SSLSplit

Далее в терминале ставим sslsplit:

```
sudo apt-get -y install sslsplit
```

Когда установка завершена, создаем директории:

```
mkdir logs
```

И в текущей директории (где лежат файлы `cert.pem` и `key.pem`)

```
cp /dev/null logfile.log
```

Выходим из аккаунта в приложении на телефоне.

В текущей директории выполняем:

```
sudo sslsplit -k key.pem -c cert.pem -l logfile.log -j logs -S . https 0.0.0.0 8443 http 0.0.0.0 8080
```

Вводим phrase `key`, который указывали при создании сертификата.

В `logfile.log` будут записываться неполные логи (именно домен, адрес, порт), в директорию `logs` будут записываться подробные запросы, заголовки и ответы.

Далее авторизуемся в приложении и видим, как в терминале, в `logfile.log` и в директории `logs` появляются данные. Для остановки сниффинга жмем в терминале `Ctrl+C`.

Логи в директории logs будут записываться под владельцем и группой root без доступа к чтению и записи от текущего пользователя. Поэтому нужно изменить владельца. В директории с сертификатами вводим

```
sudo chown -R vlad805:vlad805 logs
```

Где вместо "vlad805" - имя Вашего пользователя.

Далее можно просматривать файлы с помощью обычного текстового редактора.

Update

Как позже подсказал [Антон](#), снифинг можно выполнить двумя кликами с помощью приложений для Android, и тогда вот эта длинная инструкция не понадобится. Но... кому как удобнее.

Благодарности

Также выражается благодарность [Константину](#) за наводку и подробную инструкцию по снифингу.

Обсуждение

Здесь в комменариях: https://vk.com/wall23048942_5017

Продолжение

Перейти ко [второй части](#).