Лаба 3

Требования к 3й лабе (WireShark) : 10 интересных перехваченных пакетов. Интерес представляет те пакеты, которые могут харакетриозвать другого пользователя (аккаунты, приложения, название устройства в случае с Apple и т. д.), можно указать в качестве интересного сообщения и mac-адрес устройства, но только 1 из 10 сообщений.

Скачиваем вайршарк



Читаем гайдик о том, как работает TLS и как сделать расшифровку

<https://wiki.wireshark.org/TLS#using-the-pre-master-secret>

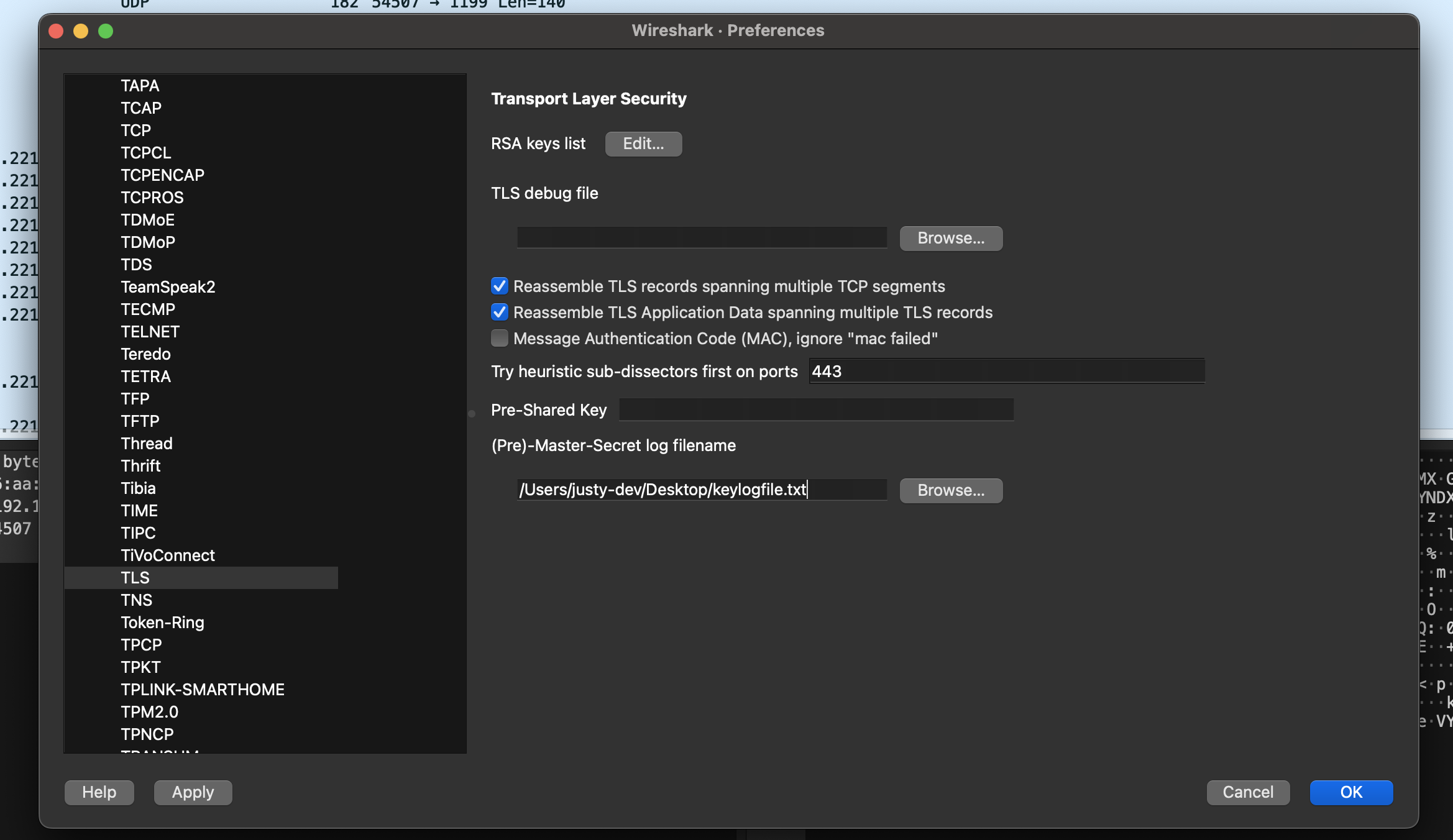
Для мака нужно открыть браузер с переменной

export SSLKEYLOGFILE=$HOME/Desktop/keylogfile.txt

open -a yandex

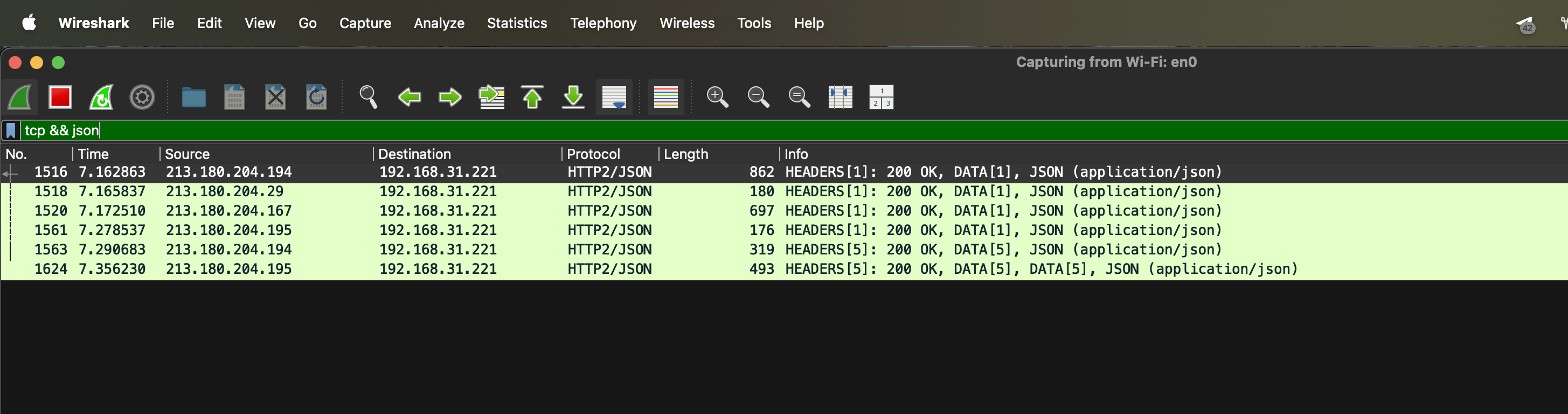
В этом файле либа, которую браузер использует для расшифровки SSL сертификатом. Там будет дамп ключей, и вайршарк сможет его сохранить.

Идём в настройки и ставим этот файл вайлшарку

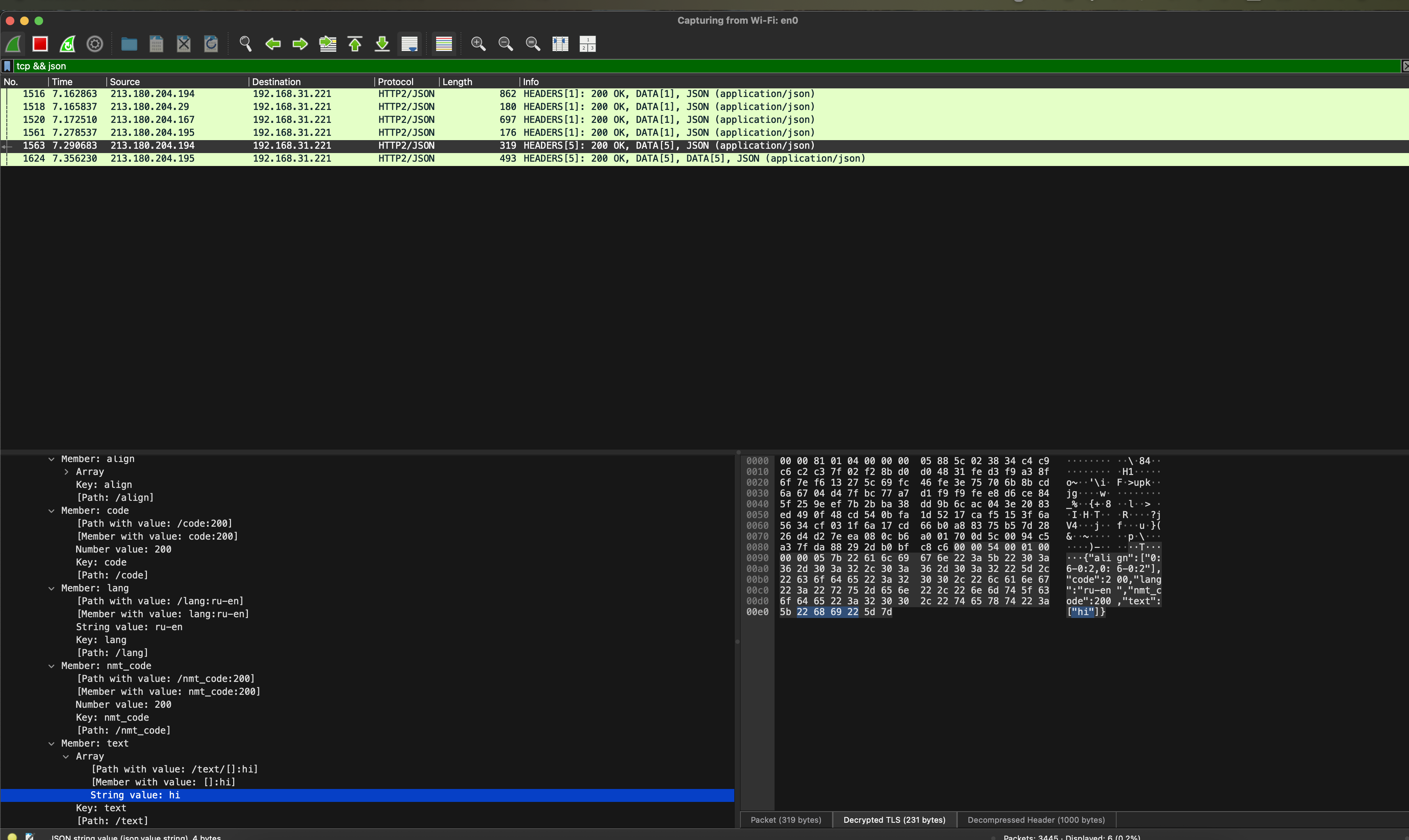


Дальше можно поставить фильтр, анпример json, чтобы видеть запросики и ищем что-то интересное. Поставил фильтр json && tcp, чтобы видеть соединения в браузере.

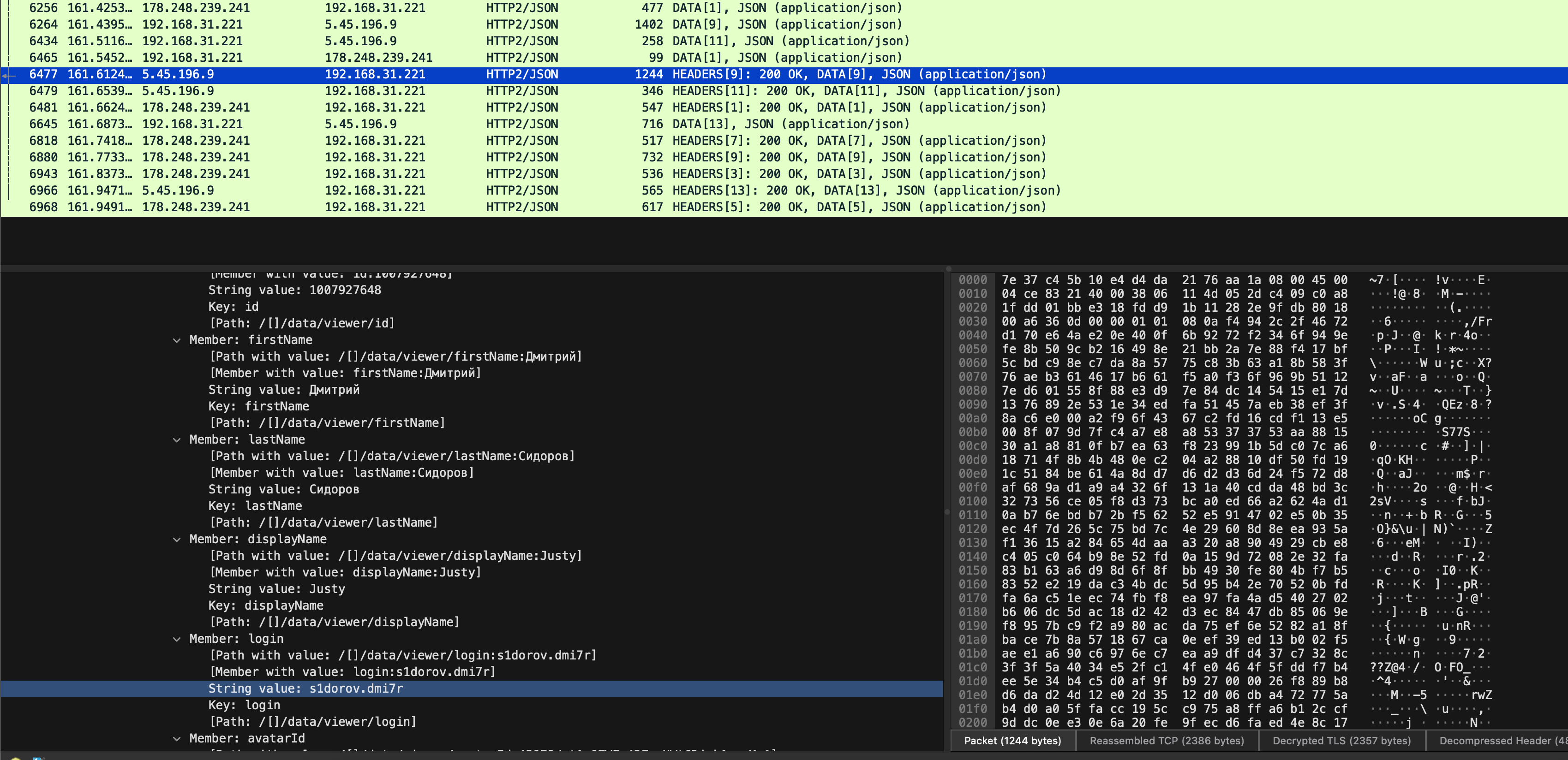
1. Заходим в переводчик и переподим слово, сразу видим json запросы



Видим в запросе как исходящий пакет, так и пришедший, в пришедшем видем введёное в перевод слово

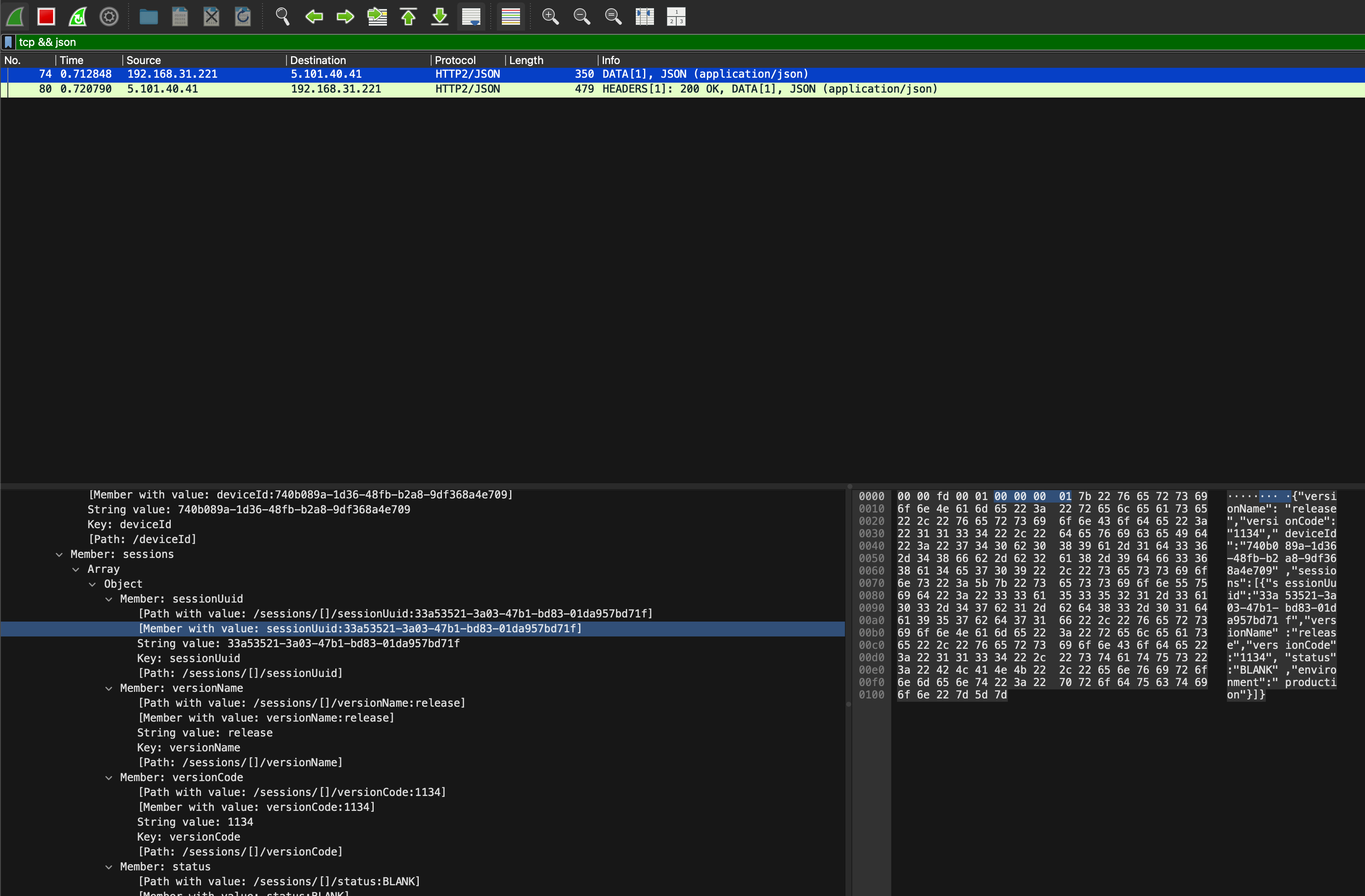


Далее заходим в пей и также по запросам видим личные данные

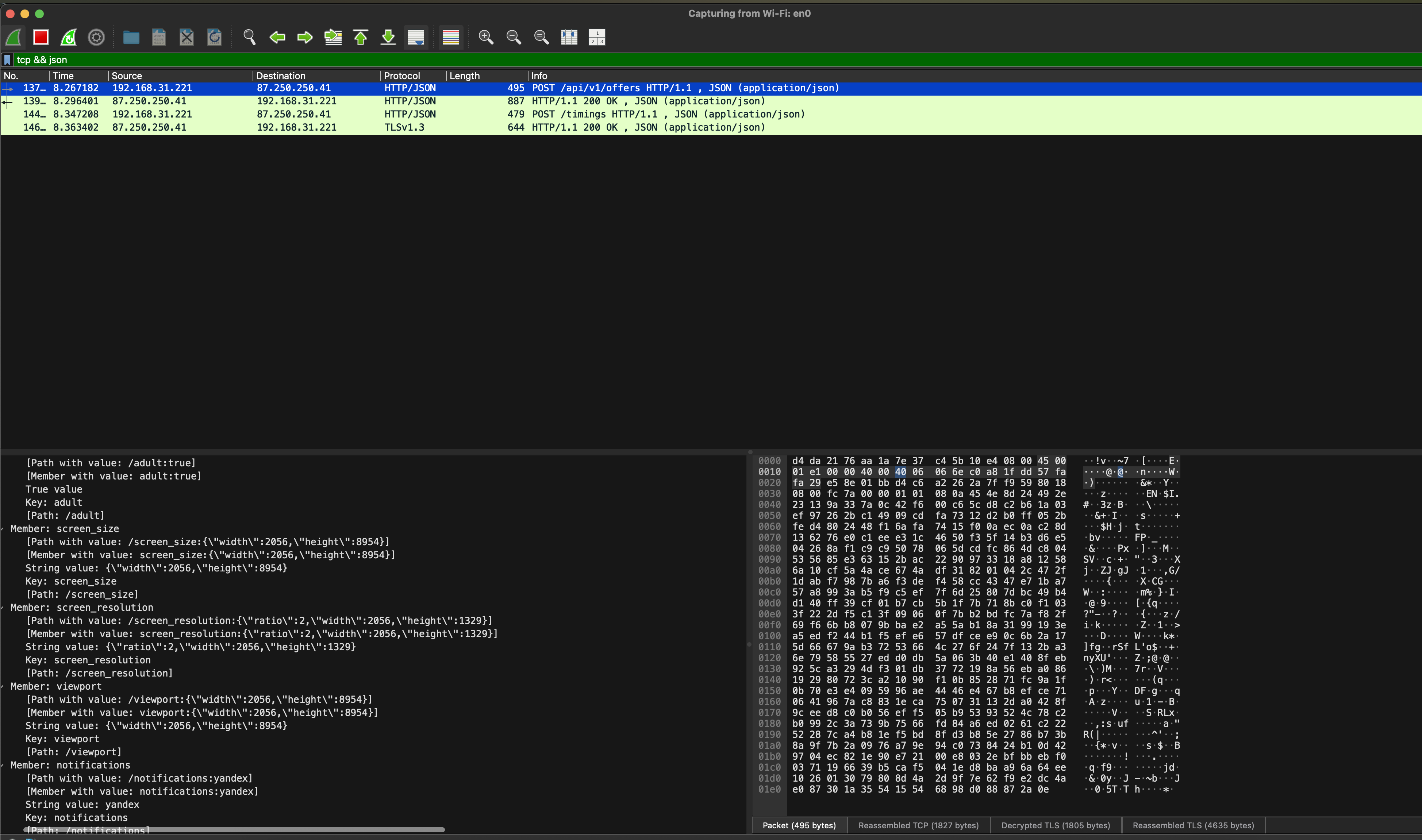


Имя, фамилию, почту и т.д.

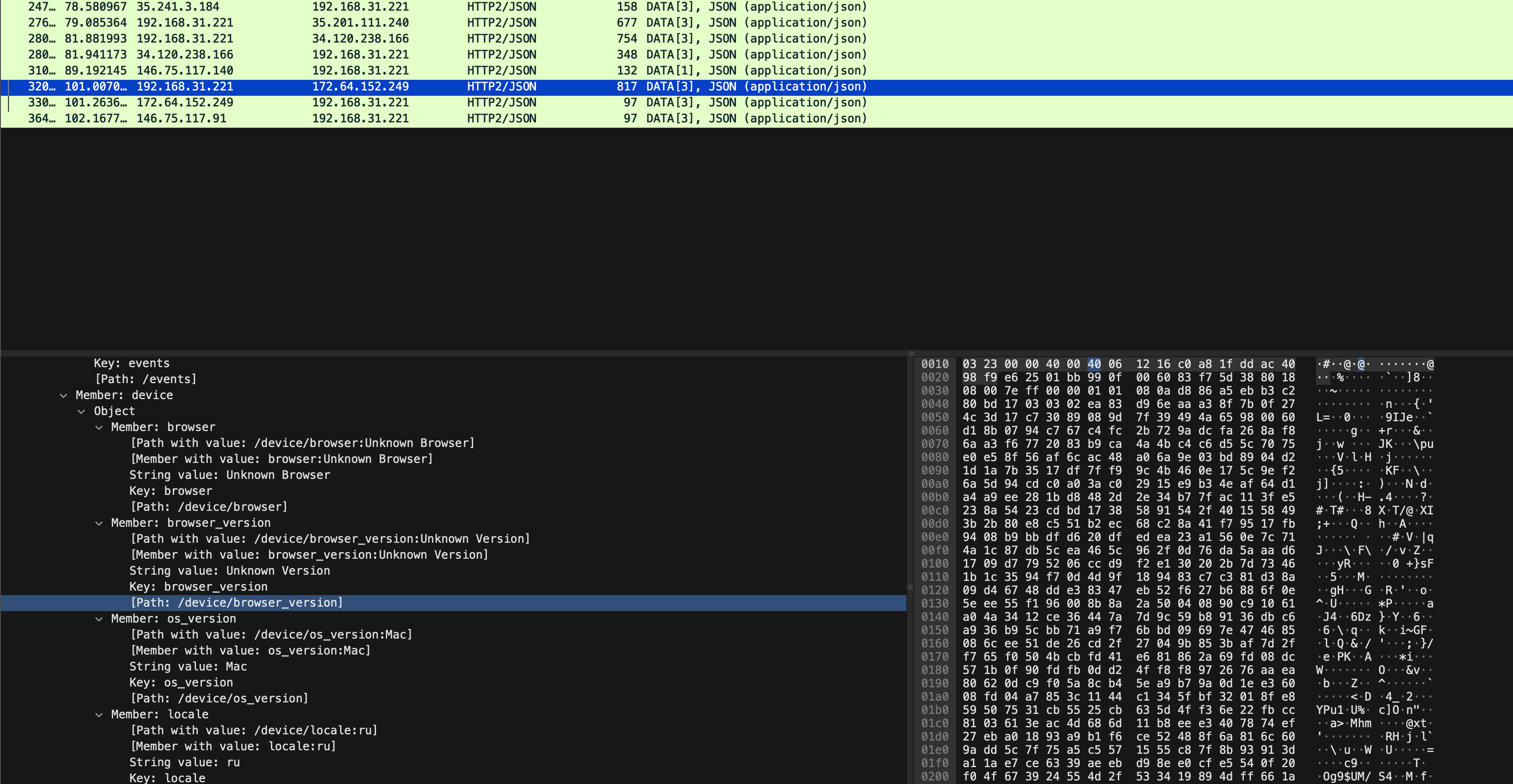
1. Заходим на сайт вк и видим в запросах session uid, а также все кукисы



Заходим на озон и видим данные которые улетели при заходе в корзину, например размер экрана, а прилетели данные о товарах



Далее идём на фейсит, видим улетевшие даннеые об устройстве, браузер, система



Аналогичным образом делаем на других сервисах, перехватывая запросы.