

Снифферы. Charles

Часть 1

Содержание

- Сравнение Charles и Fiddler
- Charles. Начало работы
- Установка сертификата на устройство
- Режим Sequence
- Режим Structure
- Функция Breakpoints. Настройка
- Функция Breakpoints. Перехват
- Функция Rewrite
- Rewrite Rule
- Map Local

Charles,

Плюсы

- Кроссплатформенность..
- Удобная панель инструментов с такими функциями как очищение сессии, редактирование и перевыполнение запроса, остановкой перехвата трафика и другими.
- Классификация запросов по хостам.
- Возможность экспортировать настройки.
- Возможность просматривать несколько сессий в соседних закладках.

Минусы

- Нет возможности наложить таймаут на запрос.
- Нет возможности экспортировать сессию в формате txt или json.
- Это платный инструмент

Fiddler Classic,

Плюсы

- Удобная подмена ответов.
- Много функций вынесены на панель инструментов
- Возможность цветового выделения запросов.
- Бесплатный инструмент
- Два способа редактирования запросов

Минусы

- Только под Windows
- Редактирование ответа только в текстовом формате

Fiddler Everywhere

Плюсы

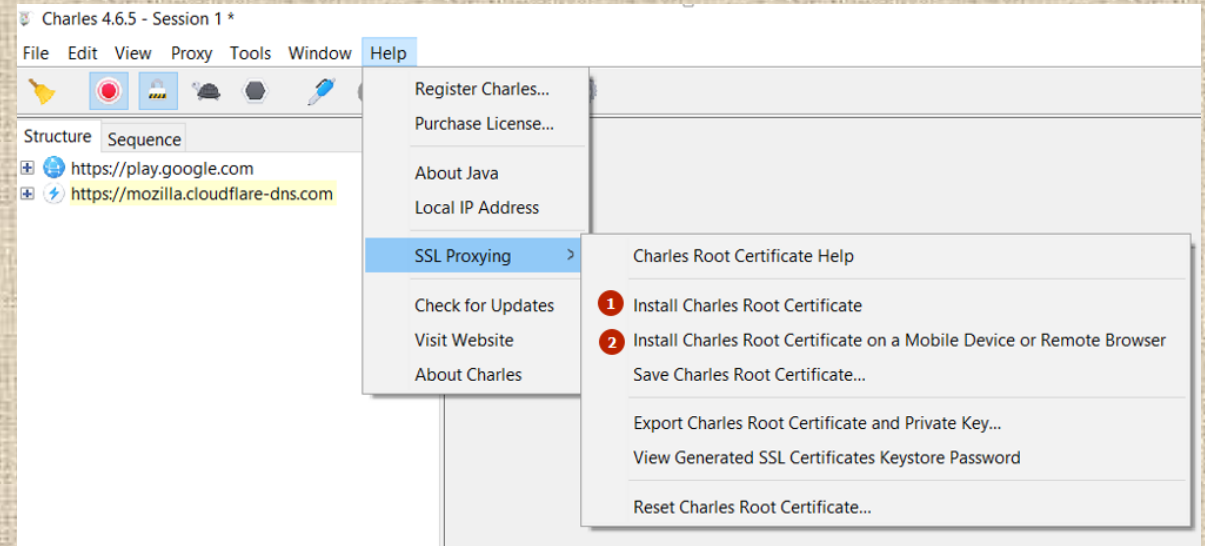
- Кроссплатформенность
- Удобные фильтры запросов
Сохранение сессий внутри инструмента
- Отправка сессий другим пользователям
- Сохранение коллекций.

Минусы

- Нет брейкпоинтов.
- Это платный инструмент

Charles. Начало работы

1. Установка сертификата безопасности на ПК
2. Установка сертификата безопасности на мобильное устройство (см. след слайд)



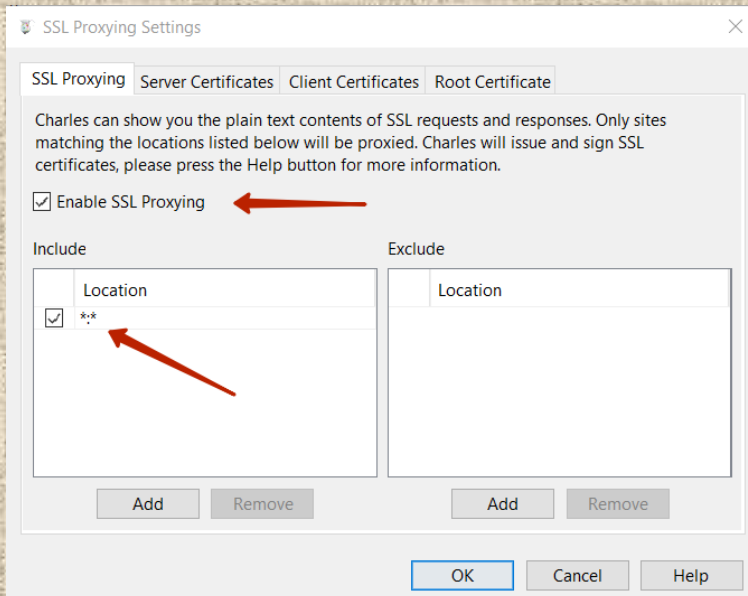
3. Настройка расшифровки протоколов: меню Proxy -> SSL Proxying Settings

Во окне SSL Proxying находятся два блока:

Include: здесь указывают ресурсы или хосты, которые нужно расшифровать. *.* для расшифровки всех запросов

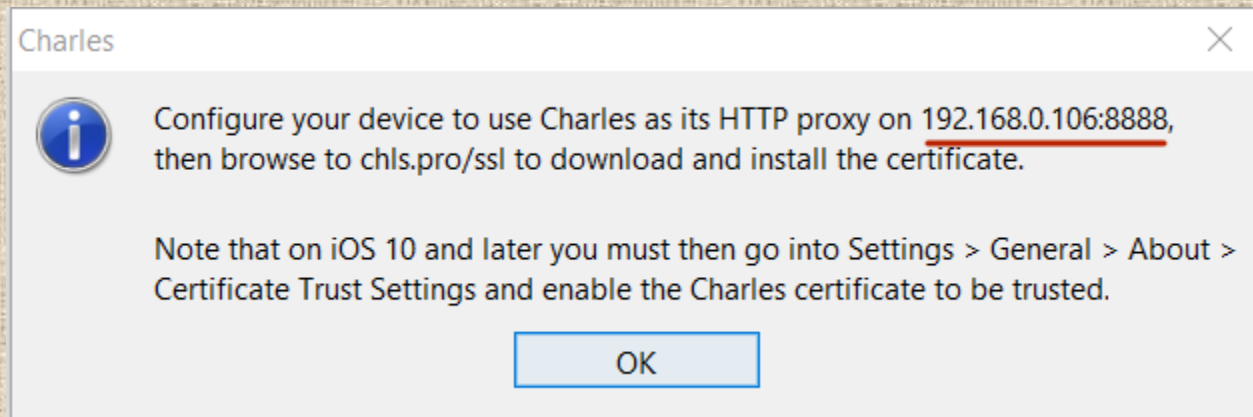
Exclude: здесь указывают ресурсы, которые нужно исключить из расшифровки.

4. Убедись, что в меню Proxy стоит галочка напротив Windows Proxy или macOS Proxy



Установка сертификата на устройство

Help -> SSL Proxying -> Install Root Certificate on a Mobile Device or Remote Browser.

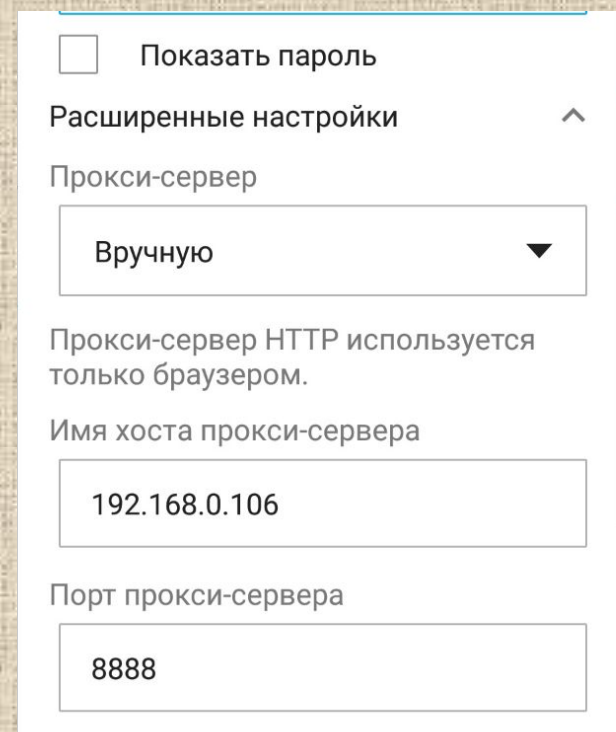


Настройки -> Настройки сети -> «Прокси» выбираем параметр «Вручную»

В поле «Имя хоста прокси» вводим ip, а в поле «Порт прокси» - порт, которые получили в открывшемся окошке Charles`а

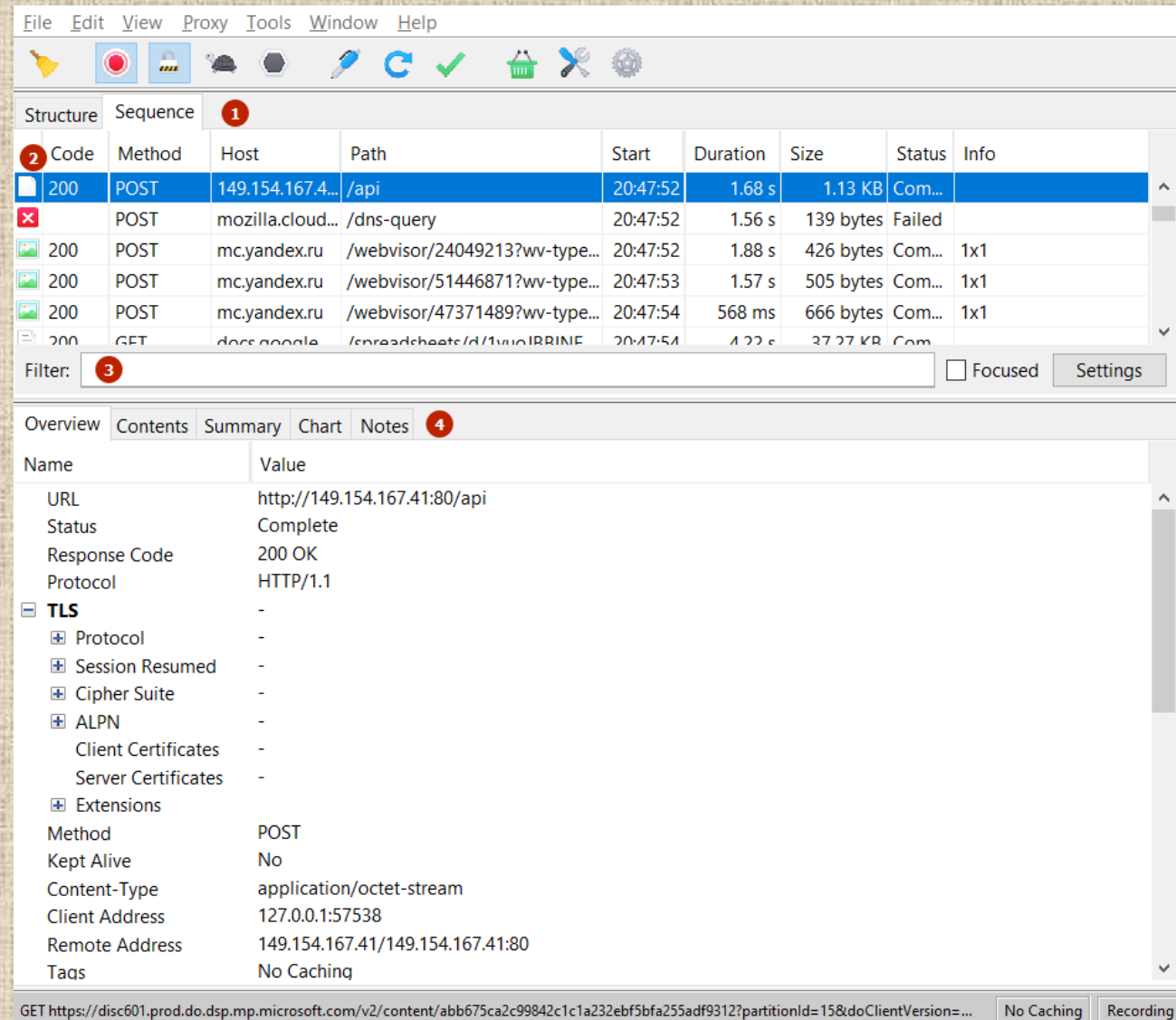
После того, как сохранили настройки сети, в окне Charles должно появиться уведомление с просьбой разрешить или отклонить доступ к девайсу. Жмем «Разрешить»/«Allow».

Вводим в браузере **телефона** следующий URL: <http://chls.pro/ssl> или charlesproxy.com/getssl, скачиваем и устанавливаем сертификат



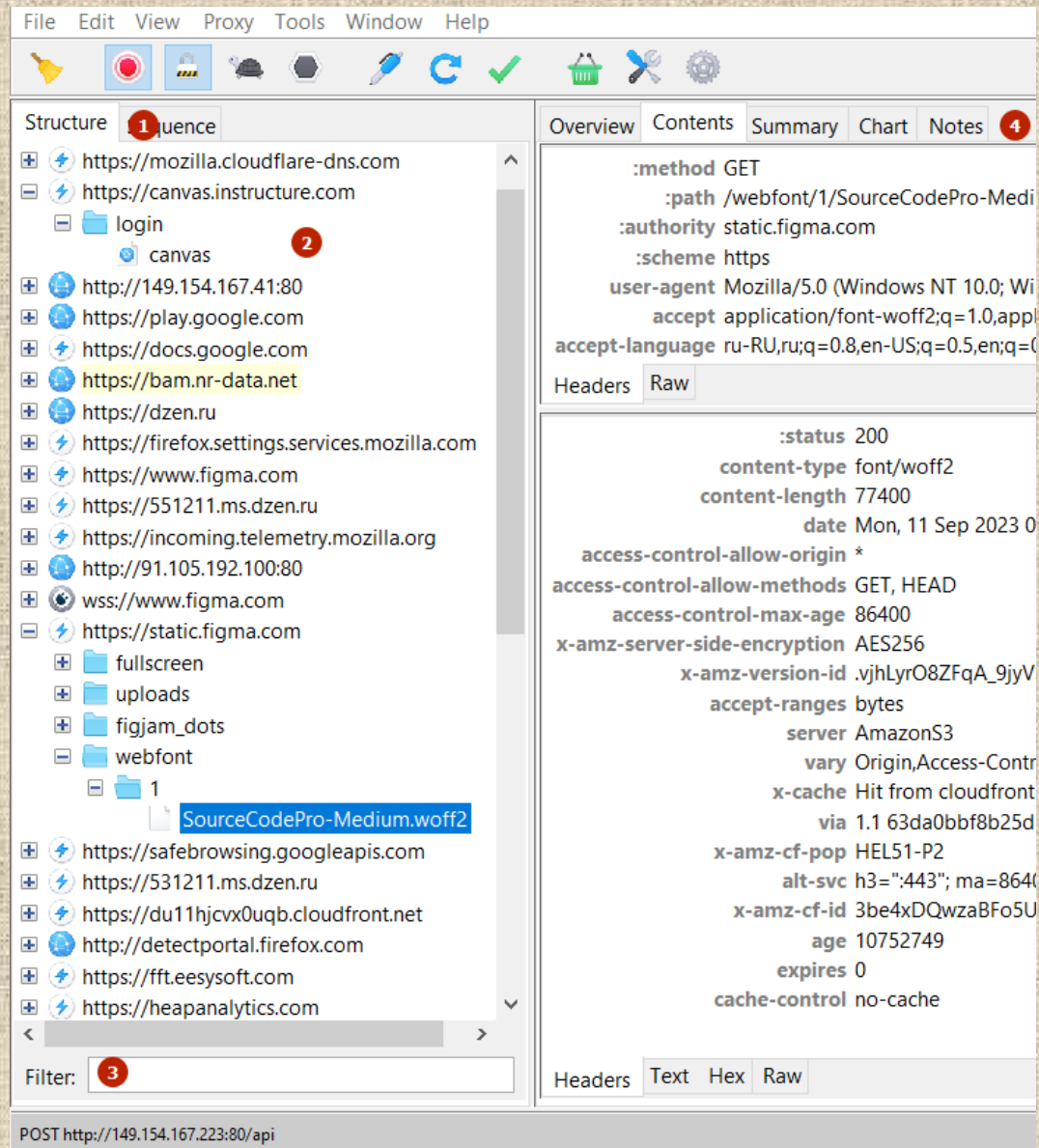
(1) Режим Sequence

2. Ресурсы отображаются в хронологическом порядке: от недавнего — к старым.
3. Поле Filter : можно ввести только хост или весь запрос целиком.
4. Вкладки Overview, Content, Summary, Chart, Notes



(1) Режим Structure

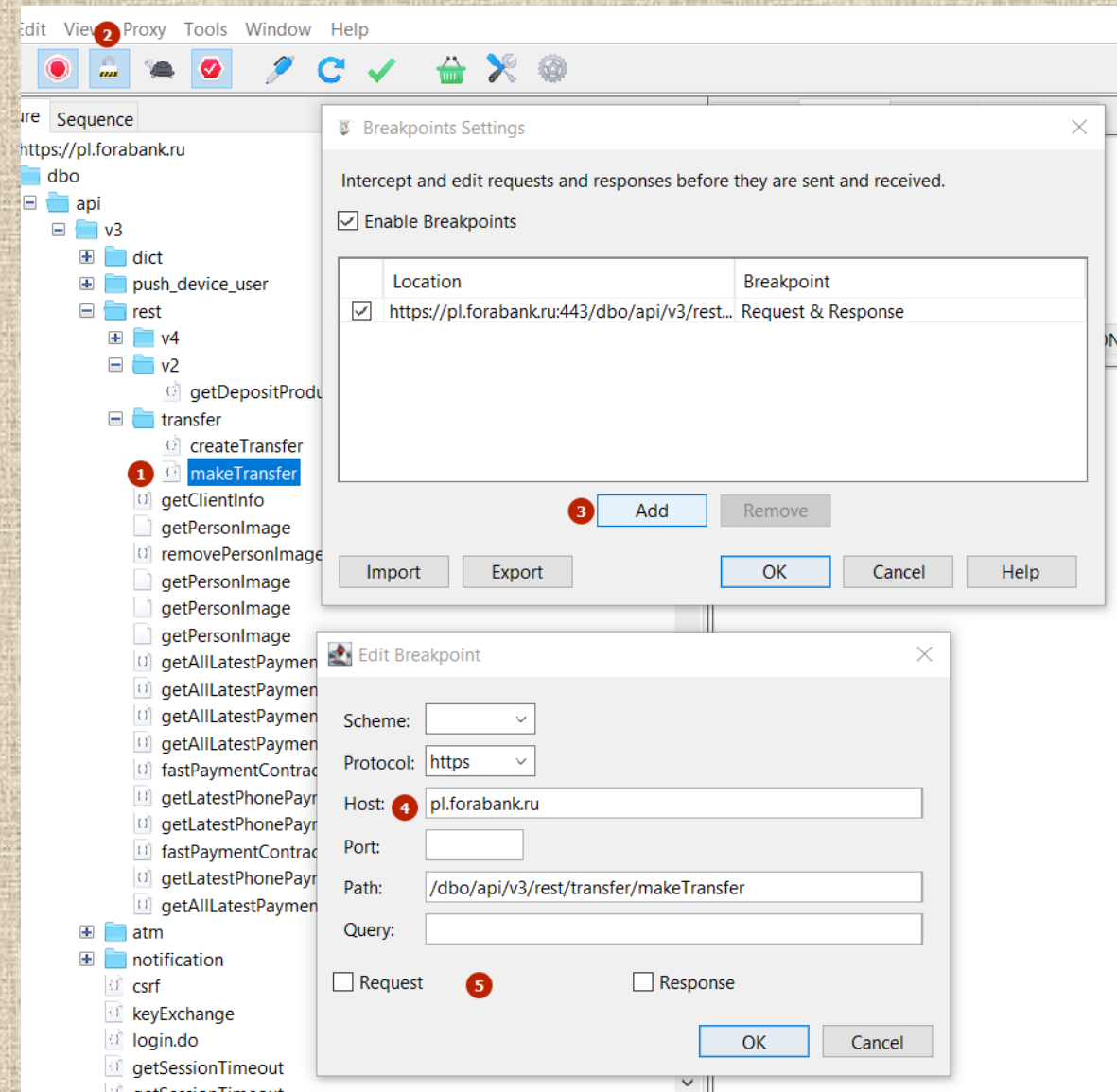
2. Ресурсы группируются по хостам (host) и путям (path)
3. Через поле Filter можно искать только по хосту
4. Вкладки Overview, Content, Summary, Chart, Notes



Функция Breakpoints. Настройка

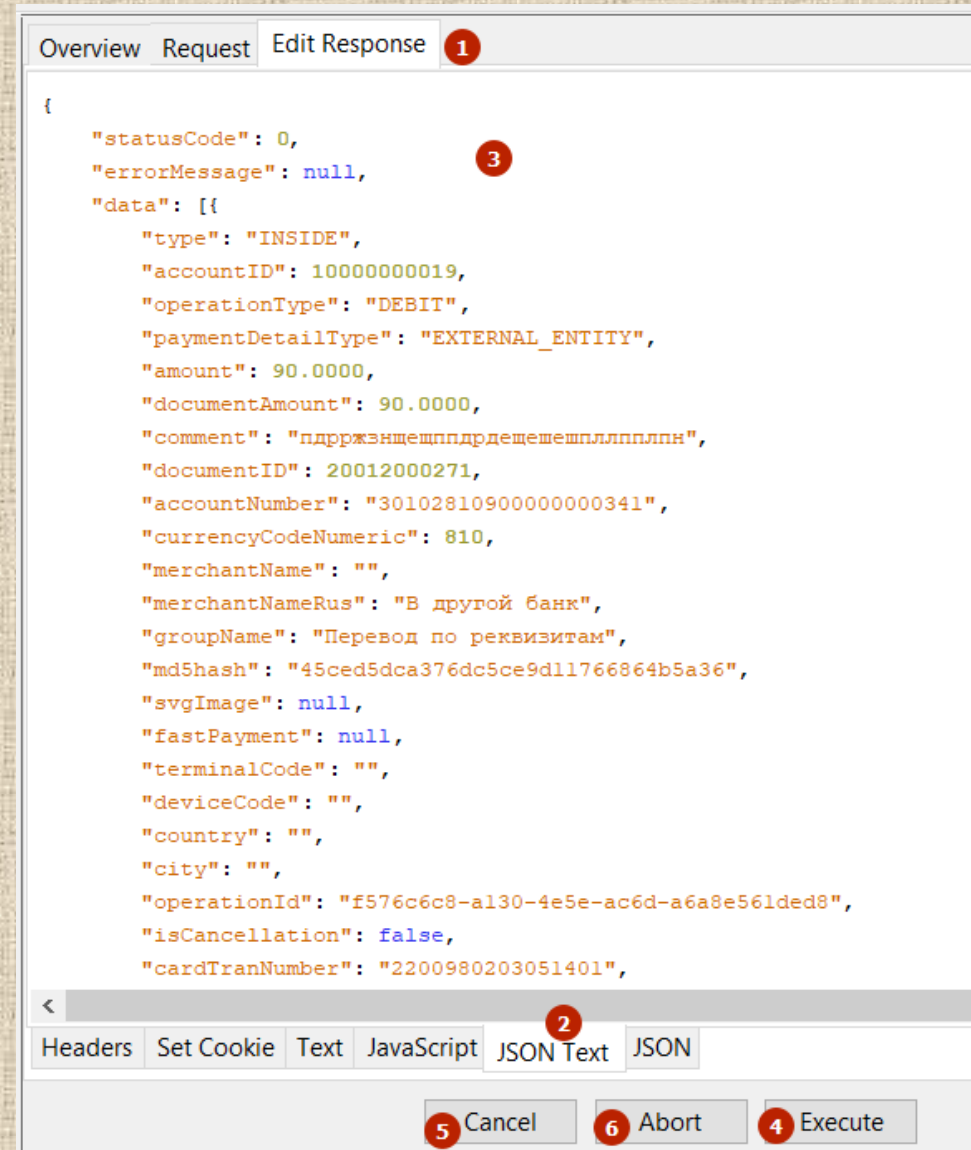
1. ПКМ по нужному запросу Copy URL
2. меню Proxy -> Breakpoint Settings
3. Add
4. В поле Host Ctrl+V
5. отмечаем, что хотим перехватить: Request и/или Response

Можно быстрее: ПКМ по нужному запросу поставить галочку у Breakpoints, по умолчанию к перехвату добавляется и запрос и ответ



Функция Breakpoints. Перехват

1. Edit Request/Response - отредактировать запрос/ответ
2. Выбрать что и в каком формате редактировать
3. Поле доступно для редактирования
4. Execute - применяет внесенные изменения и пропускает запрос/ответ дальше
5. Cancel - отменяет изменения, внесенные за время работы breakpoint, и пропускает запрос/ответ дальше в оригинальном виде.
6. Abort - сбрасывает запрос/ответ и возвращает ошибку.

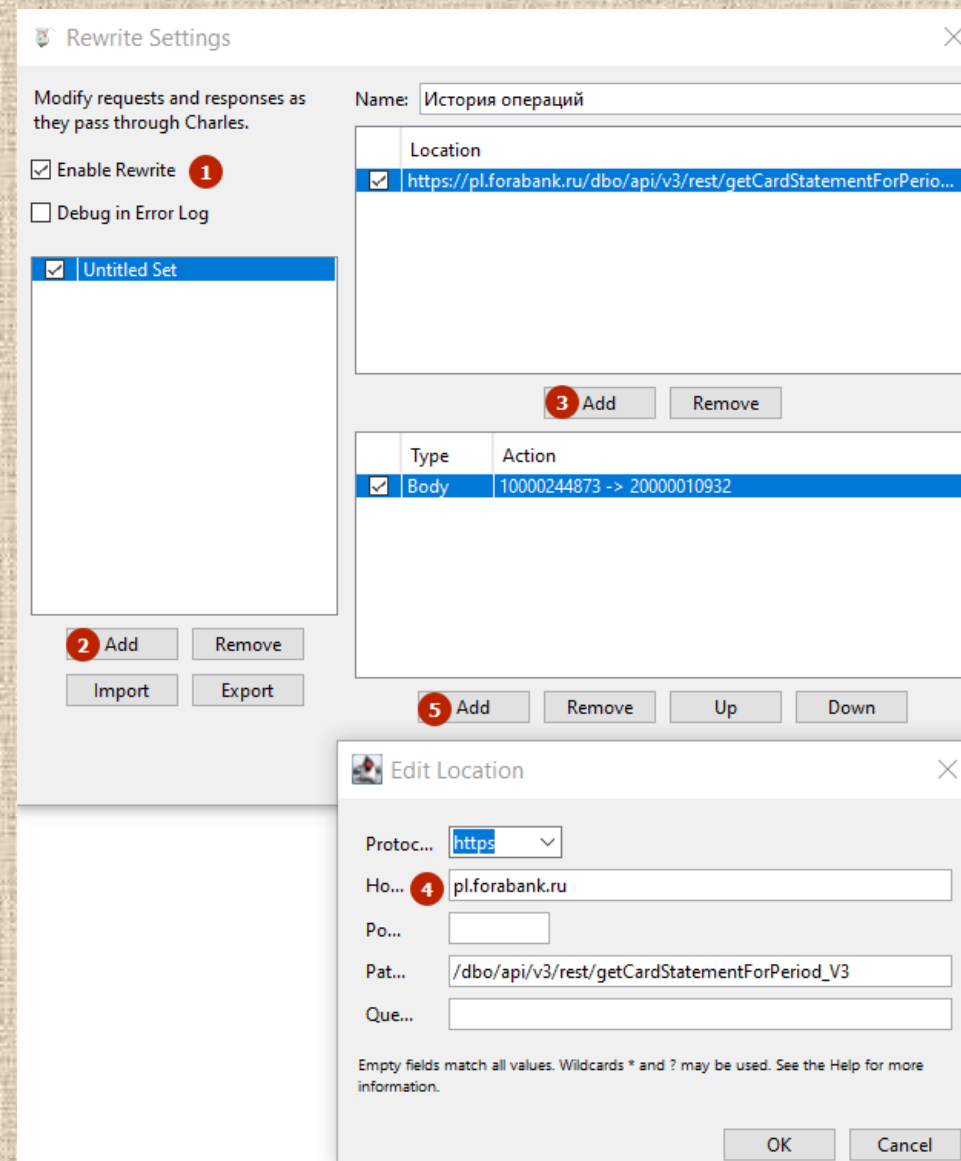


Функция Rewrite

ПКМ по нужному запросу Copy URL

Меню Tools -> Rewrite

1. Включение режима Rewrite
2. Добавление правила
3. Добавление локации перехвата
4. URL запроса
5. Добавление правила подмены



Rewrite Rule

1. Тип подмены (Работа с заголовками, URL, Query-параметрами, Response Status, телом запроса)
2. Подменять запрос и/или ответ
3. Блок Match: что именно нужно подменить
4. Replace: на что именно нужно подменить значение
5. Replace first заменяет первое совпадающее значение. Replace all — все совпадающие значения

The screenshot shows the 'Rewrite Rule' dialog box with the following configuration and annotations:

- 1** Type: Body
- 2** Where: ☒ Request, ☒ Response
- 3** Match: Value: 10000244873
- 4** Replace: Value: 20000010932
- 5** Replace: ☐ Replace first, ☒ Replace all

Buttons at the bottom: OK, Cancel, Help.

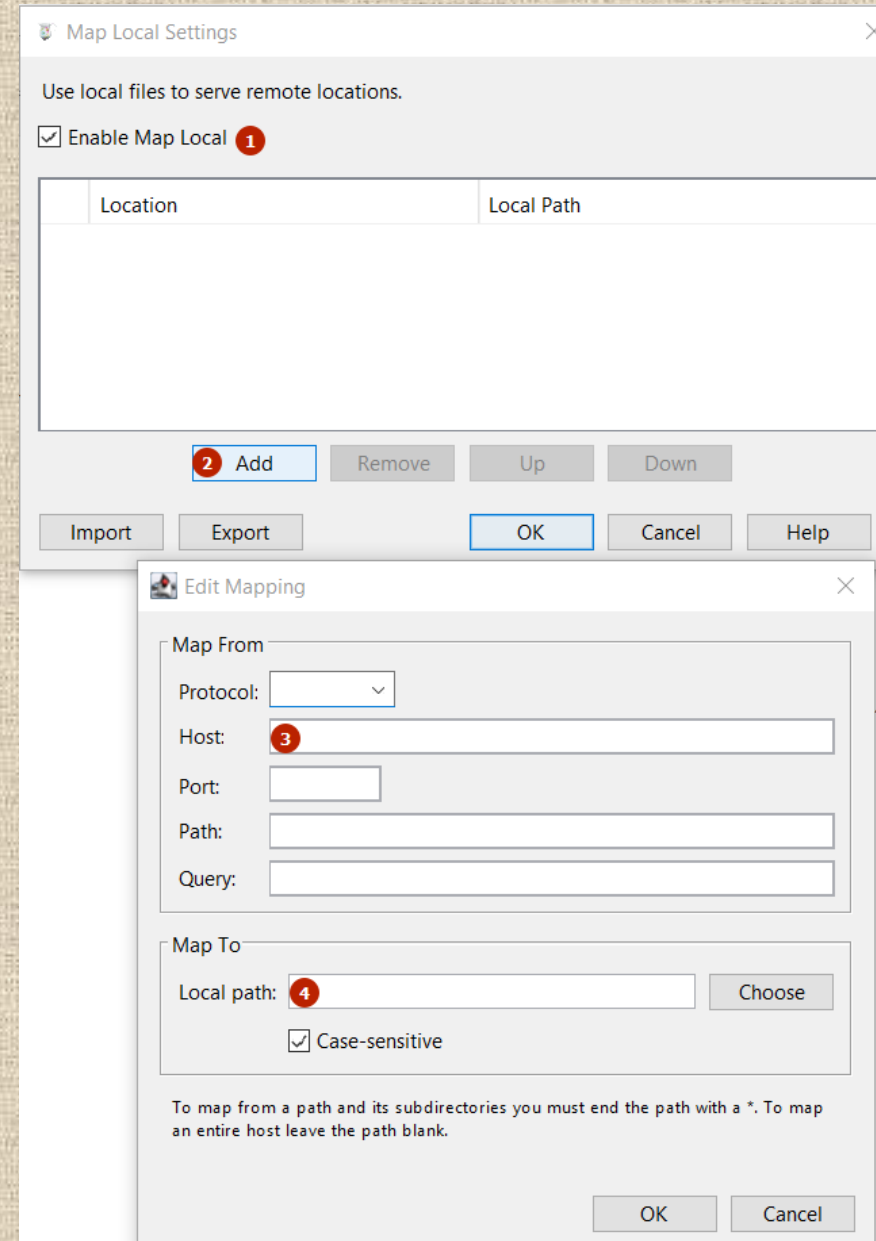
Функция Map Local

Нужно создать на компьютере файл с json

ПКМ по нужному запросу Copy URL

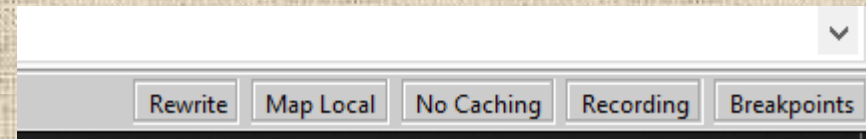
Tools -> Map Local

1. Включение Map Local
2. Добавление правила подмены
3. URL, который нужно подменить
4. Путь до файла для подмены



Полезности

- Панель быстрого доступа
- Правый нижний угол окна Charles
- Tools (Инструменты) -> No Caching...



Установка сертификата

- **Windows:** Install Charles Root Certificate -> Установить сертификат-> Текущий пользователь -> Поместить все сертификаты в следующее хранилище -> Обзор... -> Доверенные корневые центры сертификации. В остальных пунктах нажми «Далее». После установки Windows покажет предупреждение. Нажми «Yes» или «Да»
- **macOS:** Install Charles Root Certificate -> Установить сертификат-> «Связка ключей» найди добавленный сертификат. В разделе «Доверие» нужно заменить на «Всегда доверять»

Ссылки на полезные ресурсы и не только

- Установка CharlesProxy <https://www.charlesproxy.com/download/>
- Установка сертификатов <http://chls.pro/ssl> или charlesproxy.com/getssl
- Больше об установке <https://testengineer.ru/charles-proxy-quick-guide/>
- Настройка сертификата на мобильном устройстве
<https://habr.com/ru/companies/sbermegamarket/articles/690220/>
- Чуть больше о сравнении **Charles** и **Fiddler**
<https://habr.com/ru/companies/atisu/articles/583334/>
- Чуть больше о **Breakpoints** и **Rewrite**
<https://habr.com/ru/companies/redmadrobot/articles/269109/>
- **Очень(!!!)** полезная статья обо всем или почти обо всем
<https://habr.com/ru/companies/youla/articles/527648/>