**МИНОБРНАУКИ РОССИИ ФЕДЕРАЛЬНОЕ**

**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ**

**УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО**

**ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ**

**УНИВЕРСИТЕТ» (ФГБОУ ВО «ВГУ»)**

**ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ, ИНФОРМАТИКИ И**

**МЕХАНИКИ**

Дисциплина «Безопасность мобильных устройств»

Направление 02.04.02 «Фундаментальная информатика и

информационные технологии»

Лабораторная работа №1

Выполнила магистры 2 курса 13 группы:

Бутузова Д. О.

Преподаватель:

Воронеж 2025

**Введение**

В данном отчёте рассматривается демонстрация атаки «человек посередине» с помощью программы Charles Proxy. Для эксперимента использован публичный API сайта <https://reqres.in>, а также мобильное устройство, подключённое к локальной сети.

**Цели**

1. Изучение возможностей Charles Proxy:

* Перехват HTTPS-трафика;
* Установка SSL-сертификата;
* Изменение и повторная отправка запросов (Breakpoints, Repeat, Compose);
* Фильтрация трафика.

1. Моделирование MITM-сценария на примере логина

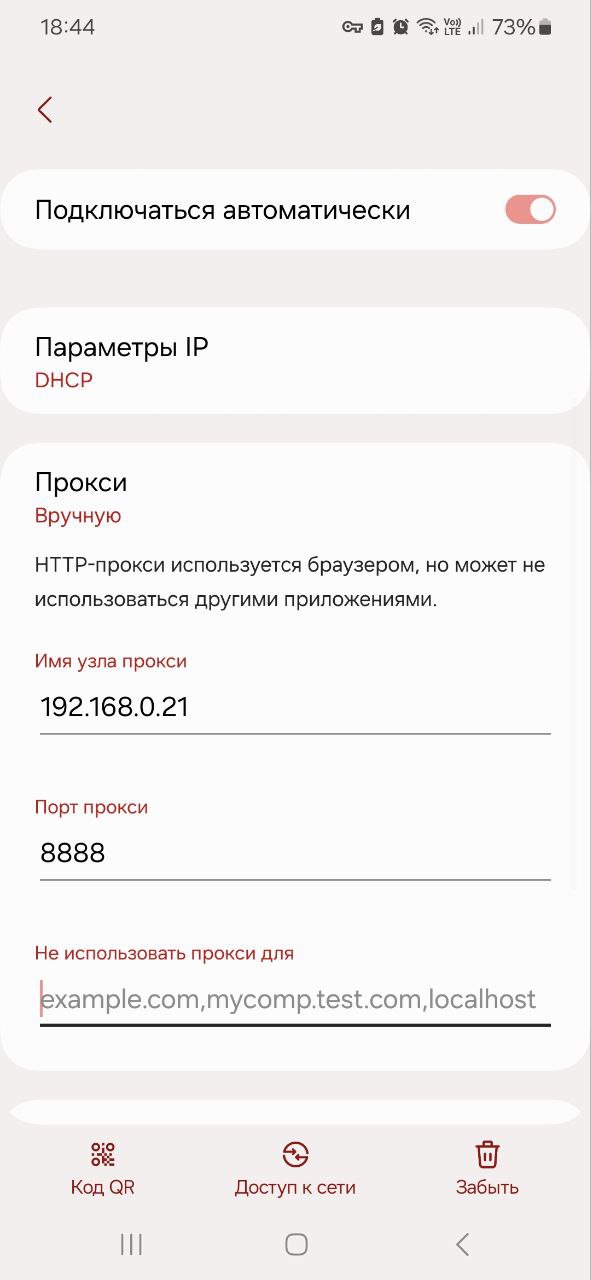
**Подготовка окружения**

**1. Установка и запуск Charles Proxy**

* Скачан и установлен Charles Proxy с официального сайта
* Запущен на ПК (macOS)

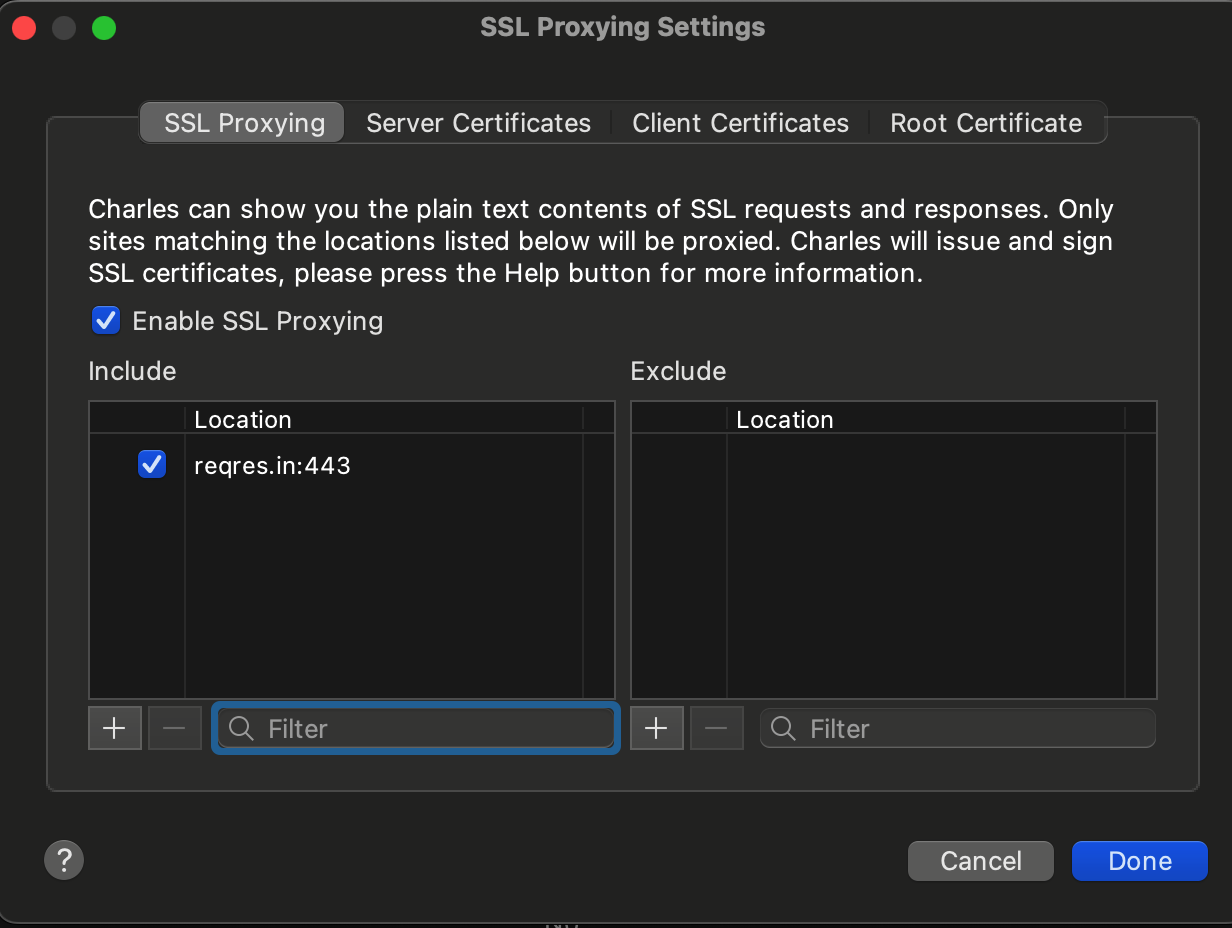
**2. Настройка прокси на телефоне**

* Телефон(Андроид) и ПК подключены к одной Wi-Fi сети;
* На телефоне вручную задан HTTP-прокси:
  + IP-адрес ПК: 192.168.1.ХХ
  + Порт: 8888



**3.** **Установка SSL-сертификата**

1. На телефоне открыт http://chls.pro/ssl в браузере;
2. Сертификат установлен и включено доверие.



**Демонстрация перехвата и изменения запроса**

**1. Запрос авторизации на сайте reqres.in**

* С телефона открыт сайт https://reqres.in
* Отправлен POST-запрос через форму авторизации:

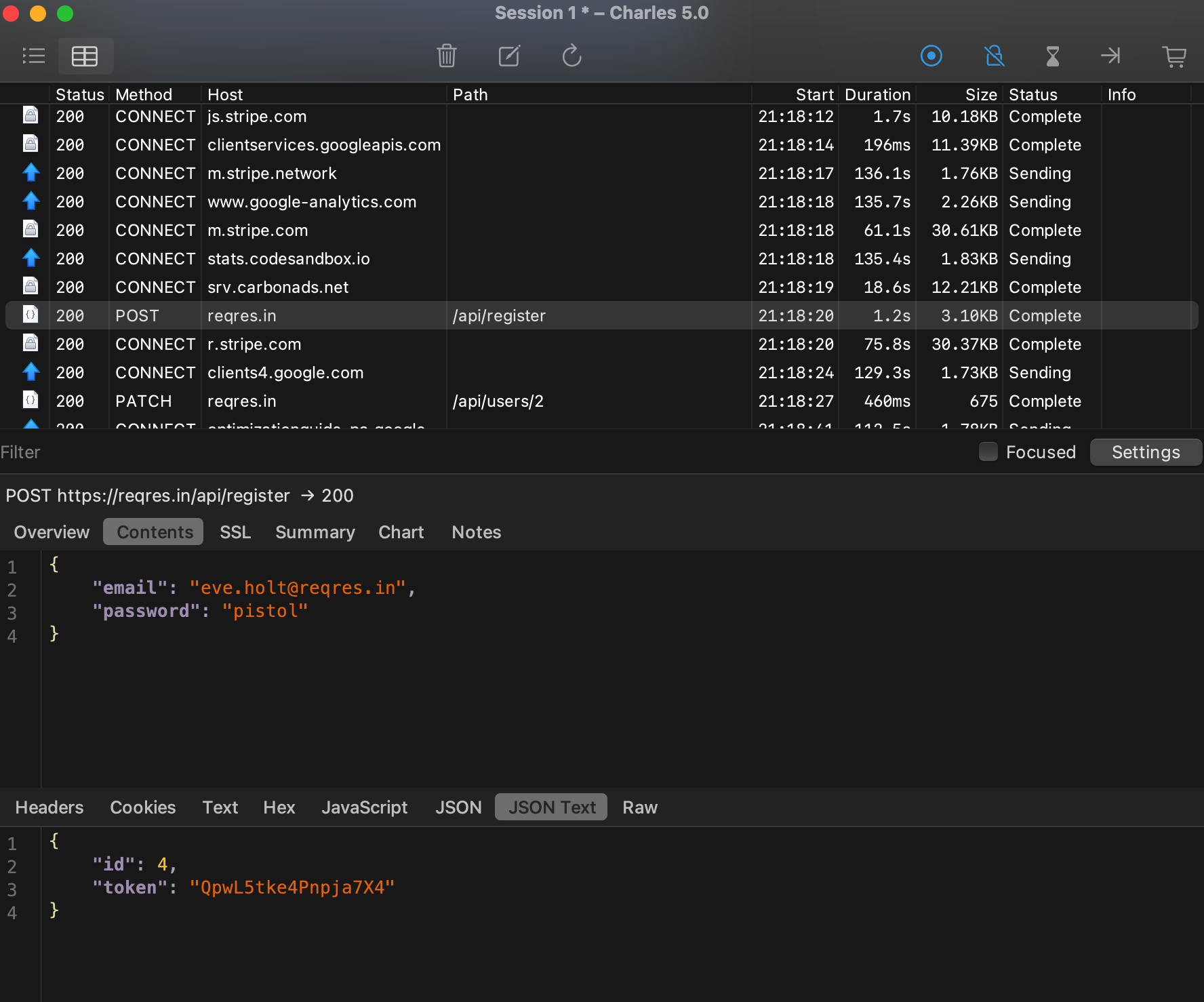
POST https://reqres.in/api/login

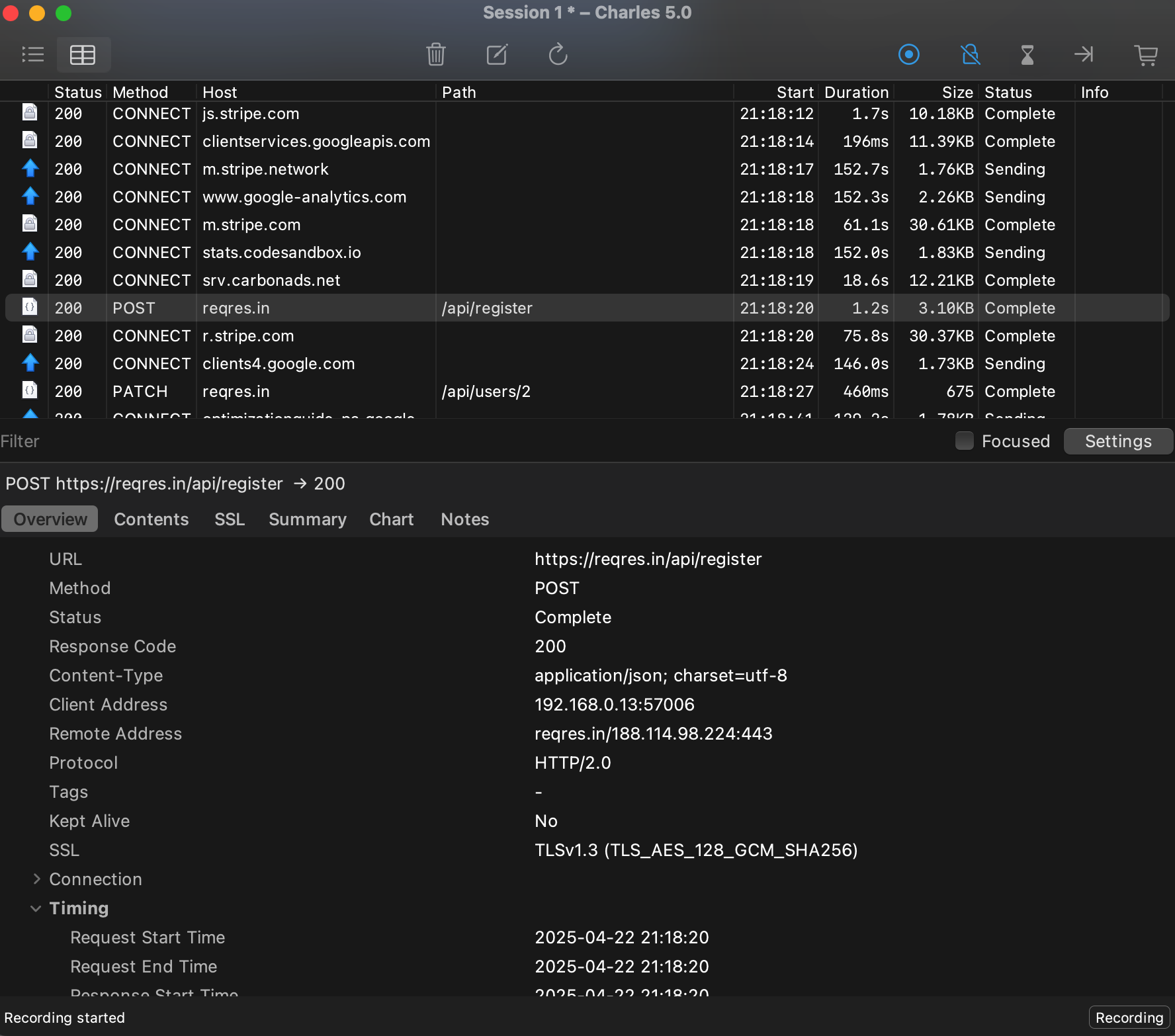
{

"email": "eve.holt@reqres.in",

"password": "pistol"

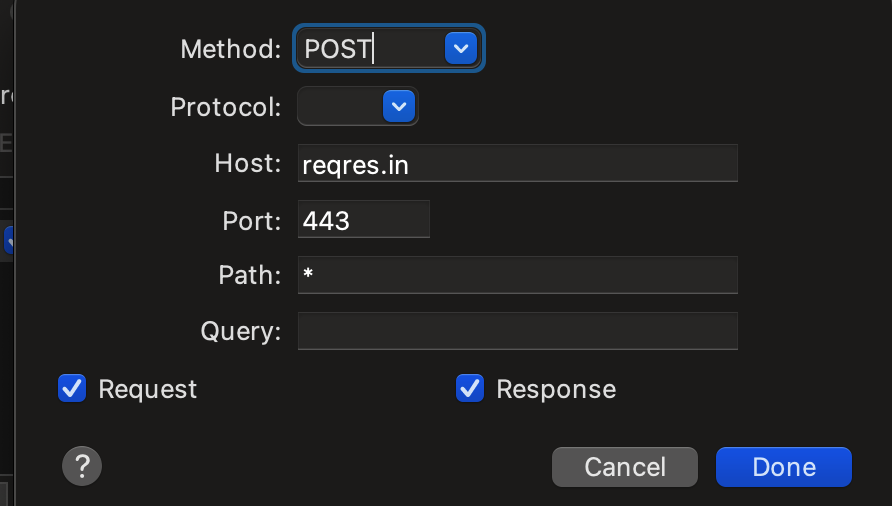
}



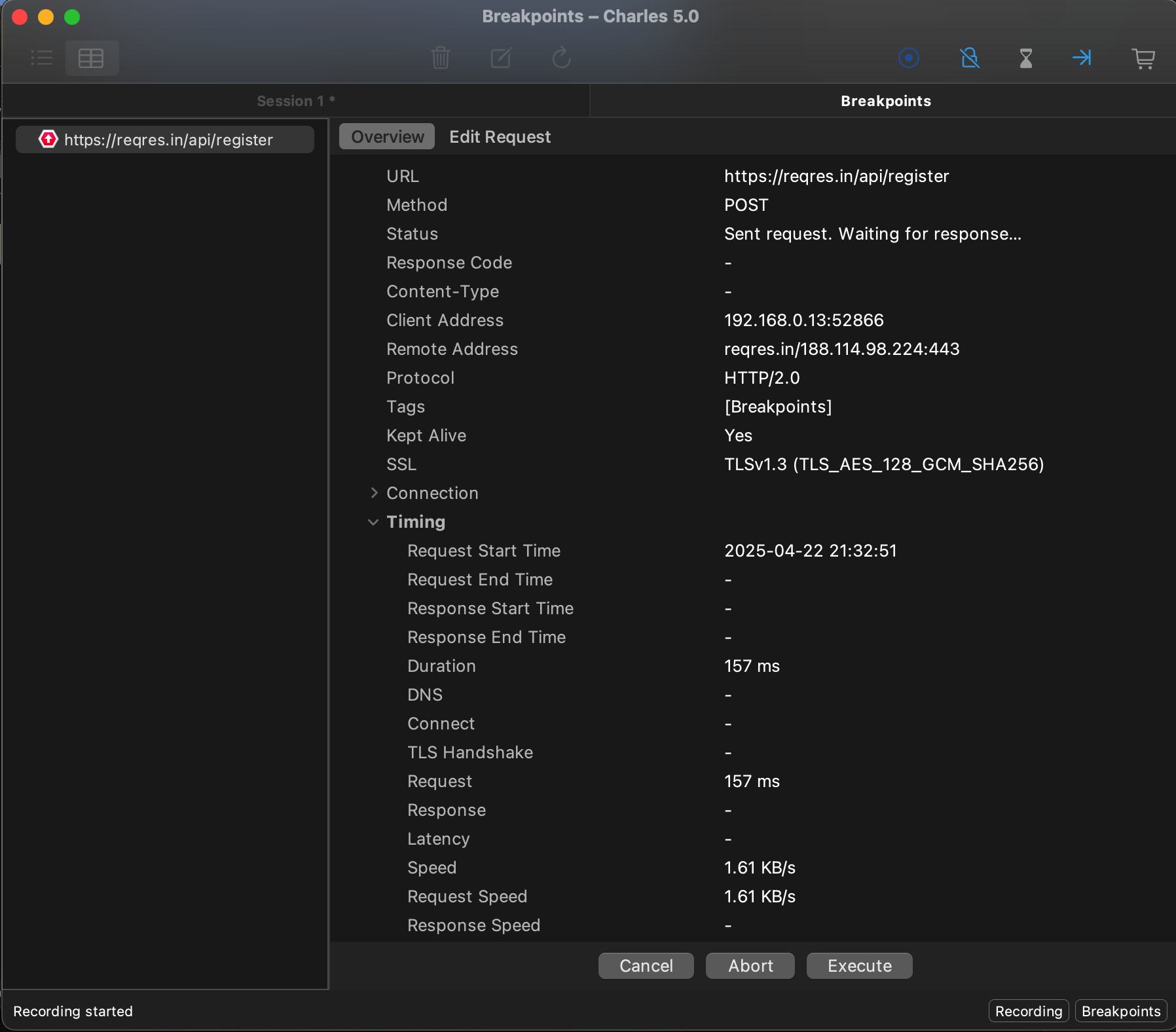


**2. Включение Breakpoints**

* В Charles был установлен breakpoint на сайт <https://reqres.in>;

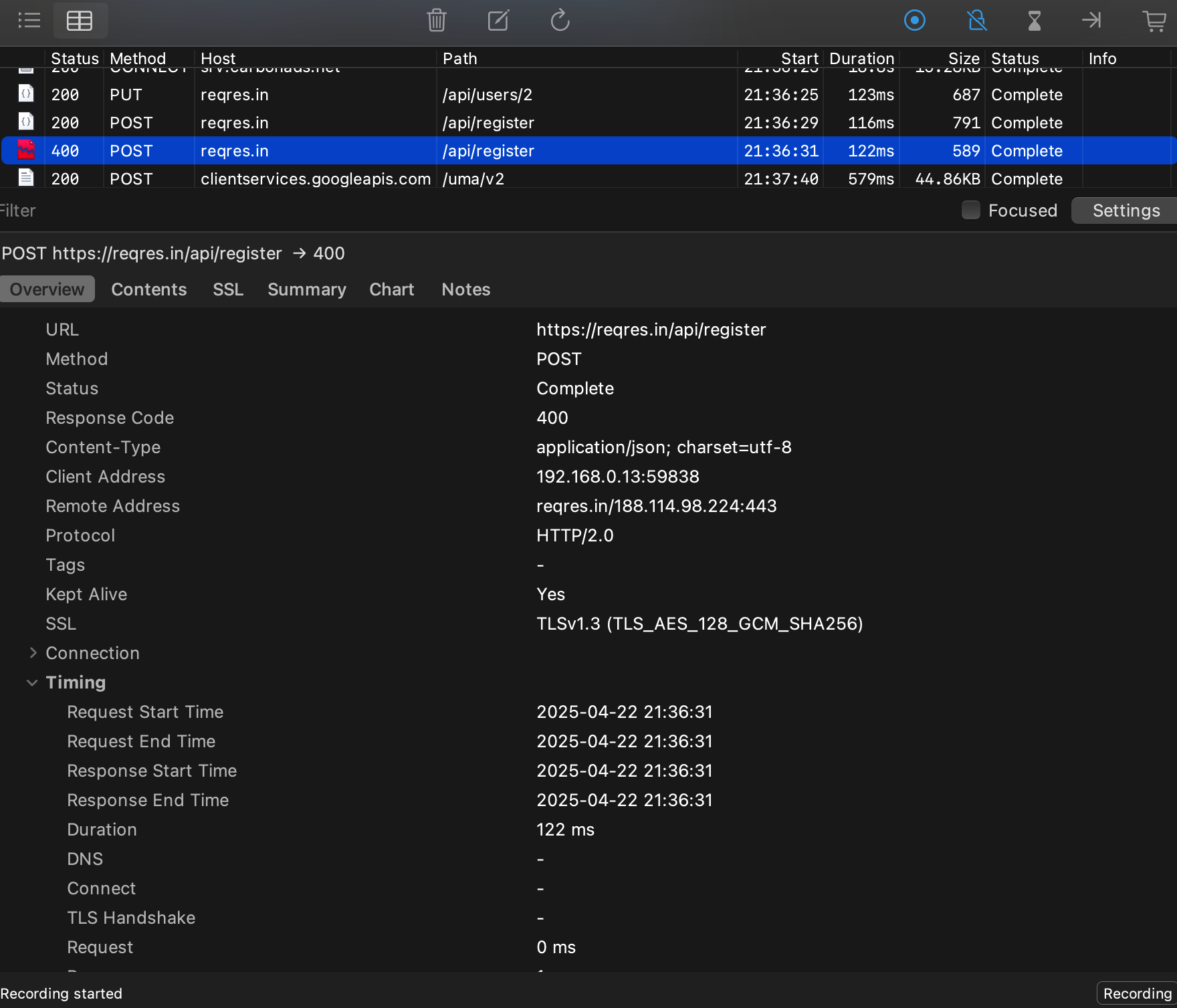


* Повторная отправка запроса – Charles перехватывает его.

****

#### Изменение запроса

* В теле запроса удален пароль;
* Нажата кнопка **Execute;**
* Сервер возвращает ошибку 400 (неверный логин/пароль).

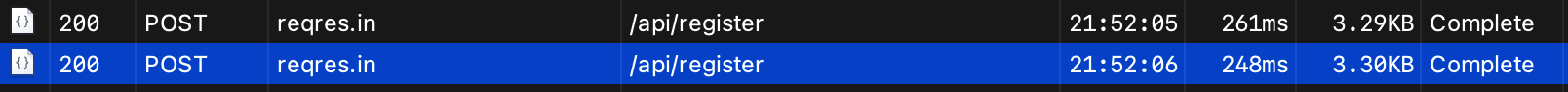


**Повторная отправка запросов (Repeat)**

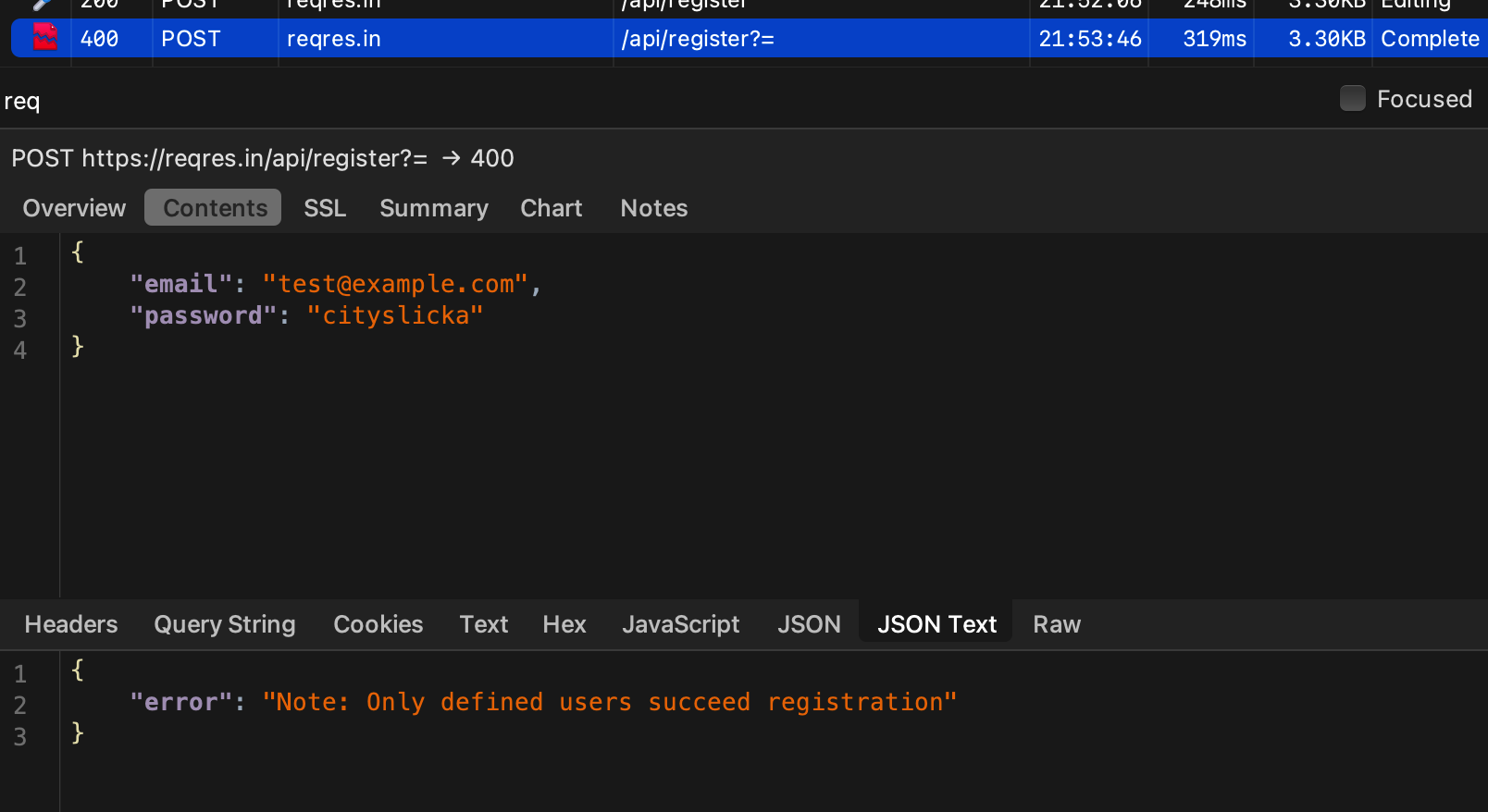
1. **Повторная отправка (Repeat):**
   * С помощью данного инструмента можно отправить запрос без изменений повторно;



* + Запрос отправится повторно.



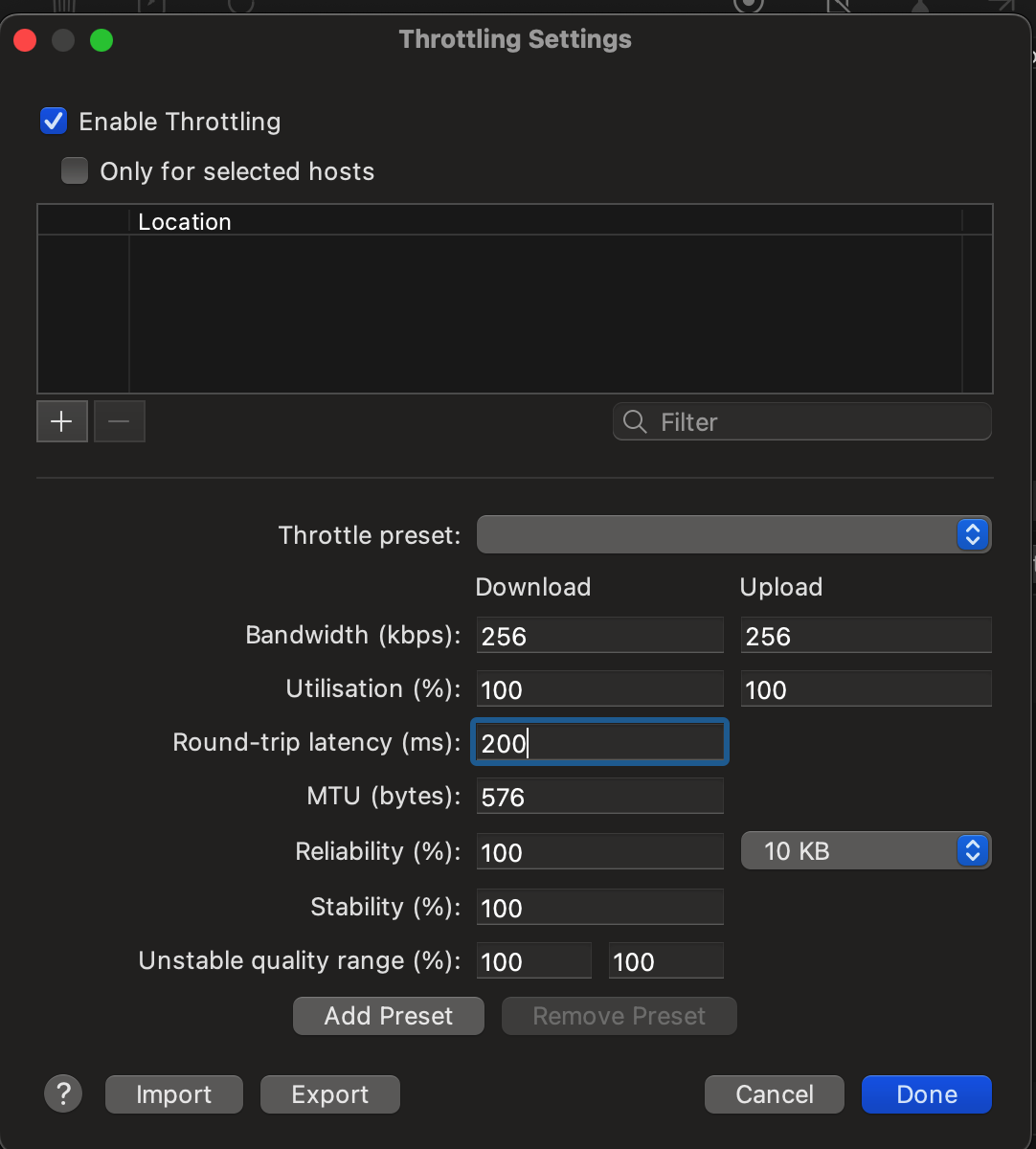
1. **Изменение параметров (Compose):**
   * Выбран инструмент **Compose**;
   * Изменены данные (заменен "email": "test@example.com");
   * Нажат **Execute**.



Сервер вернул ответ с новыми данными (ошибку 400, т.к. email невалидный).

**Throttling (Имитация медленного интернета)**

Включение Throttling:



При отправке запроса произошла задержка, появился лоадер. Throttling помогает выявить проблемы в обработке медленных соединений (например, отсутствие индикатора загрузки или падение приложения).

### **Выводы**

В ходе выполнения лабораторной работы была успешно смоделирована атака типа «человек посередине» (MITM) с использованием программы Charles Proxy. Были подробно изучены и продемонстрированы ключевые функции Charles, такие как перехват и изменение HTTPS-трафика, установка SSL-сертификата на мобильное устройство, использование Breakpoints для редактирования запроса, а также инструменты Repeat и Compose для повторной отправки и модификации запросов. Дополнительно была показана функция Throttling, позволяющая эмулировать медленное интернет-соединение для анализа поведения приложения при нестабильной сети.

Результаты эксперимента наглядно показали, что при отсутствии дополнительных мер безопасности (например, SSL-pinning) мобильные приложения и веб-сайты подвержены атакам MITM при условии, что атакующий может внедрить доверенный сертификат в систему пользователя. Это подтверждает необходимость использования современных механизмов защиты трафика, таких как строгая проверка сертификатов и реализация SSL-pinning, особенно в приложениях, работающих с конфиденциальными данными.