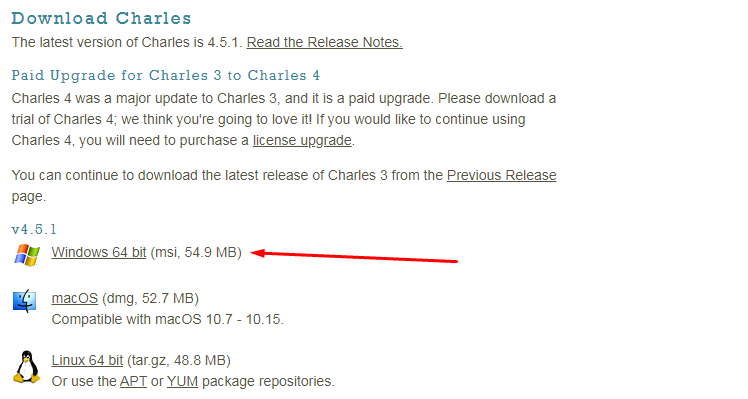
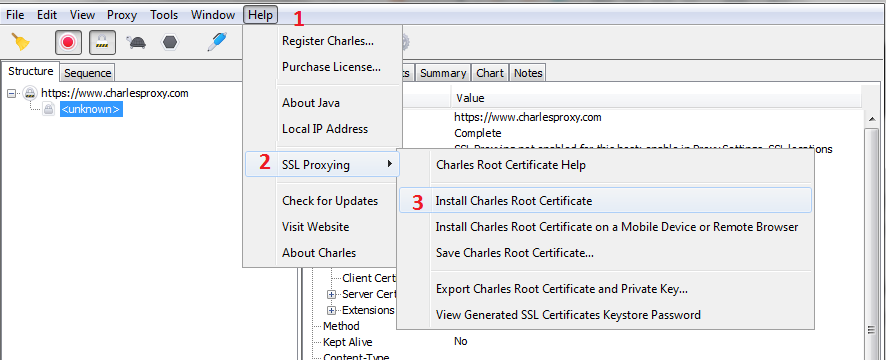
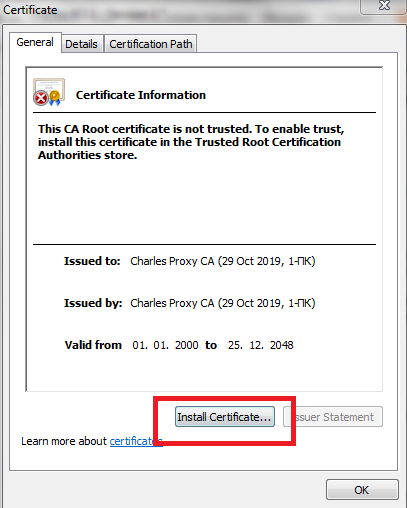
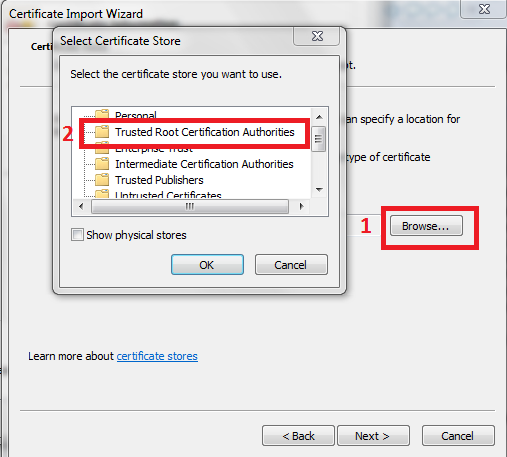
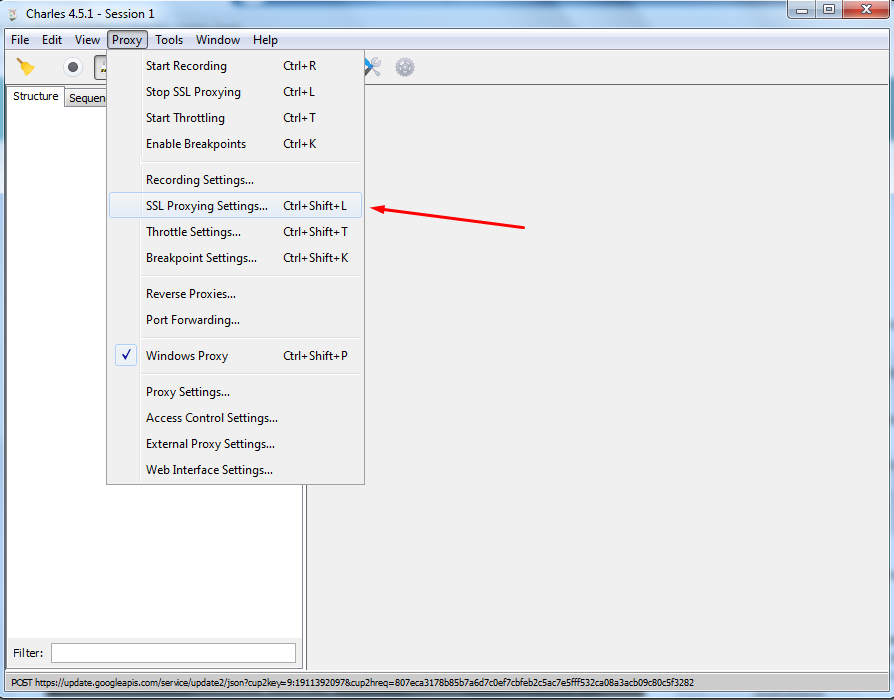
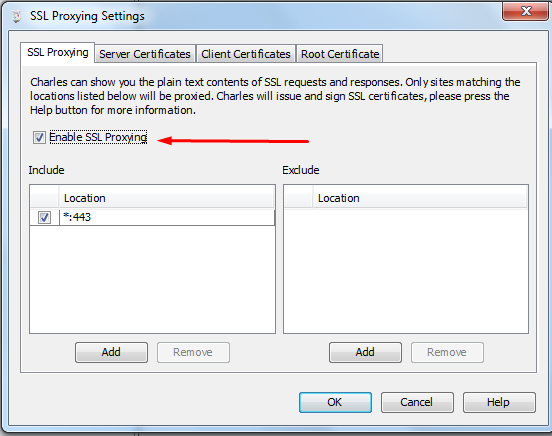
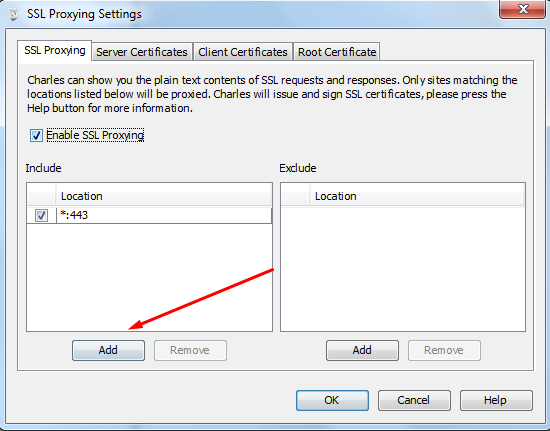
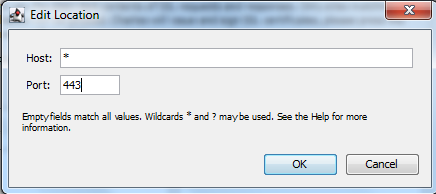
**Первоначальная установка Charles Proxy**  
  
1. Скачиваем и устанавливаем Charles Proxy отсюда: <https://www.charlesproxy.com/download/>  
  
2. Запускаем Charles.  
3. В самой программе нажимаем “Help-SSL Proxying-Install Charles Root Certificate”



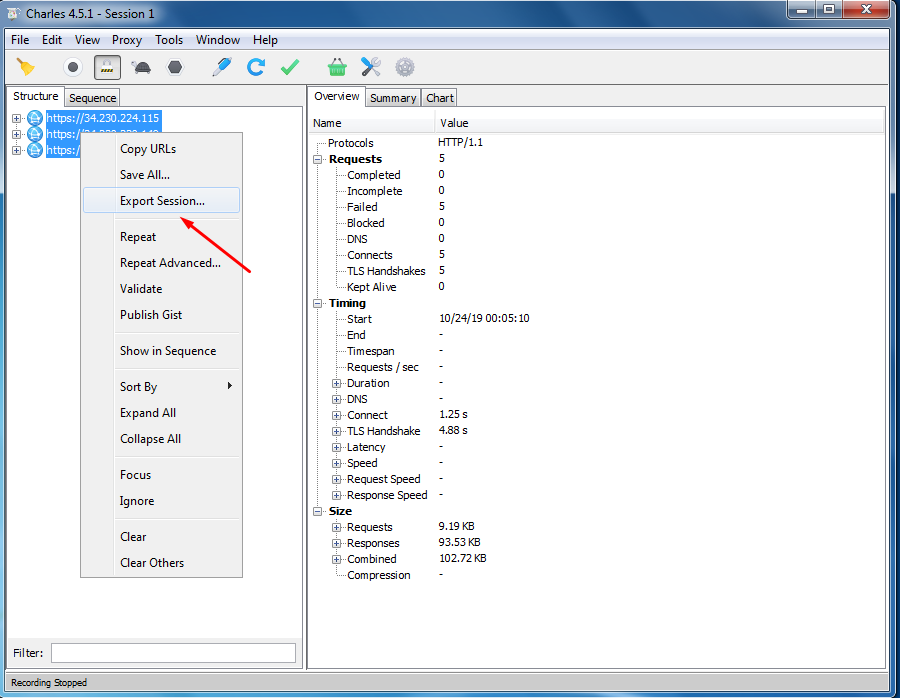
4. Нажимаем “Install Certificate”

  
5. Выбираем “Current user”, если есть , в следующем окне нажимаем “Browse” и выбираем “Trusted Root Certification Authorities”



До того момента как появится окошко что все нормально (с синим значком), везде нажимаем “Yes”.  
6. Идем обратно в главное меню Charles Proxy и нажимаем кнопку, указанную на скриншоте:  
6. Обязательно (!) ставим вот эту галочку  
  
7. Нажимаем «Add»  
  
8. В «Host» ставим звездочку «\*» а в «Port» ставим цифры 443 и нажимаем ОК.  
  
  
**Настройка FireFox:**

Тут все просто.  
1. Закройте Charles Proxy  
2. Откройте FireFox и нажмите на меню (три перпедикулярные полоски в правом верхнем углу)  
3. Нажмите «Options»  
4. В поиске введите «Proxy»  
5. Нажмите на кнопку «Settings»  
6. Выберите пункт указанный на скриншоте и нажмите «OK» :  
  
7. Запустите Charles Proxy  
8. В FireFox перейдите на <https://chls.pro/ssl>  
9. Откроется окно в котором нужно будет выбрать «Trust this CA to identify websites» и нажмите ОК.  
  
Вы великолепны! Если вы все сделали правильно, то Charles Proxy будет работать корректно.  
  
P.S Всегда при записи логов (!) проверяйте что бы в Чарльз был «закрытый замочек» (см. скриншот)  
****

Если замочка нет, то тогда его и не ищем. ☺  
 P.S.S Как выгрузить лог?  
Когда вы закончили логировать нажмите знак остановки, после этого с помощью CTRL выделите весь лог , нажмите правой кнопкой мыши на него и далее нажмите «Export Session»   
Лог обязательно сохраняйте в формате .chls  
****

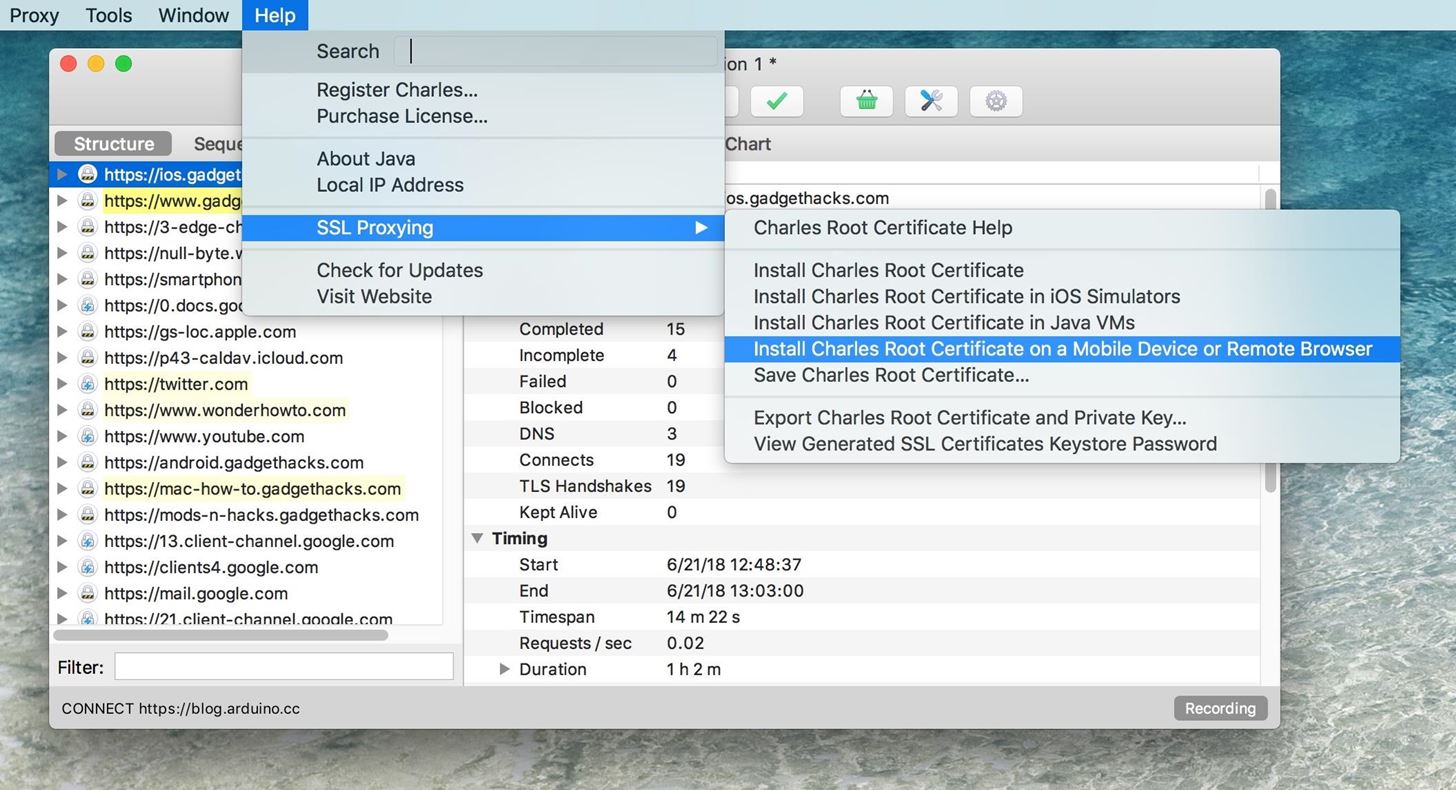
**Настройка мобильного девайса для работы с Chirles Proxy:**

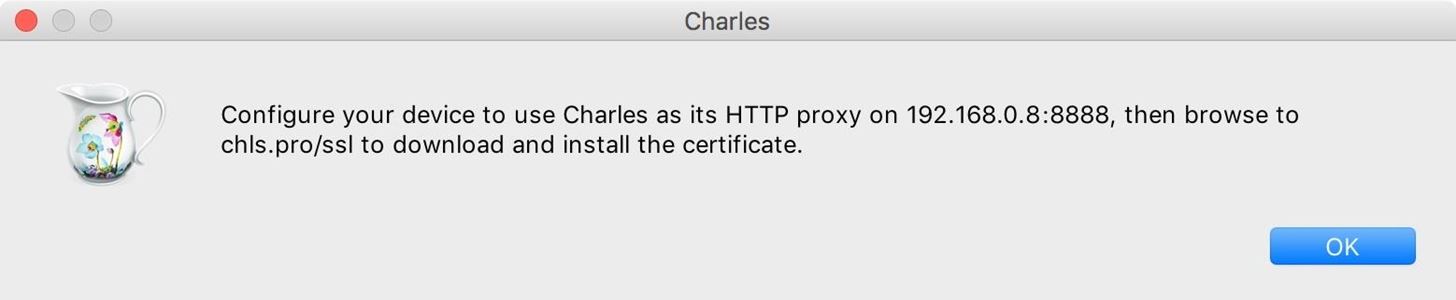
!!!Важно: Отключаем все антивирусы на Пк и смартфоне, включая Windows Defender и все, что может блокировать трафик!!!

1. Заходим в “Help – Local Address” и запоминаем значение

2. Заходим в “Proxy – Proxy Setting – HTTP Proxy – Port” и запоминаем значение порта

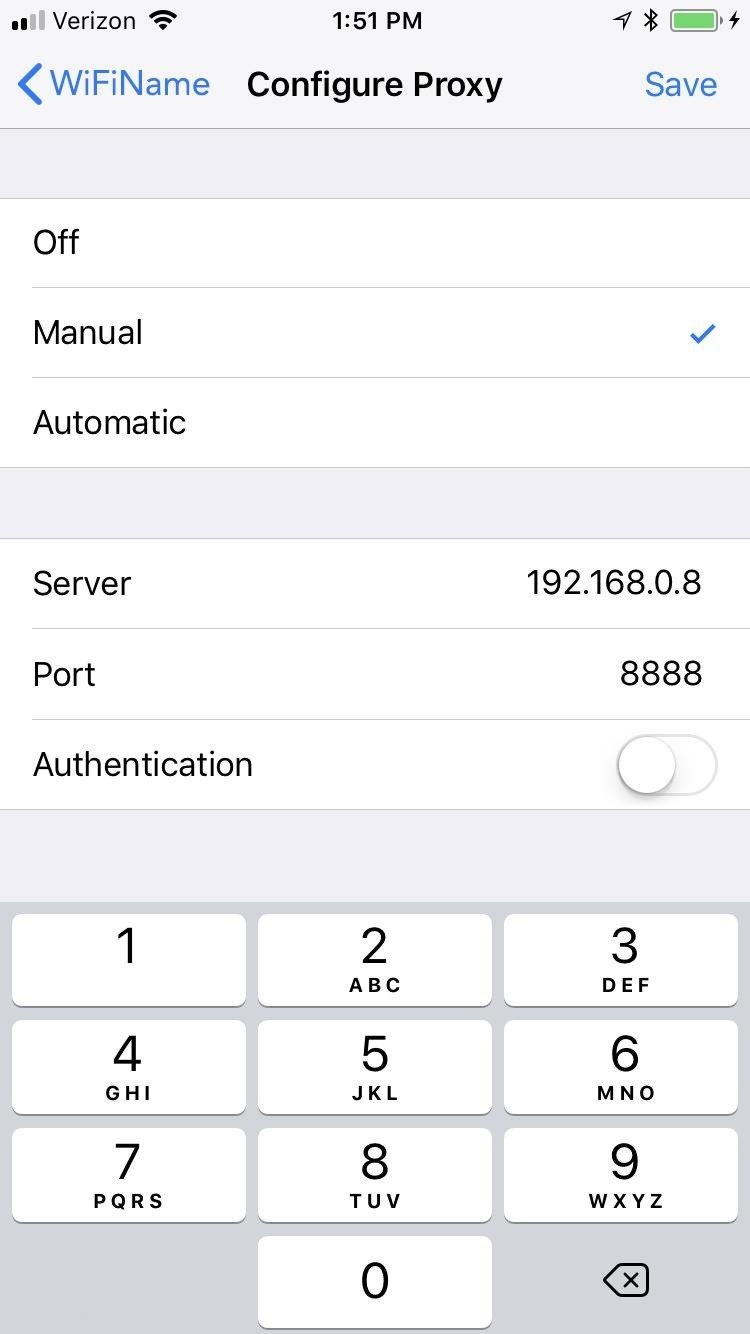
Можно проигнорировать эти два пункта и просто зайти в “Help” в меню, затем “SSL Proxying” и выбрать “Install Charles Root Certificate on a Mobile Device or Remote Browser”

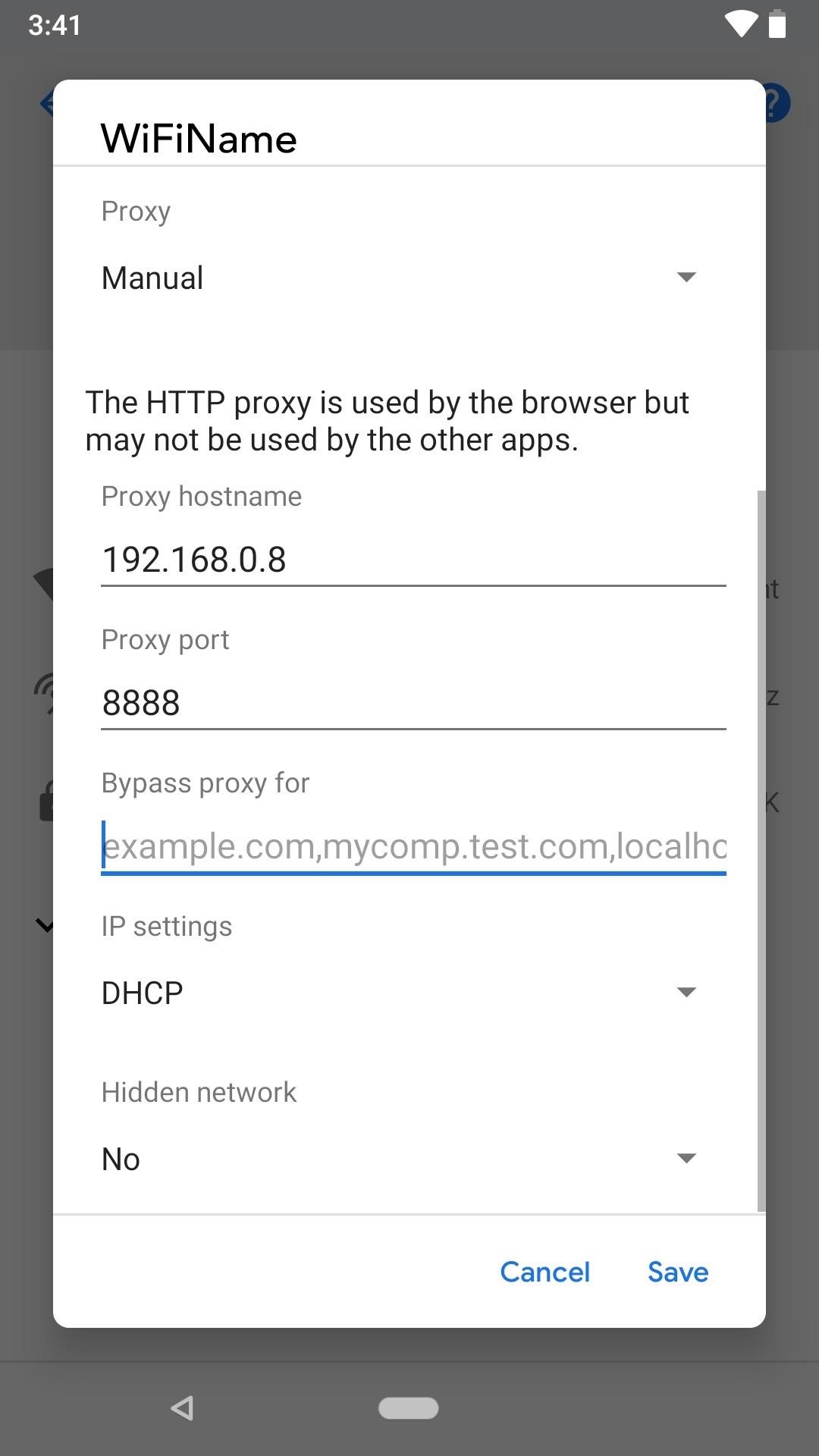
 Вы увидите диалоговое окно, подобное указанному на скриншоте, которое предоставляет IP-адрес и порт для машины, на которой работает Charles:



3. На iPhone перейдите к меню «Wi-Fi» в приложении «Settings», затем убедитесь, что он находится в той же сети, что и Charles. Нажмите значок информации рядом с подключенной сетью, а затем прокрутитесь вниз и выберите «Configure Proxy». Выберите строку «Manual» и введите номера сервера и порта из последнего диалогового окна, которое выдал вам Charles. Нажмите «Сохранить», чтобы закончить.

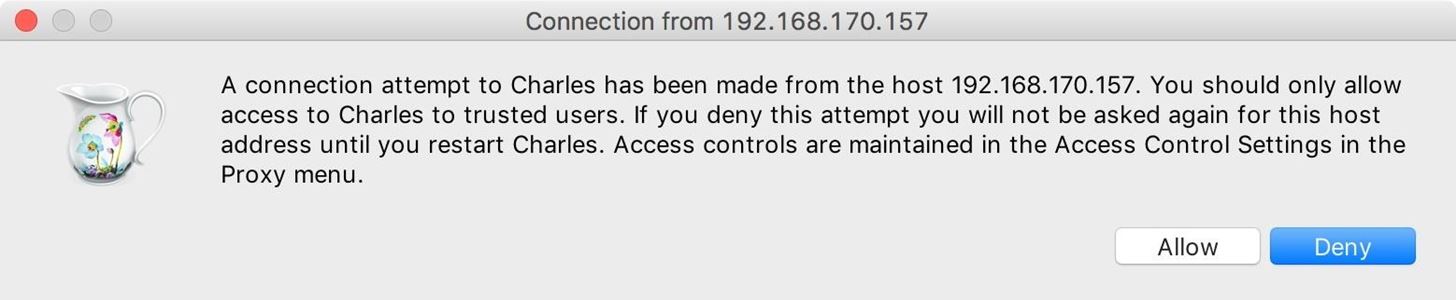
Для телефонов на Android процесс немного отличается в зависимости от версии OEM и программного обеспечения. Как правило, вы открываете настройки Wi-Fi, нажимаете и держите меню общей сети. Затем нужно выбрать что-то вроде «Управление сетевыми настройками» или «Изменить сеть» или значок карандаша. Найдите отображение дополнительных параметров, а затем откройте настройки «Прокси» и вручную введите номера серверов и портов, которые Charles дал вам раньше. Не забудьте нажать на «Сохранить», чтобы закончить.





Теперь ваш смартфон настроен на маршрутизацию HTTP-трафика через Charles Proxy.

4. Когда ваш смартфон будет подключен к Charles, то вы на вашем компьютере увидите диалоговое окно, предупреждающее вас о том, что Charles получил входящее соединение. Выберите «Разрешить». Если вы вдруг случайно запретите входящее соединение, то для того, чтобы еще раз получить это приглашение, вам придется перезапустить Charles.



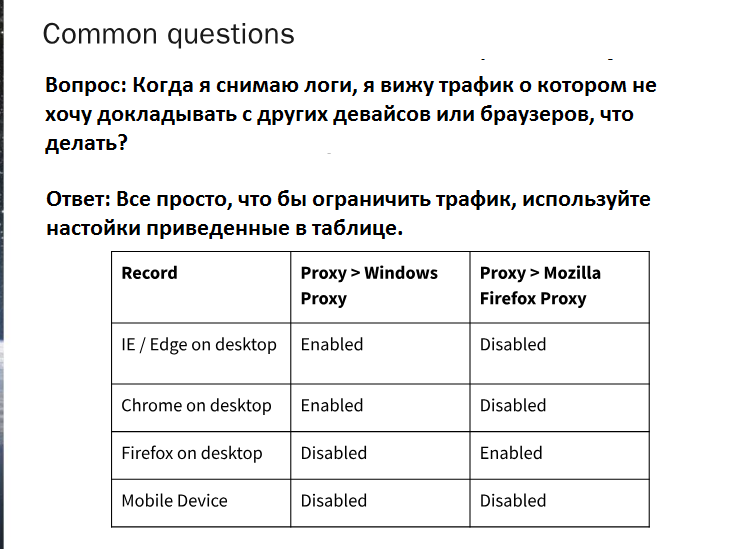
5. С помощью веб-браузера на вашем смартфоне (в браузере “Chrome”, если Android) перейдите на chls.pro/ssl.

На iPhone вы сразу же получите запрос с просьбой разрешить сайту показывать вам профиль конфигурации. Нажмите «Разрешить». После этого вы попадете на экран Install Profile для Charles Proxy CA. Нажмите «Установить», вас перенаправят на страницу предупреждения. Нажмите «Установить» еще раз, и еще раз на всплывающем окне. Наконец, нажмите «Готово», чтобы закончить.

Если вы находитесь на iOS 10 или выше, то вам также придется посетить «Общие» в приложении «Settings». Выберите меню «About», а затем «Certificate Trust Settings» ниже. В разделе «Enable Full Trust for Root Certificates» нажмите на слайдер, расположенный рядом с CA Charles.

На Android-устройстве файл попытается немедленно загрузиться на ваше устройство. Если этого не произошло, то вы можете получить приглашение для его загрузки и тогда вам нужно нажать на «Скачать». После загрузки введите ваш PIN-код или отпечаток пальца. После этого откроется окно сертификата, в котором вам нужно назвать сертификат чем-то вроде «Charles Proxy CA». Нажмите «ОК», когда закончите.

Обратите внимание, что для установки сертификата из Charles Proxy вам необходимо выключить блокировщики рекламы, работающие на основе DNS. Кроме того, в дальнейшем при анализе данных включение вашего блокировщика рекламы будет только маскировать трафик, поэтому лучше оставить его выключенным, пока вы используете Charles.



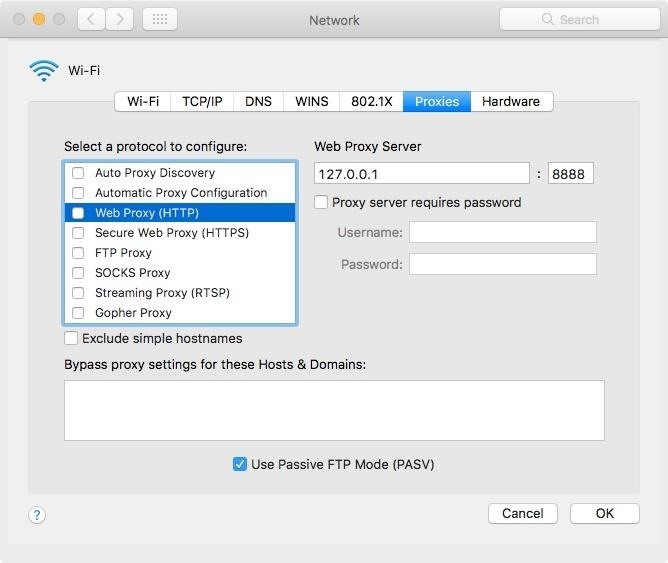
Видео инструкция от utest: <https://www.youtube.com/watch?v=pj3C3IL75ig>

Не обязательные пункты:

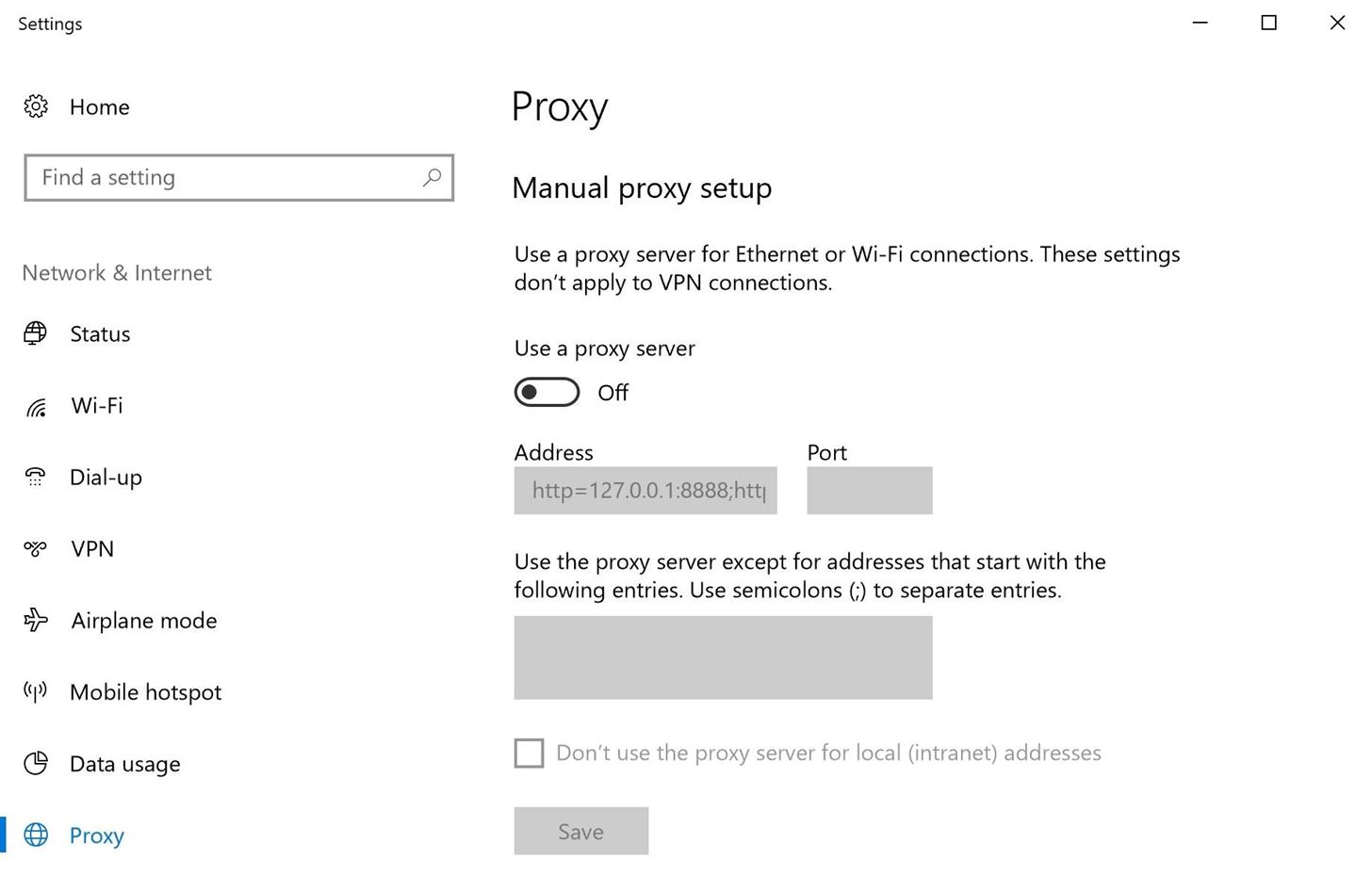
**Изолируйте трафик телефона от трафика других устройств**

В зависимости от того, какой веб-трафик генерируется на машине, на которой работает Charles, трудно будет сказать, какие запросы поступают от вашего телефона. Charles автоматически изменит ваши сетевые настройки в целях маршрутизации HTTP-трафика на вашем компьютере через прокси-сервер, но довольно просто изменить это поведение вручную так, чтобы можно было видеть только трафик с вашего телефона.

В macOS вы можете изменить это в «System Preferences». После этого перейдите в раздел «Network», затем «Advanced», а на вкладке «Proxies» снимите флажки с «Web Proxy (HTTP)» и «Secure Web Proxy (HTTPS)». Charles автоматически будет изменять эти настройки всякий раз, при своем запуске, поэтому вам нужно будет повторять эти шаги каждый раз, когда вам нужно будет изолировать трафик телефона.



В настройке Windows вам необходимо открыть «Settings». Затем выберите «Network & Internet», затем «Proxy». Находясь там же, прокрутитесь вниз до Manual proxy setup, затем переключите слайдер «Use a proxy server». В отличие от Mac, вам не придется делать это каждый раз после перезапуска Charles.



**Когда закончите — удалите все, что не нужно**

После того как вы закончите анализ трафика мобильных приложений на вашем смартфоне, вы должны удалить установленный сертификат. Не стоит оставлять на вашем устройстве дольше, чем вам нужно, сертификат, который использовался для реализации атаки «Человек-по-Середине». Также стоит удалить настройки прокси.

На iPhone, чтобы удалить сертификат, перейдите в «General» в «Settings», затем в самом низу выберите «Profile». Затем нажмите профиль конфигурации «Charles Proxy CA» и нажмите «Remove Profile». Нажмите «Remove» для подтверждения. Чтобы остановить прокси-сервер, выберите «Wi-Fi» в «Settings», нажмите «Wi-Fi network», выберите «Configure Proxy», затем переключите слайдер в «Off», а затем нажмите «Save».

Для всех пользователей Android процесс будет отличаться в зависимости от вашего устройства. Выберите «Security & location» или «Lock screen and security» в «Settings», нажмите «Advanced» или «Other security settings», затем «Encryption & credentials» или «View security certificates». На стоковом Android’е вам также придется нажать «Trusted credentials». Теперь выберите вкладку «User», а затем нажмите «Charles Proxy CA». Нажмите «Remove», затем «ОК», чтобы удалить его. Что касается прокси-сервера, просто вернитесь к параметрам сети Wi-Fi и измените настройки прокси-сервера с «Manual» на «None».

**EBD457553EFAF1BBAC - ключ активации Charles proxy**