**Инструкшион**

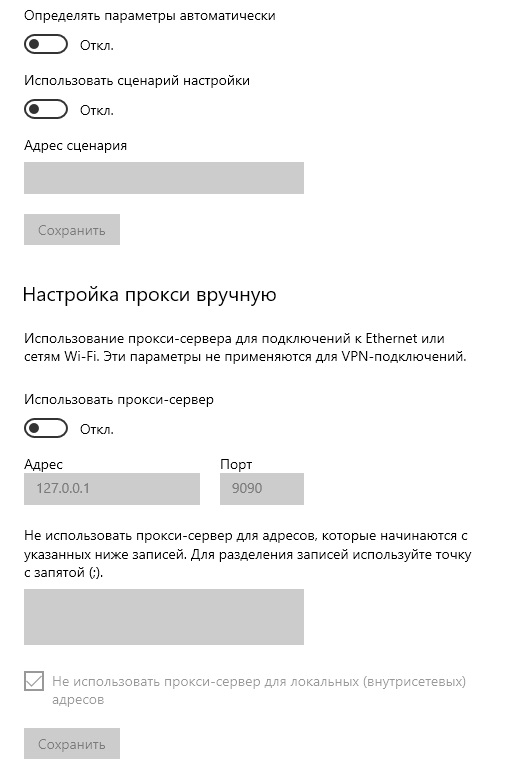
**Аттеншион!**

Автор не несет ответственности за ваши утерянные данные, банковские карты или еще какие-то интимные фото… все делаете на свой страх и риск!

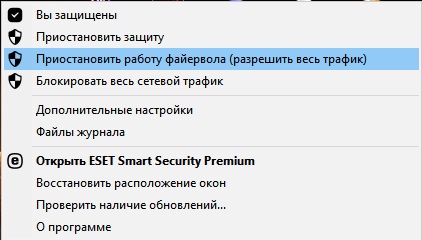
**Глава первая. ВиндоВс 10**

*Почему все пишут виндовс в поиске?) бррр…*

Итак, для начала надо разобраться, что там у нас в настройках прокси в самой винде, поэтому отправляемся туда

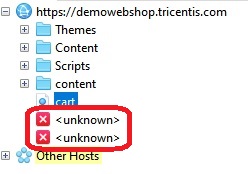
Должно быть примерно так (при выключенном Charles Proxy – ЧП далее)

И еще – должны быть выключены все впн-ы, файерволлы и прочие защитнички…



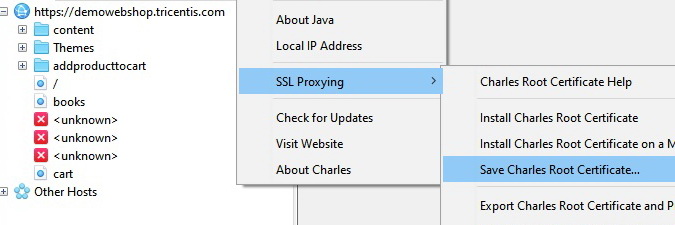
С этим разобрались. Запускаем ЧП, устанавливаем сертификат (как это сделать - полно инструкций и видео в интернете, поэтому здесь расписывать не буду).

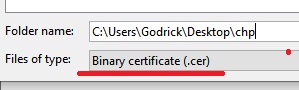
Открываем наш браузер и идем серфить и перехватывать траффики, радостно изменять данные и творить прочие хакерские штуки. Но радость будет недолгой, если у вас обнаружатся вот такие unknown

 Несмотря на то, что сертификат стоит, все- таки нет к нему доверия из каких-то функций виндоус или самого браузера (хром, опера, эдж), я уже так глубоко не вникал…

Руки не опускаем – делаем следующее

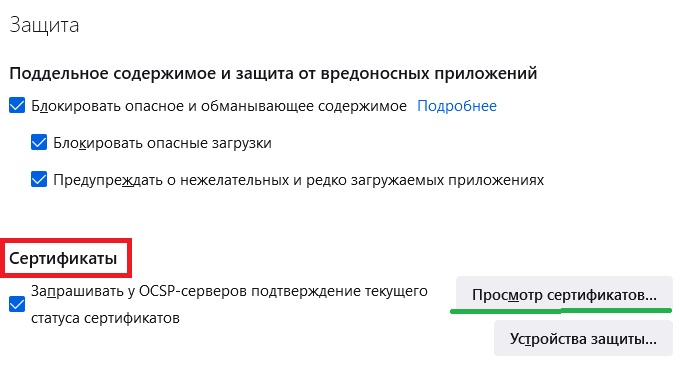
В самом ЧП жмем **help** и сохраняем сертификат куда-нибудь поближе, лучше на рабочий стол. Не забудьте задать ему имя, например, chtotebeeshenado.cer



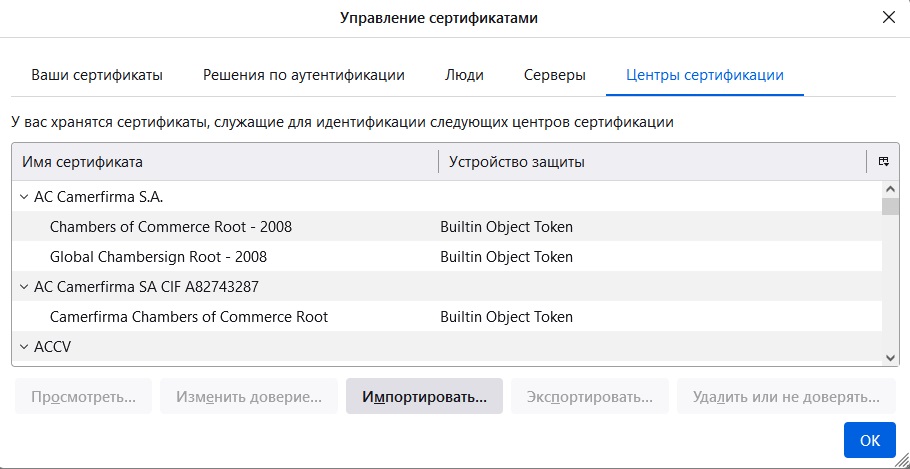


Именно в бинарном формате, не в .pem

Теперь нам понадобится mozilla firefox. Качаем, если нет, или запускаем, если установлен. Идем в настройки – приватность и защита – и мотаем в самый низ к защите

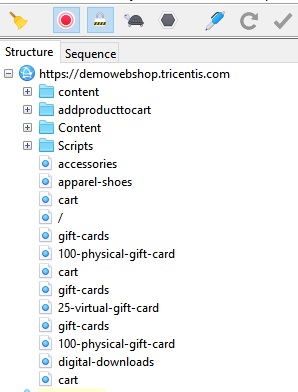


Жмем просмотр сертификатов и импортируем туда наш заранее подготовленный chtotebeeshonado.cer



Можно проверить, встал ли сертификат, если попробовать его импортировать еще раз – лиса напишет, что и так все норм, нечего тут жмякать по сто раз…

Ну и все – открываем наш сайт в мозилле и перехватываем!



В свое время пришлось порядочно повозиться, чтоб, подобрать ключик к ЧП в windows. Документация на самом сайте ЧП немного устаревшая и не актуальная во многих параметрах.

Если вам повезло, и вы сразу нашли сей документ, надеюсь он вам поможет;)

Хотя, обычно, такие инструкции читают, когда уже перепробовано все, что можно…

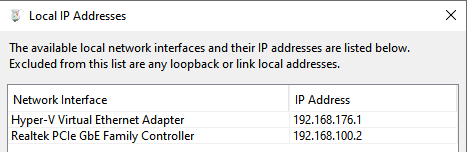
**Глава вторая. Андроид**

*Без манифестов, скриптов и прочих лишних телодвижений…*

Подопытный: Samsung A50 Android 11 / Opera

Для начала нам нужен локальный IP

Ищем в самом ЧП



У меня их два, но правильный нижний, который от сетевой карты

Идем в телефон – настройки – подключения – ваша сеть вай-фай – настройки – дополнительно.

Заполняем прокси: вручную \192.168.100.2\8888 – сохраняем

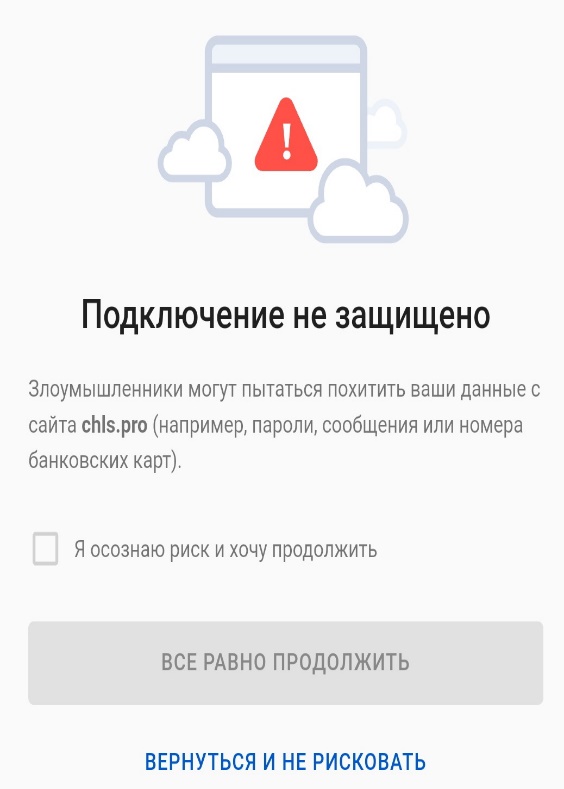
Если видите такое – значит, что-то блочит ваш интернет – файерволл, антивирус и т.п.



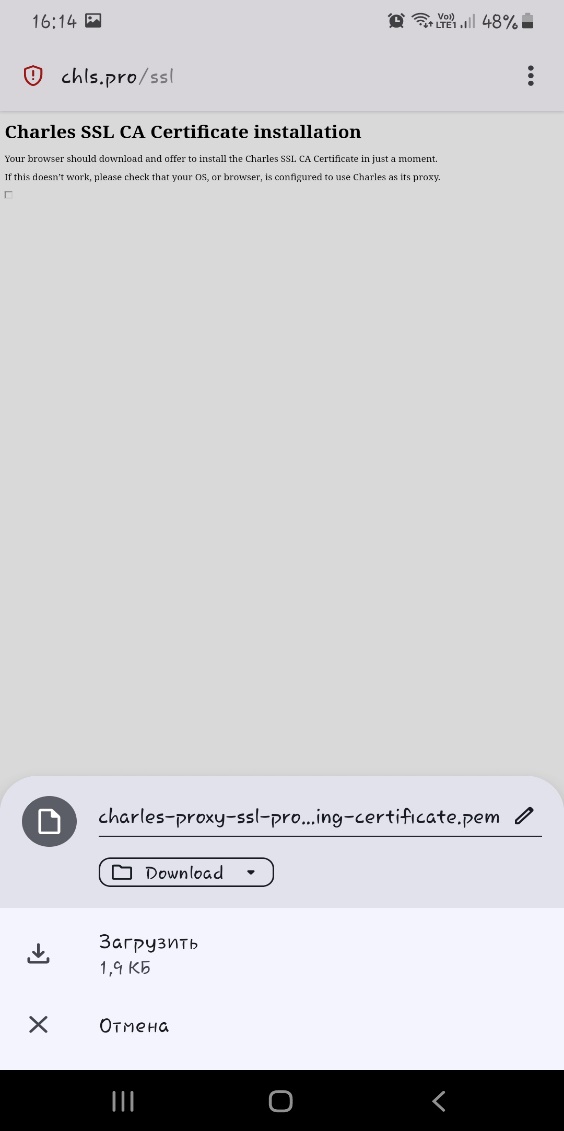
Разобрались с блокировкой, двигаемся дальше

Теперь нам нужен сертификат – открываем браузер в телефоне и идем по ссылке <https://chls.pro/ssl> - сохраняем его

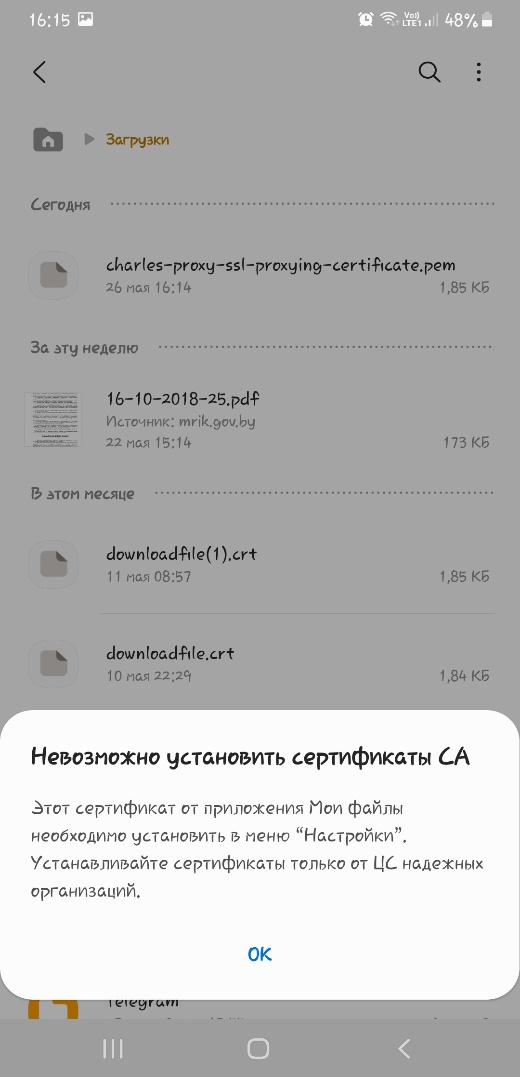
Может быть предупреждение, что сайт небезопасный и все такое – принимаем риски и жмем далее.



Получаем такую картину



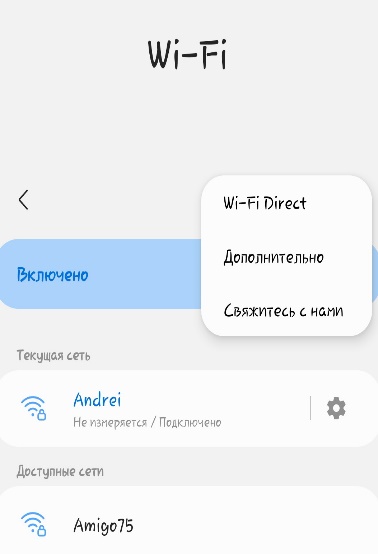
Если попробовать его установить из «моих файлов», то тоже ничего не получится



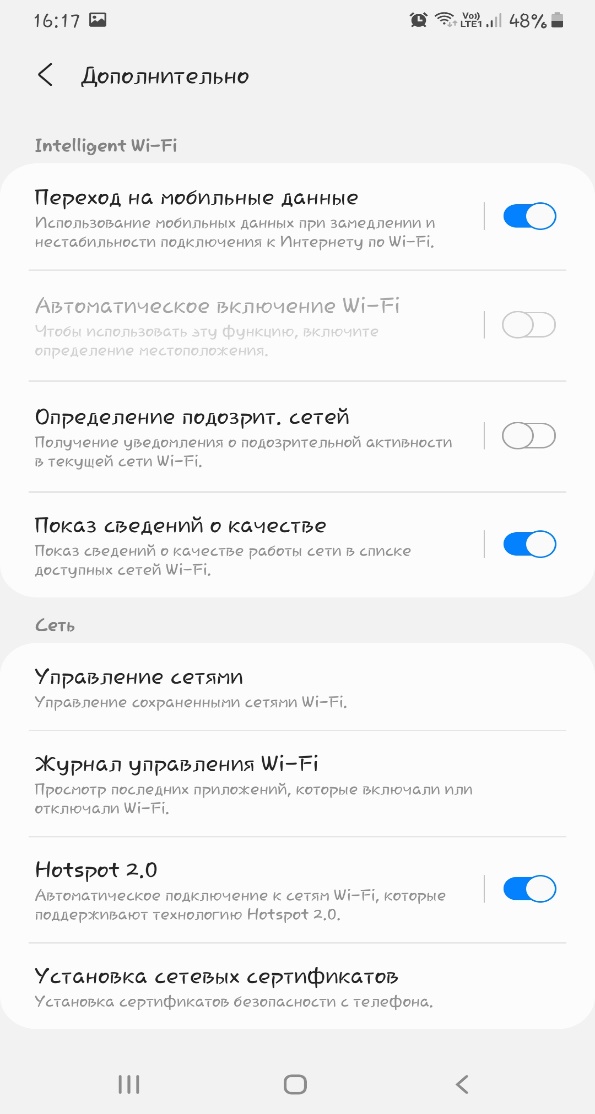
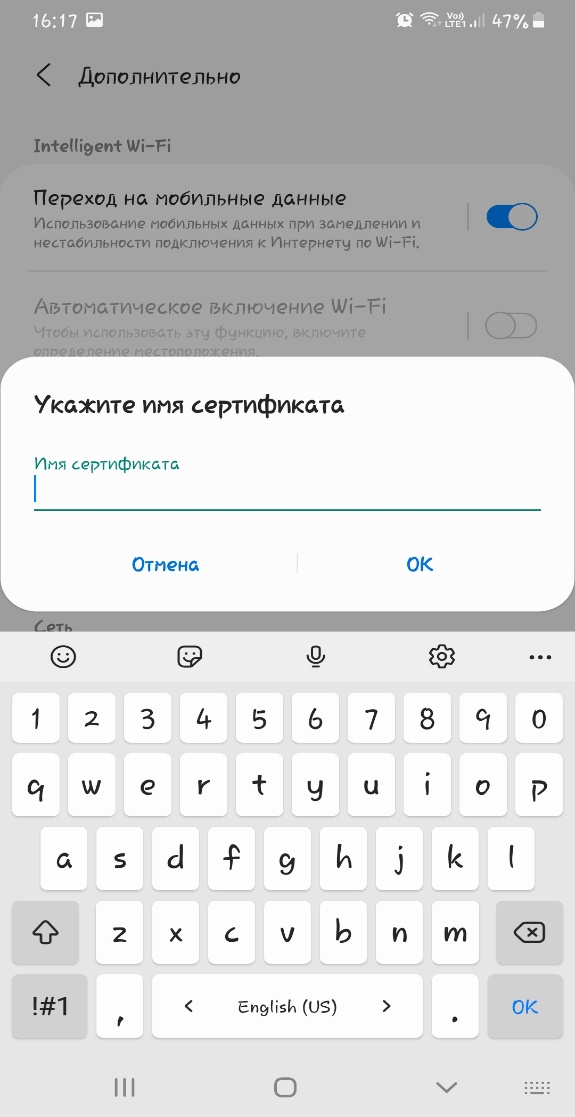
Значит, идем в «биометрия и безопасность» - «другие параметры безопасности» - «установить из памяти» - «сертификат СА»

Ставим наш скачанный сертификат. Но это еще не все. Можно попробовать тут же установить сертификат Wi-Fi, но я делал немного по-другому

В настройках подключения – Wi-Fi - жмем кебаб-меню и выбираем дополнительно



Здесь в самом низу нас ждет **установка сетевых сертификатов**



Указываем любое имя, готово.

Если все настроено правильно, то на ПК в самом ЧП на каком то из этапов появится окошко (при написании этой заметки у меня ничего не выскакивало, видимо из за ранее уже принятых обязательств, а может из за того, что раньше он скачивался в формате .srt, а сейчас .pem) – нужно выбрать allow.

Через хром в телефоне все хорошо, unknown нет, только кривое отображение user-agent, а вот в опере все отлично. Так что, подбирайте для себя наиболее подходящий вариант.

