**Как перехватить http/https запрос. Как измерить скорость его обработки? Как и зачем менять запросы при тестировании?**

При тестировании сайтов или мобильных приложений иногда возникает необходимость не только отловить трафик между клиентом и сервером, но и модифицировать его, чтобы посмотреть, как это обработает бэкенд и что поменяется на UI.

Например если браузер ждет проставление какого то флажка, но на тестовом окружении этот флажок не может быть проставлен (допустим флажок что ответили все внешние API, но часть из них не настроена на тестовом окружении), то можно перехватить ответ от сервера и проставить нужный флажок, что бы проверить как браузер себя поведет

**FIDDLER**

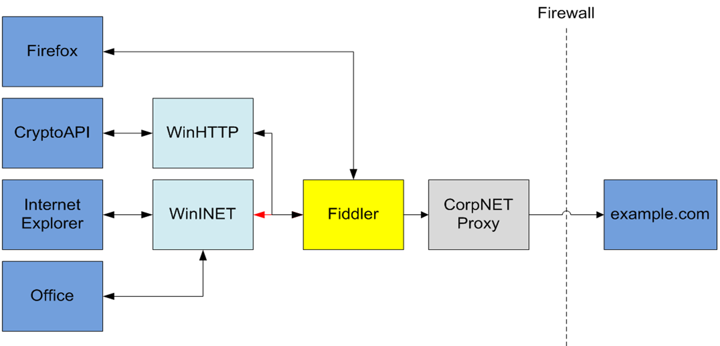
Очень часто для данных целей используется инструмент Fiddler — универсальный прокси, способный перехватывать HTTP(S) трафик и обеспечивать работу с ним. Fiddler работает на локальной машине, и видит трафик только нашей машины

Бесплатный, мощный и гибкий Fiddler позволяет инспектировать, устанавливать контрольные точки, манипулировать входящими или исходящими данными. Используют его как промежуточное звено между клиентом (браузер, мобильное приложение и т. д.) и целевым сервером. В настройках браузера указываем Proxy 127.0.0.1:8888. Это будет значить что все запросы пройдут через локальную машину, где собственно и установлен Fiddler.

Основные возможности инструмента Fiddler:

* предоставляется бесплатная платформа для отладки;
* работает как локальный прокси и регистрируется как системный прокси во время захвата;
* есть возможность просматривать, анализировать и изменять веб-трафик из любого приложения, поддерживающего прокси;
* включает перехват HTTPS через самозаверяющий сертификат.

Схематически перехват веб-трафика выглядит следующим образом:



Step 1 - Preparing Fiddler. Убедиться заранее что не включен VPN, и что в Chrome не включен сторонний Proxy

Fiddler set up

1- Click 'Tools'

2- Click 'Telerik Fiddler Options'

3- Go to HTTPS Tab

4- Select 'Capture HTTPS CONNECTs' !! Verify/Confirm/Allow any pop ups that show when you click this, it will need your authorization! !! !!

5- Select 'Decrypt HTTPS traffic

6- Click the 'Actions' button

7- Click 'Export Root Certificate to Desktop'

8 – Install Certificate

Step 2 - Connecting fiddler to browsers

Chrome set up

1- Click the options button in top right

2- Click Settings, scroll down and click advanced

3- Scroll down, find 'Privacy and Security' section

4- Click the 'Manage Certifications' option

5- Click 'Trusted Root Certificates' tab

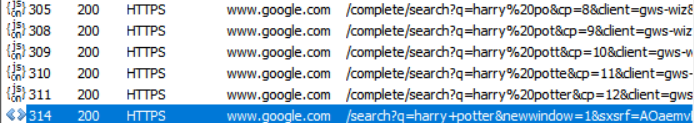
6- Click 'Import' button

7- Press next, browse to desktop and click FiddlerRoot

8- Next, next, next - confirm all from here.

Справа выбираем запрос который нужно просмотреть. То что отмечено серым не трогае – это служебные файлы. Ищем нужный запрос по иконке в #, по Host, и по URL

В данном случае мы выбрали запрос поиска Harry Potter в Google



*Statistics -* Здесь мы можем смотреть инфу по запросам.

*Inspector -* Здесь содержится основная инфа по запросу сверху и по ответу снизу

Запрос*:*

*- Headers*: отображаются заголовки

*- WebForms*: все параметры по запросу здесь представлена в читаемом виде

*- Auth*: инфа по аунтефикации

*- Cookies*: куки

*- JSON*: JSON файл (если ест)

*- XML*:XML файл (если есть)

Ответ:

*- Headers*

*- TextView*:видеть ответ в виде текста

*- SyntaxView*: видеть ответ в виде текста, но с подсвеченным синтаксисом

*- HexView*

*- WebView*: посмотреть ответ в виде страницы как это выглядит

*- Auth*

*- Cookies*

*- Raw*

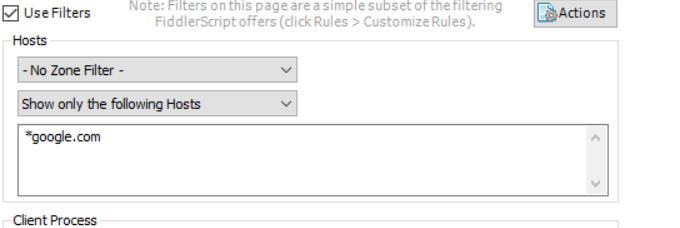
*- JSON*

*- XML*

---------------------------------------------------------------------------------------------------------------------------------

Rules > Hide CONNECTs – не перехватывает запросы на соединение

Filters – фильтровать трафик. Например перехватывать только с конкретного хоста (сайта). \*google.com – перехватывает с гугла. \* значит что принимает любые символы до google.com ([https://www.google.com](https://www.google.com/) )



Filter > show only if URL contains – можем ставить breakpoint, как только подгружается какой то конкретный элемент (например картинка) потом ее можем подменить используя after response breakpoint

Rules > Automatic breakpoints – позволяет останавливать передачу протокола, и подменять данные (полезно что бы проверить как сервер обрабатывает не валидные данные. Скажем если ввести корректный email, дабы frontend пропустил, а потом поменять на некорректный, и посмотреть как сервер обработает. Если выдаст 5хх ошибку, значит все плохо)

Rules > Automatic breakpoint > before request – до отправки запроса

Rules > Automatic breakpoint > after response – после получения ответа

Внизу есть строка [QuickExec]. Можно установить breakpoint для конкретного сайта на:

* запрос: bpu google.com
* ответ: bpa google.com
* что бы отменить пишем: bpu/bpa

Save – можно сохранить сессию в .saz формате

**Подключение телефона, что бы видеть его трафик**

*Телефон и ПК с Fiddler должны находиться в 1 сети*

Fiddler

1. Open Fiddler and select Tools -> Options
2. Choose the Connections tab
3. Select the Allow remote computers to connect checkbox to enable the setting.
4. Restart Fiddler in order the changes to take effect.

Phone:

1. Open Settings -> WiFi
2. Find your current network and click the i icon
3. Scroll to bottom and choose Manual on the HTTP Proxy choice
4. Type your IP address in the Server field
5. Type the Fiddler listening port (8888 by default) in the Port field

**CHARLES**

VPN должен быть отключен для корректной работы

*Сертификат*

#### Windows / Internet Explorer

In Charles go to the Help menu and choose "SSL Proxying > Install Charles Root Certificate". A window will appear warning you that the CA Root certificate is not trusted.

Click the "Install Certificate" button to launch the Certificate Import Wizard. The certificate must be imported into the "Trusted Root Certification Authorities" certificate store, so override the automatic certificate store selection.

Complete the wizard and your Charles Root Certificate is now installed. You may need to restart IE before the installation takes affect.

Then export certificate and Import it via Chrome, so you can use chrome as Proxy and not IE only.

Proxy > Windows Proxy

**macOS**

In Charles go to the Help menu and choose "SSL Proxying > Install Charles Root Certificate". Keychain Access will open. Find the "Charles Proxy..." entry, and double-click to get info on it. Expand the "Trust" section, and beside "When using this certificate" change it from "Use System Defaults" to "Always Trust". Then close the certificate info window, and you will be prompted for your Administrator password to update the system trust settings.

You may need to quit and reopen Safari to see the change.

-----------------------------------------------------------------------------------------------------

Proxy > SSL Proxying Settings > Enable SSL Proxying. Include – add \* for host and \* for port. – что бы запросы дешифровались

Right Click > Focus – позволяет фокусироваться только на 1 хосте. Другие хосты скрываются

*Overview* – отображает общую информацию про запрос

*Contents* – информация сверху – запрос. Инфа с низу – ответ

Breakpoints. Нажимаем Right Click на папку, или на отдельный запрос >