
Chе browser Documentation

Выпуск 0.2.2

gcc

апр. 22, 2020

1	Революционный антидетект для мультиаккаунтинга	1
1.1	Профили	1
1.2	Магазин	10
1.3	Платежи	14
1.4	Кастомизации	15
1.5	О отингерпринтах	20
1.6	Проблемы и их решения	23
1.7	Ф.А.О.	24
1.8	Контакты	31

Революционный антидетект для мультиаккаунтинга

Для создания, ведения множества аккаунтов и предотвращения банов.

Web site: beta.chebrowser.site

Version: 0.2.2

1.1 Профили

Содержание

- *Профили*
 - *Описание процесса настройки профиля (Диалоговое окно Settings)*
 - * *Настройка типа соединения: Connection*
 - * *Настройка таймзоны и языка*
 - * *Настройка WebRTC*
 - * *Настройка Geo location*
 - * *Поле «Notice»*
 - * *Кнопка «WIPE»*
 - * *Кнопка «SAVE»*
 - * *Кнопка «SAVE & RUN»*
 - * *Replacement*
 - * *Browser CLI params*

- * *Cookies manager*
- * *Advanced Options*
- * *Time shifting*

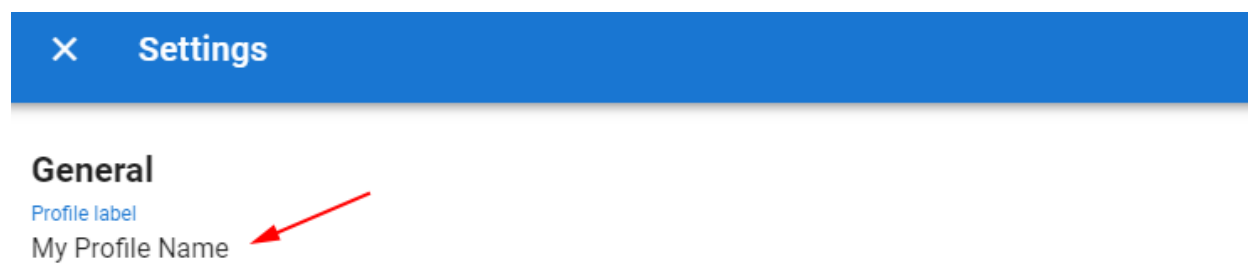
В разделе Profiles представлена таблица, в которой отображаются купленные ранее профили. Для того, чтобы запустить браузер с требуемым Вам профилем, нужно выполнить следующие действия:

- Выбрать интересующий Вас профиль (навести мышь на строку описывающую профиль)
- Кликнуть на него
- В открывшемся диалоге (Settings) указать требуемые настройки
- В верхнем правом углу диалога кликнуть на кнопку **SAVE & RUN**

Profiles		Search				
Label	Resolution	Browser	OS	Sate	Sold at	Last at
Label for Chrome Dev 78	1920x1080	Chrome Dev 78	Windows 7	off	30.01.20 00:23	04.02.20 15:49
Label for Chrome Dev 79	1024x768	Chrome Dev 78	Windows 10	off	30.01.20 16:53	31.01.20 19:12
Label for Chrome Dev 78	1920x1200	Chrome Dev 78	Windows 8.1	off	30.01.20 18:00	04.02.20 02:32

1.1.1 Описание процесса настройки профиля (Диалоговое окно Settings)

В поле **Profile label** можно ввести название, символизирующее для чего предназначен данный профиль. На пример: **facebook Ivanov Ivan**. Это название профиля будет отображаться в таблице со списком Ваших профилей. Внутри профиля, можно задать произвольное имя:



После сохранения профиля, в общем списке будет отображаться нужное вам название:

Настройка типа соединения: Connection

В данный момент поддерживается два типа соединения:

- **direct** - прямое соединение, без использования прокси
- **socks5 proxy** - соединение через socks5 прокси

Profiles Search

Label	Resolution	Browser	OS	Sate	Sold at	Last at
My Profile Name	1920x1080	Chrome Dev 78	Windows 7	off	30.01.20 00:23	04.02.20 15:49
Label for Chrome Dev 79	1024x768	Chrome Dev 78	Windows 10	off	30.01.20 16:53	31.01.20 19:12

Connection: direct

 IP

 Port

 Login

 Password

CHECK PROXY

0 / 15
0 / 5
0 / 45
0 / 45

Для того, чтобы активировать соединение через socks5 прокси, Вам следует выполнить следующие действия:

- **кликнуть на переключатель рядом со словом Connection** Вы увидите, что тип соединения сменился с direct на SOCKS5 proxy Поля **IP, Port, Login, Password** и кнопка **CHECK PROXY** стали активными
- **вбиваем данные IP, Port, Login, Password и кликаем на кнопку CHECK PROXY** Приложение выполнит проверку работоспособности указанного Вами socks5 прокси Определит внешний IP адрес и выведет его в поле **External IP** По внешнему IP адресу будут определены **Country, Region, City, Zip** и выведены в соответствующих информационных полях (в низу формы)
- если в процессе тестирования прокси возникнут ошибки, то приложение отобразит эту информацию красным цветом под переключателем типа соединения

Чтобы использовать прямое соединение, просто кликните на переключатель рядом с словом **Connection** Тип соединения будет переведен из **Connection: SOCKS5 proxy** в **Connection: direct**

При этом приложение отобразит:

- в поле **External IP** Ваш внешний IP адрес
- в информационных полях **Country, Region, City, Zip** отобразятся данные соответствующие Вашему внешнему IP адресу

Итоговый вариант должен выглядеть примерно так:

Настройка таймзоны и языка

После получения данных о внешнем IP адресе становится активна кнопка **SET AUTO** рядом с полями **Timezone** и **Language**. Кликнув на эту кнопку, можно установить автоматически определенную таймзону и язык для Вашего внешнего IP адреса.

Учтите, что если внешний IP сменится, то данные в полях **Timezone** и **Language** останутся теми, которые Вы установили ранее. Т.е. если Вы сменили socks5 прокси и страна/регион вашего внешнего

15 / 255

Connection: SOCKS5 proxy

 IP

 Port

 Login

 Password

CHECK PROXY

12 / 15
4 / 5
8 / 45
7 / 45

Connection: SOCKS5 proxy

IP: 10.10.0.5 Port: 30000 Login: Password: CHECK PROXY

Internal IP: 10.10.10.10 External IP: 18.12.33.45

Latitude: Longitude: SET AUTO

Timezone: (GMT-05:00) America/New_York Language: (en-US,en) English in United States SET AUTO

Country: China Region: Senhui City: Uhna Zip: 181255

IP изменились, то Вам может потребоваться кликнуть повторно на кнопку **SET AUTO** для установки новых значений в полях **Timezone** и **Language**.

Вы должны понимать и отдавать себе отчет, в том в какой момент Вам требуется настраивать или перенастраивать таймзону и язык. Обычно это делается при первом использовании профиля и далее оставляется без изменений, т.к. многие сайты/сервисы анализируют эти данные и могут крайне негативно относиться к их смене. На самом деле, обычный пользователь крайне редко меняет эти данные.

При нажатии на кнопку «SET AUTO» применится та таймзона и язык, к которой принадлежит IP:

Timezone: (GMT-11:00) Pacific/Pago_Pago Language: (ar-SO,ar) Arabic in Somalia SET AUTO

Настройка WebRTC

Подмена Web RTC имеет два режима:

- **WebRTC: original** В данном режиме подмена не осуществляется. И данные о WebRTC остаются в неизменном виде. Т.е. браузер возвращает реальные данные.
- **WebRTC: fake** Этот режим позволяет подменить данные WebRTC. Вам потребуется вбить в поле **Internal IP** свой фейковый внутренний IP адрес. Вы можете вбить, на пример: 192.168.1.18 (последний октет в котором содержится 18 может принимать любое значение от 1 до 254) На разных профилях рекомендуется вбивать разные внутренние IP.

Совет: Внутренние IP адреса из диапазона 10.0.0.0/24 обычно назначаются open vpn сервисами. И если Вы хотите скрыть использование open vpn, то не следует вбивать IP из этого диапазона.

В google chrome была пофикшена утечка IP локальных интерфейсов через WEB RTC. И теперь сайты не видят списка локальных интерфейсов, но все же они видят внешний IP И для подмены требуется заполнение обоих полей. В ближайших релизах функционал подмены WEB RTC вероятно будет переработан. Есть отличные идеи на эту тему.

Настройка Geo location

Подмена Geo локации имеет два режима:

- **Geo location: original** В данном режиме подмена не осуществляется. И данные о геолокации остаются в неизменном виде. Т.е. браузер возвращает реальные данные.
- **Geo location: fake** Этот режим позволяет подменить данные о Вашей геолокации. При активации режима подмены Вы можете вбить в ручную широту и долготу в соответствующие поля

Latitude и **Longitude**. Либо же кликнуть на кнопку **SET AUTO** рядом с полями широты и долготы. И приложение автоматически заполнит эти поля данными соответствующими внешнему IP адресу указанному в поле **External IP**

Совет:

Web сайты не могут скрытно опрашивать API геолокации браузера.

Когда сайт пытается обратиться к API геолокации, Ваш браузер выдаст запрос в котором укажет, какой сайт пытается получить данные о Вашей геолокации.

Нормальной практикой является - запрещать сайту получить данные о вашей геолокации.

По этой причине, Вы можете не подменять геолокацию и в момент когда браузер отобразит запрос от сайта просто запретите доступ к данным геолокации.

Поле «Notice»

В данном поле Вы можете хранить какие то заметки о текущем профиле. Оно находится в самом низу профиля.

Кнопка «WIPE»

Данная кнопка расположена в верхнем правом углу диалога **Settings** Нажатие на эту кнопку позволит очистить все пользовательские данные. Такие как: cookies, localStorage, history, ... Данное действие откатить обратно нельзя!

Кнопка «SAVE»

Данная кнопка расположена в верхнем правом углу диалога **Settings** Нажатие на эту кнопку позволит сохранить настройки профиля которые Вы указали. Имейте в виду, что сохраняемые настройки не применяются к уже запущенной сессии.

Кнопка «SAVE & RUN»

Данная кнопка также расположена в верхнем правом углу диалога **Settings**. Нажав на нее, Вы сохраните настройки профиля и запустите браузер с этими настройками. Имейте в виду, что данная кнопка может быть не активна если браузер с данным профилем уже запущен.

Replacement

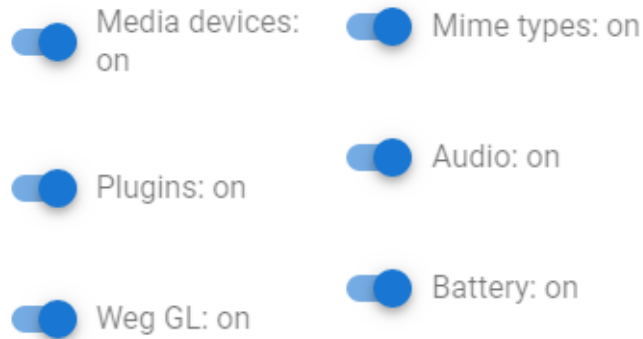
В этом блоке находятся переключатели, позволяющие включать и отключать подмену данных: media devices, mime types, plugins, web gl, audio, battery.

Данные переключатели управляют именно подменой данных. За перехват и подмену отпечатков отвечают другие механизмы.

Переключатели из блока **Replacement** рекомендуется использовать для тестирования и локализации проблем с паливом со стороны сайтов. Если Вы заметили, что на целевом сайте не работает часть функционала или странное поведение, не такое, как в обычном браузере, то рекомендуется следующая схема тестирования и выявления проблемного функционала:

- отключать по одному переключателю

Replacement

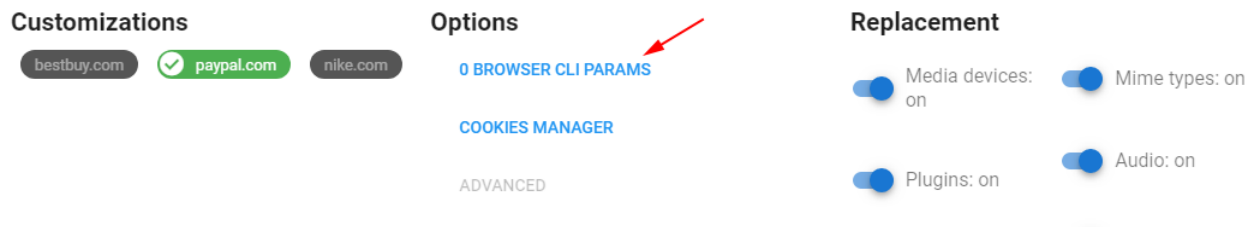


- заходить на целевой сайт/страницу и проверять изменилось ли поведение со стороны сайта
- повторять итерацию тестирования

Таким образом, Вы скорее всего сможете локализовать и понять, что конкретно не нравится сайту и какой функционал палится. Далее смело связывайтесь со мной в ПМ и скидывайте баг репорт с описанием проблемы. Я в самое кратчайшее время разберусь и пофиксую баг.

Browser CLI params

Нажатие на эту кнопку откроет модальное окно. В котором Вы можете указывать параметры командной строки для браузера:



Пожалуйста указывайте каждый параметр с новой строки - один параметр на строку.

Так будет правильно:

```
--param1  
--param2  
--param3
```

А так нет:

```
--param1 --param2 --param3
```

Список актуальных параметров Вы можете уточнить <https://peter.sh/experiments/chromium-command-line-switches>. Обратите внимание, что с каждым релизом google chrome список актуальных параметров может меняться.

Совет:

Если при тестировании **Web GL** у Вас выявилась проблема с поддержкой **Web GL2**, то попробуйте использовать параметр

```
--ignore-gpu-blacklist  
--use-angle=gl
```

В разделе *Тестирование поддержки Web GL* описан данный кейс.

Cookies manager

Нажатие на эту кнопку откроет модальное окно. В котором Вы можете импортировать или экспортировать куки для текущего профиля.

Поддерживается два формата импорта и экспорта:

- JSON
- Netscape

Обратите внимание, что при импорте возможно затирать существующие куки или обновлять их значение. По дефолту значения существующих кук будут обновляться. Если же Вы хотите что бы старые куки полностью были удалены перед импортом новых, то установите значение переключателя в положение включено, как это показано на скриншоте ниже.

Совет:

Для того что бы проверить какие куки загрузились в адресной строке браузера вбейте:
chrome://settings/siteData

Advanced Options

Кнопка «Advanced» разрешает выполнять более тонкую настройку профиля после покупки. Она находится в том же блоке «Options», где и менеджер куков:

Совет:

Если профиль еще ни разу не запускался, то редактировать эти параметры можно в любой момент времени.

После того, как вы запустите профиль первый раз, кнопка «Advanced» будет доступна **еще 15 минут**. После этого, она станет неактивной и редактирование этих параметров будет **невозможно!**

В этом блоке, вы можете скорректировать следующие параметры:

- OS
 - Разрядность
 - Версию браузера
-

Cookies manager

Import cookies

Old cookies will be wipe



JSON or Netscape cookies file

Выберите файл Файл не выбран

IMPORT

Export cookies

Export format

Netscape

EXPORT

CLOSE

Customizations

bestbuy.com

paypal.com

nike.com

Options

[0 BROWSER CLI PARAMS](#)

[COOKIES MANAGER](#)

[ADVANCED](#)

Replacement

Media devices: on

Mime types: on

Plugins: on

Audio: on

- Количество CPU
- Количество памяти
- Конфигурацию окна
- Глубину цвета
- Размеры viewport'a

А так же другие параметры браузера

Advanced options

Windows 7	64	78.0.3904.97
OS	Bits	Chrome version

Navigator	
navigator.hardwareConcurrency	navigator.deviceMemory
2	2

Screen	
screen.width	screen.height
1366	768
screen.availWidth	screen.availHeight
1366	728
screen.availLeft	screen.availTop
0	0

Time shifting

Time shifting - это сразу несколько мощнейших технологий позволяющих управлять тайминговым профилем.

- уменьшение разрешения внутренних таймеров chromium
- растягивание времени между замераами

Не секрет, что практически все крупные сайты при сборе браузерного фингерпринта обращают пристальное внимание на замеры времени тех или иных действий или функций. Тайминговый профиль это довольно обширная тема, но вот несколько примеров:

- замер времени между нажатиями кнопок на клавиатуре при заполнении формы
- замер времени перемещения мыши из точки А в точку Б
- замер времени выполнения определенного javascript функционала

Выше перечисленные техники сбора тайминговых профилей не единственные, так же существуют и другие более изощренные и навороченные. Но суть сводится к одному - это вычислить, что вбив происходит с одной и той же физической машины или одним и тем же человеком. **Time shifting** позволяет влиять и изменять тайминговые профили во всех их проявлениях.

Для включения функционала понижающего разрешение внутренних таймеров chromium следует включить галочку **Timer correction** и установить значение **timer resolution** (μs) в диапазоне от 5 до 5000 микросекунд.

- стандартное значение для chromium/chrome - 5 μs
- стандартное значение для firefox - 1000 μs

Вы можете свободно пробовать задавать любые значения из диапазона 5 - 5000 μs и подобрать то, которое для Вашего сайта будет давать приемлемый результат. Какие конкретно значения устанавливать на конкретном сайте можно вычислить опытным путём и это будет сильно меняться от сайта к сайту, но мы рекомендуем попробовать с 1000 μs .

Для включения функционала растягивания времени между замерами выберите одну из доступных стратегий

- off - отключено
- static - статически заданный % на сколько увеличивать дельту времени между замерами
- random - динамический % (из диапазона) на сколько увеличивать дельту времени между замерами

Учтите что стратегия **random** меняет значение % увеличения дельты времени между замерами при каждом рефреше страницы. Диапазон допустимых значений 0 - 10000 %.

В стратегии **static** Вы так же можете указать интересующий Вас % на который следует растягивать дельту времени при замерах. Диапазон допустимых значений 0 - 10000 %. Данная стратегия устанавливает статическое значение и не меняется при каждом рефреше страницы.

ВАЖНО: не задавайте одинаковые значения или очень близкие на всех профилях подряд, т.к. это сведет на нет всю суть технологии. На разных профилях старайтесь задавать разные значения отличающиеся на десятки, а может и сотни процентов. Опять же точные пределы в которых Вы можете работать зависят от сайта, но мы рекомендуем попробовать остановиться максимум на 300-500%.

Совет:

Данная технология еще находится в стадии доработки и если Вы испытываете проблемы при работе с какими то сайтами с включенным time shifting, то пожалуйста сообщите об этом сапорту.

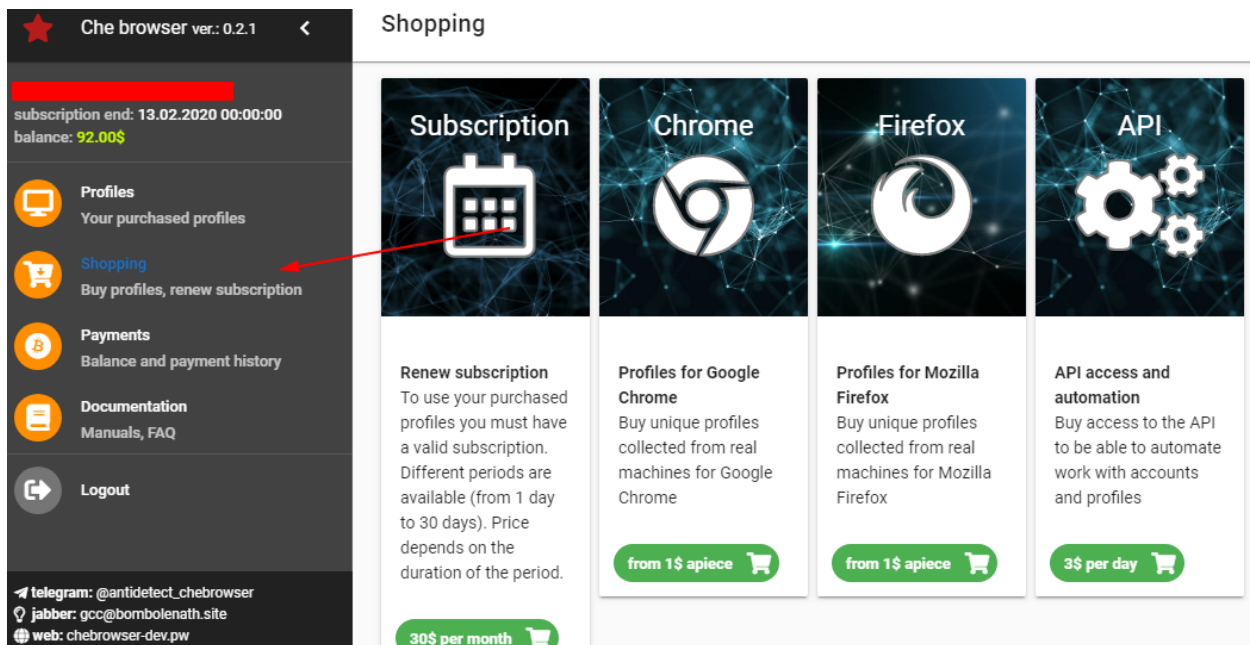
1.2 Магазин

Содержание

- *Магазин*
 - *Покупка профилей для google chrome (Диалоговое окно Checkout Chrome profiles)*
 - *Запрос на добавление кастомизаций для Ваших доменов*

В разделе Shopping представлен список товаров и услуг доступных для приобретения. Для того, чтобы приобрести товар или услугу, нужно выполнить следующие действия:

- Выбрать интересующий Вас товар или услугу
- Кликнуть
- В открывшемся диалоге выбрать интересующие вас характеристики
- В нижнем правом углу диалога кликнуть на кнопку подтверждения покупки




1.2.1 Покупка профилей для google chrome (Диалоговое окно Checkout Chrome profiles)

В соответствующих полях, Вы можете выбрать точные значения для:

- OS
- Разрядность
- Версию браузера
- Видеокарты
- Разрешение экрана
- Кастомизации под определенный сайт
- Количество профилей к покупке

Если Вам это необходимо. Если Вам не критичны вышеописанные параметры, то Вы можете оставить значение соответствующих полей по умолчанию **Any**.


Checkout Chrome profiles

 **Any** ▼

OS


Any ▼

Bits


 **Any** ▼

Chrome version


Type or choose video card

 **Any** ▼

Video card

 **Any** ▼

Resolution

 **Select customizations for target domains** ▼

Customizations

	required quantity
Quantity	1
Available quantity	7496 pieces
Total price	1 USD

[CLOSE](#) [BUY NOW](#)

Подмены fingerprints будут работать так как нужно, на тысячах сайтах, где используются распространенные библиотеки для сбора fingerprints. Хотя так же существует множество сайтов на которых используются кастомизированные или полностью уникальные решения для сбора fingerprints. Именно для этих случаев, в поле **Customization** Вы можете выбрать те домены, кастомизации для которых Вам нужны. Если при покупке профилей, Вы не указали домены для которых Вам требуются кастомизации, то Вы не получите требуемого качества подмены на этих доменах. В свою очередь, это означает, что антифрод системы сайтов, для которых есть кастомизации, будут палить Вас.






Хотелось бы обратить внимание на то, что каждая кастомизация стоит по разному. И выбор той или иной кастомизации прямо влияет на итоговую цену профиля. В ближайшее время будет специальный раздел со списком всех кастомизаций и прайсом под каждый домен.

В поле **Quantity** Вы можете указать интересующее количество профилей для покупки. И если это количество меньше или равно **Available quantity**, то можно подтвердить покупку профилей, кликнув на кнопку **BUY NOW**. Имейте в виду, что после подтверждения покупки профилей отменить покупку будет уже невозможно. Пожалуйста перепроверяйте параметры перед покупкой.

Совет:





Если под заданные параметры доступных к продаже профилей нет, то необходимо выбрать

Checkout Chrome profiles


 Windows 10  64   79.0.3945.130 


OS Bits Chrome version

Type or choose video card

 Any   Any 

Video card Resolution



bestbuy.com 

facebook.com

nike.com

paypal.com

CLOSE

BUY NOW

OS+Видео, а в остальных полях оставить «Аду». Остальные параметры можно донастроить в разделе «Advanced options» в разделе редактирования профиля

1.2.2 Запрос на добавление кастомизаций для Ваших доменов

Мы постоянно добавляем кастомизации для самых разных доменов. И если Вы не нашли кастомизации для своего домена, то Вы всегда можете написать нашей поддержке (support) запрос на добавление кастомизации для интересующего домена. В каких - то случаях добавление кастомизации может быть для Вас абсолютно бесплатным, в других же случаях, за отдельную плату. Все вопросы обсуждаются в индивидуальном порядке.

Контакты

telegram: @chebrowser

jabber: gcc@bombolenath.site

Поддержка

telegram: @chesupport

jabber: chesupport@bombolenath.site

1.3 Платежи

Содержание

- *Платежи*
 - Пополнение баланса
 - Активация промокода

1.3.1 Пополнение баланса

Вы можете пополнить баланс при помощи **bitcoin** в разделе **Payments**. Для этого:

- перейдите в раздел **Payments**
- кликните по зеленой кнопке **ADD MONEY TO BALANCE** находящейся в верхнем правом углу
- после клика вы увидите модальное окно с формой оплаты и инструкцией как оплатить
- в открывшемся модальном окне найдите поле **Amount USD** и введите требуемую сумму в **USD** (на пример 100\$)
- в поле **Total**, указанная Вами сумма в **USD**, автоматически пересчитается в **BTC**
- переведите получившееся в **Total** количество **BTC** на кошелек указанный в поле **Pay to BTC address**
- после трех подтверждений сети деньги автоматически зачислятся на Ваш внутренний баланс и Вы сможете приобретать товары и услуги

Совет:**Предостережение**

Пополнение баланса осуществляется самим пользователем в личном кабинете (в приложении).

Весь процесс полностью автоматизирован и не требуется никакая сторонняя помощь.

Если к Вам обращаются с предложением пополнить баланс в ручном режиме и на какие-то сторонние кошельки, то очень вероятно, что это мошенники.

Будьте бдительны и не поддавайтесь на уловки.

1.3.2 Активация промокода

Вы можете активировать промокод в разделе **Payments**. Для этого:

- перейдите в раздел **Payments**
- кликните по синей кнопке **REDEEM PROMO CODE** находящейся в верхнем правом углу
- после клика вы увидите модальное окно с формой активации промокода
- в поле **Promo code** вставьте выданный Вам код
- нажмите на кнопку **REDEEM**

После активации Вы получите бесплатную подписку и некоторое количество профилей. Номинал промокода может варьироваться и выбирается партнером выдавшим Вам код.

Совет:

Промокод можно активировать только один раз и только до первого пополнения баланса!

Все промокоды **выдаются бесплатно!**

Если Вам предлагают купить промокод, то скорее всего Вы столкнулись с мошенником.

1.4 Кастомизации

Содержание

- *Кастомизации*
 - *Что это такое?*
 - *Сообщение о том, что кастомизация/сэмплы не найдены*
 - *bestbuy.com*
 - *facebook.com*
 - *paypal.com*
 - *amazon.com*
 - *Заказать разработку кастомизации*

1.4.1 Что это такое?

Кастомизация - **адаптация антидетекта** под подмену конкретной реализации того или иного вида отпечатка.

Кастомизация состоит из нескольких частей:

- сбор сэмплов-образцов данных с реальных браузеров (точно таким же кодом как на целевом сайте)
- сэмплы-образцы данных собранные с реальных браузеров
- механизм подмены данных при посещении целевого сайта

Кастомизации могут быть заточены под конкретные сайты (на пример под **paypal.com**) и **массовые**, те которые работают **на тысячах сайтах**.

Как было сказано выше, существуют **публичные javascript библиотеки** для организации браузерного фингерпринтинга. Эти библиотеки используются на **тысячах сайтах**. И **кастомизации** для этих библиотек включены в каждый профиль по дефолту. Т.е. при покупке профиля дополнительно ничего не нужно докупать.

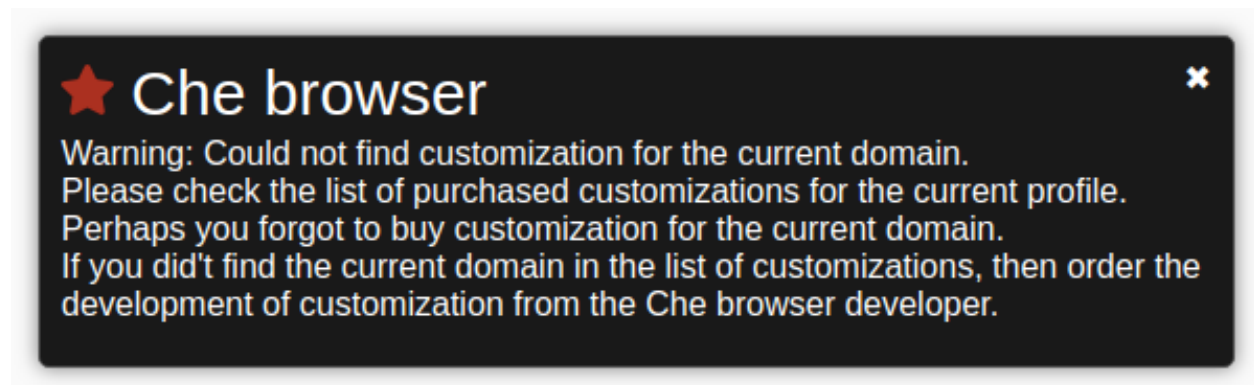
Хотя следует отметить, что есть и кастомизации **под конкретные сайты**.

Список этих кастомизаций постоянно пополняется и обновляется.

Т.к. разработка кастомизаций под конкретные сайты бывает довольно не тривиальной задачей, то они тарифицируются отдельно.

В ближайшее время будет реализован специальный раздел со списком и ценами на кастомизации по конкретным доменам.

1.4.2 Сообщение о том, что кастомизация/сэмплы не найдены



В процессе работы Вы можете встречать сообщение о том, что **Che browser** не смог найти кастомизацию или сэмплы для подмены **canvas/audio фингерпринтов**.

Это может свидетельствовать о следующем:

- **на сайте используется уникальное решение для сбора фингерпринта и требуется разработка кастомизации**
О разработке кастомизаций читайте ниже.
- **Вы забыли приобрести кастомизацию для данного домена в момент покупки профиля.**
При учете того, что под данный домен уже реализована кастомизация и доступна для

приобретения. Пожалуйста проверьте приобретена ли требуемая кастомизация для используемого профиля. Посмотреть это можно в окне **Settings** - настройки профиля. В поле **Customizations** рядом с названием требуемого домена должна стоять галочка ✓

- **установленный в системе google chrome не поддерживает WebGL1 или WebGL2**

Прочитайте пункт документации *Тестирование поддержки Web GL*

- **иногда бывает ложное срабатывание.** На сайте используются какие то методы которые так же могут использоваться при сборе фингерпринта, но совершенно в других целях. На пример для **проигрывания звука** или отрисовки картинок на **canvas**.

Так же, иногда после обновления ОС может перестать работать web gl2 и в профилях с кастомизацией на сайтах может начать отображаться, что Че не смог подобрать семплы. В таких ситуациях проверьте работоспособность web gl2. Как это сделать описано в разделе *Тестирование поддержки Web GL*

В любом случае Вы можете просто закрыть сообщение. А работать или не работать дальше зависит от выше описанных пунктов.

1.4.3 bestbuy.com

Эту кастомизацию нужно приобрести при покупке профиля если Вы планируете работать с данным ресурсом. Особых указаний по использованию нет.

1.4.4 facebook.com

Facebook полностью отказался от canvas фингерпринта. И очень активно использует замеры времени для фингерпринта браузера и пользователя. По этой причине рекомендуем использовать *Time shifting* - эта технология позволит влиять на фингерпринты основанные на замерах времени.

1.4.5 paypal.com

Укажите данную кастомизацию при покупке профиля если планируете взаимодействовать с paypal.com или ebay.com. В самое ближайшее время будет проведен аудит кода paypal и внесены коррективы, если они требуются.

Так же хотелось бы отметить, что в ближайших релизах будет доработан функционал для взаимодействия с ebay.com. Т.к. было выявлено еще несколько механизмов при помощи которых ebay.com персонализирует Ваш компьютер.

Совет:

Paypal так же как и многие другие сайт активно использует методики фингерпринта основанные на замераз времени.

Производятся замеры времени работы кусков js кода, замеряется время между нажатиями кнопок на клавиатуре, замеряется время возникновения событий mousemove и тд. и тп.

По этой причине крайне рекомендует использовать *Time shifting*, что позволит качественно влиять на выше описанные замеры времени.

И тем самым менять фингерпринты основанные на замерах времени.

1.4.6 amazon.com

Фингерпринт в амазон реализован не совсем стандартным образом. Общая схема canvas фингерпринта выглядит так:

- Первый этап: классический canvas фингерпринт. На canvas рисуются различные геометрические фигуры и накладывается статический текст.
- Второй этап: на картинку из первого этапа накладывается текст с email адресом логина
- Третий этап: амазон получает сырые данные из CanvasRenderingContext2D и строит по этим данным гистограмму

Таким образом амазон отслеживает изменение железа и привязку акаунта к данному железу. И исходя из выше описанной схемы следует, то что нельзя просто собрать один раз данные с реального браузера. Т.к. при сборе данных наша система еще не знает какой email Вы будете использовать для логина. По этой причине был реализован много ступенчатый сбор данных. Во время сбора профиля мы собираем canvas фингерпринт из первого этапа. Далее, после того как Вы приобрели профиль Вам нужно указать какие email адреса будут использоваться в этом профиле при входе в амазон. После этого сборщик профилей отслеживает появление подходящего браузера и собирает данные из второго и третьего этапов.

Т.е. после приобретения и настройки профиля Вам нужно будет дождаться, когда сборщик профилей до собирет требуемые сэмплы. И только после этого Вы сможете использовать этот профиль. После того как все необходимые данные будут собраны при логине в амазон Вы не увидите сообщений о том, что каки либо сэмплы не были найдены ЧЕ.

И так, для работы с кастомизацией под амазон Вам нужно выполнить следующие действия

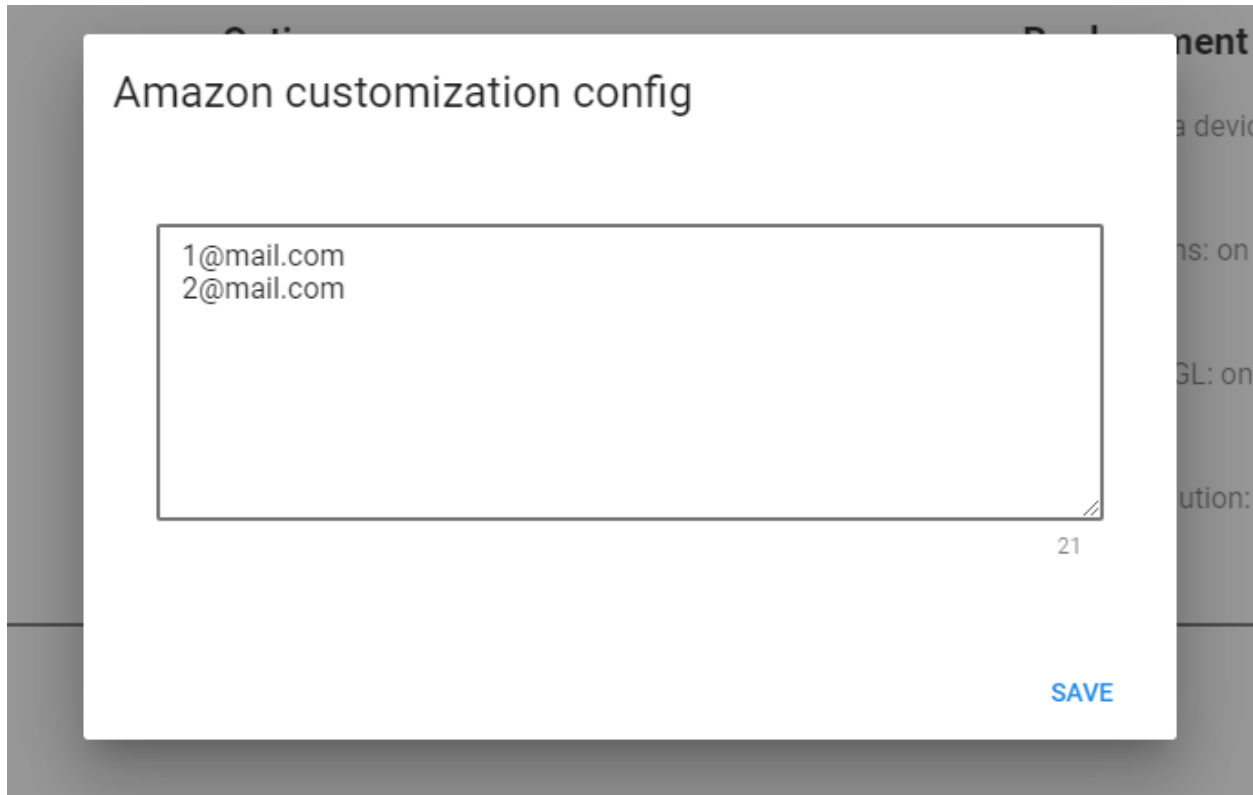
- приобрести профиль с кастомизацией под amazon.com
- в настройках профиля (в блоке Customization) найти бэдж в котором будет написано amazon.com
- кликнуть на иконку, как показано на картинке ниже
- в открывшемся модальном окне ввести список email адресов под которыми Вы планируете логиниться в amazon.com. Каждый email должен располагаться на новой строке.
- дождаться когда сборщик профилей до собирет данные с подходящего браузера
- после того как в настройках профиля исчезнет плашка с информацией о том, что еще не все сэмплы собраны можно приступать к работе

Customizations



Обязательно дождитесь когда эта плашка исчезнет и только после этого начинайте работу.

Сбор требуемых семплов осуществляется только с подходящего браузера (зависит от ОС, браузера и драйверов видео карты). В среднем сбор данных в дневное время может занимать несколько часов. В ближайшее время мы увеличим кол-во сайтов на которых размещаются скрипты сбора профилей и процесс до сбора семплов будет проходить на много быстрее.



Совет:

Amazon так же как и многие другие сайт активно использует методики фингерпринта основанные на замераз времени.

Производятся замеры времени работы кусков js кода, замеряется время между нажатиями кнопок на клавиатуре, замеряется время возникновения событий mousemove и тд. и тп.

По этой причине крайне рекомендует использовать *Time shifting*, что позволит качественно влиять на выше описанные замеры времени.

И тем самым менять фингерпринты основанные на замерах времени.

1.4.7 Заказать разработку кастомизации

Вы всегда можете обратиться с вопросом о разработке кастомизации **под интересующий Вас сайт**.

Кастомизации могут быть как **приватными** - не доступны для широкой публики.

Так и **паблик** - доступны всем пользователям продукта и представлены в общем списке.

Все условия и цены обсуждаются в индивидуальном порядке. Заявки под кастомизации оставлять нашей поддержке.

Контакты

telegram: @chebrowser

jabber: gcc@bombolenath.site

Поддержка

telegram: @chesupport

jabber: chesupport@bombolenath.site

1.5 О фингерпринтах

Содержание

- *О фингерпринтах*
 - *Виртуальные машины*
 - *OS фингерпринтинг*
 - *Идеальный антидетект*
 - *Куки, трек, счетчики, виджеты*

1.5.1 Виртуальные машины

При помощи javascript можно довольно точно определять, запущен браузер в виртуальной машине или на реальном железе.

Мне известны, по крайней мере, две техники детекта виртуалок при помощи js из браузера. Хотя я склонен полагать, что подобных техник существует куда больше.

На данном этапе я не вижу адекватных методов противодействия подобным техникам детекта. По этой причине, если Вы хотите добиться максимальной маскировки, то я рекомендую запускать софт на реальном железе, а не в виртуалках.

1.5.2 OS фингерпринтинг

Хотелось бы обозначить, то что при помощи javascript можно определять на какой OS запущен браузер. Зачастую это делается по анализу реализации низкоуровневого функционала OS/системных библиотек, которым пользуется браузер.

Например это могут быть особенности вычисления чисел с плавающей запятой.

На данном этапе я не вижу адекватных методов противодействия подобным техникам детекта. По этой причине, если Вы хотите добиться максимальной маскировки, то я рекомендую запускать софт на той же ОС профиль которой Вы используете в антидетекте.

1.5.3 Идеальный антидетект

При качественном браузерном фингерпринтинге зачастую анализируется низкоуровневый, платформозависимый, железозависимый функционал OS, системных библиотек, драйверов и тп.

По этой причине реализовать антидетект, который работал бы одинаково хорошо на всех сайтах, технически не представляется возможным.

Приведу простой пример с **canvas фингерпринтом**. Суть метода проста - отрисовка текста и геометрических фигур на **canvas** таким образом, что бы задействовать низкоуровневый системный функционал.

Примером такого функционала может быть рендеринг шрифтов при отрисовки текста на **canvas**. Рендеринг шрифтов очень сильно зависит от OS, драйверов видео карты и системных библиотек.

Две картинки отрисованные на разных компьютерах (с разным железом) при помощи одного и того же javascript кода будут отличаться. Визуально они будут выглядеть практически одинаково, но если сравнивать их попиксельно, то различия будут очевидны.

Из данного примера становится понятно, что невозможно эмулировать рендеринг шрифтов на машине с видео картой одного вендора, так же как на машине с видео картой другого вендора.

Собранные данные при помощи **canvas фингерпринта** отправляются на backend. Где в свою очередь проходят **статистический анализ**.

Этот анализ позволяет легко выявлять **фэйковые сэмплы-образцы**, такие как:

- сэмплы-образцы с наложением шума (**слишком уникальные образцы**)
- сэмплы-образцы сгенерированные не на той OS/видеокарте, что заявлена

Плюс следует учитывать, что реализация **canvas фингерпринта** может отличаться от сайта к сайту. К примеру на сайте **paypal.com** на **canvas** накладывается текст: **PayPal.com, <!@#%>**

Хотя также следует сказать, что тысячи сайтов используют хорошо зарекомендовавшие себя публичные библиотеки для браузерного фингерпринтинга.

Исходя из выше сказанного, было принято решение развивать софт по пути кастомизаций. Т.е. **сбирать сэмплы-образцы** данных с реальных браузеров тем же кодом, что и сайты. И в момент посещения целевого сайта выдавать ранее собранные данные. По сути получается, что сайты получают реальные данные, а не синтетически сгенерированные.

1.5.4 Куки, трек, счетчики, виджеты

Для многих я точно не открою Америку.

Хотя считаю нужным затронуть эту тему, вероятно какой-то части пользователей эта информация будет полезна.

Очень долгое время существуют разномастные конторы, которые собирают информацию о посещении различных сайтов пользователями.

Виджеты и скрипты установленные на множестве сайтов проставляют куки (маркируют пользователя) и отстукивают на базу информацию о браузере и действии пользователя.

Таким образом, создается след пользователя (трек) по которому можно проследить на каких сайтах/страницах пользователь был, сколько времени провел, что читал, куда кликал (тепловые карты) и тп.

По этому следу можно понять:

- интересы пользователя
- пол
- возраст
- наличие профилей в соцсетях

И уйму другой информации. Данную информацию активно продают и обменивают эти конторы между собой.

Не так давно, тот же **facebook** был пойман за руку на продаже подобной информации. Хотел бы напомнить, что у **facebook** кроме своего сайта есть еще и виджеты которые установлены на **миллионах сайтов**. И **facebook** может отслеживать, чем Вы интересуетесь и какие сайты посещаете да же вне своей площадки.

Данная информация помогает качественно таргетировать рекламу. Но я хотел бы обратить внимание, что и в работе антифрод систем анализ подобной информации о пользователе помогает отлично выявлять фрод.

Если Вы пришли на целевой сайт без подобного наработанного следа, то велика вероятность, что Ваши действия будут рассматривать под микроскопом. Т.е. ни о какой автоматике речи тут уже идти не может. Анализом вашей транзакции, с большой долей вероятности, будет заниматься специально обученный индус.

Вопрос относительно кук и следа вашей фейковой личности остается открытым. С какой стороны к нему подойти - это решать Вам.

Из очевидных методов:

- **покупка кук в шопах**

Тут стоит отметить, что если Вы покупаете только куки и пихаете их в браузер, то информация о браузерах будет не совпадать.

Т.е. информация о браузере откуда куки и информация о браузере профиля будут отличаться.

Кроме информации естественно будут отличаться и отпечатки пальцев.

Хотя, как показывает практика наличие кук с историей и треком решает множество проблем.

- **нагулять трек и куки самостоятельно**

Речь идет о банальном фарминге. Т.е. Вы можете «выгуливать» профиль самостоятельно.

Посещая различные сайты, поисковики, сервисы, ...
 Изображая активность обычного пользователя.
 Этот процесс не быстрый и для некоторых сервисов может занимать недели.

1.6 Проблемы и их решения

Содержание

- *Проблемы и их решения*
 - *Тестирование поддержки Web GL*
 - *Браузер подвисает на некоторых сайтах*
 - *Proxifier и проблемы с софтом*

1.6.1 Тестирование поддержки Web GL

Для полноценной работы **Che browser** требуется поддержка **WebGL1** и **WebGL2**.

Что бы протестировать Ваш браузер выполните следующие действия:

- **запустите установленный google chrome** Через ярлык с рабочего стола. Не через антитекст!
- перейдите на страницу: <https://beta.chebrowser.site/tools/webgl>
- **вы должны увидеть сообщение о том, что WebGL1 и WebGL2 поддерживаются** (надписи будут з...

Test Web GL support

Web GL 1 - ✓ support

Web GL 2 - ✓ support

- **если же Вы увидите, что WebGL1 или WebGL2 не поддерживается, то Вы не сможете полноценно**
 Т.к. профили собираются с реальных машин с полной поддержкой **WebGL**.

Google ведет черный список драйверов видео карт в которых были выявлены проблемы с безопасностью. Скорее всего, Ваш драйвер попал в этот список. И по этой причине у Вас не работает **WebGL2**.

Общее решение для всех систем

Вы можете попробовать отключить этот черный список, благо в chrome есть специальный параметр.

- В настройках требуемого профиля найдите кнопку *Browser CLI params* и кликните на нее.
- В появившемся модальном окне в поле для ввода параметров введите

```
--ignore-gpu-blacklist
```

```
--use-angle=gl
```

- Закройте модальное окно кликнув на кнопку **Close**.

После этого, запускайте браузер и попробуйте пройти тест повторно. В большинстве случаев проблема будет решена.

Решение для windows 7

- если у Вас отключена служба Windows Update, то запускаете ее
- скачайте update **KB2670838** по ссылке <https://www.microsoft.com/en-us/download/details.aspx?id=36805>
- установите
- перезагрузите систему
- отключаете службу Windows Update если Вам это необходимо

1.6.2 Браузер подвисает на некоторых сайтах

Если Вы обнаружите что-то подобное пожалуйста напишите в jabber или телеграм. Будем править.

1.6.3 Proxifier и проблемы с софтом

Proxifier инжектится во все процессы и процессы che browser не исключение.

Если в proxifier будет установлен не рабочий socks проху, то процессы che browser не смогут получить доступ к сети. И по этой причине могут возникать различные ошибки.

Если у Вас в системе установлен proxifier и Вы наблюдаете ошибки при работе с che browser, то отключите proxifier и попробуйте перезапустить che browser.

1.7 F.A.Q.

Содержание

- *F.A.Q.*
 - *Как это все работает?*
 - *Профили*
 - *Памятка по горизонтальному скроллу страницы при больших разрешениях*
 - *Не отображается контент в новом окне*
 - *Тип подмены разрешения*
 - *Смена сокса без перезагрузки сессии*
 - *Утечка DNS*
 - *IPv6*
 - *Request failed with status code 419*
 - *Почему на browserleaks.com я вижу одинаковые отпечатки?*

- *Использование совместно с 911 proxy*
- *Использование совместно с 911 proxy (Вариант #2)*
- *Системные требования*

1.7.1 Как это все работает?

Данный софт состоит из нескольких частей:

- **нативное приложение запускаемое на linux или windows**
 - Позволяет удобно управлять множеством профилей браузеров
 - Приобретать профили собранные с реальных браузеров
 - Пополнять баланс
 - Продлевать аренду
- **расширение для браузера chrome**
 - Выполняет подмены различных данных
 - перехватывает и корректирует разные техники фингерпринта
 - Применяет кастомизации реализованные под определенные сайты
- пропатченная версия браузера chromium

1.7.2 Профили

Профиль браузера - это набор самых разнообразных данных, из которых в последствии антифрод системы составляют уникальный отпечаток.

Все предоставляемые нами профили:

- были собраны с реальных устройств
- предоставляются только в одни руки
- не содержат генеренных данных
- не содержат ГМО ;)

1.7.3 Памятка по горизонтальному скроллу страницы при больших разрешениях

Мы перенесли подмену разрешения из расширения на уровень исходников хромium и постарались сделать так, что бы сайты и сервисы получали максимально точные значения разрешения экрана, размера окна, размера вьюпорта и тп. По этой причине мы решили отображать страницу реального размера. Если разрешение профиля будет больше чем физическое разрешение Вашего экрана, то Вы увидите страницу уходящую за правый край окна. Не пугайтесь отсутствию скроллбаров и для горизонтального скролла страницы используйте следующие приемы

- Нажмите среднюю кнопку мыши и просто тяните страницу влево или вправо, в зависимости куда Вам нужно отскроллить страницу (предпочтительный вариант)
- Так же можно скроллить кнопками клавиатуры стрелками в лево и в право

- Либо же можно зажать шифт и крутить колесо мыши

Имейте в виду, что некоторые сайты (на пример raural.com) собирают информацию по нажатию кнопок клавиатуры, трекинг перемещения мыши. По этой причине на данном этапе мы рекомендуем скроллить посредством зажатия средней кнопки мыши. Мы работаем над еще одним более интеллектуальным и удобным способом скролла. Он появится в одном из ближайших релизов. К сожалению пока пришлось отказаться от обычных скроллов, т.к. их использование будет заметно специально обученному индусу, который будет разбирать инциденты.

1.7.4 Не отображается контент в новом окне

Некоторые сайты могут открывать новое окно браузера. В котором может выполняться какой то функционал или отображаться какая то информация. В том случае если Ваше реальное разрешение экрана меньше разрешения профиля, Вы можете лицезреть небольшое окно в котором просто однотонный фон (обычно белый). В этом случае просто растяните это окно мышью. Контент может быть отцентрирован на странице и он просто не помещается в видимую область. Данная недоработка будет пофикшена в ближайших релизах.

1.7.5 Тип подмены разрешения

Поддерживается два типа подмены разрешения новый - native и старый - extension.

- native - эта подмена производится на уровне исходников хрома и имеет некоторые недоработки со скролом
- extension - данная подмена производится на уровне расширения и недостатки в работе выявлены не были

Имейте в виду, что данные два типа подмены реализованы координально разным образом. Используйте ту которая Вам максимально удобна и показывает хорошие результаты при работе с аккаунтами.

1.7.6 Смена сокса без перезагрузки сессии

Если во время сессии у Вас в друг перестал работать сокс, то Вы можете просто открыть профиль на редактирование и сменить сокс на новый. При этом браузер перезагружать не нужно. Все соединения пойдут через новый сокс. Хотя следует отметить, что при подмене web rtc останется прежний внешний адрес сокса. Данное поведение будет исправлено в последующих релизах. Если Вы используете ф-цию подмены web rtc, то Вам придется перезагрузить сессию.

1.7.7 Утечка DNS

В chrome браузере имеется не очень приятный баг. При первом запуске браузера (с новым профилем) DNS трафик периодами начинает течь в обход сокса. По этой причине, приходится автоматически закрывать окно браузера при первом запуске и перезапускать браузер снова. Имейте это ввиду и не пугайтесь, когда окно браузера бьмает при первом запуске с новым профилем.

1.7.8 IPv6

Мы настоятельно рекомендуем в системе отключать IPv6! Да бы иселючить любые утечки через этот протокол. Следует понимать, что все поставщики socks проху, что присутствуют в данный момент на рынке предоставляют решения поддерживающие только IPv4 протокол.

Replacement

Media devices: on

Mime types: on

Plugins: on

Audio: on

Weg GL: on

Battery: on

Resolution: native



1.7.9 Request failed with status code 419

Если Вы видите данное сообщение, то это говорит о том, что сессия завершилась. Просто перезагрузите софт и можно работать дальше.

1.7.10 Почему на browserleaks.com я вижу одинаковые отпечатки?

Если при тестировании Вы видите одинаковый отпечаток (на пример canvas) на разных профилях, вероятно Вы еще не прочитали документацию полностью. Пожалуйста, выделить совсем чуть-чуть времени и сделать это. Начните с раздела *Кастомизации*

Замечу, что на <https://browserleaks.com/> используется своя реализация сбора canvas отпечатка. Кастомизацию конкретно под <https://browserleaks.com/> я не стал реализовывать, т.к. не вижу смысла пускать пыль в глаза.

Попробуйте лучше кастомизацию под bestbuy.com ;))

1.7.11 Использование совместно с 911 proxy

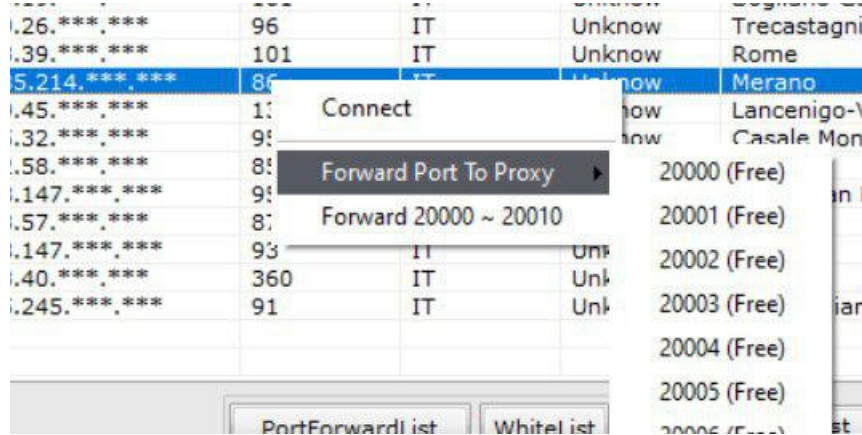
В 911 настраиваем port forwarding

- Port Forwarding — 20000-20010
- Proxy Tool — Other Proxy Tools

Выбор socks5 proxy

- кликаем правой кнопкой мыши
- выбираем свободный порт

В che browser в настройках socks5 proxy вписываем ip 127.0.0.1 и выбранный ранее порт.



General

Profile label
Label for Chrome Dev 78

Connection: SOCKS5 proxy
 WebRTC: original
 Geo location: fake

IP: 127.0.0.1 | Port: 20001 | Login: | Password: | [CHECK PROXY](#)

Internal IP: 71.83.176.25 | External IP: 71.83.176.25

Latitude: 42.1253 | Longitude: -71.1074 | [SET AUTO](#)

Timezone: (GMT-05:00) America/New_York | Language: (en-US,en) English in United States | [SET AUTO](#)

Country: United States | Region: California | City: Riverside | Zip: 92506

Customizations

- paypal.com
- nike.com
- bestbuy.com

Options

[BROWSER CLI PARAMS](#)

COOKIES MANAGER

Replacement

- Screen: on
- Window: on
- Media devices: on
- Mime types: on

1.7.12 Использование совместно с 911 проху (Вариант #2)

Данный вариант исключает утечку DNS и для его реализации Вам потребуется proxifier.

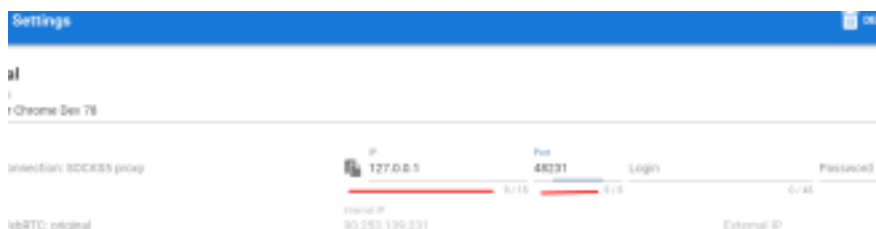
- в 911 настраиваем port forwarding: 20000-20050
- proxy port: custom (выставляется автоматически)
- proxy settings: Proxifier standart edition
- proxy rules: only «proxy» the applications in 911 s5 program tab, the others go through your local network
- Выбор socks5 proxy
- кликаем левой кнопкой мыши два раза



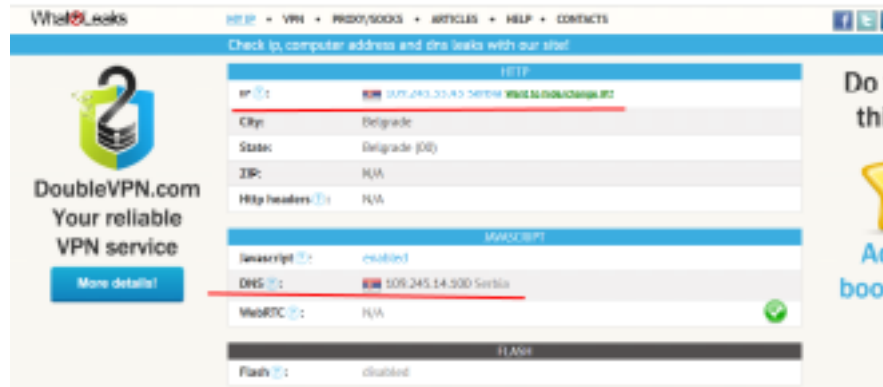
Во вкладке Program - выбираем наш браузер (если его нет то добавляем +)

ProxyIP	Ping	Country
82.78.***.***	104	RO
96.44.***.***	24	US
88.130.***.***	75	DE
108.20.***.***	91	US
86.0.***.***	87	GB
193.24.***.***	79	HR
86.24.***.***	85	GB
98.29.***.***	41	US
93.32.***.***	77	IT
146.241.***.***	86	IT
41.***.***.***	***	***

В che browser в настройках socks5 проху вписываем ip 127.0.0.1 и выбранный ранее custom порт



Проверяем



1.7.13 Системные требования

Виртуальная или реальная машина на windows 7 или windows 10.

- RAM от 2ГБ (лучше 4ГБ+)
- CPU 1 ядро (лучше 2+)

1.8 Контакты

1.8.1 Проект

web site: chebrowser.site

telegram group: @antidetct_chebrowser

telegram channel: @antidetct_chebrowser_channel

1.8.2 Разработчик

telegram: @chebrowser

jabber: gcc@bombolenath.site

Поддержка

telegram: @chesupport

jabber: chesupport@bombolenath.site

Проект

telegram group: @antidetct_chebrowser

telegram channel: @antidetct_chebrowser_channel

Разработчик

telegram: @chebrowser

jabber: *gcc@bombolenath.site*

Поддержка

telegram: @chesupport

jabber: *chesupport@bombolenath.site*