Автор: Sinhammer
22.06.2008 23:17 -

При соединении с интернет пользователь получает от провайдера уникальный номер – IP адрес. Причем выделяется не любой адрес, а свободный из диапазона IP адресов, выделенный данному провайдеру.
Таким образом, зная IP адрес, можно легко определить провайдера и соответственно страну, населенный пункт, адрес провайдера.
Учитывая, что провайдеры обязаны записывать историю каждого соединения, про анонимность в сети можно забыть.
Некоторые пользователи могут быть соединены в местную (локальную) сеть, управляемую сервером, и именно сервер соединяется с интернет и получает IP адрес. Таким образом все пользователи локальной сети имеют один интернет IP адрес. Такие локальные сети используются как правило организациями.
Казалось бы, вот она – анонимность! Однако сервер организации конечно же записывает историю как соединения с интернет, так и историю соединений по локальной сети.
Да и компьютер пользователя записывает столько информации о его действиях, причем в самых неожиданных местах, что надо быть очень подготовленным специалистом, чтобы стереть за собой следы.
Получается, что главная информация по которой можно идентифицировать посетителя сайта – его IP адрес.
Вы можете легко узнать IP адрес, который назначен Вам в настоящий момент.
А на сервисе whois ip получите все данные о провайдере, его диапазоне адресов, контактную информацию.
Скрыть свой IP адрес можно с помощью так называемых прокси-серверов, которые пропускают через себя поток данных как от пользователя к сайту, так и в обратную сторону. А сайту "виден" только IP адрес прокси-сервера.
Но как правило полностью анонимные прокси встречаются крайне редко. Большинство из них выдают свое присутствие, сообщая сайту не только о своем участии, но и IP адрес пользователя. Такие прокси служат в основном для уменьшения трафика, сохраняя в своей памяти часто посещаемые страницы сайтов.
Даже если Вы нашли такой полностью анонимный прокси, то можно задуматься, зачем и кому понадобилось это сделать.
Еще и поэтому взломщики распространяют вирусы, чтобы зараженные компьютеры пользователей использовать в качестве анонимных прокси, подставляя естественно самого пользователя.
Браузеры также "сообщают" о себе массу сведений, например о языке пользователя, операционной системе и других, служащих для корректности отображения страницы сайта. На картинке видно, какие именно сведения может сообщать о себе браузер сайту.

Язык программирования, встроенный в браузер – JavaScript, также может "сообщить" сайту о параметрах экрана монитора, версии браузера, также о языке пользователя, операционной системе. Пример таких сведений показан на другой картинке.

Если посетителя не пускают на сайт, то можно отсоединиться от сети и подключиться вновь, тем самым получив от провайдера другой IP адрес в пределах диапазона адресов провайдера. Желательно сменить браузер, благо имеется несколько разновидностей. Конечно владелец сайта может заблокирокировать доступ к сайту из всего диапазона IP адресов провайдера, но скорее всего только на время, поскольку крупные провайдеры могут обслуживать до половины большого города, так что владелец сайта заблокирует заодно и других посетителей.
Для других сайтов бывает необходимо все-таки применение прокси, пусть даже и не анонимного. На таких сайтах не проводится проверка на использование прокси. В таком случае нужно стереть так называемые файлы cookie, либо включить опцию в браузере Opera, кстати самом безопасном, очищать cookie при выходе. В интернете можно легко найти списки таких прокси, только необходимо проверять их на работоспособность непосредственно перед применением.
Если же необходимо применение полностью анонимных прокси, то их списки проще купить, чем найти или создать самому. Но проверка на работоспособность и анонимность перед применением обязательна. Можно выявить применение прокси, в том числе и анонимных, заставив посетеля открыть флеш-картинку или какой-нибудь документ (Word) с картинкой или включить поддержку Java в браузере, и Ваш истинный IP адрес будет выявлен. Что бы скрыть все-таки IP адрес, нужны программы, полностью перехватывающие сетевой трафик и направляющие его через прокси.
Принудив посетителя включить поддержку полноценного языка программирования Java в браузере, можно получить полные сведения об операционной системе, в том числе mac адрес, т.е. уникальный адрес сетевой карты, и таким образом точно идентифицировать компьютер посетителя. Однако и программ, меняющих (подменяющих) mac адрес имеется предостаточно. И сменить операционную систему легко, загрузившись с одного из многочисленных LiveCD.
Для обеспечения анонимности можно воспользоваться платными анонимайзерами, имеющими некоторую репутацию. Но все равно нет уверенности, что на таких сервисах не ведется логов (истории соединений). Большинство же бесплатных анонимайзеров сразу выдают свое участие, да для владельцев сайтов нетрудно получить их список с IP адресами
Таким образом обеспечить себе анонимность в сети можно, либо обладая серьезными знаниями в области сетевой безопасности, либо заплатив некоторую сумму денег, но и анонимность в таком случае все-таки будет под вопросом.