честный обмен провадера с помощью google web accelerator

крис каспески ака мыщъх, a.k.a nezumi el raton, no-email

интернет редко бывает хорошим и дешевым одновременно, что толкает многих хакеров на незаконные действия, зачастую заканчивающиеся условной судимостью, если не хуже, но мы пойдем другим путем — загрузим google web accelerator и путем ковыряния в настройках, выжмем из него все, на что он только способен (в том числе застав его работать на официально неподдерживаемой опере), сэкономив как на модемном подключении, так и на DSL, причем при настройках по умолчанию на DSL'е можно "попасть" на трафик, который google web accelerator генерирует в очень больших количествах.

введение

Программы, ускоряющие доступ в сеть и экономящие трафик (с общим названием "акселераторы"), появились не вчера и даже не позавчера, а очень давно появились. Делятся они на две больших группы — хорошие (платные) и отстойные (бесплатные). Google создал свой собственный акселератор, занимающий промежуточное положение между ними и потому представляющий для любителей халявы огромный интерес. Настолько огромный, что первое время после запуска проекта, Google был вынужден прикрыть к нему доступ, поскольку имеющихся вычислительных мощностей и пропускной способности сетевых каналов для обслуживания всех желающих оказалось недостаточно.

И вот сейчас доступ открыт вновь (правда неизвестно — надолго ли), так что ловите свой шанс! Google web-accelerator (далее по тексту для краткости называемый просто GWA), действительно _реально_ увеличивает скорость работы с web'ом или экономит трафик (именно "или" — согласно основному правилу оптимизации: за все приходится платить и улучшая одни показатели мы неизбежно ухудшаем другие). И хотя GWA _значительно_ отстает от своих коммерческих конкурентов (о которых мы поговорим в отдельной врезке), он бесплатен, что для многих является решающим фактором.

установка GWA на свой компьютер

Заходим на www.google.com, видим там ссылку "more", щелкаем по ней, в открывшемся окне выбираем "even more" и там среди множества проектов в самом низу находим затерявшийся "Web Accelerator": http://webaccelerator.google.com. Давим по кнопке "download now" (интересно, почему еще никто не догадался написать "download latter"?) и получаем в свое распоряжение файл GoogleWebAcceleratorSetup.msi весом "всего" в полтора мегабайта (см. рис. 1), содержащий версии акселератора под Горящего Лиса и IE. Только так — обе версии сразу и никак по раздельности! Ну да ладно, не будем обижаться, даже если у нас нету Лиса или мы, как настоящие хакеры, давно забили на IE, полтора мегабайта не повод для жалоб.

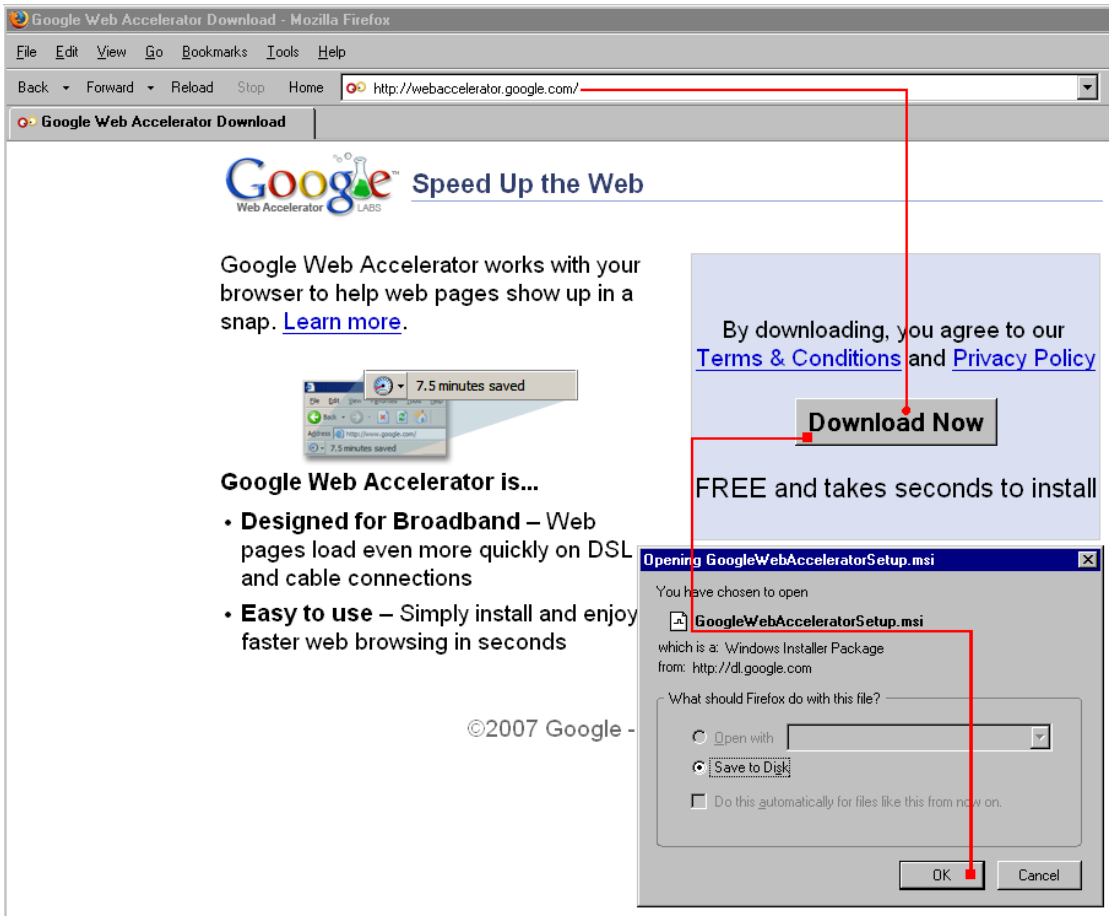

Рисунок 1 скачиваем GWA

Файл GoogleWebAcceleratorSetup.msi представляет собой обыкновенный cab-архив, содержимое которого можно просмотреть, например, RAR'ом, а запустить двойным кликом мыши или "start GoogleWebAcceleratorSetup.msi" (из командной строки), передавая управление инсталлятору.

Все устанавливаемые файлы помещаются в каталог \Program Files\Google\ и в системную папку Windows никакого барахла не добавляется, правда, без модификации пользовательской ветви реестра дела все-таки не обходится, но, по крайней мере, установщик не требует прав администратора, что уже очень хорошо. К тому же в комплект поставки входит достаточно корректный де-инсталлятор, позволяющий в любой момент удалить GWA, если он нам не понравится (кстати, он все еще остается сырым и глючным местами).

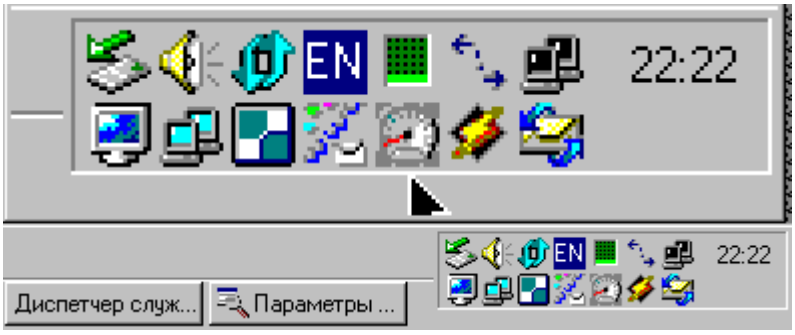

Рисунок 2 GAW в системном трее

По завершении установки в системном трее появляется изображение настольных часов аналогового типа (см. рис. 2), такие же точно часы появляются и на панели Горящего Лиса (см. рис. 3) или IE, причем, GWA остается активным вне зависимости от состояния панели. Даже если она выключена, акселерация все равно продолжается и остановить ее можно только щелкнув по "часам" и выбрав в контекстом меню пункт "Stop Google Web Accelerator", при этом

иконка исчезает из системного трея и чтобы запустить акселератор обратно, необходимо нажать на "часы", расположенные на панели инструментов Горячего Лиса/IE, выбрав пункт "Start Google Web Accelerator". (***внимание***: *в случае W2K, инсталляция GWA требует SP3, т.к. "голая" W2K формат .msi просто не понимает, как обстоят дела с XP мыщъх не в курсе, поскольку не может использовать ее по религиозным соображениям*).

Перезагрузка системы не требуется, но изменения вступят в силу только после закрытия всех окон Горящего Лиса/IE.

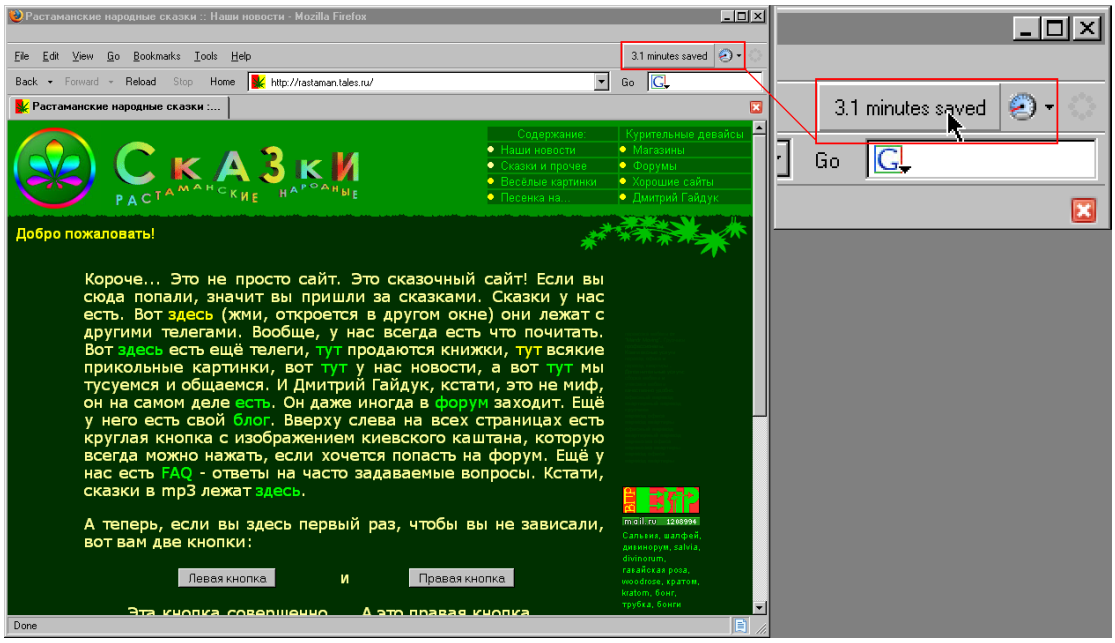

Рисунок 3 GWA на панели инструментов Горящего Лиса

Сразу же после повторного запуска Горящего Лиса/IE, персональный брандмауэр (который в наше неспокойное время должен быть установлен на каждой машине) тут же завопит, что приложение GoogleWebAccClient.exe (кстати говоря, не содержащее никакой иконки), ломится в сеть на **sb.google.com** [66.248.93.93] по 80'му порту (см. рис. 4). Вот это тот самый акселератор и есть! Попытка блокировки доступа делает работу Горящего Лиса/IE невозможной вообще, поскольку отныне и вовеки веков они ходят в сеть не напрямую, а через GoogleWebAccClient.exe, так что нажимаем "yes".

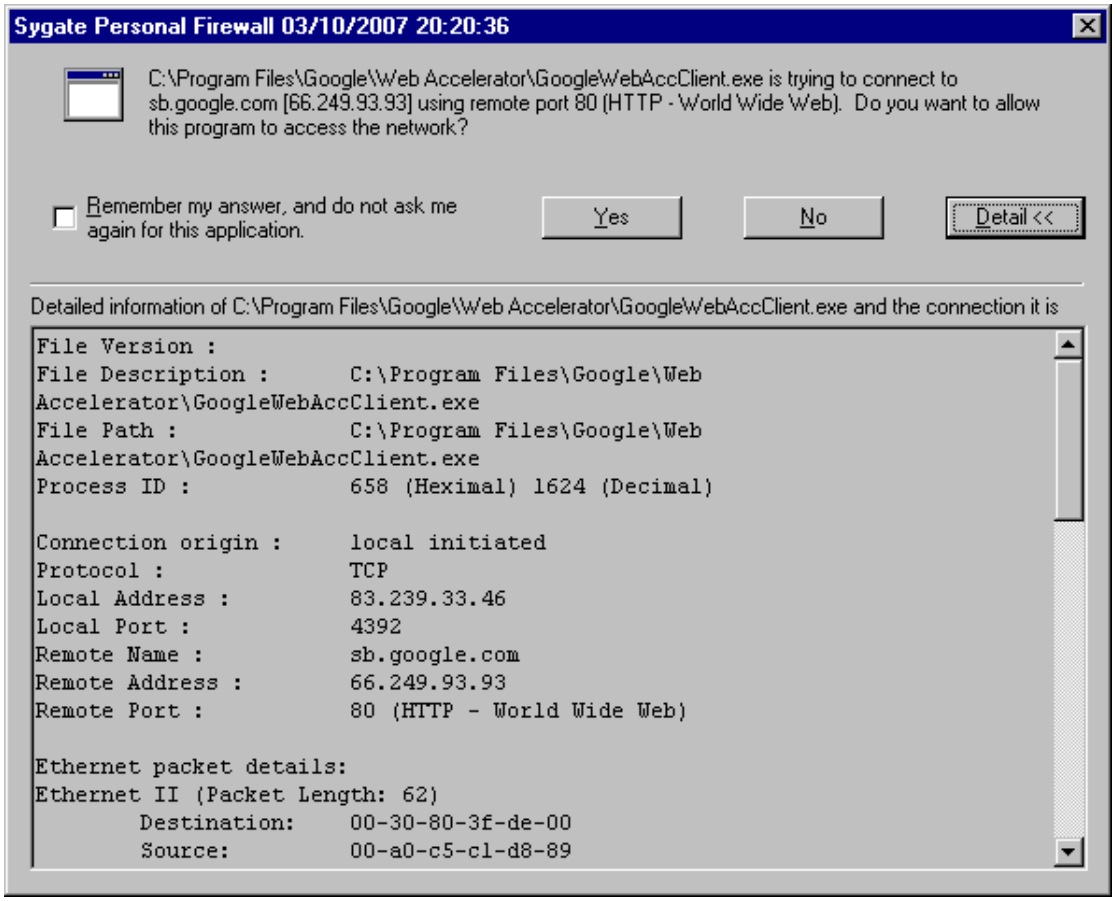

Рисунок 4 персональный брандмауэр SyGate Personal Firewall засекает попытку GWA выйти в сеть

Следом за GWA в сеть ломиться Горящий Лис/IE и все по тому же самому адресу и порту — sb.google.com:80, вынуждая нас давить "yes" еще раз (см. рис. 5). Фактически, sb.google.com:80 выступает в роли proxy-сервера, только очень хитрого и… местами даже коварного, но не будем забегать вперед.

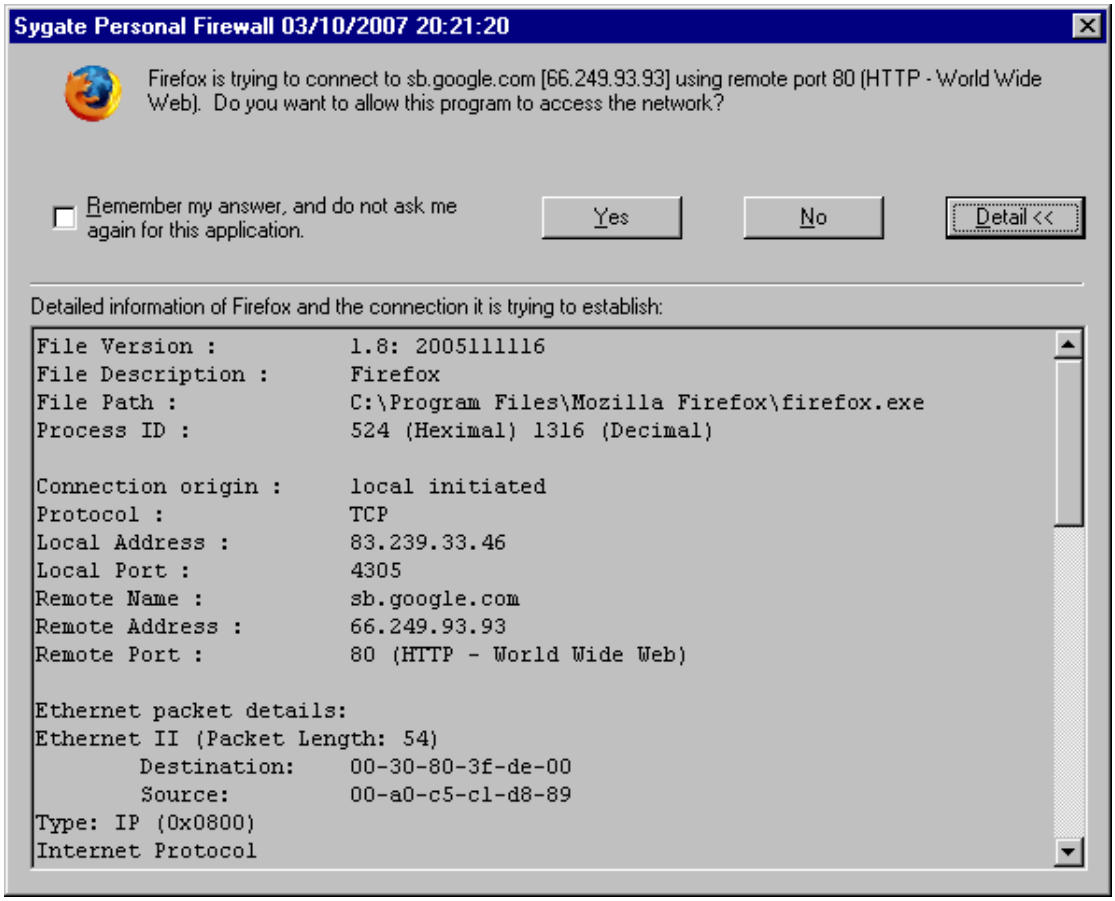

Рисунок 5 персональный брандмауэр SyGate Personal Firewall засекает попытку Горящего Лиса подключится к GWA

как это работает

Алгоритмы, заложенные в GWA, никакого секрета не представляют и в тех или иных вариациях используются практически во всех акселераторах, причем в значительно большем объеме, чем в GWA, который реализует следующий перечень возможностей:

- **выступает в роли быстрого proxy-сервера**: как известно, пропускная способность сетевых каналов (как на dial-up, так и на DSL) практически никогда не достигает 100% загрузки, поскольку большинство WEB-серверов сильно перегружено и они обслуживают пользователей не одновременно, а по очереди: передав "квант" информации, сервер ставит пользователя в очередь и принимаются за следующего, причем величина кванта определяется не только (и не столько!) размером блока данных, но и временем, требующимся на его пересылку. отсюда — чем шире у нас канал, тем больше информации мы может выкачать за один квант и тем выше эффективная скорость скачки. GWA, располагающей распределенной сетью серверов с толстыми каналами, довольно резво стягивает информацию даже с перегруженных серверов, отдавая ее нам без задержек, в результате чего КПД нашего канала приближается к 90%, что очень хорошо;
- **распределенная сеть GWA автоматически выстраивает наиболее благоприятный маршрут передачи пакетов**, что так же увеличивает скорость передачи, причем весьма значительно (особенно при работе с "далекими" серверами, разделенными десятками промежуточных узлов);
- **GWA оптимизирует параметры соединения:** TCP/IP – очень сложный протокол со множеством тонких настроек, не учитываемых ни операционной системой, ни Горящим Лисом, ни… правда, существует специальные утилиты типа MTUSpeed, позволяющие настраивать параметры TCP вручную, но… прежде чем достичь реального ускорения с ними приходится повозиться, а GWA настраивает оптимальные параметры

автоматически, уменьшая количество потерянных пакетов (которые сервер вынужден передавать повторно) и обеспечивая так называемый "быстрый старт", без которого протокол TCP довольно медленно "раскачивается" и прежде чем будет достигнута номинальная пропускная способность, запрошенная WEB-страница уже успеет загрузиться, в результате чего чем меньше размер страницы, тем с меньшей скоростью она качается. на файлах размеров в несколько десятков мегабайт это, правда, практически никак не сказывается;

- **осуществляет предвыборку (prefetching)**: основываясь на данных популярности различных web-страниц, полученных не без помощи закладок, _изначально_ встроенных в Оперу и Горящего Лиса, GWA выполняет упреждающую загрузку наиболее популярных ссылок с текущих страниц. то есть, пока мы читаем WEB-страницу, вникая в материал, GWA активно качает остальные страницы по ссылкам, вероятность перехода на которые максимальна. если GWA предугадает маршрут нашего дальнейшего WEB-путешествия, скорость открытия уже загруженных страниц нас просто сразит на повал. вот это акселерация! вот это ускорение! на модемном соединении такой подход экономит уйму времени (а, значит, и денег), правда, при условии, что web-серфинг не сочетается с фоновой скачкой файлов в ReGet'e. а вот на DSL… ой, а вот на DSL предвыборка способна кинуть нас на трафик, "обув" на весьма недетские бабки. ведь никакой гарантии, что мы реально зайдем на предвыбранные страницы у нас нет, а платить за них все равно придется, поэтому, предвыборку лучше сразу же отключить, но даже при этом GWA будет отображать ссылки, которые бы он хотел загрузить и это будут не просто ссылки, а наиболее популярные ссылки, на которые щелкают все остальные пользователи — неплохое средство для упрощение для навигации по неизвестному сайту, экономящее не только время, но и трафик;
- **GWA передает только изменения страниц**: допустим, мы имеем страницу размером в 1 Мбайт, владелец которой неожиданно изменил 10 байт в разных местах (исправил орфографические ошибки, например). в обычной ситуации мы вынуждены повторно скачивать весь этот мегабайт целиком, но GWA позволяет передать лишь изменения, то есть реально по нашему каналу скачается 10 байт плюс накладные расходы на организацию передачи. экономия времени и трафика налицо!
- **поддержка докачки**: при нестабильной связи и частных разрывах, серверы, не поддерживающие докачки, становятся настоящим исчадием ада, но… только не с GWA, который "заглатывает" файл внутрь себя и затем отдает нам. с докачкой! экономя и время, и трафик!
- **сжатие web-содержимого**: подавляющее большинство современных WEB-серверов и браузеров поддерживают сжатие текстовых web-страничек в формате gzip, экономя и скорость, и трафик, однако, до сих пор находятся такие сервера, не поддерживающие этого режима и вот тут-то GWA оказывает нам существенную помощь, правда, учитывая незначительную долю таких серверов, много сэкономить не получается;

настройки, оптимальные для модемного соединения

Щелкаем по часам, в появившемся меню выбираем "Preferences" (или набираем в адресной строке Горящего Лиса/IE следующий URL: http://127.0.0.1:9100/preferences), после чего получаем доступ ко всем настройкам (см. рис. 6).

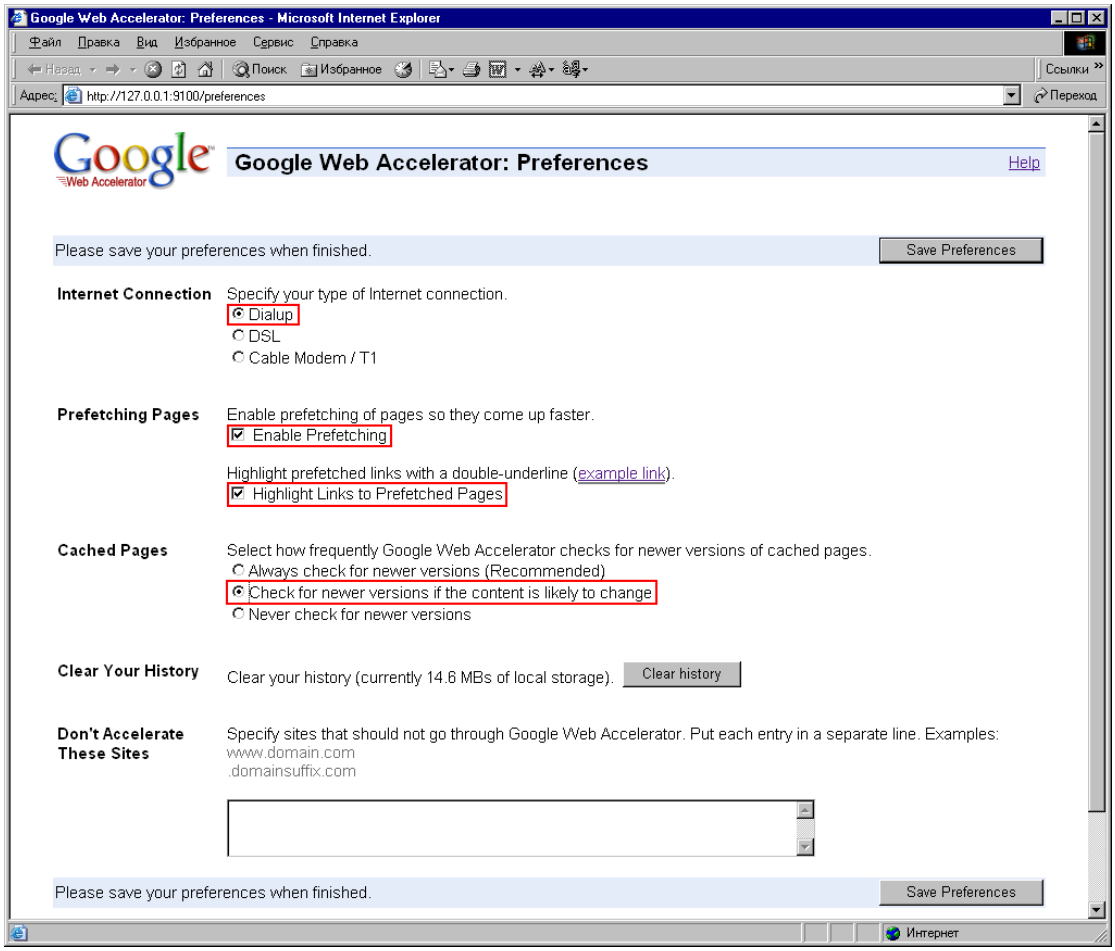

Рисунок 6 настраиваем GWA для модемного соединения

Первым делом переводим радио-кнопку "Specify your type of Internet connection" в положение "Dialup", активируем предвыборку страниц ("Enable Prefetching") и подсвечивание уже предвыбранных страниц двойным подчеркиваем, как это показано в "example link", приведенном в качестве образца. Это поможет нам просматривать страницы в том порядке, в котором их загружает GWA и который далеко не всегда совпадает с порядком их следования на текущей странице (напоминаем, что предвыборка осуществляется на основе рейтинга популярности). Для достижения максимальной скорости переводим радио-кнопку "Select how frequently Google Web Accelerator checks for newer versions of cached pages" в положение "Check for newer versions if the content is likely to change", чтобы GWA передавал только реально измененные страницы, однако, следует помнить, что этот механизм не застрахован от ошибок и в некоторых случаях GWA не замечает, что страница была изменена, показывая нам старую версию, поэтому для надежности лучше все-таки оставить эту радио-кнопку в положении "Always check for newer versions (Recommended)", в котором она и находилась по умолчанию.

Сохраняем параметры кнопкой "Save Preferences" и начинаем блуждать по сети. Часы на панели инструментов вращают стрелкой, отображая текущую скорость скачки, и показывая сэкономленное время, рассчитываемое по недокументированному алгоритму, поэтому, этим цифрам нельзя доверять, тем не менее, это не мешает получать удовольствие от наблюдения за ними. Для просмотра более детальной статистики выберите в контекстом меню GWA пункт "Performance Data" (или наберите http://127.0.0.1:9100/races в Горящем Лисе или IE), после чего откроется окно следующего вида (см. рис. 7).

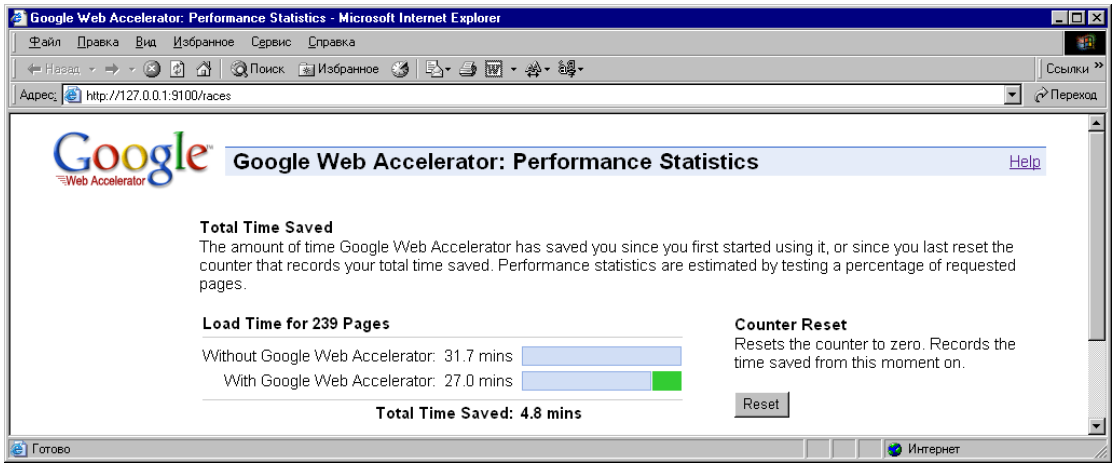

Рисунок 7 окно статистики GWA

Отсюда можно узнать, сколько времени удалось сэкономить GWA, правда, как обстоят дела с экономией трафика остается только гадать.

настройки, оптимальные для DSL-соединения

Щелкаем по часам, в появившемся меню выбираем "Preferences" (или набираем в адресной строке Горящего Лиса/IE http://127.0.0.1:9100/preferences), после чего изменяет настройки следующим образом: (см. рис. 7):

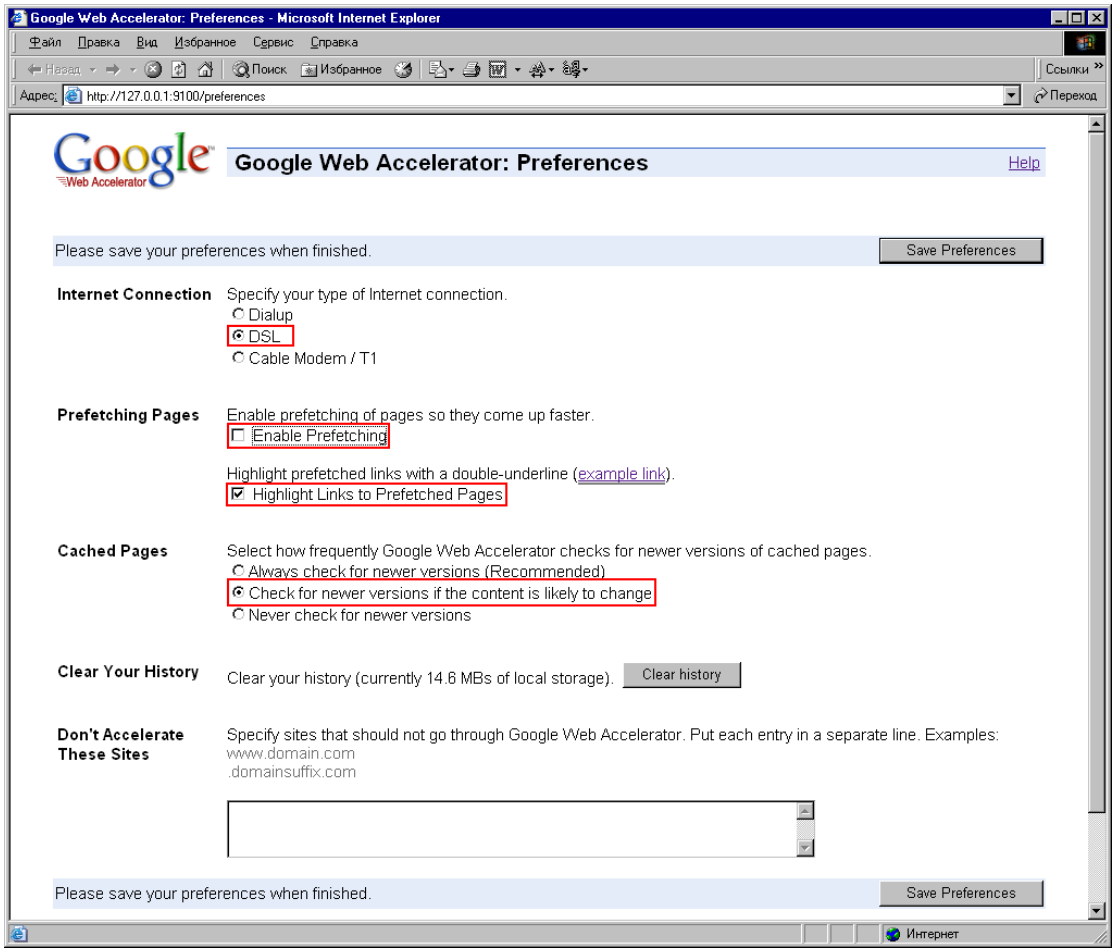

Рисунок 8 настраиваем GWA для DSL-соединения

Радио-кнопку "Specify your type of Internet connection" оставляем в положении по умолчанию: "DSL", вырубаем предвыборку, снимая галочку с "Enable Prefetching", чтобы не

попасть на трафик, но оставляем взведенной "Highlight Links to Prefetched Pages" — чтобы популярные ссылки сразу же бросались в глаза (прим. это работает не на всех сайтах). Положение "Select how frequently Google Web Accelerator checks for newer versions of cached pages" определяется в соответствии с личными предпочтениями. Позиция "Always check for newer versions" дает 100% гарантию увидеть страницу "как она есть", а "Check for newer versions if the content is likely to change" нехило экономит трафик с некоторым риском пропуска последних изменений.

Нажимаем на "Save Preferences" и… наслаждаемся "спидометром" пока не надоест, а кот когда надоест — тут же возникнет естественно для всех хакеров желание: распотрошить GWA и посмотреть что у него внутри.

как устроен GWA (технический раздел)

Технически GWA представляет собой "расщепленный" proxy-сервер, одна половина которого работает на сервере sb.google.com, другая же устанавливается локально и открывает порт с номером 9100, через который работает IE, Горящий Лис, а так же все остальные программы (например, Опера), вот только панели с часами для них не будет. Во всяком случае пока они (браузеры) не обретут достаточную популярность.

Для следующих экспериментов нам потребуется собственный **WEB-сервер**, ведущий подробные логи (мыщъх рекомендует small-http, который можно скачать с smallsrv.com, причем для граждан xUSSR он бесплатен), любой достойный **TCP/IP-dumper** и **персональный брандмауэр** (мыщъх использует SyGate Personal Firewall – брандмауэр и TCP/IP-dumper в одном флаконе, до версии 4.2 он был бесплатен, а теперь требует регистрации), а так же **утилита для мониторинга за открытыми портами** — от штатной netstat, запущенной с ключом -a, до TCPView Марка Руссиновича (www.sysinternals.com). Но тут, как говорится, на вкус и цвет товарищей нет.

Собрав все инструменты, необходимые для вскрытия, заходим в каталог \Program Files\Google\Web Accelerator и видим там два файла: GoogleWebAccClient.exe: "сердце" акселератора — локальный proxy-сервер, открывающий порт номер 9100 для общения с Горящим Лисом/IE (см. рис. 9) и взаимодействующий с удаленным GWA-proxy сервером sb.google.com по стандартному 80 порту.

GoogleWebAccWarden.exe реализует "спидометр" в системном трее и на панели управления, общающийся с GoogleWebAccClient.exe через средства межпроцессорного взаимодействия, а конкретно — через socket'ы. Если "снести" этот процесс (в "Диспетчере Задач" или FAR'e), спидометр тут же исчезнет, но акселератор продолжит работать с ничуть не меньшим усердием. Кстати, говоря, GoogleWebAccWarden.exe является пусковым файлом и если его "остановить", а потом запустить повторно, то мы получим две копии GoogleWebAccClient.exe ведущих себя довольно непредсказуемым образом.

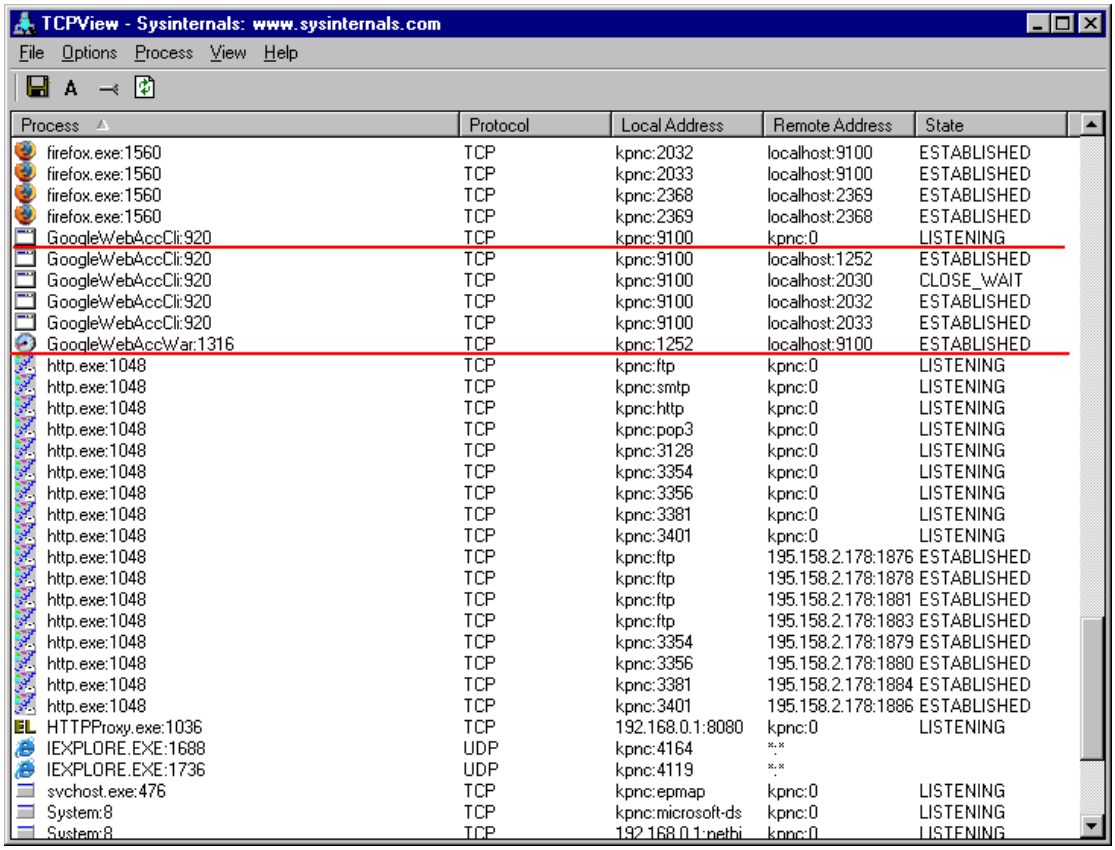

Рисунок 9 наблюдение за GWA с помощью "TCPView": GoogleWebAccClient.exe открывает порт 9100 на просушку, а GoogleWebAccWarden.exe не открывая никаких "своих" портов взаимодействует с GoogleWebAccClient.exe через его 9100 порт

Теперь ненадолго отключим GWA и зайдем на свой собственный http-сервер, роль которого в данном случае исполняет http://nezumi.org.ru недавно переведенный в орбитальный режим, то есть запущенный на круглосуточную работу. В лог-файле немедленно появляется следующая запись (см. листинг 1, рис. 10):

```
!->10/03 22:22:22 [83.239.33.46:4323>80] (t1 5229)
GET / HTTP/1.1
Host: nezumi.org.ru
User-Agent: Mozilla/5.0 (Windows NT 5.0; en-US; rv:1.8) Gecko/20051111 Firefox/1.5
Accept:text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;…
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
```

Листинг 1 заходим на мыщъх'ный сервер без GWA

Здесь все ясно и понятно. Адрес 83.239.33.46 — это мой IP, запрос "GET / HTTP/1.1" посланный Горящим Лисом, предписывает серверу возвратить главную страницу.

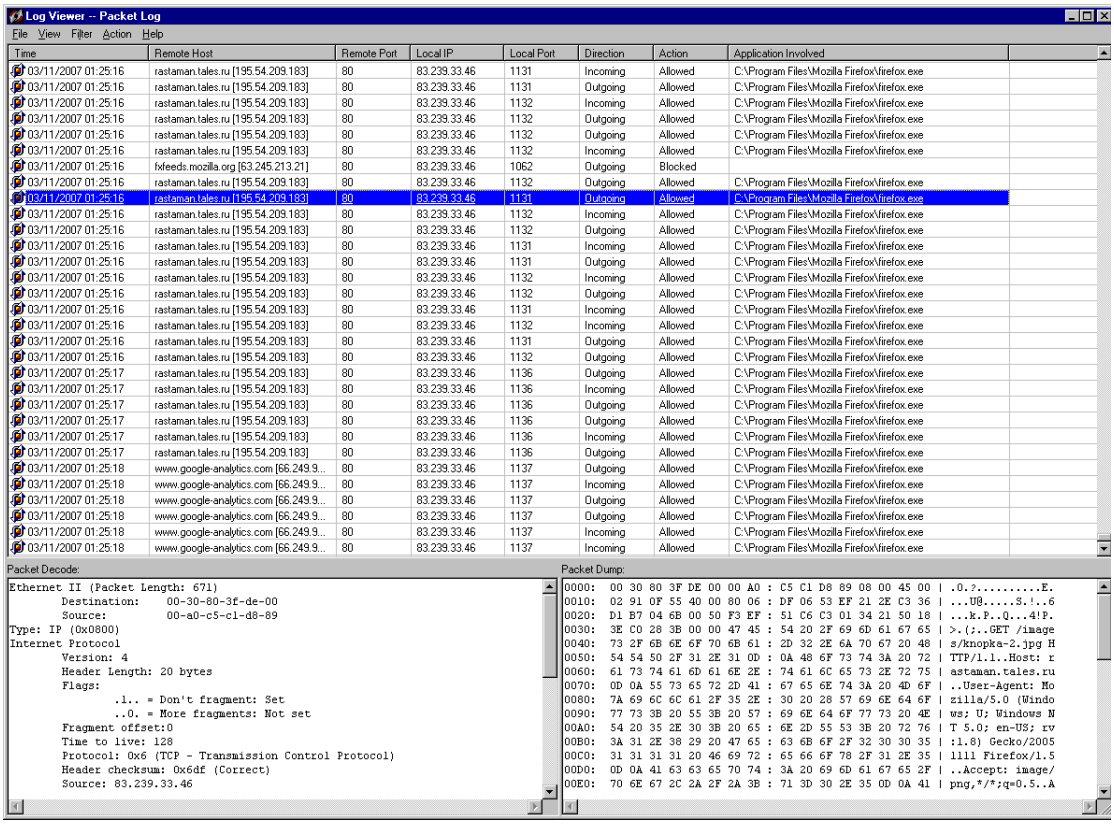

Рисунок 10 заход Горящим Лисом на сервер rastam.tales.ru с выключенным GWA, как видно, все запросы поступают от приложения firefox.exe

А теперь запустим GWA и попробуем зайти на сервер еще раз:

```
!->10/03 22:22:22 [72.14.192.1:50514>80] (t1 5286)
GET / HTTP/1.1
Host: nezumi.org.ru
User-Agent: Mozilla/5.0 (Windows NT 5.0; en-US; rv:1.8) Gecko/20051111 Firefox/1.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;…
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
X-navid: 524-e8a56370
Cache-Control: max-age=0
X-Forwarded-For: 83.239.33.46
################################################################################
!->10/03 22:22:22 [72.14.192.1:61502>80] (t1 5263)
GET / HTTP/1.1
Host: nezumi.org.ru
User-Agent: Mozilla/5.0 (Windows NT 5.0; en-US; rv:1.8) Gecko/20051111 Firefox/1.5
Accept:text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;…
Accept-Language: en-us,en;
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Cache-Control: max-age=0
################################################################################
!->10/03 22:22:22 [72.14.192.1:50670>80] (t1 5293)
GET /k_hiteev-pack.zip HTTP/1.1
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;
User-Agent: Mozilla/5.0 (Windows NT 5.0; en-US; rv:1.8) Gecko/20051111 Firefox/1.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;
Referer: http://nezumi.org.ru/
Host: nezumi.org.ru
X-moz: prefetch
X-Forwarded-For: 83.239.33.46
Accept-Encoding: gzip
```

Листинг 2 заходим на мыщъх'ный сервер под GWA

Ну не хвоста же себе!!! Во-первых, теперь запросы идут не от того узла, где установлен Лис, а совсем из другого места — 72.14.192.1, которым, как нетрудно догадаться, является один из серверов входящих в распределенную сеть GWA, и который мы можем использовать как Proxy, вот только… скрыть свой истинный IP все равно не получится, поскольку GWA явно прописывает его в заголовке: "X-Forwarded-For: 83.239.33.46", так же указывается подлинная строка идентификации браузера вместе с остальными параметрами.

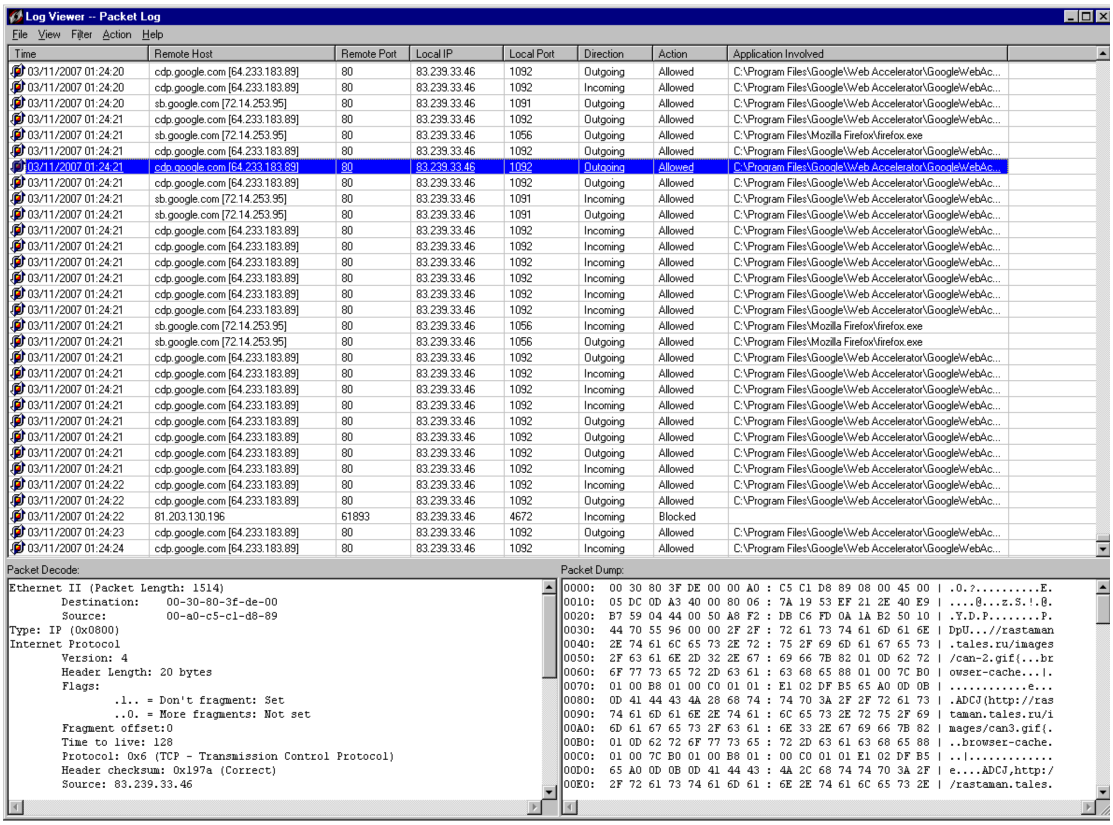

Рисунок 11 заход Горящим Лисом на сервер rastam.tales.ru с активным GWA — как видно, все запросы поступают от приложения GoogleWebAccClient.exe, а сам firefox.exe получает данные от sb.google.com, как и положено при работе через proxy

Во-вторых, один и тот же запрос "GET / HTTP/1.1" выполняется _дважды_ — один раз для Горящего Лиса, второй — для удаленного кэш-сервера GWA. Таким образом, интенсивное использование GWA многими миллионами пользователями приводит к повышенной загрузке WEB-серверов по всему миру. Ажурная перспектива, не правда ли?!

В-третьих, при активной предвыборке, GWA тут же начинает загружать k_hiteev-pack.zip (сборник из 96 статей), а он почти 37 Мбайт (!!!) весит, следом за ним качается hacker-disassembling-uncovered-second-edition-chapter_10-only(eng).zip — кусок второго издания одноименной книги на английском языке (меньше метра будет). Обратите на нестандартное поле "X-moz: prefetch" в заголовке HTTP-запроса. И вся эта информация насильно впихивается пользователю, зашедшему на сервер, не дожидаясь пока он сделает запрос!!! А по широкому DSL-каналу мегабайты пролетают очень быстро…

Предвыборка — это понятно. Непонятно другое. Как (и почему?!) GWA выбрал именно эти два архива из более чем 80'ти остальных файлов, валяющихся на сервере?! Да очень просто! По критерию популярности. Закладки, встроенные в Горящего Лиса и Оперу, нашептали Google'е, что именно качают пользователи с мыщъх'иного сервера чаще всего и мыщъхиные log'и эту информацию полностью подтверждают!!!

Таким образом, при использовании предвыборки трафик увеличивается во много раз, поскольку вовсе не факт, что скаченная информация будет затребована пользователем (в частности, русские пользователи не читают английские переводы мыщъхиных книг, а жители США и иных земель довольно равнодушны к русским статьям). Поэтому, предвыборку лучше всего отключать: прирост скорости намного меньше роста оплаты за мегабайты. На

безлимитных тарифах, конечно, картина несколько другая, но и там предвыборка нагружает канал мешая фоновым соединениям.

Независимо от активности предвыборки, GWA сохраняет считанные страницы в кэш-папке Горящего Лиса или IE, то есть работает как обычный кэш-proxy сервер, только не простой сервер, а кривой. Лучше бы он сохранял их в отдельной папке, тогда бы при просмотре одних и тех же страниц из-под разных браузеров, мы бы экономили на трафике.

Еще один факт, скорее относящийся к области курьезов, но все-таки достаточно интересный сам по себе и достойный описания. Сразу же после установки GWA на узел мыщъх'а обрушилось большое количество UDP-пакетов, направленных на 1030 порт (сервис обмена сообщениями), отсекаемых брандмауэром, но нервирующими своим рекламным содержимым при просмотре log'ов, к тому же, несмотря на все блокировки, это _входящий_ трафик, за который мыщъх'у приходится платить. Один из образцов подобного творчества приведен ниже (см. листинг 3). Поскольку пакеты приходят с разных IP, то решить проблему путем ведения black-list'а не удается. Во всяком случае пока не будет накоплена статистика наиболее активных узлов. Случайность это или закономерность — кто знает?

```
Ethernet II (Packet Length: 943)
        Destination:    00-a0-c5-c1-d8-89
        Source:         00-30-80-3f-de-00
Type: IP (0x0800)
Internet Protocol
        Version: 4
        Header Length: 20 bytes
        Flags:
                .1.. = Don't fragment: Set
                ..0. = More fragments: Not set
        Fragment offset:0
        Time to live: 47
        Protocol: 0x11 (UDP - User Datagram Protocol)
        Header checksum: 0x5ce8 (Correct)
        Source: 218.27.16.183
        Destination: 83.239.33.46
User Datagram Protocol
        Source port: 47472
        Destination port: 1030
        Length: 8
        Checksum: 0x76c0 (Correct)
Data (909 Bytes)

0000:  00 A0 C5 C1 D8 89 00 30 : 80 3F DE 00 08 00 45 00 | .......0.?....E.
0010:  03 A1 00 00 40 00 2F 11 : E8 5C DA 1B 10 B7 53 EF | ....@./..\....S.
0020:  21 2E B9 70 04 06 03 8D : C0 76 04 00 28 00 10 00 | !..p.....v..(...
0030:  00 00 00 00 00 00 00 00 : 00 00 00 00 00 00 00 00 | ................
0040:  00 00 F8 91 7B 5A 00 FF : D0 11 A9 B2 00 C0 4F B6 | ....{Z........O.
0050:  E6 FC 00 00 00 00 00 00 : 00 00 00 00 00 00 00 00 | ................
0060:  00 00 00 00 00 00 01 00 : 00 00 00 00 00 00 00 00 | ................
0070:  FF FF FF FF 35 03 00 00 : 00 00 10 00 00 00 00 00 | ....5...........
0080:  00 00 10 00 00 00 53 59 : 53 54 45 4D 00 00 00 00 | ......SYSTEM....
0090:  00 00 00 00 00 00 10 00 : 00 00 00 00 00 00 10 00 | ................
00A0:  00 00 41 4C 45 52 54 00 : 00 00 00 00 00 00 00 00 | ..ALERT.........
00B0:  00 00 F1 02 00 00 00 00 : 00 00 F1 02 00 00 59 6F | ..............Yo
00C0:  75 72 20 73 79 73 74 65 : 6D 20 72 65 67 69 73 74 | ur system regist
00D0:  72 79 20 69 73 20 63 6F : 72 72 75 70 74 65 64 20 | ry is corrupted
00E0:  61 6E 64 20 6E 65 65 64 : 73 20 74 6F 20 62 65 20 | and needs to be
00F0:  63 6C 65 61 6E 65 64 20 : 69 6D 6D 65 64 69 61 74 | cleaned immediat
0100:  65 6C 79 2E 0A 0A 0A 43 : 6F 6D 70 72 6F 6D 69 73 | ely....Compromis
0110:  65 64 20 72 65 67 69 73 : 74 72 79 20 66 69 6C 65 | ed registry file
0120:  73 20 63 61 6E 20 6C 65 : 61 64 20 74 6F 20 74 68 | s can lead to th
0130:  65 20 66 6F 6C 6C 6F 77 : 69 6E 67 3A 0A 0A 31 2E | e following:..1.
0140:  20 43 6F 6D 70 6C 65 74 : 65 20 61 63 63 65 73 73 |  Complete access
0150:  20 6F 66 20 79 6F 75 72 : 20 50 43 20 62 79 20 68 |  of your PC by h
0160:  61 63 6B 65 72 73 0A 32 : 2E 20 53 6C 6F 77 20 73 | ackers.2. Slow s
0170:  70 65 65 64 73 20 72 65 : 73 75 6C 74 69 6E 67 20 | peeds resulting
0180:  69 6E 20 73 6C 6F 77 20 : 64 6F 77 6E 6C 6F 61 64 | in slow download
0190:  73 20 6F 66 20 69 6E 74 : 65 72 6E 65 74 20 66 69 | s of internet fi
01A0:  6C 65 73 0A 33 2E 20 54 : 68 65 20 63 6F 6D 70 72 | les.3. The compr
01B0:  6F 6D 69 73 65 20 6F 66 : 20 70 65 72 73 6F 6E 61 | omise of persona
01C0:  6C 20 69 6E 66 6F 72 6D : 61 74 69 6F 6E 20 73 74 | l information st
01D0:  6F 72 65 64 20 6F 6E 20 : 79 6F 75 72 20 63 6F 6D | ored on your com
01E0:  70 75 74 65 72 0A 34 2E : 20 43 6F 6D 70 6C 65 74 | puter.4. Complet
01F0:  65 20 73 79 73 74 65 6D : 20 66 61 69 6C 75 72 65 | e system failure
0200:  20 72 65 73 75 6C 74 69 : 6E 67 20 69 6E 20 74 68 |  resulting in th
```

```
0210:  65 20 6E 65 65 64 20 66 : 6F 72 20 61 20 63 6F 6D | e need for a com
0220:  70 6C 65 74 65 20 72 65 : 69 6E 73 74 61 6C 6C 20 | plete reinstall
0230:  6F 66 20 79 6F 75 72 20 : 68 61 72 64 20 64 72 69 | of your hard dri
0240:  76 65 2E 0A 0A 54 6F 20 : 66 69 78 20 74 68 69 73 | ve...To fix this
```

Листинг 3 рекламные сообщения, обрушившиеся на мыщъх'иный компьютер _сразу_ же после установки GWA

>>> врезка как прикрутить GWA к опере

Официально GWA поддерживает только Горящего Лиса и IE, но при желании его можно заставить работать с любым браузером, например, Рысем или Оперой. Ведь в основе GWA лежит локальный proxy-сервер, а всякие там "спидометры" на панели инструментов — это чиста для красоты.

Короче, берем Оперу (любой версии), заходим в меню "Tools", выбираем пункт "Preferences" (или нажимаем <CTRL-F12>, но мыщъх жать эту комбинацию не может т. к. у него на нее повешен вызов cmd.exe). В открывшемся диалоговом окне переходим к вкладке "Advanced", щелкаем по строке "network", давим на кнопку "proxy servers" и в строке HTTP пишем: 127.0.0.1, port 9100 (см. рис. 12) не забыв взвести напротив него галочку. Так же можно задействовать "HTTP 1.1 for proxy", а вот HTTPS проксировать не надо, все равно GWA (по соображениям секретности) не поддерживает этот протокол.

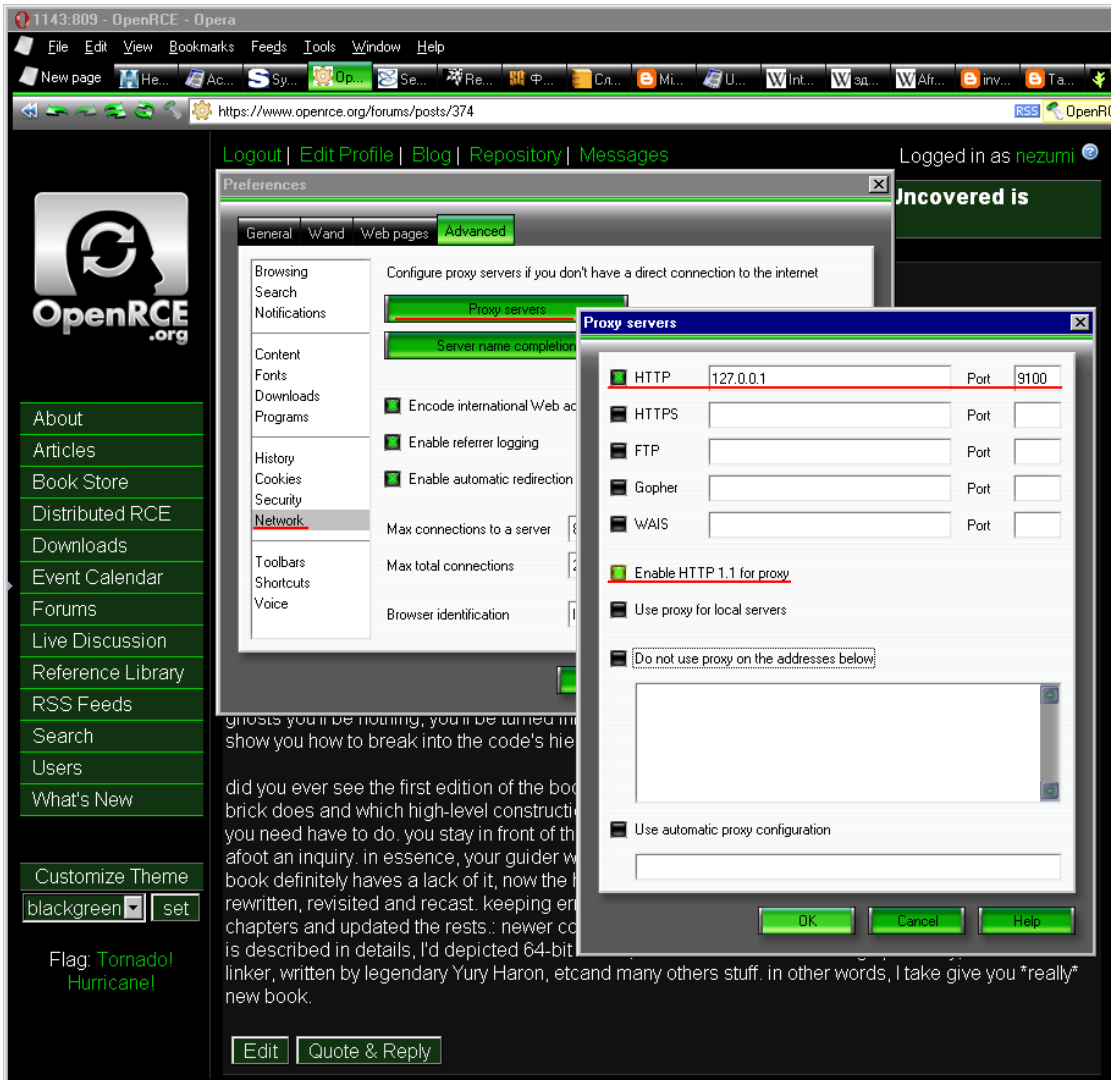

Рисунок 12 заставляем Оперу работать через GWA

GWA как источник угрозы

Инсталлируя GWA на своей компьютер, мы тем самым устанавливаем локальный proxy-сервер и открываем 9100 порт, необходимый для его работы Сразу же возникает вопрос: а как насчет безопасности?! Вдруг какой-нибудь умник пропишет наш IP и 9100 порт в свойствах своего браузера и будет гнать через нас трафик, за который _нам_ придется платить? Атаки такого типа очень широко распространены и повсеместно встречаются. Как правило, внутрисетевой трафик (т. е. трафик внутри сети провайдера) стоит ощутимо дешевле внешнего трафика, за который самому провайдеру приходится платить.

В это же самое время, многие клиенты устанавливают у себя proxy-севера, обслуживающие сеть организации или даже домашнюю локалку. Грамотный администратор первым делом прописывает список разрешенных IP (принадлежащих, естественно его локалке) или указывает с каких сетевых интерфейсов разрешен доступ. Однако, если администратор лох, сервер остается открыт всем желающим! Обнаружив "жертву" простым сканированием, хакер (точнее, не хакер, а голимый "пионер") указывает его IP в адресе proxy-сервера своего браузера и начинает гнать трафик, оплачиваемый из чужого кармана. Естественно, скрыть свой IP ему не удается и дело обычно заканчивается мордобоем. Правда, в случае действительно крупных провайдеров, локалка которых покрывает целый край (например, Краснодарский), пионер может территориально находится за сотни километров, что затрудняет процедуру разборки.

А как обстоят дела с GWA? Анализ показывает, что он разрешает доступ только с адреса 127.0.0.1, т.е. непосредственно с самой локальной машины и блокирует попытки подключения извне. Правда, насколько надежно он это делает и не содержится ли в нем ошибок переполнения — мыщъх'у неизвестно, поэтому заткнуть порт 9100 на персональном брандмауэре будет совсем нелишне.

Кстати говоря, какой идиот разработчик придумал такие ограничения?! Нормально настроенный акселератор _должен_ допускать к себе остальных членов локальной сети, если администратор этого хочет, он ведь неспроста этого хочет! Локальный кэш — великое дело, особенно если разные узлы обращаются к одним и тем же серверам, как чаще всего и бывает. Даже в домашней сети простейший кэширующий прокси (вроде уже упомянутого small-http) экономит трафика больше, чем GWA!!!

Еще одна проблема, связанная с GWA — к нему могут обращаться любые программы (а не только Горящий Лис, опера и IE), в том числе и зловредные утилиты, ворующие информацию с компьютера и скрытно передающие ее через сеть. В обычной ситуации их остановит брандмауэр, но в случае с GWA – нет.

сравнение с конкурентами

Главным, можно даже сказать фундаментальным, недостатком GWA является его органическая неспособность сжимать графические изображения, а ведь именно на них приходится львиная доля сетевого трафика.

Коммерческий акселератор http://www.propel.com разработал специальный алгоритм сжатия, позволяющий уменьшать размер jpeg-файлов (которые, как известно, практически не поддаются сжатию) в 15 раз (см. рис. 13), сохраняя при этом приемлемый уровень качества (то есть, можно смотреть без содроганий, поскольку изображение остается субъективно приятным).

Акселератор поддерживает практически все существующие на данный момент браузеры (IE, Netscape, Opera, Mozilla и Firefox) и даже дает 7 дней пробного доступа!

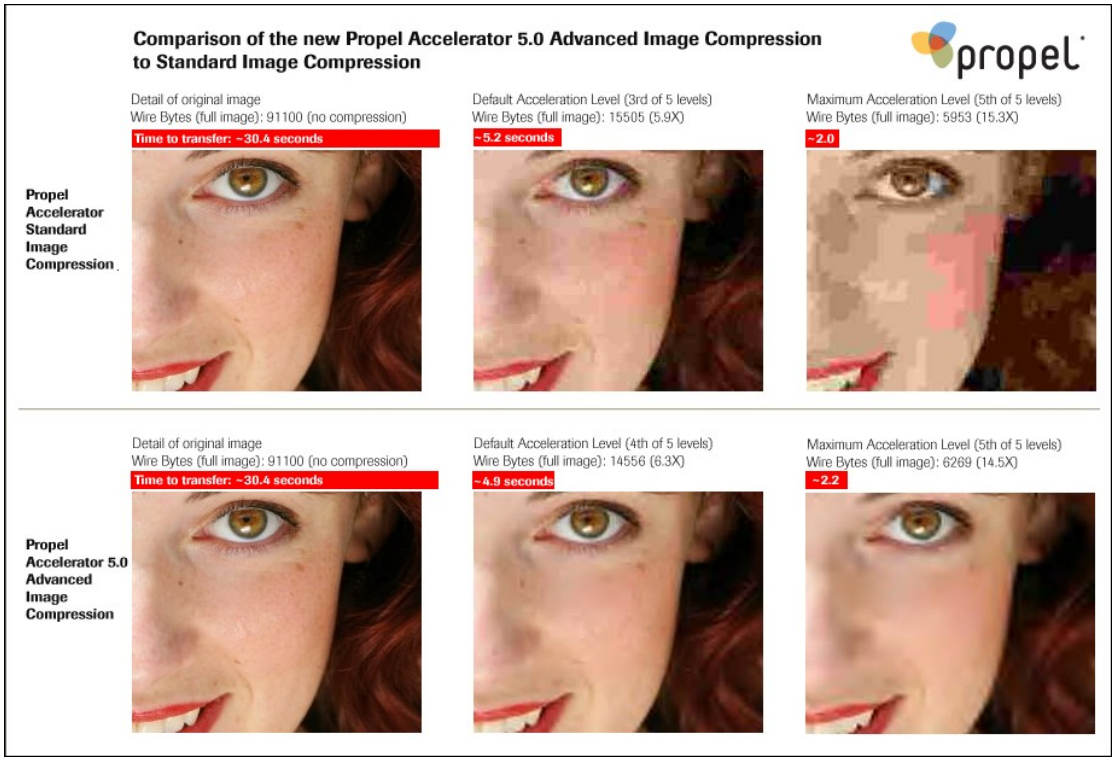

Рисунок 13 сжатие изображений коммерческим акселератором

заключение

Так все-таки, стоит использовать GWA или нет? Вопрос не имеет однозначного ответа. Что GWA представляет собой лучший _бесплатный_ акселератор, никто не спорит и спорить не собирается, но по сравнению с коммерческими он полный отстой и тот же http://www.propel.com позволяет экономить гораздо больше мегабайт, правда, ценою потери качества картинок, которое в некоторых случаях важнее денег.

Словом, выбирайте сами, благо выбор есть.