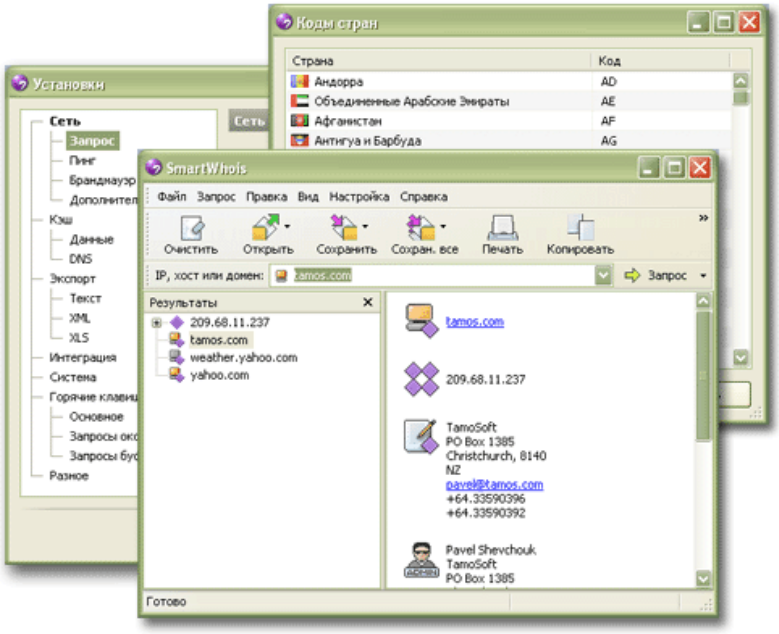
SmartWhois®
Краткое руководство
Домены и IP-адреса без мифов

Об этом руководстве

Домены, IP-адреса, имена хостов, сайты и URL всегда были терминами, вокруг которых возникали неверные представления, даже среди продвинутых пользователей. Эти понятия часто понимают неверно и/или путают между собой. *В чем же состоит разница между именем домена и именем хоста? Что означают численные представления IP-адресов? Как я могу узнать, кто является владельцем домена? Как я могу отследить пользователя по IP-адресу?*



В этом обзоре мы постараемся дать ответы на эти и многие другие распространенные вопросы и покажем вам, как использовать SmartWhois от TamoSoft для выполнения Whois-запросов.

Изучаем основы

Доменные имена, IP-адреса, имена хостов, веб-сайты, URL и Whois

Давайте начнем с определения базовых понятий.

Домен: Домен, или доменное имя – это логическая область Интернета. Доменные имена состоят из одной или нескольких частей, разделенных точками, например, "yahoo.com". Часто говорят, что все компьютеры, у которых одна и та же правая часть имени, принадлежат к одному домену. Например, "weather.yahoo.com" и "finance.yahoo.com" принадлежат к домену "yahoo.com".

Высшим уровнем в иерархии доменов являются домены верхнего уровня (TLD, или Top Level Domains). TLD – это крайняя правая часть доменного имени и, разумеется, вы знаете множество известных доменов верхнего уровня, например, .RU, .COM или .NET. Семь основных TLD (.COM, .EDU, .GOV, .INT, .MIL, .NET и .ORG) были созданы в 1980-х годах,

семь новых были представлены в 2001 и 2002 годах (.BIZ, .INFO, .NAME, .PRO, .AERO, .COOP и .MUSEUM). Помимо них, существует более двухсот TLD, относящихся к странам. Такие TLD содержат две буквы, например, .CA относится к Канаде, а .DE – к Германии. Полный список можно найти на веб-сайте IANA.

Следующей частью (справа налево) доменного имени являются домены второго уровня (Second Level Domains, SLD). Например, в доменной зоне первого уровня .COM зарегистрированы миллионы доменных имен второго уровня (такие, как "yahoo.com"). Далее идут домены третьего уровня, например "Finance.yahoo.com" или "www.yahoo.com", и т. д. У каждого домена второго уровня есть владелец – компания, организация или частное лицо. Определить владельца поможет инструмент Whois.

IP-адрес: каждому компьютеру, подключенному к Интернету, назначается уникальное число, известное как адрес Интернет-протокола (IP-адрес). Этот адрес однозначно определяет получателя или отправителя информации, передаваемой в пакетах через Интернет. Формат IP-адреса имеет 32-битный численный вид и записывается как четыре числа, разделенных точкой. Каждое число находится в диапазоне от 0 до 255. Примеры IP-адресов - 4.90.50.60 или 208.1.0.15.

Вашему компьютеру также назначен IP-адрес, поскольку без действительного адреса вы не получите доступа к веб-сайту и не сможете пользоваться такими Интернет-сервисами, как электронная почта. Многие IP-адреса назначаются динамически из пула адресов, хотя некоторые выделяются на постоянной основе. Поскольку IP-адреса обычно выделяются из блоков, привязанных к конкретным странам, IP-адреса часто используются для идентификации компьютера, подключенного к Интернету.

Имя хоста: имя хоста является лишь псевдонимом для IP-адреса. Это имя присваивается компьютеру исключительно для удобства человека. Рассмотрим, к примеру, веб-сервер "www.lookup-ip.com". Его IP-адрес - 66.39.117.110, но это число непросто запомнить. Маловероятно, что вы выучите его наизусть и введете его в адресную строку браузера, когда вы захотите посетить веб-сайт. Название "www.lookup-ip.com" запоминается гораздо лучше. Когда вы вводите это имя в браузер, он быстро связывается с сервером доменных имен (DNS) и получает информацию о том, что имени www.lookup-ip.com соответствует IP-адрес 66.39.117.110. С этого момента для обмена информацией с веб-сайтом ваш браузер будет использовать численный IP-адрес. У компьютера, подключенного к Интернету, может и не быть имени хоста, но IP-адрес должен быть обязательно.

Примеры имен хостов: www.google.com (веб-сайт), pop-server.austin.rr.com (почтовый сервер), cs2416713-236.houston.rr.com (имя хоста, закрепленное за пользователем широкополосного Интернета), dialup134.ts521.cwt.esat.net (имя хоста, закрепленное за пользователем dial-up).

Веб-сайты и URL: веб-сайт – это группа веб-страниц, хранящихся на определенном сервере. Веб-сервер – это компьютер, подключенный к Интернету, на котором работает программное обеспечение, необходимое для выдачи веб-страниц. В основном, веб-серверы имеют имена хостов, которые начинаются с "www", например, "www.google.com", хотя это не всегда так. Единый указатель ресурсов (Universal Resource Locator, URL) – это адрес ресурса, доступного с помощью Интернет-протоколов, как правило, гипертекстового (HTTP). Пример URL: "http://www.google.com/about.html".

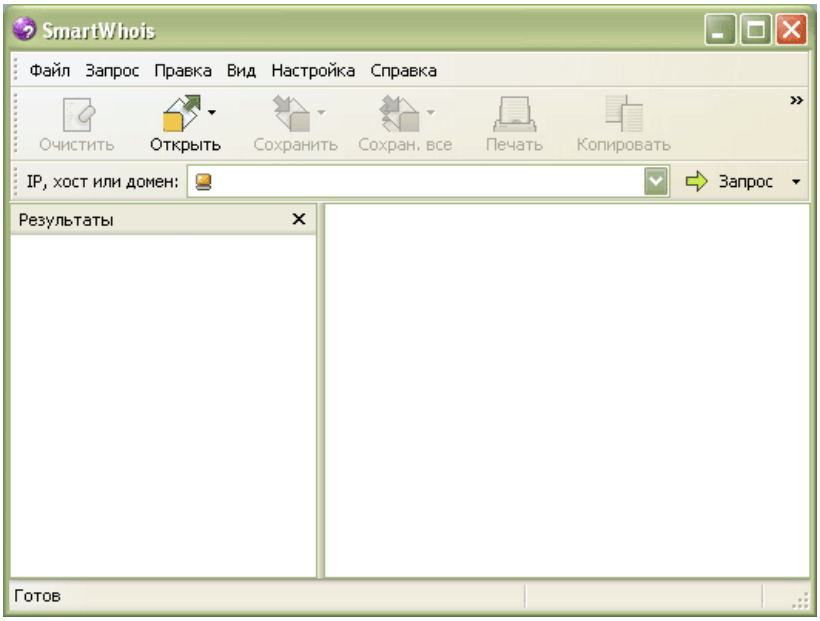
Whois: Whois – это Интернет-программа, которая дает пользователям возможность делать запросы к базе данных доменов и IP-адресов с целью получения информации о владельцах, администраторах, географическом местоположении и т. д. Как и говорит само название

программы, SmartWhois – это интеллектуальная, многофункциональная утилита для выполнения подобных запросов. В следующей главе вы узнаете, что можно сделать с помощью этой программы.

Работа со SmartWhois

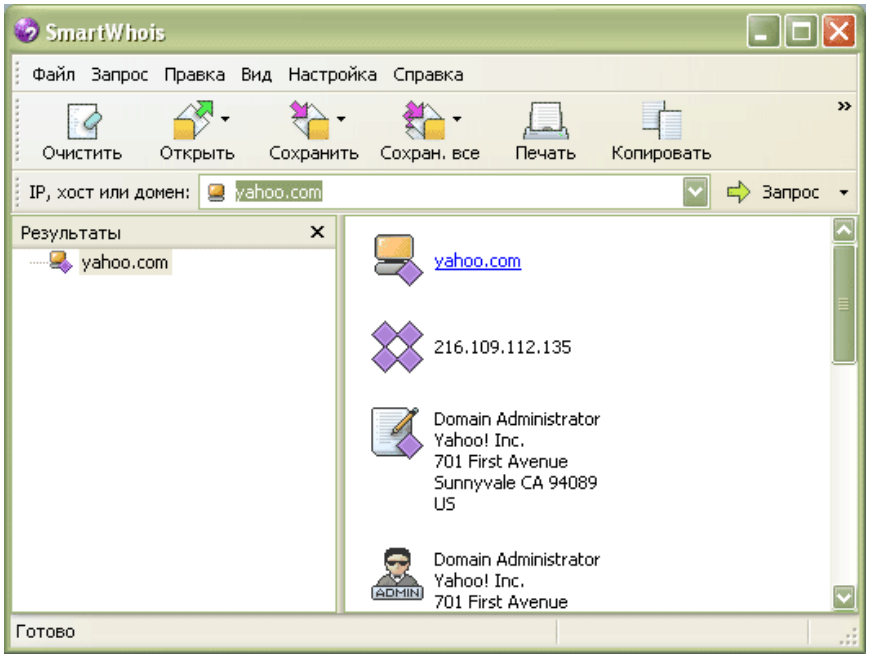
Разбираемся с доменами и IP-адресами

Разобравшись с интернет-терминологией, мы можем начать работу со SmartWhois. Если вы еще не скачали программу, то скачайте ее, запустите инсталляцию в любой из систем Windows 2000/XP/2003/Vista/2008, а потом запускайте программу:

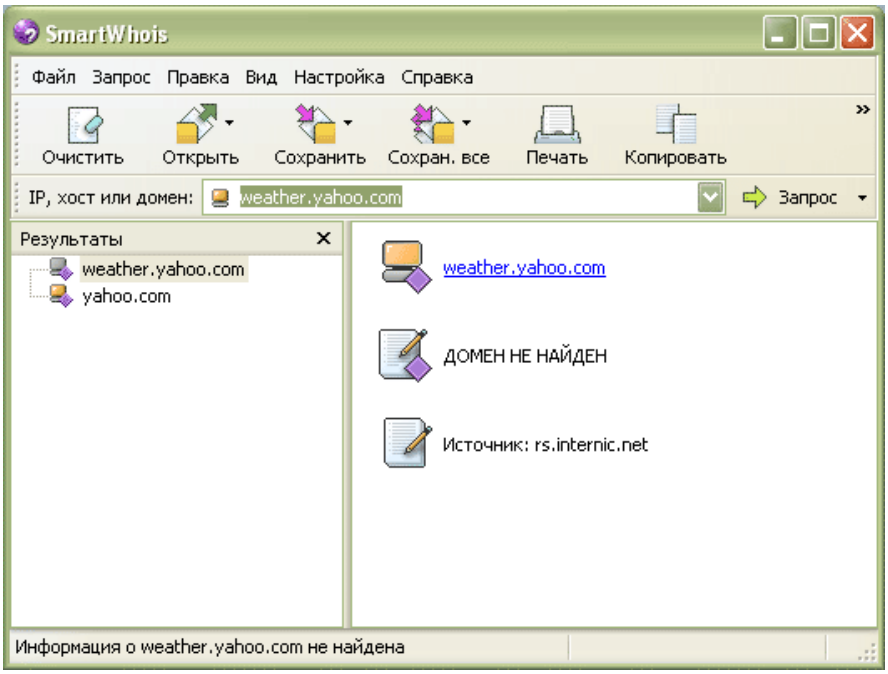


Ключом к успешной работе со SmartWhois является понимание разницы между доменными запросами и запросами по IP-адресу/имени хоста. При поиске информации по определенному веб-сайту пользователи зачастую сомневаются, какой запрос совершить, и что именно следует ввести в самой строке запроса. Давайте рассмотрим пример:

Предположим, вы хотите узнать, кто является владельцем известного сайта прогноза погоды - weather.yahoo.com. Чтобы узнать имя владельца сайта, нужно узнать, кто владеет доменом. В этом примере имя домена это "yahoo.com". Таким образом, в строке запроса надо ввести "yahoo.com", нажать кнопку **Запрос** и выбрать опцию **Как домен**:



Всего через несколько секунд вы выясняете, что "yahoo.com" принадлежит калифорнийской компании Yahoo!. Но почему мы ввели "yahoo.com", а не "weather.yahoo.com"? Причина состоит в том, что "weather.yahoo.com" не является доменом второго уровня! Помните предыдущую главу? В большинстве случаев вам нужно выполнять запросы **только** по доменным именам второго уровня, таким, как "yahoo.com", а не по доменам третьего уровня вроде "weather.yahoo.com." На самом деле, вы все же можете сделать запрос к "weather.yahoo.com" как к доменному имени:



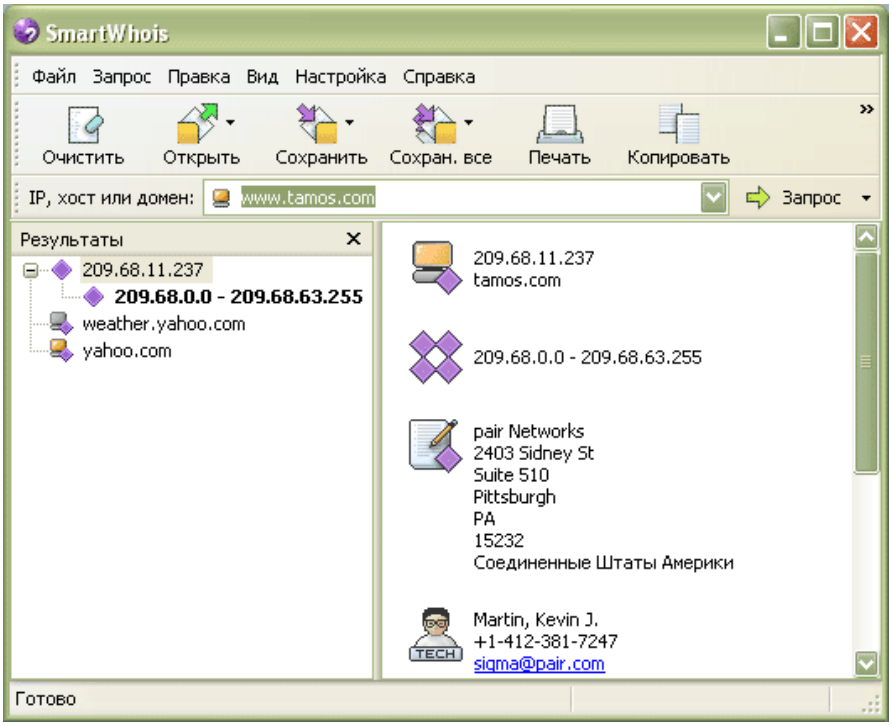
Да, все верно – домен не найден. В базе данных Whois содержатся данные только по доменам второго уровня. Хотя из этого правила есть некоторые исключения, например,

домены UK. В некоторых странах доменная система основана на доменах третьего уровня, т. е. вы покупаете домен, уже содержащий в своем имени две точки, например, "jaguar.co.uk" или "bbc.co.uk". Но такое встречается нечасто.

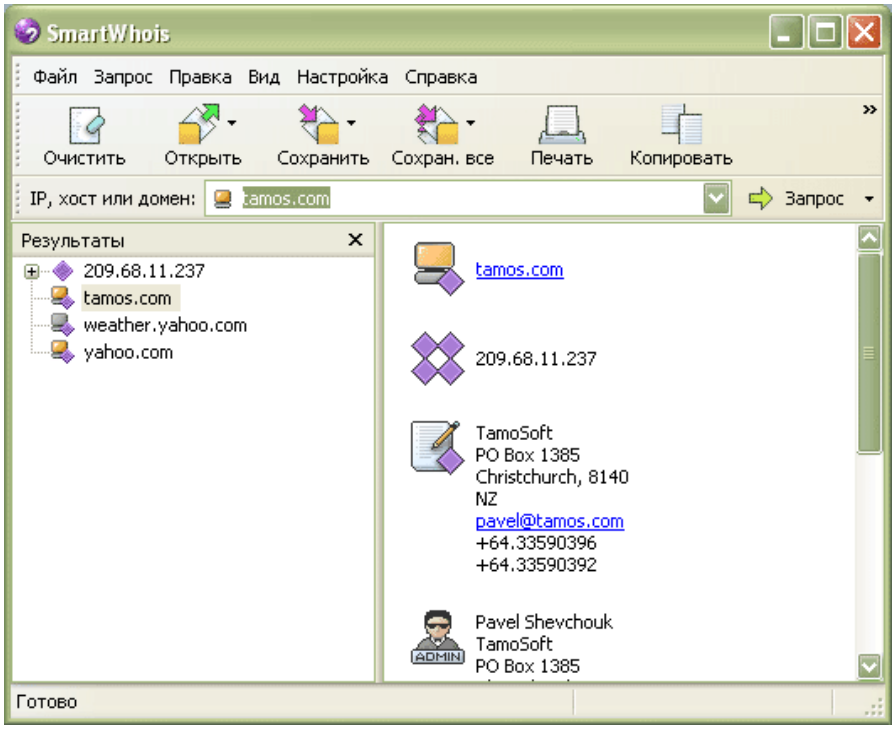
Теперь давайте разберемся с запросами по IP-адресам и именам хостов. Почему мы объединяем эти два вида запросов? По той причине, что с технической точки зрения между ними нет никакой разницы. Как мы уже рассказывали в первой главе, имя хоста представляет собой лишь легко запоминаемый псевдоним для IP-адреса; поэтому запросы по имени хоста и соответствующему IP-адресу одни и те же. Запрос по имени хоста занимает на один шаг больше: программе надо связаться с DNS-сервером и преобразовать имя хоста в IP-адрес. Затем, после получения IP-адреса, по нему будет выполнен запрос к одной из баз данных Whois.

Зачем может потребоваться запрос по IP-адресу/имени хоста, а не по домену? Например, вы хотите узнать, где физически располагается веб-сайт. Или вы хотите узнать, кто отправил вам сообщение электронной почты с определенного IP-адреса. Или вы хотите отправить сообщение провайдеру о спаме или каком-либо нарушении. Как видите, подобная информация может быть нужна в самых разных ситуациях.

Когда вам потребуется проверить IP-адрес или имя хоста, просто введите или вставьте нужное значение в поле ввода, нажмите кнопку **Запрос** и выберите **Как IP / Имя хоста**. Полезный совет: можно просто нажать кнопку "Enter" :-) При выполнении доменных запросов перед нажатием на Enter нажмите и удерживайте кнопку "Ctrl".



Мы ввели "www.tamos.com" и выяснили, что сайт расположен в США и размещен фирмой Pair Networks. Теперь сделаем запрос к "tamos.com" как к домену:



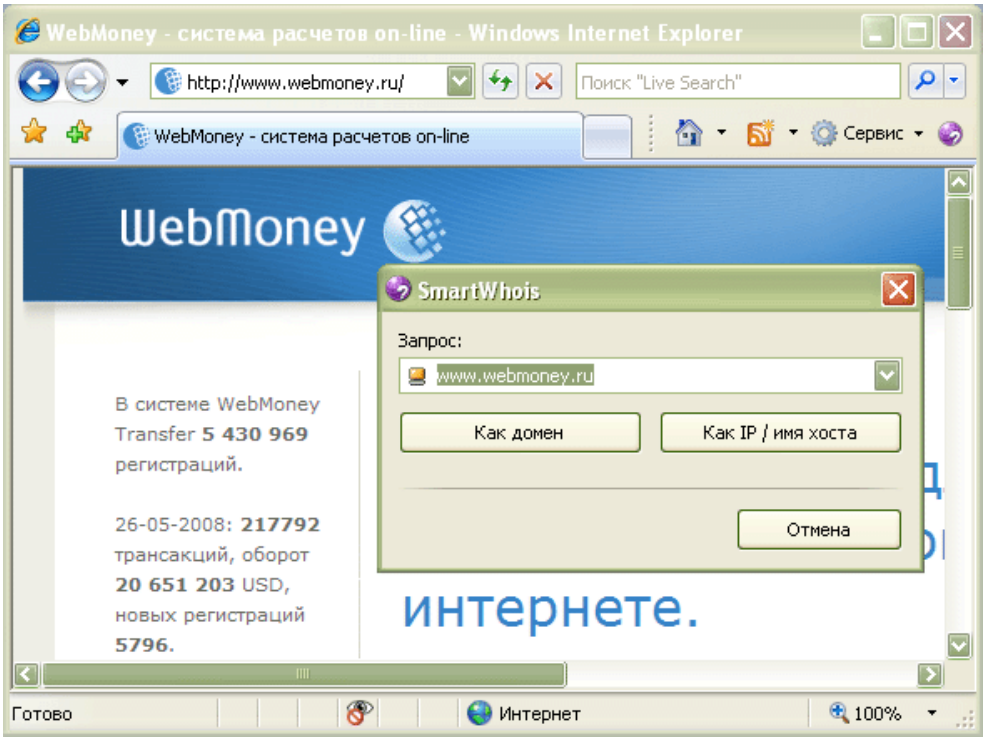
Все верно; "tamos.com" принадлежит TamoSoft, новозеландской компании. Мы сделали важное наблюдение: запросы по доменам и IP-адресам/именам хостов обычно дают разные результаты, и это понятно. Когда вы делаете запрос по домену, вы узнаете, **кто** им владеет. Когда вы делаете запрос по имени хоста или IP-адресу, вы узнаете, **где** физически расположен компьютер с данным именем хоста и **кому** принадлежит диапазон IP-адресов. Домен "tamos.com" принадлежит компании из Новой Зеландии, но веб-сервер компании "www.tamos.com" (на момент написания статьи IP-адрес 209.68.11.237) находится в США, в дата-центре, который принадлежит Pair Networks.

На этом закончим с основами и посмотрим несколько интересных примеров работы со SmartWhois.

SmartWhois и Microsoft Internet Explorer

До чего же полезная кнопка!

Вы заметили эту маленькую кнопку SmartWhois в панели инструментов Internet Explorer (IE)? Если ее там нет, убедитесь, что вы активировали модуль расширения для IE (зайдите в программу SmartWhois и выберите в меню **Настройка => Установки => Интеграция** опцию **Установить расширение Microsoft Internet Explorer**; перезапустите IE. С помощью этой удобной кнопки вы всегда сможете узнать информацию о сайте, на котором вы в данный момент находитесь:



При нажатии на кнопку в адресное поле автоматически введется адрес сайта. Заметьте, что SmartWhois обрезал все ненужные для запроса части URL. Например, если в строке браузера вы видите "http://www.anypay.com/site/ml/eng/htm/home/index.htm", SmartWhois автоматически убирает все, что не относится к имени хоста самого сайта, "www.anypay.com".

Теперь, когда у нас есть имя хоста, мы можем выполнить доменный запрос по "anypay.com" (да, при выполнении доменного запроса SmartWhois автоматически уберет ненужный префикс "www") и узнать, кто владеет доменом. Если вы хотите узнать, где находится веб-сервер, сделайте запрос по IP-адресу/имени хоста.

SmartWhois и Microsoft Outlook

Смотрим на заголовки сообщений E-mail

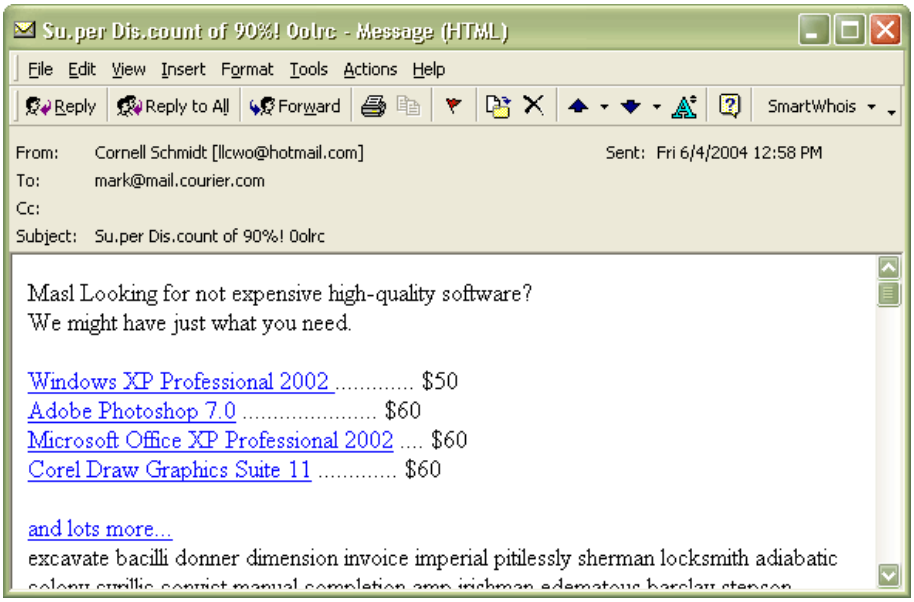
Аналогично IE, вы увидите кнопку SmartWhois на панели инструментов MS Outlook. Если ее там нет, убедитесь, что вы активировали модуль расширения для Outlook (зайдите в программу SmartWhois и выберите в меню **Настройка => Установки => Интеграция** опцию **Установить плагин для Microsoft Outlook**; перезапустите Outlook.

Каждое сообщение электронной почты, которое вы получаете, включает в себя так называемые "заголовки" – непонятный с виду текстовый блок перед телом письма. Заголовки включены в каждое письмо, но обычно не видны пользователю. При этом каждый e-mail клиент можно настроить на показ этой информации, а модуль расширения SmartWhois поможет вам быстро ее отобразить.

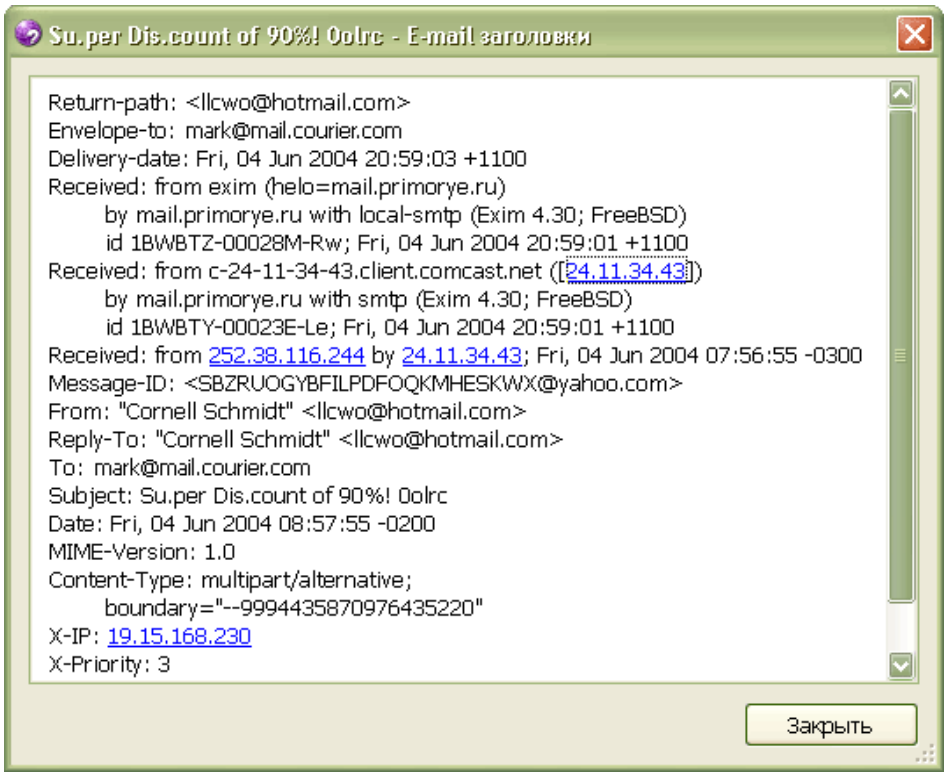
В заголовках содержится информация о пути прохождения сообщения до того, как оно попадет в наш почтовый ящик. Каждый компьютер, через который проходило письмо, оставляет свою запись в заголовке. Мы можем использовать эту дополнительную информацию для того, чтобы отследить путь сообщения от его отправителя. Чтение и

понимание заголовков сообщений не требует экстраординарных усилий, но некоторых знаний и навыков все же потребует. Эта тема находится за рамками нашего обзора, но в Интернете можно найти много хороших статей, например, эту: What Email Headers can Tell You About the Origin of Spam. Мы ограничимся тем, что покажем вам, как с помощью SmartWhois можно получить информацию по IP-адресу, найденному в заголовках.

Вот пример типичного спам-сообщения:



Для просмотра заголовков нажмите на панели инструментов кнопку **SmartWhois** и выберите **Отправить заголовки E-mail в SmartWhois**:



Все IP-адреса, найденные в заголовках, будут выделены как гиперссылки на веб-странице. При переходе по такой ссылке SmartWhois извлечет информацию о выбранном IP-адресе. Вы можете также выделить часть текста и сделать по этому тексту запрос по домену или по имени хоста.

Зачем может понадобиться IP-адрес отправителя сообщения? Этому может быть несколько причин. Вам может быть интересно узнать о физическом местоположении того лица, с которым вы ведете переписку (кто-то, заявляющий, что он во Франции, может на самом деле быть в Италии). Вы можете выяснить, какой организации принадлежит IP-адрес (например, если вы получили письмо с адреса customerservice@citibank.com, но фактически оно пришло из Нигерии, хорошенько подумайте перед тем, как вводить свой пароль доступа к счетам в предложенную веб-форму). Вы также можете пожаловаться на спам.

Независимо от целей ваших запросов, важно понимать ограничения, связанные с этим подходом. Одинаково важно понимать разницу между фактами и вымыслом. Об этом в следующей главе.

Насколько точна информация

Мифы и реальность

Как правило, вы можете получить точную информацию о владельце домена, поскольку при регистрации домена требуется указать контакты. Из этого правила есть исключения, поскольку домен может быть зарегистрирован с помощью украденной кредитной карты, или же владелец мог предоставить недостоверные личные данные, несмотря на то, что во многих странах закон запрещает это делать.

В отличие от доменов, IP-адреса не так привязаны к владельцу. Чаще всего, если вы сделаете запрос по IP-адресу, вы получите сведения об организации, которой принадлежит

определенная область IP-адресов. Обычно это провайдер или компания. Таким образом, вы можете выяснить, через какого провайдера выходит в сеть или в какой фирме работает интересующий вас человек, но вы не сможете узнать имя или адрес человека, который подключился к Интернету с этого IP-адреса. Степень точности данных может варьироваться. IP-адрес может принадлежать небольшой фирме или провайдеру, у которого всего 16 IP-адресов. В этом случае вам повезло: вы сможете точно определить местонахождение человека, вплоть до района города. Но если в вашем случае это не мелкий провайдер, а крупный, как AOL в США, то все, что вы сможете узнать – это адрес главного офиса. Вы даже не выясните регион проживания пользователя, хотя есть некоторые способы, которые могут помочь (например, часовой пояс или имя хоста, по которому зачастую можно определить местонахождение). Это наихудшие из возможных случаев; как правило, степень точности гораздо выше.

Высказывание наподобие такого: "я могу вычислить адрес и номер телефона по IP-адресу" в большинстве случаев не соответствует действительности, если мы имеем в виду среднестатистического "исследователя". Естественно, правоохранительные органы могут отследить пользователя, связавшись с провайдером и проверив журналы соединений. Есть еще один популярный миф, связанный с тем, что по заголовкам сообщений всегда можно вычислить IP-адрес отправителя. Это не всегда правда, потому что несложно спрятать IP-адрес с помощью прокси-сервера (HTTP проски-сервер в случае онлайн-почты или SOCKS прокси-сервер в случае использования стандартных клиентов электронной почты POP/SMTP). И, опять-таки, правоохранительные органы иногда могут отследить пользователя даже в случае использования прокси-сервера.

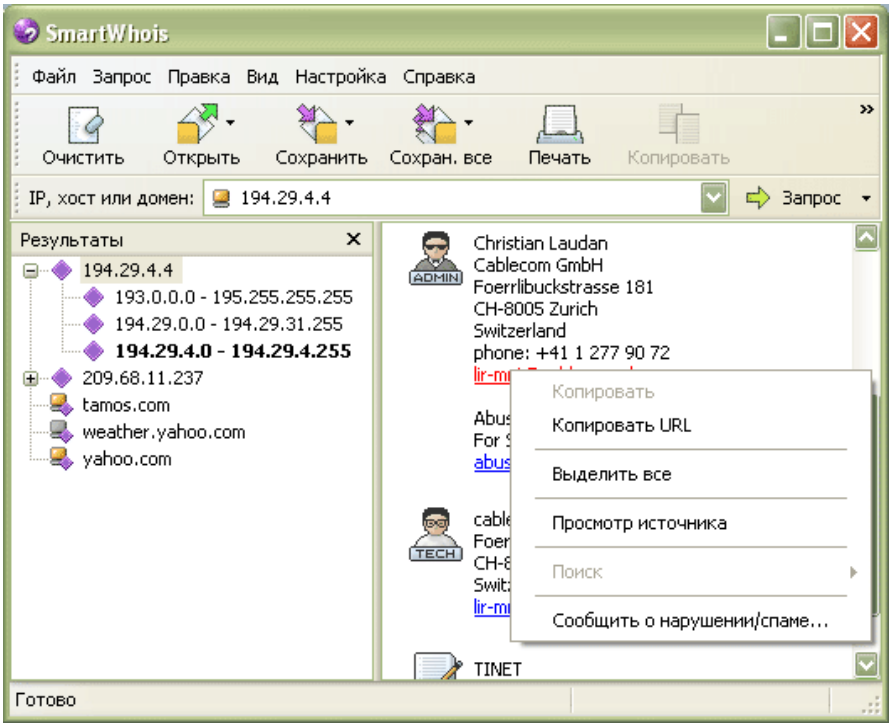
Интересно взглянуть на ситуацию с точки зрения пользователя, чей IP-адрес исследуется или анализируется. Безопасно ли не скрывать его? Надо ли его прятать? Ответ на этот вопрос совсем непрост и лежит за рамками нашего обзора. Вкратце – если вас интересует анонимность, вы можете пойти на некоторые меры и спрятать адрес. Если анонимность и секретность вас особо не беспокоят, все равно есть ситуации, в которых лучше скрыть свой IP-адрес. Возьмем, к примеру, сообщение, которое вы сегодня написали в ньюс-группе или на форуме под псевдонимом и другое, которое вы оставили месяц назад под своим реальным именем. Если вы используете статический IP-адрес, то поиск по вашему IP-адресу покажет все ваши сообщения, независимо от того, какое имя вы использовали. И это лишь один из возможных сценариев.

Теперь вернемся к SmartWhois …

Жалуемся на спам

Всего несколько кликов

Устали от спама? Мы тоже, иногда до такой степени, что нам хочется пожаловаться на особо настойчивого спамера.

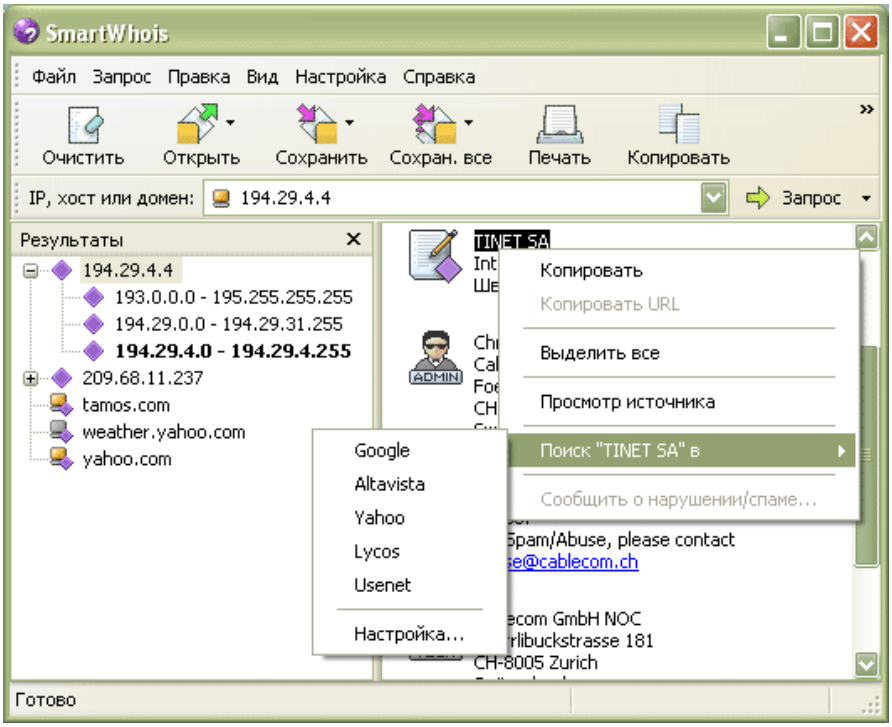


Тщательно изучите заголовки сообщения, найдите IP-адрес спамера (для отправки почты спамер может использовать открытый для всех почтовый сервер или зомби-компьютер, но все равно неплохо оповестить провайдера), выполните запрос SmartWhois, найдите контактную информацию администратора или службы обращений по нарушениям (abuse), кликните правой кнопкой мыши по адресу электронной почты и выберите **Сообщить о нарушении/спаме**. В вашем почтовом клиенте по шаблону будет создано новое письмо. Вам останется только отредактировать текст и добавить некоторые детали. Как видите, отсылка отчета – дело всего нескольких минут!

Анализ данных

SmartWhois как отправная точка исследования

SmartWhois – отличное средство для начала онлайн-расследования. Если у вас есть IP-адрес или доменное имя, о которых вы хотите узнать побольше, то SmartWhois пригодится вам для тщательного анализа данных. Выберите на панели справа часть текста, кликните правой кнопкой мыши и выберите команду **Поиск**. Поиск выделенного текста будет осуществлен посредством нескольких поисковых систем.



Примеры? Пожалуйста! Домен "xyz.com" зарегистрирован на "John Doe, Ltd."? Отлично, посмотрим, что Google знает о John Doe, Ltd. Вы получили почту с IP-адреса 4.4.4.4? Хорошо, посмотрим, как "отметился" этот адрес в Интернете. Конечно, то же самое вы можете сделать и вручную, но это существенно упрощает жизнь. Это меню можно настроить на использование любой поисковой машины.

SmartWhois для продвинутых пользователей

Пакетная обработка, обмен данными, пользовательские запросы и другие советы

Поговорив об основных функциях программы, обсудим теперь и другие, не менее интересные возможности SmartWhois.

Кому-то может понадобиться сделать запросы по многим IP-адресам, именам хостов или доменам одновременно. С помощью SmartWhois это довольно просто. Для загрузки и обработки файла, содержащего множество строк, выберите в меню **Файл => Открыть => Пакетный файл => Как список доменов**. То же самое можно сделать с помощью аргументов командной строки – это подробно описано в файле-справке программы. Из командной строки вы можете запустить SmartWhois, обработать им список, сохранить результаты в файл, выйти из программы – и все это без вмешательства пользователя. Но помните: перегружать Whois-сервера нехорошо, так что, если в вашем списке тысячи записей, велика вероятность вашей временной блокировки со стороны whois-сервиса. Для снижения нагрузки на серверы в окне Установки установите временные интервалы между запросами – будьте ответственным пользователем Интернета!

После получения необходимых данных вы можете записать их в нескольких форматах. Если вы хотите быстро сохранить найденную информацию, просто перетащите содержимое правой панели на рабочий стол. Программа создаст html-файл, который можно будет просмотреть в браузере. Если вы хотите сохранить множество результатов запросов и/или импортировать данные в другое приложение, обратите внимание на ряд форматов, поддерживаемых SmartWhois, а именно XML, XLS, TXT, HTML или собственный формат

SmartWhois. Последний хорош тем, что записанный файл можно загрузить и просмотреть в самой программе SmartWhois.

Иногда требуется выполнить whois-запросы с использованием расширенного синтаксиса. Например, вы нужно запросить информацию об определенном дескрипторе (handle) из базы данных whois. Это просто: выберите **Запрос => Нестандартный запрос**, откроется whois-консоль, откуда вы сможете подключиться к любому whois-серверу и отправить любую строку-запрос.

Идем дальше

IP-адреса, имена хостов и домены – интересная область интернет-технологии. Мы надеемся, что это руководство оказалось для вас полезным в освоении этой технологии и дало несколько полезных советов по использованию отличной whois-программы, SmartWhois.

Посетив наш сайт www.tamos.ru, вы найдете более подробную информацию, отличную техническую поддержку, возможности онлайн-заказа и многое другое!