Техническая сторона обеспечения доказательств в сети Интернет

Аннотация:

Целью данной статьи является обзор основных технических вопросов, возникающих при выполнении нотариусами обеспечения доказательств в сети Интернет.

В нашем стремительно развивающемся информационном обществе сеть Интернет начинает играть все большую роль, в ней появляется все большее количество информационных ресурсов разного вида – новости, справочная информация, различная аудио- и видеоинформация, реклама и так далее.

При этом особую актуальность приобретает вопрос защиты прав интеллектуальной собственности в Интернете. Одним из наиболее частых правонарушений в данной сфере является незаконное использование таких объектов авторского права, как музыкальные, литературные и фотографические произведения. Размещение таких произведений в сети Интернет рассматривается как использование объектов авторского права, на которое, как правило, необходимо разрешение автора или правообладателя.

Соответственно, растет число граждан, желающих с помощью нотариуса зафиксировать те или иные нарушения своих прав при размещении информации в сети Интернет и обращающихся к нотариусу для выполнения такого действия, как обеспечение доказательств.

При этом нотариусу приходится вплотную сталкиваться с рядом технических вопросов, незнание которых может свести на нет все его усилия по выполнению этого нотариального действия.

Ведь далеко не всегда суд сочтет заверенную нотариусом распечатку веб-страницы бесспорным доказательством правонарушения. Протокол осмотра может легко быть оспорен, если в нем нотариус не зафиксировал ряд технических вопросов, например, каким образом было установлено соединение с сетью Интернет.

Целью данной статьи является обзор основных технических вопросов, возникающих при выполнении нотариусами обеспечения доказательств в сети Интернет.

Адресация в сети Интернет. Система доменных имен

В Меморандуме о правовом понимании доменного имени и интернет-сайта, подготовленном рабочей группой по правовым аспектам доменных имен и интернет-сайтов при Координационном центре домена RU, приводятся следующие определения:

доменное имя (в сети Интернет) – символьное обозначение, зарегистрированное для сетевой адресации, в которой используется система доменных имен (DNS).

Интернет-сайт – совокупность информации и программ для ЭВМ, содержащихся в информационной системе, обеспечивающей доступность такой информации в сети Интернет по определенным сетевым адресам.

Пользователи Интернета привыкли к символьным адресам сайтов (наименованиям доменов), например, **www.notariat.ru** или **www.triasoft.com**. Действительно, такие адреса и набирать проще, и запоминаются они лучше. Технология доменных имен (DNS – Domain Name System), благодаря которой функционируют эти символьные адреса, настолько срослась с Интернетом, что абсолютное большинство пользователей вообще и не подозревают о ее существовании. А некоторое количество «продвинутых пользователей» вспоминают про DNS только тогда, когда с ней возникают какие-то проблемы.

Между тем для адресации узлов Интернета используются специальные числовые «коды» – IP-адреса (читается: «ай-пи» адреса). Традиционный IP-адрес может быть записан с помощью четырех чисел в десятичной системе счисления, разделенными точками, например, **217.23.156.171** или **89.111.176.61**. Система доменных имен как раз служит для перевода символьного адреса сайта, называемого также доменным именем, в

его числовой адрес, например, доменное имя **notariat.ru** преобразуется в IP-адрес **83.222.104.42**.

Также необходимо знать, что каждый из доменов может содержать множество «подчиненных» доменов, а все дерево доменных имен принято делить по уровням. Домен **.ru** является доменом первого уровня, **notariat.ru** относится ко второму уровню, **mail.notariat.ru** – к третьему уровню, и так далее. Основной составной частью системы доменных имен являются, безусловно, домены первого уровня, классифицирующие веб-сайты по географическому признаку – к этой группе относятся, например, домен всероссийской зоны Интернета **.ru**, украинской зоны **.ua,** германской **.de** и т.д.

Отдельную категорию доменов первого уровня составляют так называемые зоны общего назначения, распределяющие ресурсы по признаку тематической направленности – среди них можно перечислить коммерческую зону **.com**, зону общесетевых ресурсов **.net**, некоммерческих организаций **.org**, учебных заведений**.edu**, военных организаций **.mil** и правительственных структур **.gov**.

С точки зрения пользователя и в сильно упрощенном виде алгоритм работы DNS по поиску IP-адресов веб-сайтов можно описать следующим образом. Когда пользователь вводит в адресной строке браузера (программы, используемой для просмотра страниц сайта) адрес веб-сайта, например, **www.notariat.ru**, компьютер выполняет запрос к тому или иному известному этому компьютеру серверу DNS, «спрашивая» сервер о том, какой IP-адрес связан с доменным именем, указанным пользователем. В ответ сервер DNS, проверив соответствие по своим внутренним таблицам или выполнив запрос к другим серверам DNS, присылает искомый IP-адрес. Далее браузер устанавливает соединение с веб-сайтом уже по IP-адресу. Обычно DNS сервер предоставляется Интернет-провайдером – организацией, обеспечивающей подключение к сети Интернет.

Но можно настроить компьютер и на использование любого другого DNS сервера, а также «прописать» на нем IP-адрес нужного сайта вручную, в результате чего браузер вместо того, чтобы обращаться к подлинному серверу, будет перенаправлен по ложному адресу, содержащему поддельную страницу.

Технически это делается настолько просто, что справится даже школьник, если он получит доступ к компьютеру нотариуса на пару минут. А нотариус, если он не предпримет специальных мер, не заметит подмены. Все будет как обычно – нотариус введет в браузере адрес сайта, далее перейдет на нужную страницу, распечатает ее содержимое, сформировав тем самым ложные доказательства. Существуют и другие способы подмены, не требующие доступа к компьютеру нотариуса.

Поэтому при обеспечении доказательств в сети Интернет рекомендуется проверить соответствие символьного адреса сайта его настоящему IP-адресу и убедиться в том, что браузер отображает страницы подлинного сайта. Эта операция довольно несложная, поэтому для страховки лучше выполнять ее всегда.

Вот примерная последовательность действий, которая работает для большинства случаев (на примере сайта **www.konp42.ru**):

KONP42.RU

1. Определить имена DNS серверов, ответственных за хранение подлинного IP-адреса интересующего нас сайта. Для этого необходимо воспользоваться WHOIS сервисом (от англ. who is – «кто такой?»), например, запустить браузер и зайти по адресу https://www.nic.ru/whois/, затем в появившейся форме заполнить поле «Информация о доменах…» значением konp42.ru (без www) и нажать кнопку «ОК».

В результате выполнения данного запроса на экране будет показана некоторая информация о владельце доменного имени notary.ru, а также информация об его DNS серверах (эти сервера являются главными по предоставлению информации об IP-адресе сайта для всего мира):

Информация о домене KONP42.RU

Домен занят.

По данным WHOIS.NIC.RU:

```
domain:        KONP42.RU
nserver:       ns1.rsnx.ru
nserver:       ns2.rsnx.ru
state:         REGISTERED, DELEGATED
admin-contact:https://www.nic.ru/cgi/whois_webmail.cgi?domain=KONP42.RU
org:           Kemerovskaya oblastnaya notarialnaya palata (Association)
registrar:     RU-CENTER-RU
created:       2014.11.28
paid-till:     2016.11.28
source:        RU-CENTER

>>> Last update of WHOIS database: 2016.06.07T04:29:22Z <<<
```

В данном случае за хранение IP-адреса домена notary.ru отвечают два DNS сервера:

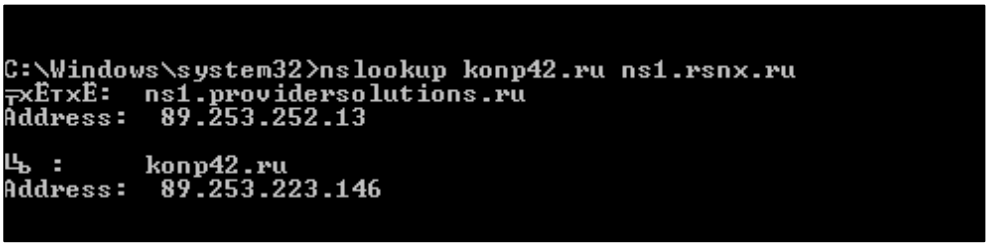
nserver: `ns1.rsnx.ru`

nserver: `ns2.rsnx.ru`

2. Определить с помощью одного из этих DNS серверов IP-адрес сайта notary.ru. Для этого можно использовать утилиту nslookup, входящую в состав ОС Windows. Эту утилиту нужно запускать из командной строки. Выберите через главное меню Windows: кнопка «Пуск»-> «Программы»-> «Стандартные» -> «Командная строка», и в появившемся черном окне введите:

C:\> nslookup konp42.ru ns1.rsnx.ru

В результате мы должны увидеть примерно такой ответ DNS-сервера:

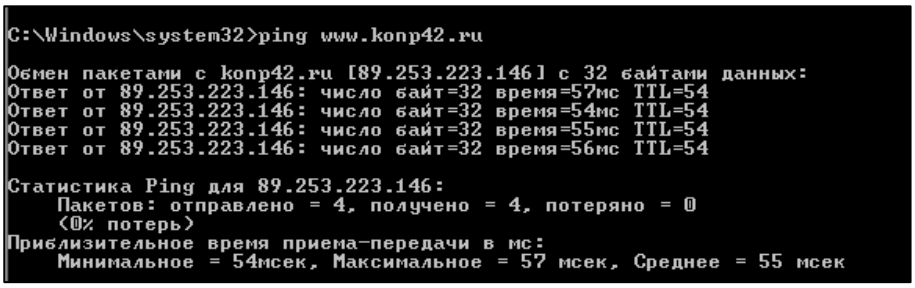


В конце ответа значение Address указывает IP-адрес сервера, на котором размещен сайт: **89.253.223.146**

3. Зная подлинный IP-адрес сайта, можно проверить, совпадает ли этот адрес с тем, к которому обращается браузер. Для этого подойдет утилита ping, также запускаемая из командной строки:

C:\> ping www.konp42.ru

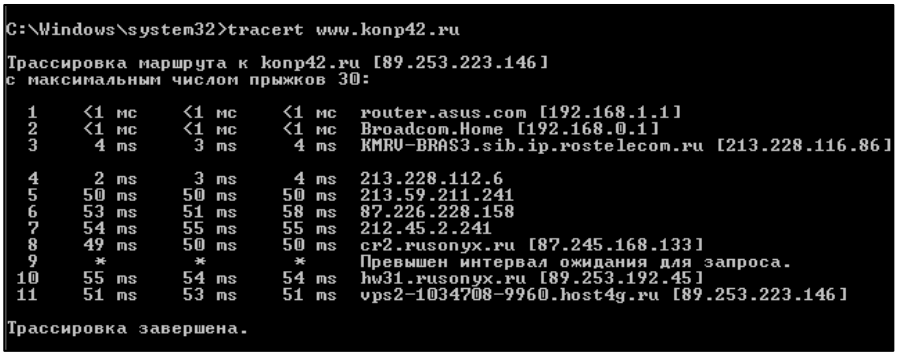
Результат выполнения ping:



Как видно, везде присутствует IP-адрес **89.253.223.146**

Утилита tracert, тоже запускаемая из командной строки, показывает цепочку серверов, через которые выполняется обмен информацией:

C:\> tracert www.konp42.ru



Результат выполнения tracert будет зависеть от точки, через которую выполняется подключение к Интернет, но в начале и конце ответа также будет указан IP-адрес сервера konp42.ru.

В приведенных примерах IP-адрес, определенный с помощью nslookup, совпадает с адресами, полученными с помощью ping и tracert. Это говорит о том, что DNS сервера работают нормально, и в браузере мы увидим содержимое подлинного сайта ***www.konp42.ru*****.**

Результаты выполнения запроса whois, утилит nslookup, ping и tracert также хорошо распечатать и приложить к протоколу осмотра.

Для сайтов в других зонах, например .com, информация, выводимая по запросу whois, может выглядеть по-другому, например, вместо nserver будет указано Name server, но суть от этого не меняется.

NOTARIAT.RU

1. Определить имена DNS серверов, ответственных за хранение подлинного IP-адреса интересующего нас сайта. Для этого необходимо воспользоваться WHOIS сервисом (от англ. who is – «кто такой?»), например, запустить браузер и зайти по адресу https://www.nic.ru/whois/, затем в появившейся форме заполнить поле «Информация о доменах…» значением notariat.ru (без www) и нажать кнопку «ОК».

В результате выполнения данного запроса на экране будет показана некоторая информация о владельце доменного имени notary.ru, а также информация об его DNS серверах (эти сервера являются главными по предоставлению информации об IP-адресе сайта для всего мира):

Информация о домене NOTARIAT.RU

Домен занят.

По данным WHOIS.NIC.RU:

```
domain:       NOTARIAT.RU
nserver:      ns1.j-vista.ru
nserver:      ns2.j-vista.ru
state:        REGISTERED, DELEGATED
admin-contact:https://www.nic.ru/cgi/whois_webmail.cgi?domain=NOTARIAT.RU
org:          Chambre Notariale Federale
registrar:    RU-CENTER-RU
created:      2004.12.16
paid-till:    2016.12.01
source:       RU-CENTER

>>> Last update of WHOIS database: 2016.06.07T04:54:56Z <<<
```

В данном случае за хранение IP-адреса домена notary.ru отвечают два DNS сервера:

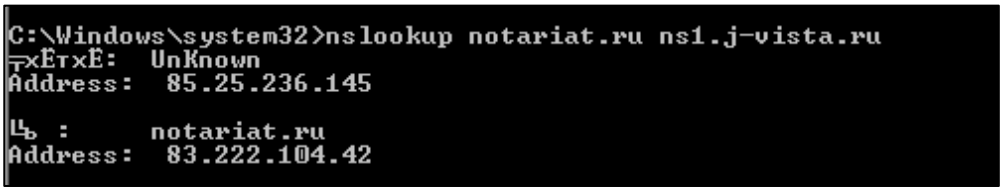
nserver: `ns1.j-vista.ru`

nserver: `ns2.j-vista.ru`

2. Определить с помощью одного из этих DNS серверов IP-адрес сайта notary.ru. Для этого можно использовать утилиту nslookup, входящую в состав ОС Windows. Эту утилиту нужно запускать из командной строки. Выберите через главное меню Windows: кнопка «Пуск»-> «Программы»-> «Стандартные» -> «Командная строка», и в появившемся черном окне введите:

C:\> nslookup notariat.ru `ns1.j-vista.ru`

В результате мы должны увидеть примерно такой ответ DNS-сервера:

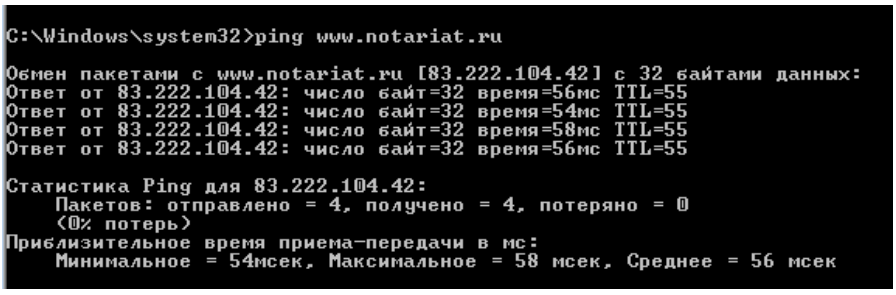


В конце ответа значение Address указывает IP-адрес сервера, на котором размещен сайт: **83.222.104.42**

3. Зная подлинный IP-адрес сайта, можно проверить, совпадает ли этот адрес с тем, к которому обращается браузер. Для этого подойдет утилита ping, также запускаемая из командной строки:

C:\> ping www.notariat.ru

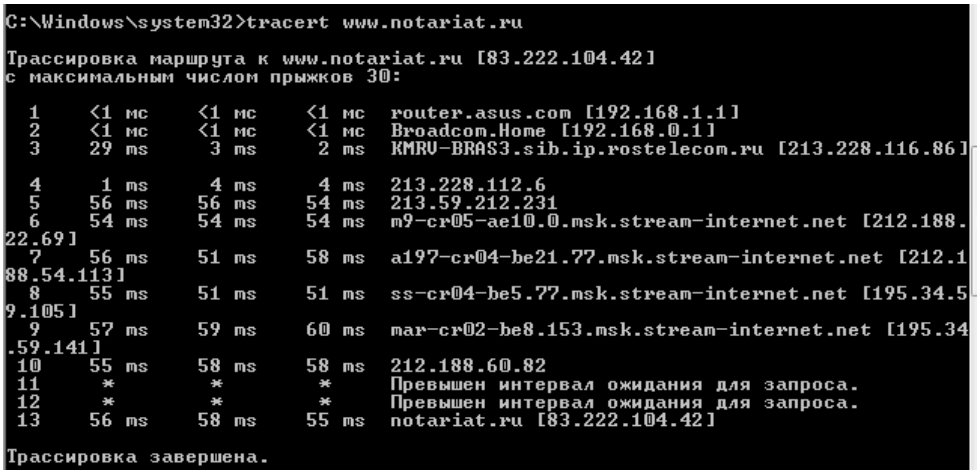
Результат выполнения ping:



Как видно, везде присутствует IP-адрес **83.222.104.42**

Утилита tracert, тоже запускаемая из командной строки, показывает цепочку серверов, через которые выполняется обмен информацией:

C:\> tracert www.notariat.ru



Результат выполнения tracert будет зависеть от точки, через которую выполняется подключение к Интернет, но в начале и конце ответа также будет указан IP-адрес сервера notariat.ru.

В приведенных примерах IP-адрес, определенный с помощью nslookup, совпадает с адресами, полученными с помощью ping и tracert. Это говорит о том, что DNS сервера работают нормально, и в браузере мы увидим содержимое подлинного сайта ***www.notariat.ru***.

Результаты выполнения запроса whois, утилит nslookup, ping и tracert также хорошо распечатать и приложить к протоколу осмотра.

Для сайтов в других зонах, например .com, информация, выводимая по запросу whois, может выглядеть по-другому, например, вместо nserver будет указано Name server, но суть от этого не меняется.