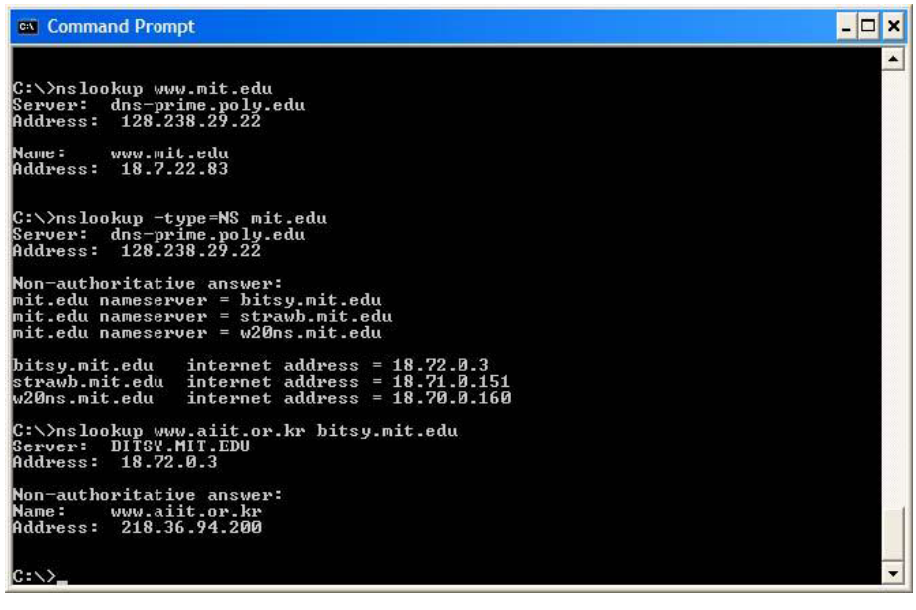
Лабораторная работа Wireshark: DNS

«Скажи мне, и я забуду. Покажи мне, и я запомню. Дай попробовать самому, и я пойму».
Китайская пословица

Как описано в разделе 2.5 книги, служба DNS транслирует имена хостов в IP-адреса, выполняя важную роль в инфраструктуре сети Интернет. В этой лабораторной работе мы более внимательно ознакомимся с клиентской частью DNS. Напомним, что роль клиента в DNS относительно проста — клиент отправляет *запрос* своему локальному серверу DNS и получает обратно *ответ*. Как показано на рис. 2.21 и 2.22 книги, большая часть работы, в которой иерархические серверы DNS общаются друг с другом, рекурсивными или итеративными методами разрешая запрос клиента, невидима для самих DNS-клиентов. С их точки зрения протокол достаточно прост — сформировать запрос на локальный сервер DNS и получить от него ответ.
Перед тем как начать работу, вы, вероятно, захотите освежить в памяти материалы раздела 2.5, в особенности, касающиеся **локальных DNS-серверов**, **DNS-кэширования**, **ресурсных записей DNS** и **поля «Тип»** в этих записях.

nslookup

В этой работе мы будем часто пользоваться утилитой `nslookup`, доступной как на платформах Linux/Unix, так и на Microsoft. Для ее запуска просто наберите `nslookup` в командной строке.
В качестве базовой функции утилита `nslookup` позволяет хосту, на котором она запущена, запрашивать записи с заданного сервера DNS. Запрашиваемым может быть корневой DNS-сервер, DNS-сервер верхнего уровня (TLD), авторитетный DNS-сервер или промежуточный сервер DNS (см. определения в тексте книги). При выполнении данного задания утилита отправляет запрос указанному DNS-серверу, получает от него ответ и отображает результат.



На снимке экрана, представленном выше, показаны результаты выполнения трех отдельных команд `nslookup` (в командной строке Windows). В данном примере клиентский хост расположен в Политехническом Университете Бруклина, а локальным DNS-сервером для него является dns-prime.poly.edu. Если в запросе `nslookup` не указан DNS-сервер, то запрос идет к серверу по умолчанию, которым и является в данном случае dns-prime.poly.edu. Рассмотрим первую команду:

```
nslookup www.mit.edu
```

Если дословно, то данная команда говорит: «пришли мне, пожалуйста, IP-адрес хоста www.mit.edu». Как видно из снимка экрана, ответная информация на эту команду состоит из двух частей: (1) имя и IP-адрес отвечающего сервера DNS; и (2) сам ответ на запрос, содержащий имя запрашиваемого хоста www.mit.edu и его IP-адрес. Хотя ответ и пришел от локального DNS-сервера Политехнического Университета, вполне возможно, что он для получения результата обменивался итеративно с другими DNS-серверами (как описано в разделе 2.5).
Теперь рассмотрим вторую команду:

```
nslookup -type=NS mit.edu
```

Здесь мы выполнили команду с параметром `-type=NS` и указали имя домена `mit.edu`. Это вызвало запрос ресурсной записи типа NS у локального сервера DNS.
Другими словами, команда гласит «пришли мне, пожалуйста, имена хостов авторитетных DNS-серверов, отвечающих за домен mit.edu». (Если параметр `-type` не используется, `nslookup` использует по умолчанию запрос записей типа A.) Ответ, отображаемый на скриншоте выше, во-первых, указывает на DNS-сервер, который предоставляет ответ (локальный сервер DNS по умолчанию), содержащий три имени DNS-серверов Массачусетского технологического института. Каждый из этих серверов является, действительно, авторитетным для хостов MIT. Тем не менее, `nslookup` указывает, что ответ будет «неавторитетным», это означает, что этот ответ пришел из кэша некоторого сервера, а не от авторитетного сервера DNS. Наконец, ответ содержит еще и IP-адреса этих авторитетных DNS-серверов Массачусетского технологического института. (Хотя `nslookup` явно не просил эти IP-адреса, локальный сервер DNS предоставляет их «просто так».) И, наконец, третья команда:

```
nslookup www.aiit.or.kr bitsy.mit.edu
```

Здесь мы указываем, что хотим отослать запрос не серверу по умолчанию (dns-prime.poly.edu), а конкретно DNS-серверу bitsy.mit.edu. Таким образом, запрос и ответ идут напрямую между нашим хостом и сервером bitsy.mit.edu, и тот предоставляет нам IP-адрес хоста www.aiit.or.kr, который является веб-сервером Института информационных технологий (в Корее).
Если перейти от примеров к общему синтаксису команды `nslookup`, то он следующий:

```
nslookup -параметр1 -параметр2 узел dns-сервер
```

Команда `nslookup` может быть выполнена с несколькими параметрами, а может и без них вообще. Как мы видели выше, указание DNS-сервера тоже необязательно — в этом случае запрос будет обрабатывать локальный сервер DNS, установленный по умолчанию.
Теперь попробуйте поупражняться с `nslookup` самостоятельно. Выполните следующее (и запишите результаты):

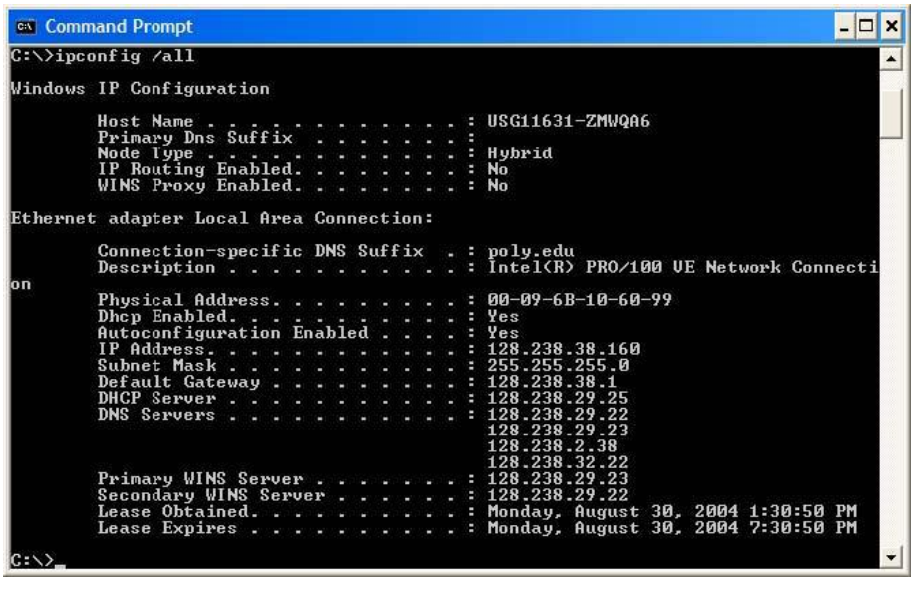
1. Выполните `nslookup`, чтобы получить IP-адрес веб-сервера в Азии. Какой адрес вы получили?
2. Выполните `nslookup`, чтобы определить авторитетные DNS-серверы университета в Европе. Какие у них адреса?
3. Выполните `nslookup` таким образом, чтобы произвести запрос адреса почтового сервера Yahoo! одному из DNS-серверов, определенных в ответе на вопрос 2. Какой адрес вы получили?

ipconfig

Утилиты `ipconfig` (для Windows) и `ifconfig` (для Linux/Unix) являются одними из наиболее простых и, в то же время, полезных команд для работы с сетевыми настройками на вашем компьютере. Здесь мы с вами рассмотрим только первую из них — `ipconfig`. (Утилита `ifconfig` *для* Linux/Unix работает аналогично*).* Ее можно использовать для отображения вашей текущей информации стека протоколов TCP/IP, включая адрес вашего хоста, адреса DNS-серверов, тип сетевого адаптера и т.д. Например, чтобы отобразить всю сетевую информацию вашего хоста, просто наберите

```
ipconfig \all
```

в командной строке, как показано на снимке ниже



Утилита `ipconfig` также очень полезна при работе с информацией службы DNS. Как вы помните из раздела 2.5, хост кэширует недавно полученные им DNS-записи. Чтобы их просмотреть, наберите команду:

```
ipconfig /displaydns
```

Каждая запись содержит срок жизни (TTL) в секундах. Чтобы очистить кэш DNS, наберите:

```
ipconfig /flushdns
```

Данная команда стирает все записи в кэше и загружает туда записи, находящиеся в файле *hosts*.

DNS-трассировка с использованием Wireshark

Теперь, после знакомства с утилитами `nslookup` и `ipconfig`, мы готовы приступить к более серьезным задачам. Давайте сначала перехватим пакеты DNS, которые создаются при обычном посещении веб-сайтов.

- Используйте `ipconfig` для очистки кэша DNS на вашем компьютере.
- Откройте браузер и очистите его кэш (для Internet Explorer можете использовать сочетание клавиш **CTRL**+**Shift**+**Del**).
- Запустите Wireshark и введите `ip.addr == ваш_IP_адрес` в строке фильтра, где значение *ваш_IP_адрес* вы можете получить, используя утилиту `ipconfig`. Данный фильтр позволит нам отбросить все пакеты, не относящиеся к вашему хосту. Запустите процесс захвата пакетов в Wireshark.
- Зайдите на страницу **www.ietf.org** в браузере.
- Остановите захват пакетов.

Если у вас нет возможности запустить захват пакетов, используя активное подключение к сети Интернет, вы снова можете использовать готовые результаты трассировки, выполненной на одном из компьютеров авторов[1]. Ответьте на вопросы ниже. Настоятельно рекомендуем вам всегда иметь под рукой распечатку результатов трассировки с пометками и комментариями, которые помогут вам с ответами[2]. Для того, чтобы распечатать информацию, относящуюся к конкретному пакету, выберите команду меню **File ⇒ Print** (Файл ⇒ Печать), установите переключатель в положение **Selected packet only** (Только выбранный пакет), активируйте параметр **Packet summary line** (Заголовок списка пакетов) и, включив таким образом минимально необходимый для ответа набор детальной информации о пакете, выведите результаты на печать.

4. Найдите DNS-запрос и ответ на него. С использованием UDP или TCP они отправлены?
5. Какой порт назначения у запроса DNS? Каков исходящий порт у DNS-ответа?
6. На какой IP-адрес отправлен DNS-запрос? Используйте `ipconfig` для определения IP-адреса вашего локального DNS-сервера. Одинаковы ли эти два адреса?

---

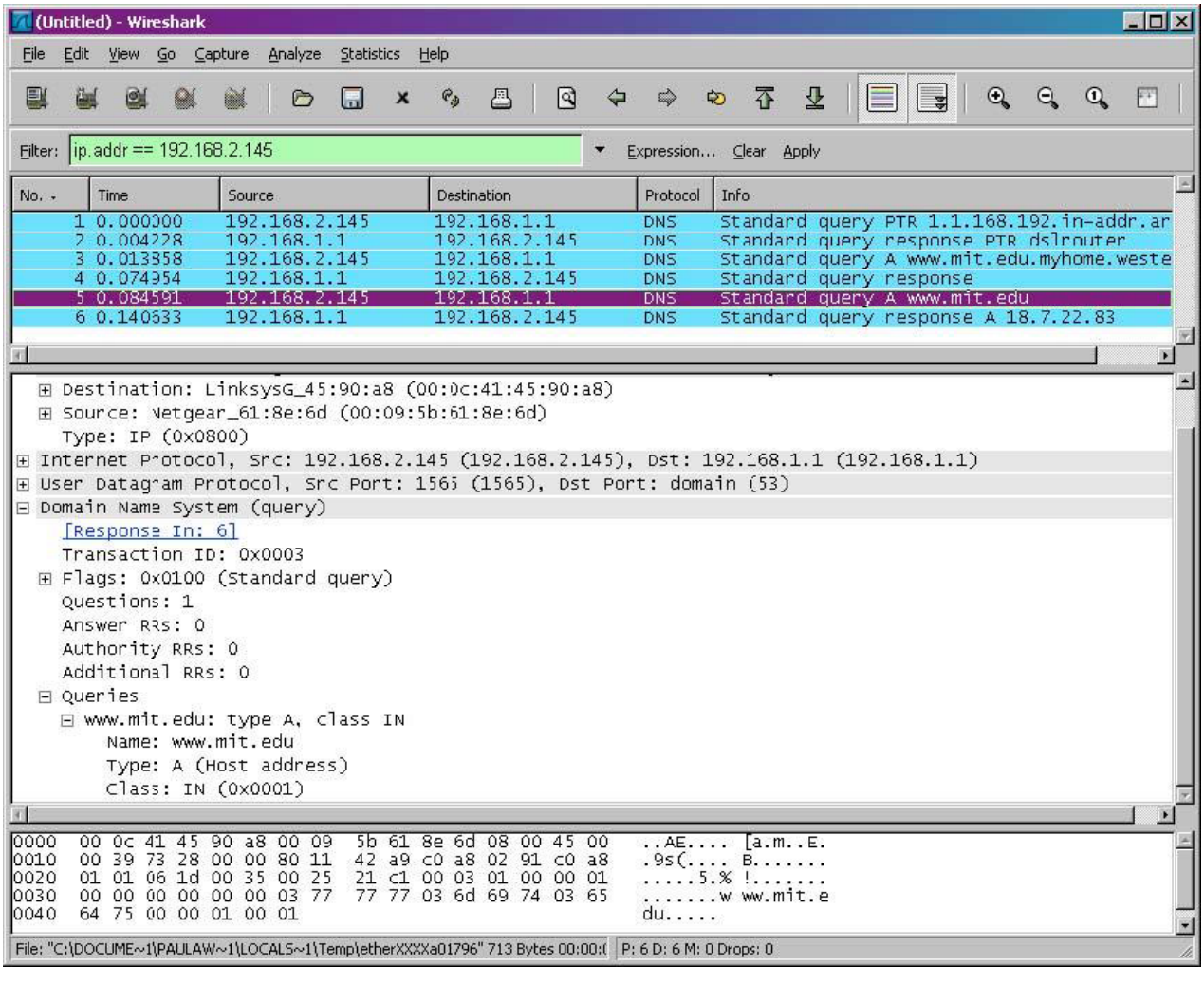
[1] Откройте папку wireshark-traces и используйте файл dns-ethereal-trace-1. Он представляет собой результат трассировки, выполненной на компьютере одного из авторов с помощью Wireshark, следуя указанным выше шагам. Вы можете загрузить данный файл в ПО Wireshark, используя команду меню **File ⇒ Open** (Файл ⇒ Открыть).

[2] Имеются в виду пометки и комментарии, которые можно нанести на бумажных копиях распечаток цветным карандашом, либо на электронных в виде выделения текста и добавления примечаний.

7. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?
8. Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?
9. Посмотрите на последующий TCP-пакет с флагом SYN, отправленный вашим компьютером. Соответствует ли IP-адрес назначения пакета с SYN одному из адресов, приведенных в ответном сообщении DNS?
10. Веб-страница содержит изображения. Выполняет ли хост новые запросы DNS перед загрузкой этих изображений?

Теперь поэкспериментируем с утилитой `nslookup`[3].

- Запустите захват пакетов.
- Выполните команду `nslookup` для сервера **www.mit.edu**.
- Остановите захват.



[3] Если у вас нет возможности запустить захват пакетов, используйте файл трассировки dns-ethereal-trace-2, находящийся в папке wireshark-traces.

Из снимка мы видим, что команда `nslookup`, в действительности, отправляет три DNS-запроса и получает три ответных сообщения DNS. Так как первые две пары запрос-ответ являются специфичными именно для `nslookup` и обычно не генерируются стандартными Интернет-приложениями, мы в этом задании сосредоточимся только на третьей паре сообщений DNS.

11. Каков порт назначения в запросе DNS? Какой порт источника в DNS-ответе?
12. На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию?
13. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?
14. Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?
15. Сделайте снимок.

Повторим эксперимент, но теперь выполним команду:

```
nslookup –type=NS mit.edu
```

Ответьте на следующие вопросы[4]:

16. На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию?
17. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?
18. Проанализируйте ответное сообщение DNS. Имена каких DNS-серверов Массачусетского института в нем содержатся? А есть ли их адреса в этом ответе?
19. Сделайте скриншот.

А теперь повторим, используя следующую команду:

```
nslookup www.aiit.or.kr bitsy.mit.edu
```

20. Ответьте на следующие вопросы[5]:
21. На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию? Если нет, то какому хосту он принадлежит?
22. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?
23. Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?
24. Сделайте снимок.

[4] При невозможности запустить захват пакетов, используйте файл трассировки dns-ethereal-trace-3, находящийся в папке wireshark-traces.

[5] Можно использовать файл dns-ethereal-trace-4 из той же папки