Санкт-Петербургский государственный политехнический университет

Институт компьютерных наук и кибербезопасности

Высшая школа компьютерных технологий и информационных систем

**Отчет по лабораторной работе №2**

**по курсу «Технологии компьютерный сетей»**

«Wireshark: DNS & HTTP»

**Работу выполнил студент группы №5130901/10203:**

Алексеев Лев Сергеевич

Подпись:

**Работу принял преподаватель:**

Богач Наталья Владимировна

Подпись:

Санкт-Петербург

2024

**Wireshark: DNS**

В данной работе будем пользоваться утилитой nslookup. 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.

1. Выполните команду nslookup, чтобы получить IP-адрес веб-сервера в Азии. Какой адрес вы получили?

Был выполнен запрос для сервера www.rediff.com. Его IP-адрес 2.19.183.47.

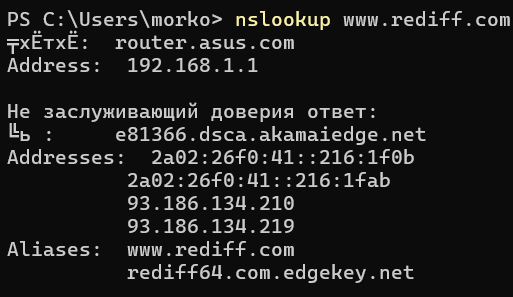


Рис. 1. Снимок к вопросу 1

1. Выполните nslookup, чтобы определить авторитетные DNS-серверы университета в Европе. Какие у них адреса?

Был выполнен запрос для сервера Университета в городе Янина, Греция. Его IP-адрес 192.168.0.1.

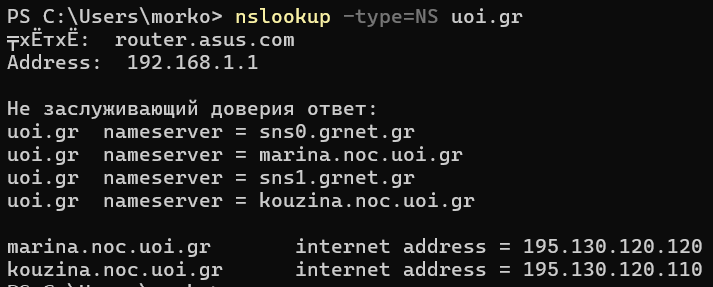


Рис. 2. Снимок к вопросу 2

1. Выполните nslookup таким образом, чтобы произвести запрос адреса почтового сервера Yahoo! одному из DNS-серверов, полученных в ответе на вопрос 2. Какой адрес вы получили?

Полученный адрес: 18.0.72.3. При попытке выполнения команды с ПК был request timeout.

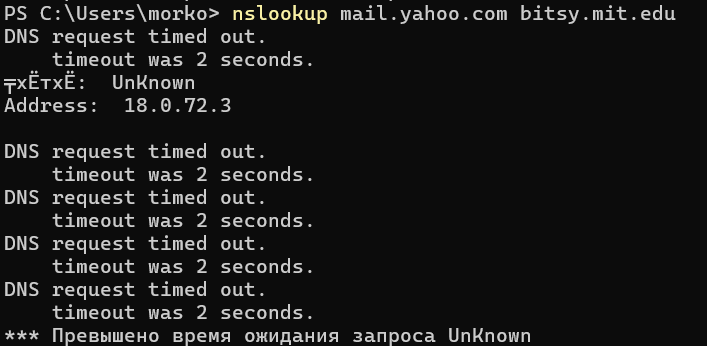


Рис. 3. Снимок к вопросу 3

**DNS-трассировка с использованием Wireshark**

1. Найдите DNS-запрос и ответ на него. С использованием UDP или TCP они отправлены?

Они отправлены через UDP

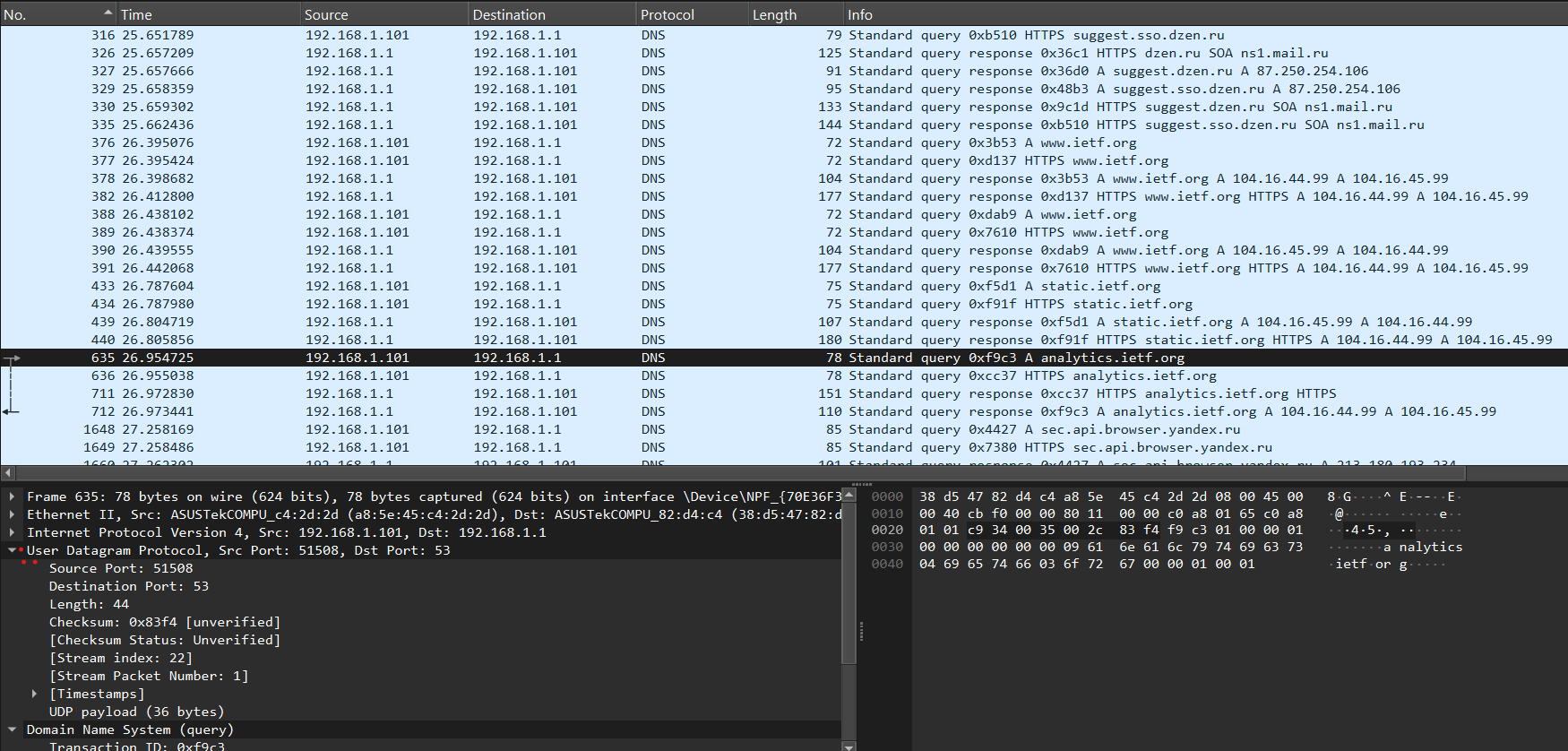


Рис. 4. DNS-запрос

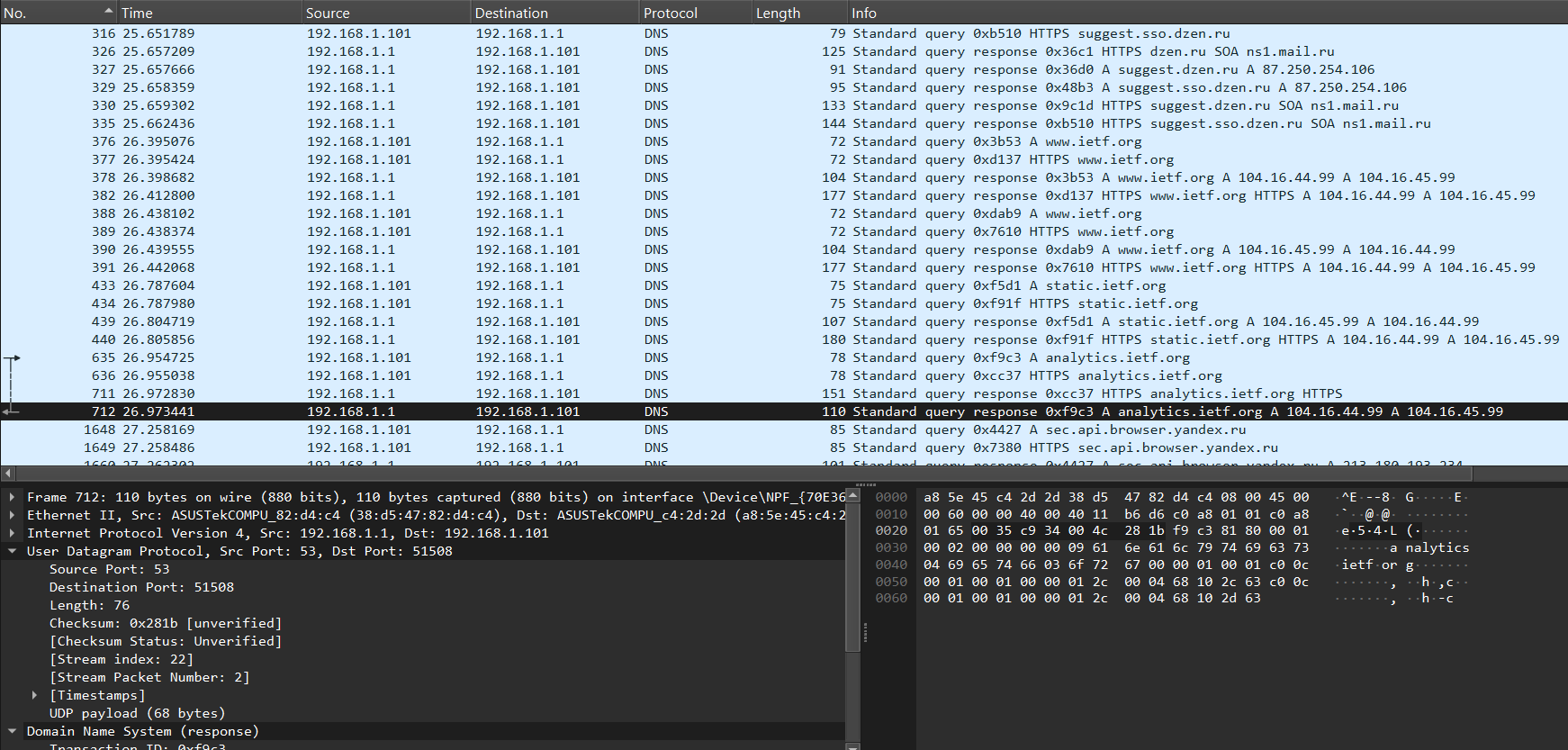


Рис. 5. DNS-ответ

1. Какой порт назначения у запроса DNS? Каков исходящий порт у DNS-ответа?

Порт назначения запроса DNS – 53, исходящий порт DNS ответа такой же.

1. На какой IP-адрес отправлен DNS-запрос? Используйте nslookup для определения IP-адреса вашего локального DNS-сервера. Одинаковы ли эти два адреса?

Запрос отправлен на адрес 192.168.1.1, который принадлежит локальному серверу DNS.

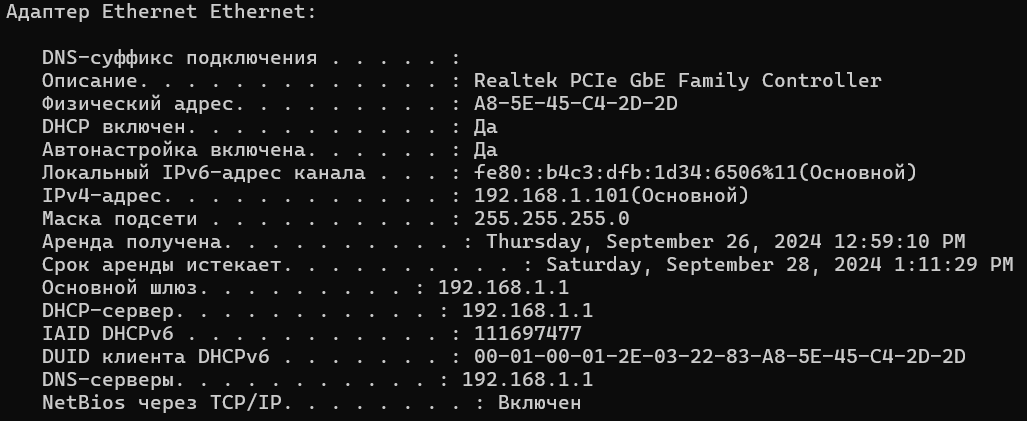


Рис. 6. Результат команды ipconfig –all

1. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?

Это стандартный запрос записи типа A не содержащий никаких ответов.

1. Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?

Было два ответа, в которых содержится информация об имени хоста, классе (типе сети), типе ресурсной записи, времени ее жизни в кэше (TTL), размере данных и IP-адресе.

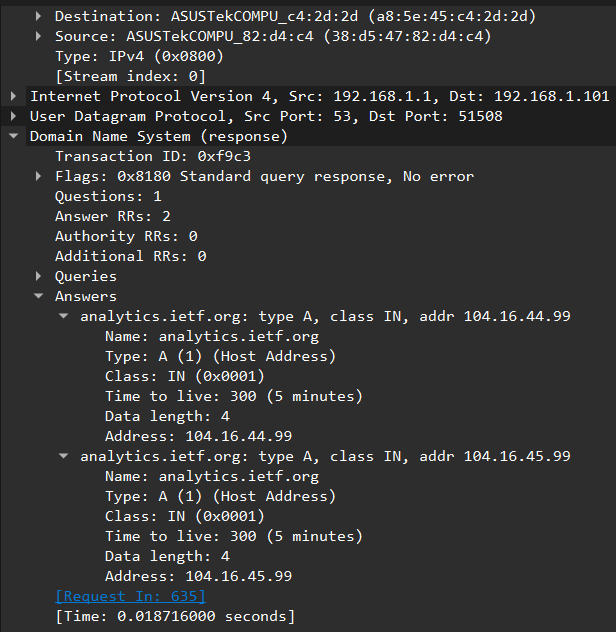
****

Рис. 7. Ответное сообщение DNS

1. 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?

Первый пакет с флагом SYN отправлен на адрес 104.16.45.99 – первый IP-адрес, полученный в ответном сообщении DNS.

1. Веб-страница содержит изображения. Выполняет ли хост новые запросы DNS перед загрузкой этих изображений?

Нет.

1. Каков порт назначения в запросе DNS? Какой порт источника в DNS-ответе?

Порт назначения запроса DNS – 53, исходящий порт DNS ответа такой же.

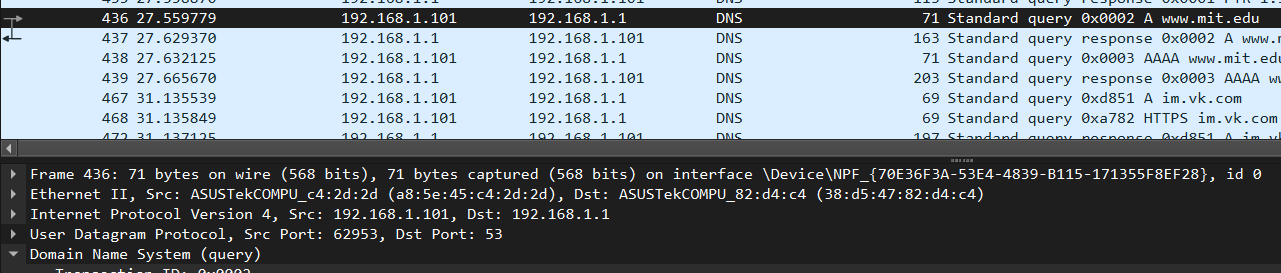
****

Рис. 8. DNS-запрос

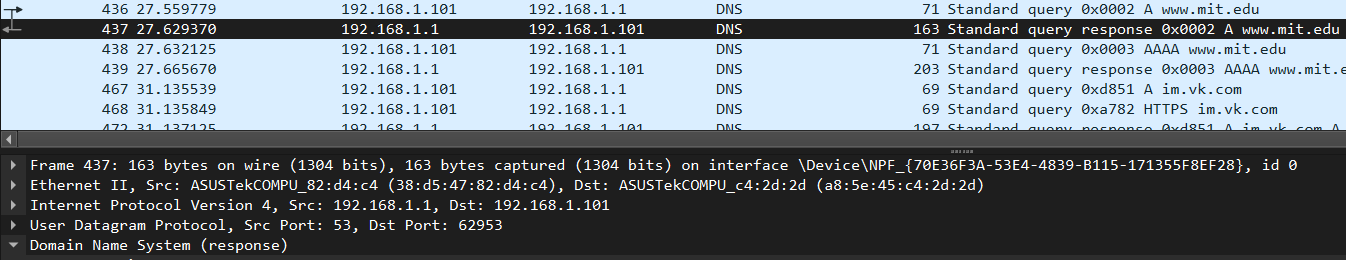
****

Рис. 9. DNS-ответ

1. На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию?

Запрос отправлен на адрес 23.34.65.247, который, как можно видеть на снимке, является адресом DNS-сервера, установленного по умолчанию.

1. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?

Это запрос записи типа A, и он не содержит никаких ответов.

1. Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?

В сообщении один ответ, в котором содержится информация об имени хоста, классе (типе сети), типе ресурсной записи, времени ее жизни, размере данных и IP-адресе.

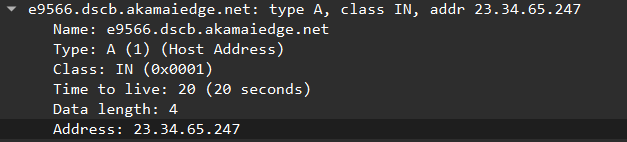


Рис. 10. Ответное сообщение DNS

1. Сделайте снимок

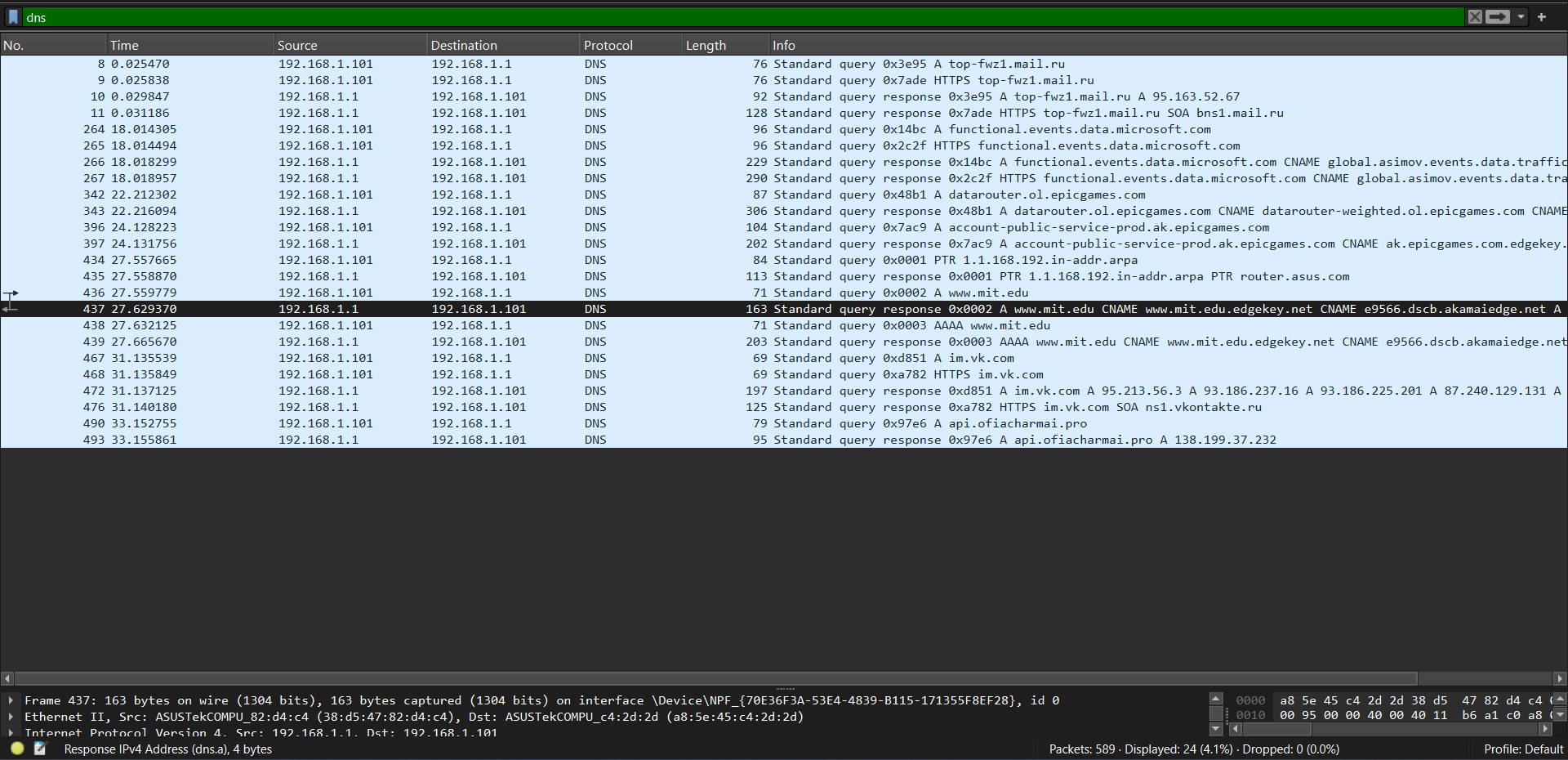


Рис. 11. Снимок DNS-ответа

1. На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию?

Да, запрос отправлен локальному DNS-серверу по умолчанию,

имеющему адрес 68.87.71.266.

1. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?

Это запрос записи типа NS, и он не содержит никаких ответов.

1. Проанализируйте ответное сообщение DNS. Имена каких DNS-серверов Массачусетского института в нем содержатся? Присутствуют ли их адреса в этом ответе?

Имена DNS-серверов –bitsy, strawb и w20ns. Их адреса можно увидеть, если раскрыть строчки с дополнительной информацией (additional records):

**Ответы:**

mit.edu: type NS, class inet, ns bitsy.mit.edu

mit.edu: type NS, class inet, ns strawb.mit.edu

mit.edu: type NS, class inet, ns w20ns.mit.edu

**Additional records:**

bitsy.mit.edu: type A, class inet, addr 18.72.0.3

strawb.mit.edu: type A, class inet, addr 18.71.0.151

w20ns.mit.edu: type A, class inet, addr 18.70.0.160

1. Сделайте снимок

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рис. 12. Снимок DNS-ответа

1. 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?

Запрос отправлен на адрес 18.72.0.3, который принадлежит серверу bitsy.mit.edu.

1. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?

Это стандартный запрос записи типа A, и он не содержит никаких ответов.

1. Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?
2. В сообщении один ответ, в котором содержится следующее:

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

1. Сделайте снимок.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рис. 13. Снимок DNS-ответа

**Wireshark: HTTP**

Для изучения протокола HTTP необходимо загрузить простой документ HTML, не содержащий никаких встроенных объектов.

Для этого откроем Wireshark, в поле фильтра введем: HTTP. После этого необходимо открыть следующую ссылку в браузере:

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

Браузер отобразит простой однострочный HTML-документ. Затем остановим захват пакетов.

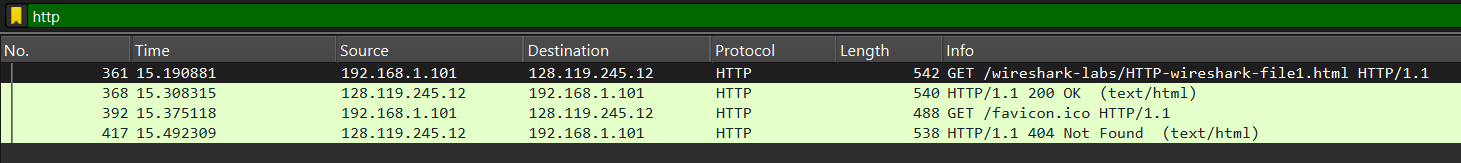


Рис. 1. Результат захвата пакетов HTTP

Видно, что в окне списка пакетов показаны перехваченные HTTP-сообщения: сообщение GET и сообщение от сервера к браузеру. В окне деталей показаны подробности выбранного сообщения.

1. Какую версию протокола HTTP использует ваш браузер –1.0 или 1.1? А какую – сервер?

Мой браузер использует версию протокола 1.1

1. Что указывает браузер серверу относительно поддерживаемых языков?

Accept-Language: ru,en;q=0.9\r\n

1. Какой IP-адрес у сервера gaia.cs.umass.edu? Каков адрес вашего компьютера?

Internet Protocol Version 4, Src: 192.168.1.101, Dst: 128.119.245.12

1. Какой код состояния возвратил сервер браузеру?

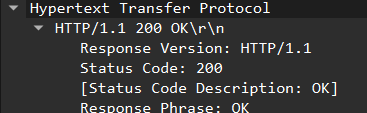


Рис. 2. Код состояния: 200

1. Какова дата последнего изменения на сервере HTML-файла, который вы вызываете?

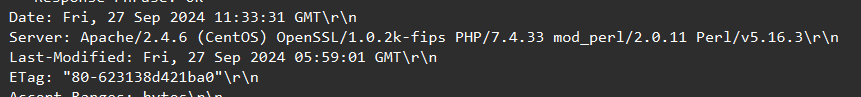


Рис. 3. Дата последнего изменения на сервере

1. Каков размер содержимого, которое возвратил сервер браузеру?



Рис. 4. Размер контента: 128

1. Проанализировав исходные данные в окне содержимого пакетов, видите ли вы какие-либо заголовки, не отображенные в окне списка пакетов? Если да, то какие?

Нет, больше никаких заголовков нет.

Далее необходимо очистить весь кэш в браузере, затем начать захват пакетов и ввести следующую ссылку в адресной строке:

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

Затем вводим тот же адрес еще раз и обновляем страницу. После останавливаем захват пакетов. Ниже представлен результат выполнения программы:

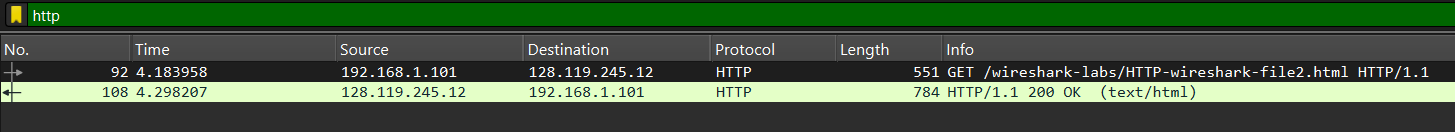


Рис. 5. Результат захвата пакетов HTTP

1. Изучите содержимое первого GET-запроса от вашего браузера серверу. Видите ли вы строку IF-MODIFIED-SINCE в запросе?

В первом GET-запросе нет IF-MODIFIED-SINCE

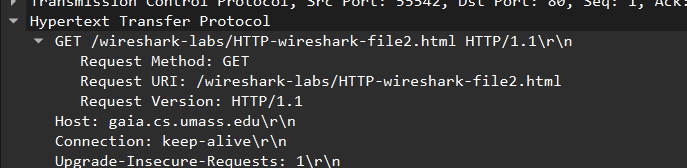


Рис. 6. IF-MODIFIED-SINCE нет

1. Проверьте ответ сервера. Возвращает ли он содержимое файла

Текст, возвращенный в ответ на первый GET-запрос:

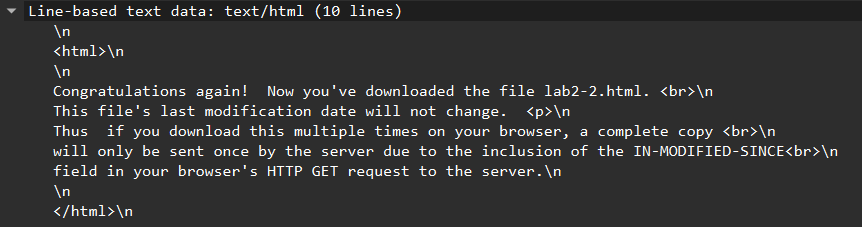


Рис. 7. Ответ на запрос

1. Теперь изучите содержимое второго GET-запроса серверу. Видите ли вы теперь строку IF-MODIFIED-SINCE в запросе? Если да, то какая информация идет после заголовка IF-MODIFIED-SINCE?

Во втором запросе есть IF-MODIFIED-SINCE. Он содержит в себе информацию о дате.



Рис. 8. Содержание строки IF-MODIFIED-SINCE

1. Что возвращает сервер в ответ на второй запрос (код состояния и фраза)? Возвращает ли он содержимое файла? Почему?

Файл не менялся. Поэтому текст файла не возвращается в HTTP-ответе.

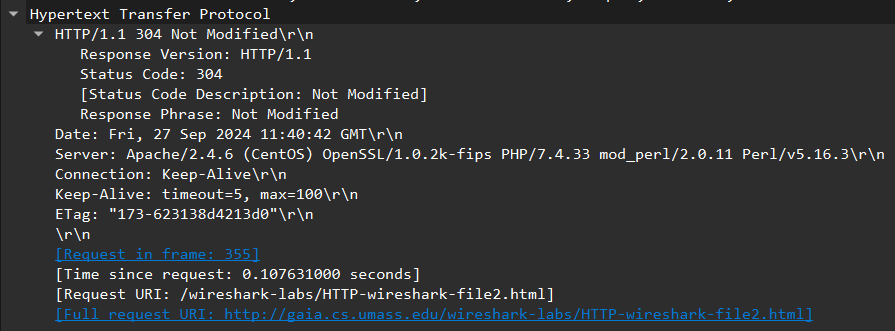


Рис. 9. Ответ на второй запрос

Теперь посмотрим, что происходит при загрузке большого HTML-документа. Для этого необходимо очистить весь кэш в браузере, затем начать захват пакетов и ввести следующую ссылку в адресной строке:

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>

После остановим захват пакетов и посмотрим на результат.

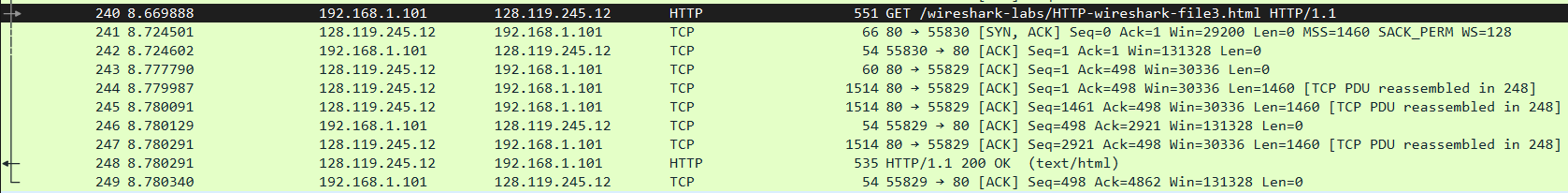


Рис. 10. Результат захвата пакетов HTTP

В окне списка пакетов виден GET-запрос, а затем несколько ответных TCP-пакетов. Их появление связано с тем, что ответное сообщение HTTP включает строку состояния, строки заголовка, пустую строку и тело объекта.

В данном случае телом объекта в ответе является весь запрашиваемый HTML-файл. Но размер нашего HTML-файла достаточно большой, и 4500 байт не помещаются в одном пакете TCP. Поэтому с помощью протокола TCP одно ответное сообщение разбивается на несколько частей, и каждая часть содержится в отдельном сегменте TCP. В последних версиях Wireshark каждый сегмент TCP показан в качестве отдельного пакета, а тот факт, что одно ответное HTTP-сообщение было фрагментировано на несколько пакетов TCP, обозначается в поле Info как TCP segment of a reassembled PDU.

1. Сколько GET-запросов отправил ваш браузер? В пакете с каким номером содержится запрос Билля о правах в файле результатов?

Браузер отправил 1 запрос

1. Какой пакет в результатах трассировки содержит код состояния и фразу, связанные с GET-запросом?

В пакете 24.

1. Какой код состояния и фраза в ответном сообщении?

200 (OK)

1. Сколько необходимо сегментов TCP для передачи одного HTTP-ответа и текста Билля о правах?

Три пакета (244, 245, 247 в файле трассировки)

Посмотрим, что происходит при загрузке браузером файла, содержащего встроенные объекты, которые хранятся на других веб-серверах. Для этого необходимо очистить весь кэш в браузере, затем начать захват пакетов и ввести следующую ссылку в адресной строке:

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>

После остановим захват пакетов и посмотрим на результат.

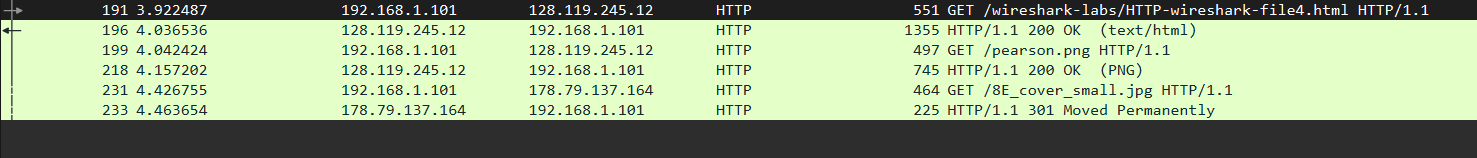


Рис. 11. Результат захвата пакетов HTTP

1. Сколько GET-запросов отправил ваш браузер? На какие IP-адреса в Интернете были отправлены эти запросы?

Было отправлено три GET-запроса: пакет 191 (получение основного файла), пакет 199 (получение логотипа Pearson) и пакет 231 (получение изображения обложки книги).

Два из трех запросов были отправлены на одинаковые IP-адреса. Пакет 191 и 199 отправлены на 128.119.245.12, а пакет 231 – на адрес 178.79.137.164.

1. Можете ли вы сказать, каким способом ваш браузер загрузил изображения с двух веб-сайтов – параллельно или один за другим? Объясните.

Два GET-запроса изображений – это пакеты 199 и 231. Ответные пакеты, содержащие запрошенные изображения – это пакеты с номерами 218 и 233. Таким, образом, мы видим, что запросы выполнены последовательно.

Посетим веб-сайт, который защищен паролем, и изучим последовательность HTTP-сообщений при обмене с сайтом. Обратимся к URL-адресу, защищенному паролем:

<http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-Wireshark-file5.html>

Для доступа используем имя пользователя wireshark-students и пароль network.



Рис. 12. Результат захвата пакетов HTTP

1. Каков первоначальный ответ сервера (код состояния и фраза) на первый GET-запрос вашего браузера?

В пакете 3359 содержится первый GET-запрос, а пакет 3369 – ответ на него с сервера. В ответе содержится: Status Code: 401 Response Phrase: Unauthorized

1. Какие новые поля добавляются в GET-сообщение при втором запросе браузера?

Новое поле в запросе – Authorization: Basic: