НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет Программной инженерии и компьютерной техники

Компьютерные сети

Лабораторная работа № 4

Выполнил студент

Шубаров Радик

Группа № P33212

Преподаватель: Маркина Т.А.

г. Санкт-Петербург

2022

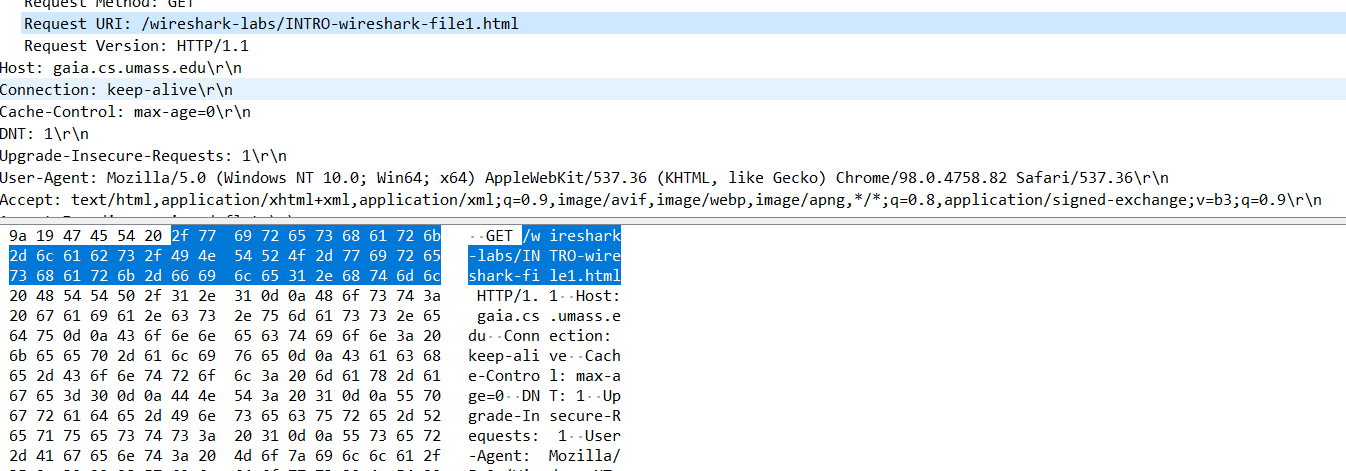
# Лабораторная работа 4. «Работа с сетевым анализатором»

**ЧАСТЬ 1.**

URL-адрес:

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

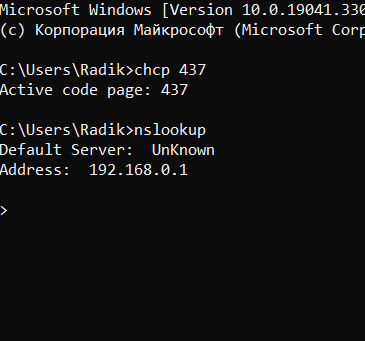
в окне спецификации фильтра отображения: http



К слову, перехватить можно только свой трафик, однако, когда устройства проходят непосредственно через наш девайс, либо если настроить свою сетевую карту на тот же канал, то можно перехватывать весь трафик, ведь Wireshark не поддерживает многоканальный режим. А если поверх http еще и TSL, то это уже отдельная песня с шифраторами и логами пре-мастера TSL.

**ЧАСТЬ 2.**

**1.Используйте nslookup для анализа сообщений DNS.**

****

Сервер не возвращает обратный поиск своего имени. Поэтому Server UnKnown. Требуется создать соответствующую зону обратного просмотра, чтобы позволить серверу выполнять обратное преобразование. Однако данный способ ничего не дал, как и ipconfig и автоматическое определение dns, поэтому я пробил ip на сайте <https://2ip.ru/> и на <https://whoer.net/ru/checkwhois>

**нашел dns нескольких серверов провайдера, полагаю провайдер не дает**

**публичный dns.**

𝑛𝑠𝑙𝑜𝑜𝑘𝑢𝑝 𝑤𝑤𝑤. 𝑖𝑡𝑚𝑜. 𝑟𝑢

ответ этой команды предоставляет две части информации

**Изображение выглядит как текст

Автоматически созданное описание**

Это означает, что сервер, к которому обращается утилита nslookup, не является авторитетным.

если мы знаем, что это доменное имя является безопасным. В этом примере мы предоставили параметр «-type = NS» и домены «itmo.ru» и «www.itmo.ru». Это заставляет nslookup отправлять запрос о записи типа NS на локальный DNS-сервер по умолчанию.

**Изображение выглядит как текст

Автоматически созданное описание**

**Изображение выглядит как текст

Автоматически созданное описание**

Ответ, показанный на приведенном выше снимке экрана, сначала указывает DNS-сервер, который предоставляет ответ (который является локальным DNS-сервером по умолчанию), а также три сервера имен ИТМО.

Однако nslookup также указывает, что ответ «неавторизованный», то есть этот ответ пришел из кэша какого-то сервера, а не от авторитетного DNS-сервера ИТМО.

**Изображение выглядит как текст

Автоматически созданное описание**

В этом примере мы указываем, что хотим отправить запрос на DNS-сервер провайдера.

Таким образом, транзакция запроса и ответа происходит непосредственно между нашим запрашивающим хостом и ns2.vuztc.ru.

1. Запустите nslookup, чтобы получить IP-адрес веб-сервера университета (любого) в России. Какой IP-адрес у этого сервера?

Изображение выглядит как текст

Автоматически созданное описание

2. Запустите nslookup, чтобы определить авторитетные DNS-серверы для университета в Европе.

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

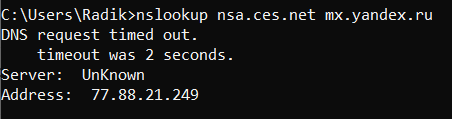
в результате отсутствует фраза «Non-authoritative answer», так как nsa.ces.net обладает всей информацией о зоне для cuni.cz

3. Запустите nslookup, чтобы один из DNS-серверов, полученных в вопросе 2, запросил почтовые серверы для почты Яндекса (или любого другого). Какой у него IP-адрес?

Изображение выглядит как текст

Автоматически созданное описание

Узнал почтовый сервер яндекса.



**Изображение выглядит как текст

Автоматически созданное описание**

**Действительно, адрес принадлежит компании Яндекс.**

**2. Используйте ipconfig для анализа сообщений DNS.**

**Изображение выглядит как текст

Автоматически созданное описание**

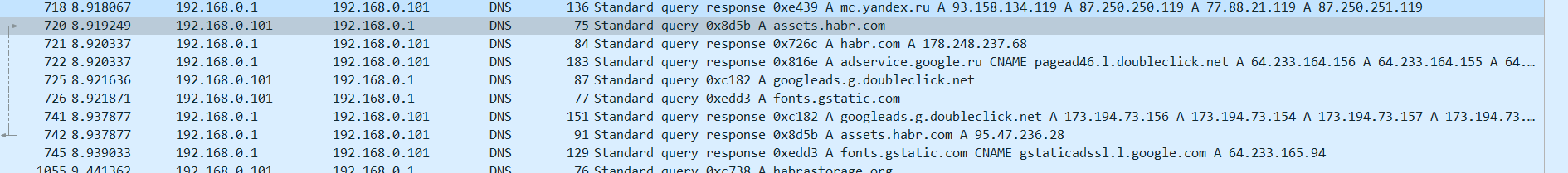
**Изображение выглядит как текст

Автоматически созданное описание** **Изображение выглядит как текст

Автоматически созданное описание**

**3. Используйте Wireshark для анализа сообщений DNS.**

**Я зашел на habr.com(статья про cicada3301).**

****

Вопросы (сделайте скриншот результатов):

1. Найдите сообщения DNS-запроса и ответа. Они отправляются по UDP или TCP?

Изображение выглядит как стол

Автоматически созданное описание

Ответ: UDP(асинхронная передача пакетов).

1. Каков порт назначения для сообщения DNS-запроса? Каков порт источника ответа DNS?
2. Изображение выглядит как стол

   Автоматически созданное описание

Ответ: порт источника 50698, порт назначения 53

1. На какой IP-адрес отправляется сообщение с запросом DNS? Используйте ipconfig, чтобы определить IP-адрес вашего локального DNS-сервера. Эти два IP-адреса одинаковы? Да, одинаковы.
2. Изучите сообщение DNS-запроса. Что это за «тип» DNS-запроса? Содержит ли запросное сообщение какие-либо «ответы»? Изображение выглядит как текст

   Автоматически созданное описание

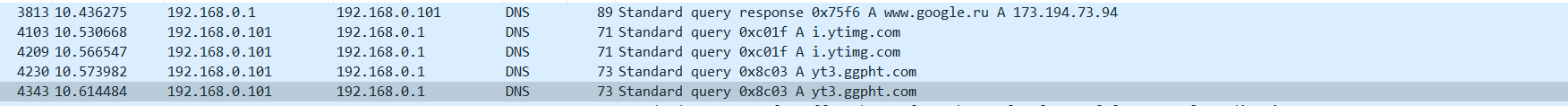
Тип А - Адресная запись, соответствие между именем и IP-адресом.

Ответы не дает.

1. Изучите ответное сообщение DNS. Сколько «ответов» дается? Что содержит каждый из этих ответов? Дается лишь один ответ. Доменное имя и IP хоста.

Изображение выглядит как текст

Автоматически созданное описание

7. Есть ли на этой веб-странице изображения? Перед получением каждого изображения ваш хост выдает новые DNS-запросы? 

Да, выдает новые запросы перед получением изображения.

Теперь - nslookup.

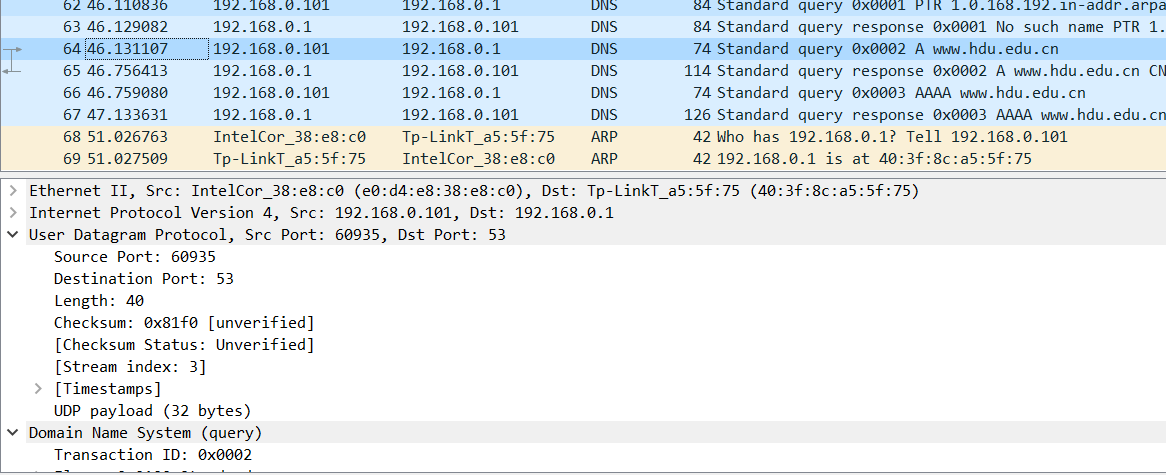
• Начать захват пакета.

• Сделайте 𝑛𝑠𝑙𝑜𝑜𝑘𝑢𝑝 𝑤𝑤𝑤. ℎ𝑑𝑢.𝑒𝑑𝑢. 𝑐𝑛

• Остановить захват пакетов.

Из приведенного выше снимка экрана видно, что nslookup действительно отправлял DNS-запросы и получал DNS-ответы.

1. Какой порт назначения для сообщения DNS-запроса? Каков порт источника ответного сообщения DNS?



Порт источника 60935.

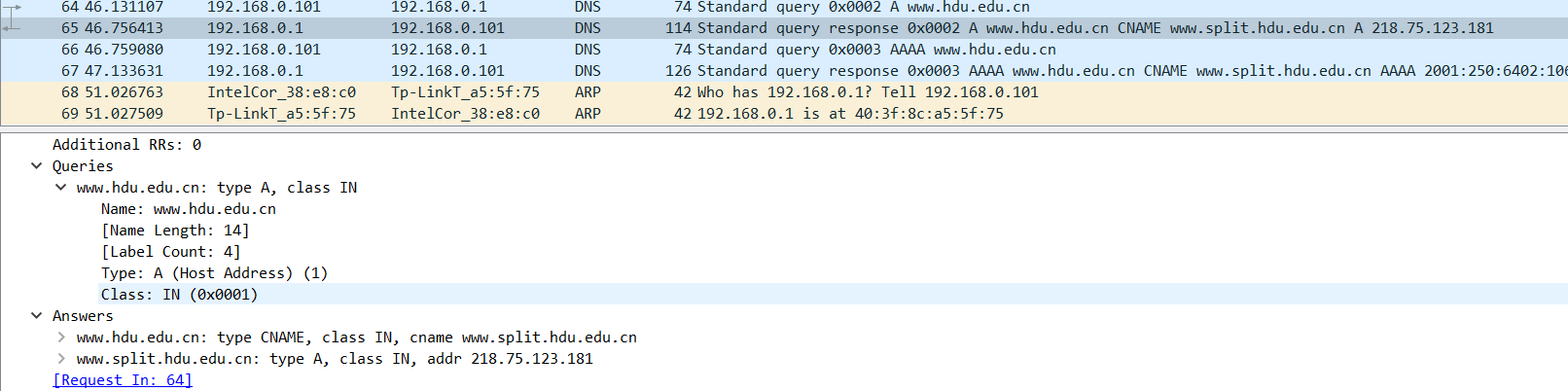
Порт назначения 53.

2. На какой IP-адрес отправляется сообщение с запросом DNS? Это IP-адрес вашего локального DNS-сервера по умолчанию? Да, проверено с помощью nslookup.

3. Изучите сообщение DNS-запроса. Что это за «тип» DNS-запроса? Содержит ли запросное сообщение какие-либо «ответы»? Тип А с кодом 1 - Адресная запись, соответствие между именем и IP-адресом.

Ответы не дает.

4. Изучите ответное сообщение DNS. Сколько «ответов» дается? Что содержит каждый из этих ответов?



Содержит два ответа. Домен и субдомен, то есть перейдя по первому, он перекидывает нас на фактический веб-сайт.

Теперь повторите предыдущий эксперимент, но вместо этого введите команду:

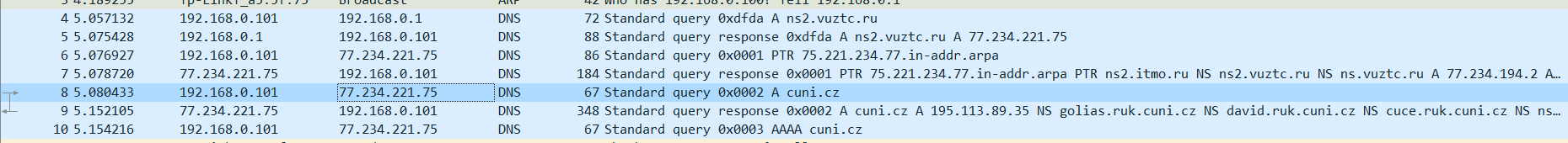
𝑛𝑠𝑙𝑜𝑜𝑘𝑢𝑝 𝑎𝑑𝑑𝑟𝑒𝑠𝑠\_𝑤ℎ𝑎𝑡\_𝑦𝑜𝑢\_𝑤𝑎𝑛𝑡 𝑦𝑜𝑢𝑟\_𝐷𝑁𝑆

Изображение выглядит как текст

Автоматически созданное описание

Ответьте на следующие вопросы:

1. На какой IP-адрес отправляется сообщение с запросом DNS? Это IP-адрес вашего локального DNS-сервера по умолчанию? Если нет, то чему соответствует IP-адрес?



IP Адрес соответствует домену ns2.vuztc.ru

2. Изучите сообщение с запросом DNS. Что это за «тип» DNS-запроса? Содержит ли запросное сообщение какие-либо «ответы»? Также тип А без ответов.

3. Изучите ответное сообщение DNS. Сколько «ответов» дается? Что содержит каждый из этих ответов? 1 ответ домена cuni.cz.