Федеральное государственное автономное образовательное учреждение высшего образования

**НИУ ИТМО**

**ФПИиКТ, Информатика и вычислительная техника**

По Дисциплине: Компьютерные сети

**Лабораторная работа №4**

**«Анализ трафика компьютерных сетей с помощью утилиты Wireshark»**

**Выполнила:**

Михайлова Анна Игоревна

**Группа:** P33302

**Проверил:**

Алиев Т. И.

Санкт-Петербург

2023

**Цель работы**

Изучить структуру протокольных блоков данных, анализируя реальный трафик на компьютере студента с помощью бесплатно распространяемой утилиты Wireshark.

Выбранный узел: mail.ru

**Этап 1. Анализ трафика утилиты ping**

Команда ping отправляет пакеты протокола ICMP в указанный узел сети и принимает пакеты-ответы. По приему ответов оценивается качество соединения.

Размеры отравляемого пакета: 100, 1000, 1500, 3000, 5000, 7000, 10000.

Команда для генерации трафика: ping -l 100 mail.ru

Из скриншотов видно, что при достижении максимального размера пакета происходит фрагментация. IP пакет разбивается на несколько меньших по размеру. Максимальный размер пакета выводится из расчетов, что на нижнем уровне размер ограничивается максимальным размером кадра Ethernet (1514 байт).

В одном из случаев, когда размер области данных 5000 байт, он разделяется 4 фрагмента, что видно из скриншота.

Конечный хост принимает все фрагменты, воссоздает ICMP запрос и далее формирует ответ. В качестве ответа он берет пакет запроса, меняет адреса отправителя и получателя и отправляет те же данные обратно. В случае ниже ответ не принят, так как таймаут по принятию был пройден.

Изображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

Структура 1 из 7 фрагментов при отправке 10000 байт

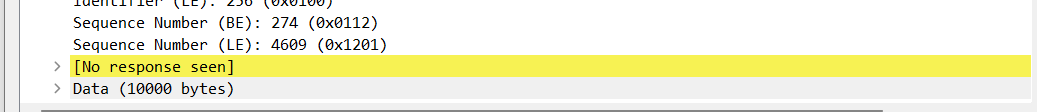
Изображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

Седьмой фрагмент

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание



Информацию о фрагментировании IP пакетов хранят флаги Don’t fragment и More fragment, а также поле Fragment Offset, содержащее номер первого байта в этом фрагменте.

Don’t fragment говорит о невозможности фрагментирования пакета по каким либо причинам.

More fragment говорит, ожидаются ли еще фрагменты еще помимо этого, то есть 0 – фрагмент не последний, 1 – последний.

При передаче ping пакетов, ICMP запросов и ответов, количество фрагментов разнилось от 1–7. Пакет фрагментируется, если его размер превышает максимально возможный размер пакета, который можно высчитать так:

Поле данных Ethernet кадра – 1500 байт, 20 байт на заголовок IPv4, 8 байт на заголовок ICMP (отсылается только в первом фрагменте) = 1473 байт – данных отправляется в первом фрагменте, далее по 1480 байт данных. Такое изменение можно изобразить в виде графика:

Изображение выглядит как текст, диаграмма, число, Шрифт

Автоматически созданное описание

Изменить TTL можно с помощью ключа -i и далее указания количества хопов, например:

Ping -i 30 -l 100 mail.ru

Тогда можно увидеть изменение в поле TTL IP пакета:

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

То, что передается в поле данных, зависит от типа ICMP пакета. Для request (8) и reply (0):

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

**Этап 2. Анализ трафика утилиты tracert (traceroute)**

Отследим и проанализируем трафик, создаваемый утилитой tracert.

Результат выполнения команды

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Для определения промежуточных маршрутизаторов traceroute отправляет целевому узлу серию ICMP-пакетов (по 3 пакета), с каждым шагом увеличивая значение поля TTL («время жизни») на 1.

Это делается для того, чтобы каждый маршрутизатор на пути отправлял ответный ICMP пакет – ICMP error (ошибка состоит в том, что TTL стал равен 0). Таким образом, traceroute составляет список адресов маршрутизаторов и помечает время, затраченное на путь.

Длина IP заголовка равна 20 байтов.

Структура первого из отправленных пакетов:

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

В пакете, отправленном маршрутизатором по истечении времени жизни, в поле данных передаются IP и ICMP заголовки отправленного запроса.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Размер поля данных ICMP-request и reply: 2 байт (id) + 2 байт (sequence number) + 64 байта нулей.

Размер поля данных ICMP-error: 4 байта (не используется) + 20 байт (IP заголовок запроса) + 4 байт (ICMP заголовок запроса) + 64 байта нулей

ICMP пакеты, генерируемые утилитой tracert, отличаются от ping в первую очередь значением поля TTL, оно инкрементируется, а не остается равным заданному значению. Поле данных несет в себе так же другие значения. Фрагментации пакетов не происходит, поле данных слишком мало для разбиения на подфрагменты.

Ключ -d не требует получения помимо IP адресов хостов еще и их имена. Это уменьшает время передачи пакетов, увеличивает скорость исполнения команды.

**Этап 3. Анализ HTTP-трафика**

При входе на сайт mail.ru в первый раз отправляется запрос HTTP GET с хостом получателя и путем к ресурсу, указанным в url. В ответ передается файл разметка страницы и другие ресурсы, необходимые для отображения страницы. Условных параметров в заголовке нет.

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

Автоматически созданное описание

Подключаясь к сайту повторно, можно заметить выборочные запросы на некоторые из ресурсов, а также условный GET запрос:

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

Здесь присутствует поле If-Modified-Since с соответствующей датой. На стороне сервера происходит ее валидация, от результата чего зависит, будет ли отправлен ресурс тому, кто его запросил.

В ответ на повторный запрос мы получаем результат от сервера со статусом 304 Not Modified, что говорит о том, что запрашиваемый ресурс не обновлялся.

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

Автоматически созданное описание

**Этап 4. Анализ DNS-трафика**

Изображение выглядит как текст, программное обеспечение, Шрифт, веб-страница

Автоматически созданное описание

Очистив локальный кэш, отправляем запрос на поиск IP адреса хоста с именем mail.ru. Посмотрим на структуру сформированного запроса:

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

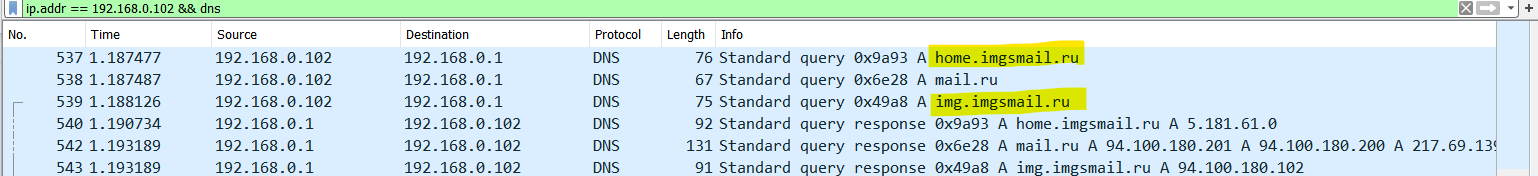
Адрес получателя в DNS запросе не равен адресу посещаемого сайта, так как мы обращаемся не к нему, а к DNS серверу, чтобы узнать IP адрес, соответствующий известному имени сайта. Этот адрес отправляется в поле данных DNS ответа.

Флаги в заголовке пакета DNS указывают на тип посылаемого запроса. Запросы могут быть:

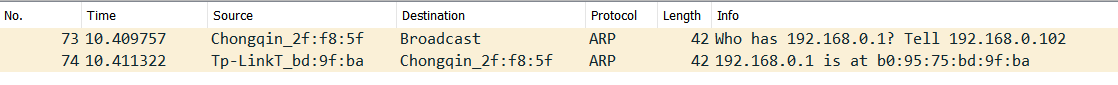
* Рекурсивными – запрос предполагает получение окончательного ответа от сервера, к которому он направлен. Рекурсию выполняет сервер.
* Итеративными – запрос предполагает выполнение рекурсии клиентом. Сервер при этом отправляет клиенту в ответ только адрес следующего DNS сервера.

За распознавание типа запроса отвечает флаг Recursion desired. Сервер может и не поддерживать рекурсивные запросы, что он и указывает в ответе.

В случае загрузки ресурсов, например картинок, лежащих на другом хосте, необходим дополнительный DNS запрос для разрешения имени этого хоста. Это можно проследить по трассе, хосты home.imgsmail.ru, img.imgsmail.ru как раз используются для подгрузки картинок для выбранного сайта:



**Этап 5. Анализ ARP-трафика**

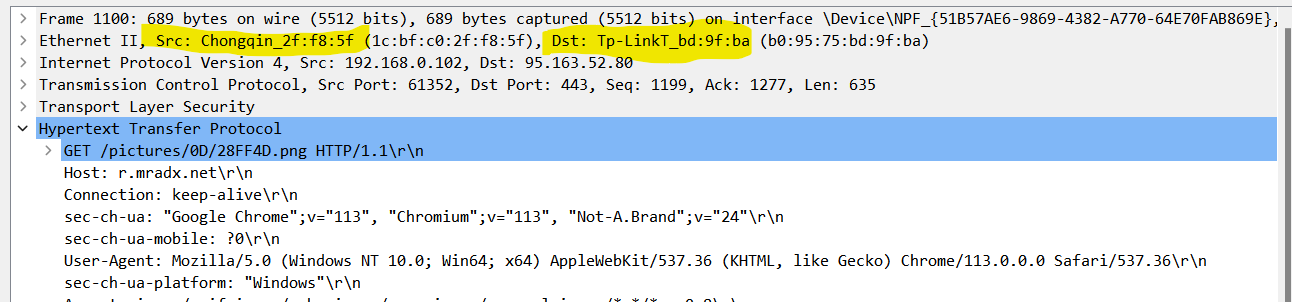


Было захвачено 2 ARP пакета, первый пересылается сразу же после удаления arp таблиц. Он является широковещательным, сообщает свой MAC и IP адреса и в то же время просит узнать MAC адрес одного устройства. Устройством с IP адресом 192.168.0.1 является маршрутизатор, который установлен как шлюз для используемого интерфейса. Далее от него приходит ответ с актуальной информацией об адресе и новая запись заносится в arp таблицу.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

В HTTP кадрах можно увидеть соответствующие интерфейсу компьютера и маршрутизатора MAC адреса, они совпадают с записями из ARP таблиц.



ARP запрос содержит IP адрес источника, чтобы сообщить устройствам в той же локальной сети актуальную информацию о себе, чтобы те (например, маршрутизатор) могли обновить ее и впоследствии верно направить пакеты к этому IP адресу.

**Этап 5. Анализ трафика утилиты nslookup**

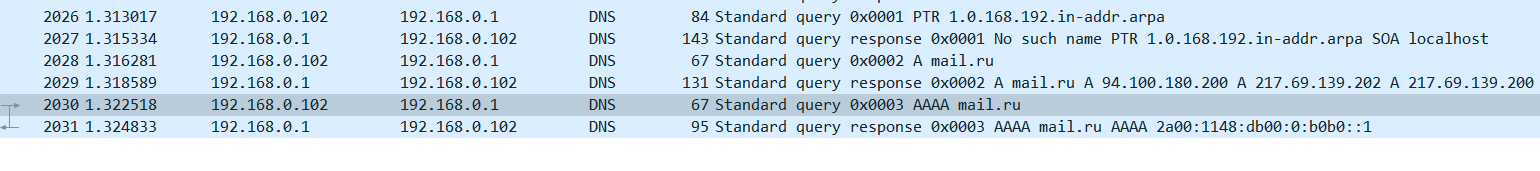
Результат выполнения команды nslookup для mail.ru.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Из скриншота видно, что мы получаем dns запись не у авторитетного сервера, а у ближайшего, хранящего кэш записей. В нашем случае это ближайший роутер. Также в результате представлен список IP адресов указанного домена, в том числе его IPv6 адрес.

Создаваемый трафик:



Структуры пакетов запроса и ответа:

Изображение выглядит как текст, снимок экрана, Шрифт, число

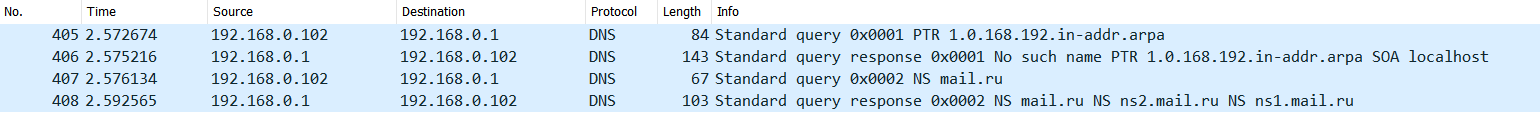
Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Ключ -type позволяет задавать тип записи, который мы хотим получить от DNS сервера.

Запустив команду повторно с ключом -type=NS мы получим названия серверов имен (name server), которые непосредственно хранят записи сайта указанным именем.



Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

В результате видно, что оба раза nslookup использовал рекурсивные запросы, однако в результате они возвращают разные данные. Первый раз от DNS сервера запрашиваются записи типа IPv6, во второй раз записи NS, соответствующие серверам, которые связаны с этим доменом. Этими авторитетными доменами стали:

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

В поле Answers содержатся все записи, которые были выбраны DNS серверами по полученному запросу. Структура каждой записи отличается и зависит от конкретного типа.

**Этап 5. Анализ FTP-трафика**

Трафик, созданный при подключении к FTP серверу и скачивании одного из файлов, изображен на скриншоте ниже:

Изображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

Сначала передаются пакеты от клиента и сервера для установления соединения, в том числе проверяются данные аутентификации. Далее устанавливаются параметры для настройки сессии с помощью запросов от клиента, сервер их обрабатывает и отправляет подтверждающие пакеты.

Файлы и данные директорий передаются по специальному протоколу FTP-DATA, по запросу LIST -a возвращаются данные корневой директории. А на запрос отправки файла arndl-test.txt возвращается содержимое этого файла, структура пакета представлена ниже:

Изображение выглядит как текст, Шрифт, снимок экрана, линия

Автоматически созданное описание

В этом пакете содержится 24 байта данных из 1460 возможных.

Для принятия/передачи FTP пакетов с данными команд на сервере используется порт 21. На клиенте он выбирается случайным образом из свободных, в текущем случае – это 58955. Пара портов – (58955,21) - используется при передаче команд между клиентом и сервером.

Чтобы передавать данные, клиент запрашивает сервер перейти в пассивный режим, тогда сервер отправляет в ответ на этот запрос свой IP адрес и временный порт, который будет использован для создания соединения для передачи данных. Клиент так же использует другой порт для этих целей, в данном случае используется пара портов (58962, 61886).

Пакеты FTP и FTP-DATA передаются по разным соединениям. FTP соединение постоянно, через него клиент отправляет управляющие сообщения серверу. По FTP-DATA соединение создается только после обработки сервером команды PASV (открыть пассивное соединение), которое просит сервер выделить еще один порт для передачи данных и исключительно для этого. После использования порты клиента и сервера для передачи данных сбрасываются.

Вывод: в ходе лабораторной работы мы научились отслеживать и анализировать трафик с помощью программы Wireshark. Были рассмотрены и разобраны пакеты таких протоколов, как DNS, ICMP, ARP, сгенерированные разными утилитами и программами.