|  | **Министерство науки и высшего образования Российской Федерации**  **Федеральное государственное бюджетное образовательное учреждение**  **высшего образования**  **«Московский государственный технический университет**  **имени Н.Э. Баумана**  **(национальный исследовательский университет)»**  **(МГТУ им. Н.Э. Баумана)** |
| --- | --- |

ФАКУЛЬТЕТ Информатика и системы управления

КАФЕДРА Системы обработки информации и управления\_\_\_\_\_\_\_\_\_\_\_

Отчет по лабораторной работе № 8  
**«Ознакомление с системой и протоколом DNS»**по дисциплине «Сети и телекоммуникации»

Студент ИУ5-51Б Т.А. Цыпышев

(Группа) (Подпись, дата) (И.О.Фамилия)

Преподаватель А.И. Антонов

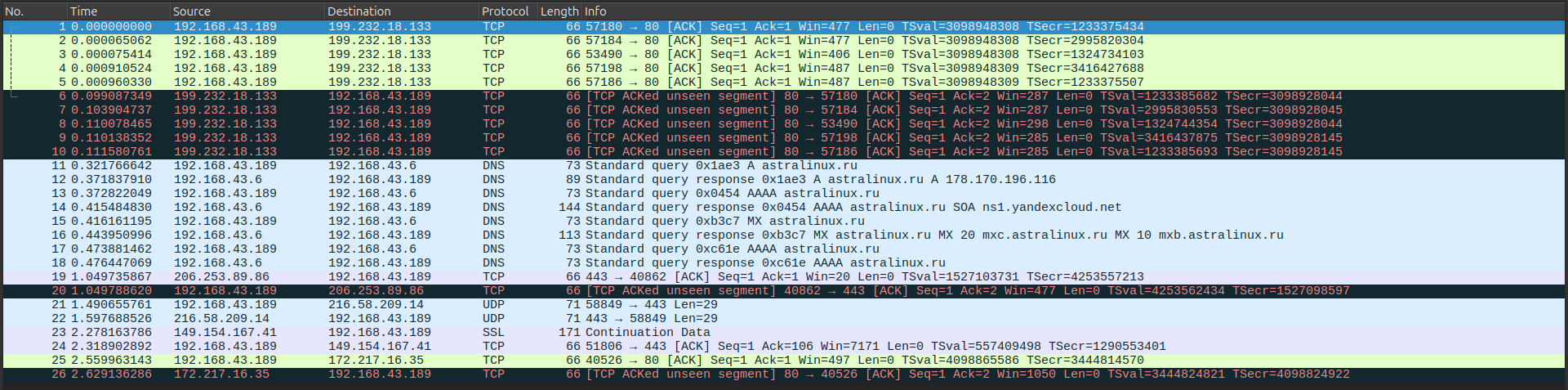
(Подпись, дата) (И.О.Фамилия)

**Москва**

**2024**

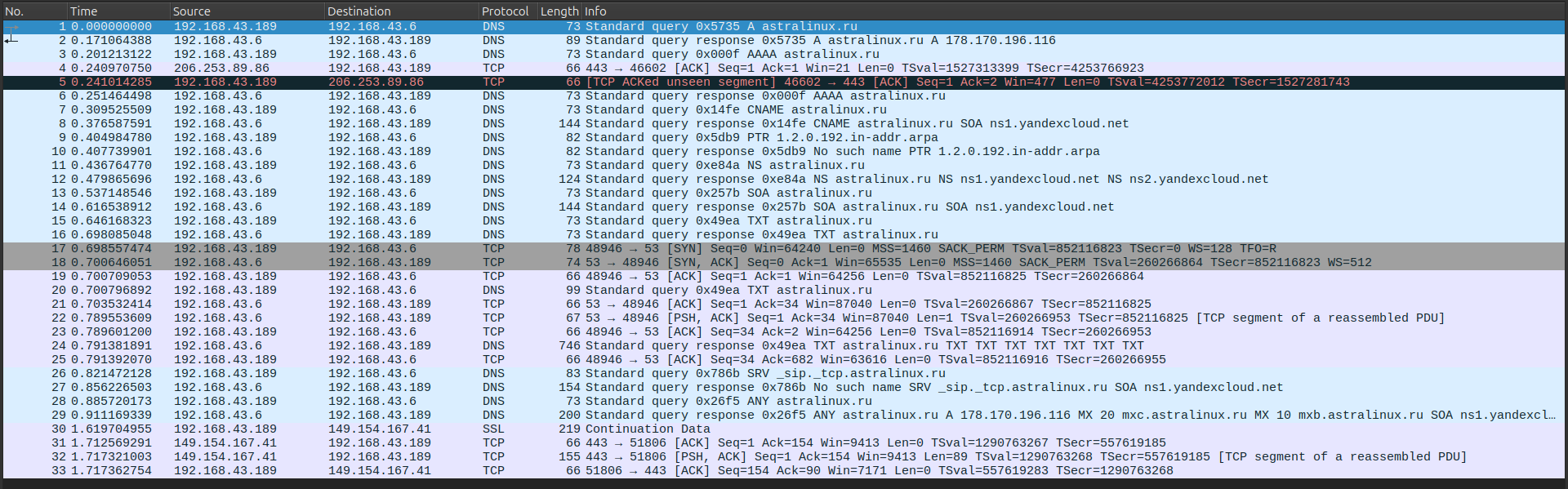
### 1. Разрешение адресов с использованием host, nslookup, dig

1. **Запуск Wireshark**:
   * Откройте Wireshark.
   * Установите фильтр: dns.
2. **Разрешение доменных имен**:  
   Откройте терминал Linux и выполните команды:  
   host astralinux.ru  
   nslookup astralinux.ru  
   dig astralinux.ru



### 2. Получение ресурсных записей разных типов с nslookup

1. **Запуск Wireshark**:  
   Установите фильтр: dns.
2. **Запрос ресурсных записей**:  
   В nslookup тип записи, который вы хотите запросить, определяется с помощью параметра -query или его сокращения -q. Этот параметр указывает DNS-запись, которую вы хотите получить из DNS-сервера. Тип записи -query=AAAA — это запрос на получение IPv6-адреса. Вот обзор основных типов записей, поддерживаемых nslookup:



**A (Address)**Возвращает IPv4-адрес узла.  
Пример:  
nslookup -query=A astralinux.ru

**AAAA (IPv6 Address)**Возвращает IPv6-адрес узла.  
Пример:  
nslookup -query=AAAA astralinux.ru

**MX (Mail Exchange)**Возвращает информацию о почтовых серверах для домена.  
Пример:  
nslookup -query=MX astralinux.ru

**CNAME (Canonical Name)**Возвращает каноническое имя для домена (указатель на другой домен).  
Пример:  
nslookup -query=CNAME astralinux.ru

**PTR (Pointer)**Используется для обратного поиска (по IP-адресу найти имя хоста).  
Пример:  
nslookup -query=PTR 192.0.2.1

**NS (Name Server)**Возвращает список DNS-серверов для домена.  
Пример:  
nslookup -query=NS astralinux.ru

**SOA (Start of Authority)**Возвращает запись, содержащую информацию об авторитетном DNS-сервере для домена.  
Пример:  
nslookup -query=SOA astralinux.ru

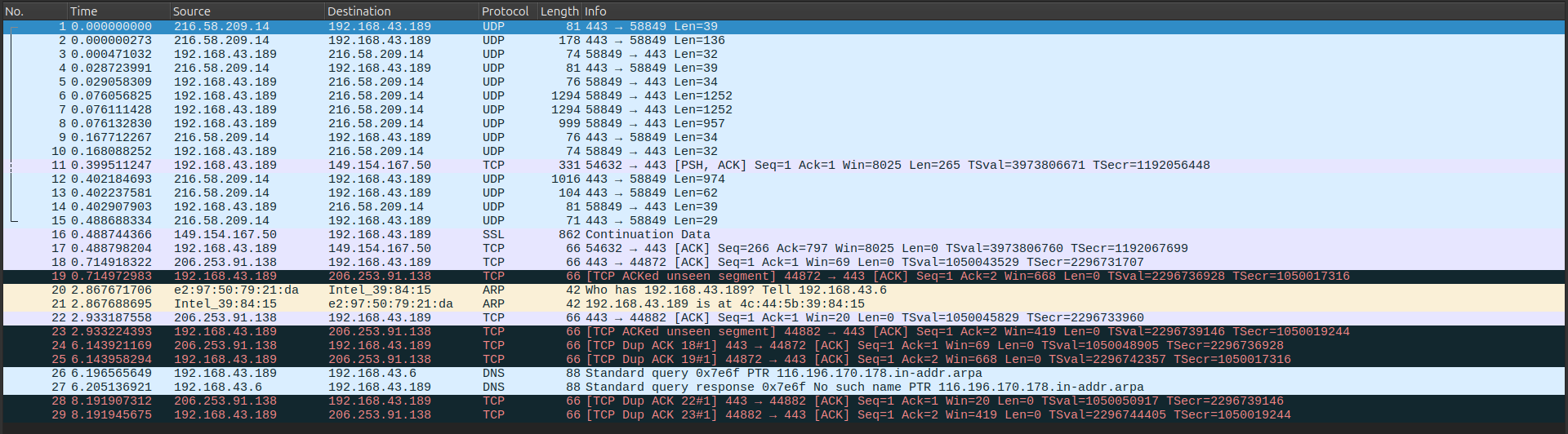
**TXT (Text Record)**Возвращает текстовые записи, часто используемые для SPF, DKIM или других настроек.  
Пример:  
nslookup -query=TXT astralinux.ru

**SRV (Service)**Запись службы, указывающая расположение серверов для определенных услуг (например, SIP или LDAP).  
Пример:  
nslookup -query=SRV \_sip.\_tcp.astralinux.ru

**ANY (Wildcard)**Возвращает все доступные записи для домена (зависит от конфигурации DNS-сервера, многие серверы отключают поддержку этого типа запроса).  
Пример:  
nslookup -query=ANY astralinux.ru

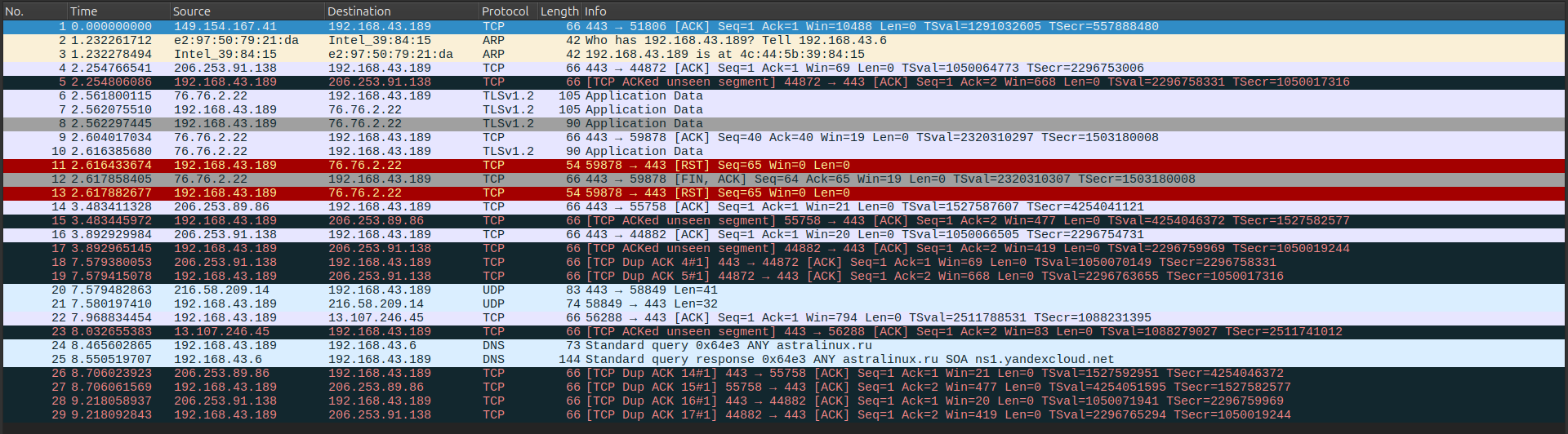
### 3. Обратный запрос DNS с host

1. **Запуск Wireshark**:  
   Установите фильтр: dns.
2. **Обратный запрос DNS**:  
   Для IPv4:  
   host <IPv4-адрес>  
   host 178.170.196.116  
     
   Для IPv6:  
   host <IPv6-адрес>



### 4. Получение всех ресурсных записей для домена с host

1. **Запуск Wireshark**:  
   Установите фильтр: IP-адреса ПК, сервера DNS, протоколы (TCP/UDP).
2. **Запрос ANY**:  
   Выполните команду:  
   host -a astralinux.ru



### Сравнение

| **Функция/Свойство** | **dig** | **host** | **nslookup** |
| --- | --- | --- | --- |
| **Сложность** | Высокая | Низкая | Низкая |
| **Мощность** | Очень высокая | Средняя | Низкая |
| **Поддержка** | Современный | Современный | Устаревший |
| **Вывод для человека** | Детальный | Удобный | Простой |
| **Интерактивность** | Нет | Нет | Да |

Если требуется простой результат для повседневного использования, выбирайте host. Для сложных DNS-диагностик лучше использовать dig. nslookup все еще полезен, но рекомендуется использовать его с осторожностью, учитывая его устаревший статус.

### 1. Что такое домен и доменное имя?

Домен — это часть иерархической системы именования, которая используется для идентификации и поиска ресурсов в интернете. Он состоит из нескольких уровней и помогает определять местоположение веб-сайта в сети.

Доменное имя — это текстовый идентификатор, который соответствует определенному IP-адресу ресурса (например, сайта). Вместо того чтобы запоминать числовой IP-адрес сервера (например, 192.168.0.1), мы используем более удобные для восприятия текстовые доменные имена, такие как [google.com](http://google.com/), [astralinux.ru](http://astralinux.ru/), и т. д.

Доменное имя состоит из нескольких частей (или "меток"), разделенных точками. Основные уровни домена:

* Топ-уровневый домен (TLD) — например, .com, .org, .ru, .gov и т. д.
* Вторичный уровень — например, в домене [example.com](http://example.com/) вторичным уровнем будет example.
* Поддомены — например, в домене [blog.example.com](http://blog.example.com/) поддоменом является blog.

### 2. DNS (Система доменных имен)

DNS (Domain Name System) — это система, которая переводит доменные имена в IP-адреса и обратно. DNS работает как телефонная книга Интернета, сопоставляя легко запоминаемые имена с числовыми IP-адресами, которые необходимы для маршрутизации запросов.

#### Основные компоненты DNS:

1. DNS-запись — информация о домене, которая хранится на сервере DNS и включает типы записей, такие как:
   * A-запись (Address) — указывает на IPv4-адрес.
   * AAAA-запись — указывает на IPv6-адрес.
   * MX-запись — указывает почтовые серверы для домена.
   * CNAME-запись — указывает, что доменное имя является псевдонимом другого домена.
   * NS-запись — указывает на DNS-серверы, которые обслуживают домен.
2. DNS-сервер — это сервер, который хранит записи DNS и обрабатывает запросы на разрешение доменных имен в IP-адреса.
3. Резолвер DNS — это клиентская программа или компонент операционной системы, который отправляет запросы на разрешение доменных имен.

#### Как работает DNS:

DNS использует иерархическую структуру серверов, которая делится на несколько уровней:

* Корневые DNS-серверы — хранят информацию о TLD.
* DNS-серверы верхнего уровня (TLD-серверы) — обслуживают запросы для определенных доменов верхнего уровня, например, для .com, .org.
* Авторитетные DNS-серверы — хранят конкретные записи для доменов второго уровня, таких как [example.com](http://example.com/).

### 3. Как работает DNS-запрос

Процесс разрешения доменного имени в IP-адрес можно описать следующим образом:

1. Запрос от пользователя:  
   Когда пользователь вводит доменное имя (например, [google.com](http://google.com/)) в браузере, браузер (или операционная система) обращается к DNS-резолверу, чтобы перевести это имя в IP-адрес.
2. Проверка кэша:  
   Резолвер сначала проверяет свой кэш. Если соответствующий IP-адрес был недавно запрашиваем, он может уже быть в кэше. Если он найден, процесс завершен.
3. Обращение к корневому серверу:  
   Если IP-адрес не найден в кэше, резолвер обращается к корневым DNS-серверам (root DNS servers). Они не хранят полные записи для всех доменов, но направляют резолвер к серверам для конкретных TLD, например, к серверам для доменов .com, .org, .ru и т. д.
4. Запрос к TLD-серверу:  
   Резолвер получает адрес TLD-сервера (например, для .com) и делает запрос к этому серверу, чтобы получить информацию о авторитетных серверах для домена (например, для [google.com](http://google.com/)).
5. Запрос к авторитетному серверу:  
   TLD-сервер перенаправляет запрос на авторитетный DNS-сервер для домена [google.com](http://google.com/). Этот сервер содержит точную запись, например, A-запись, которая указывает IP-адрес для домена.
6. Возвращение IP-адреса:  
   Авторитетный DNS-сервер возвращает IP-адрес, ассоциированный с доменом (например, 172.217.22.14 для [google.com](http://google.com/)).
7. Кэширование ответа:  
   Резолвер кэширует ответ на некоторое время, чтобы ускорить будущие запросы для этого домена.

cheese with holes, [28.12.2024 12:09]  
8. Отправка запроса на сервер:  
Теперь, зная IP-адрес, резолвер передает браузеру этот адрес. Браузер отправляет HTTP-запрос на указанный IP-адрес, чтобы загрузить веб-страницу.

### 4. Типы DNS-серверов

1. Корневые DNS-серверы — обслуживают запросы на домены верхнего уровня.
2. Серверы TLD — обслуживают домены второго уровня для определенного TLD.
3. Авторитетные DNS-серверы — содержат точную информацию о запрашиваемом домене.
4. Рекурсивные DNS-серверы — выполняют весь процесс разрешения доменных имен от начала и до конца. Обычно это серверы, предоставляемые интернет-провайдерами.