**LAB TCP и UPD в WIRESHARK**

Команда **nslookup** (Name Server Lookup) предназначена для отправки DNS-запросов и получения информации о доменных именах и их IP-адресах. Она позволяет взаимодействовать с DNS-серверами и получать информацию о доменных записях, таких как A-записи (IPv4-адреса), AAAA-записи (IPv6-адреса), MX-записи (почтовые серверы) и другие.

Когда вы вводите команду nslookup vk.com, происходит следующее:

1) Ваш компьютер обращается к DNS-серверу, который указан в его настройках сети (можно посмотреть с помощью scutil --dns на macOS или ipconfig /all на Windows).

2) DNS-сервер выполняет поиск IP-адреса, соответствующего vk.com, и отправляет ответ вашему компьютеру.

3) Выводится информация о DNS-сервере, который обработал запрос, и о найденных IP-адресах.

Server: 1.1.1.1

Address: 1.1.1.1#53

Non-authoritative answer:

Name: vk.com

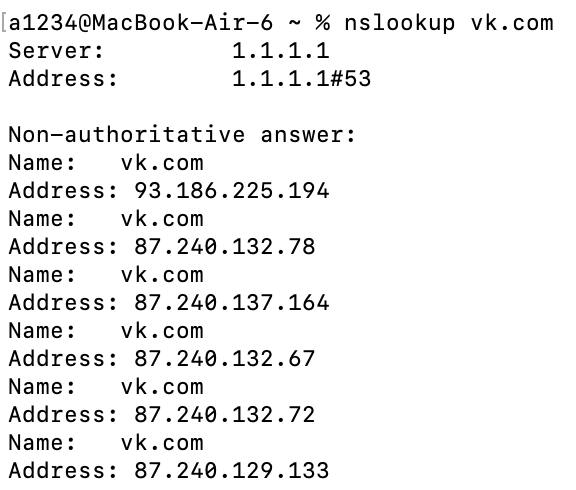
Address: 93.186.225.194

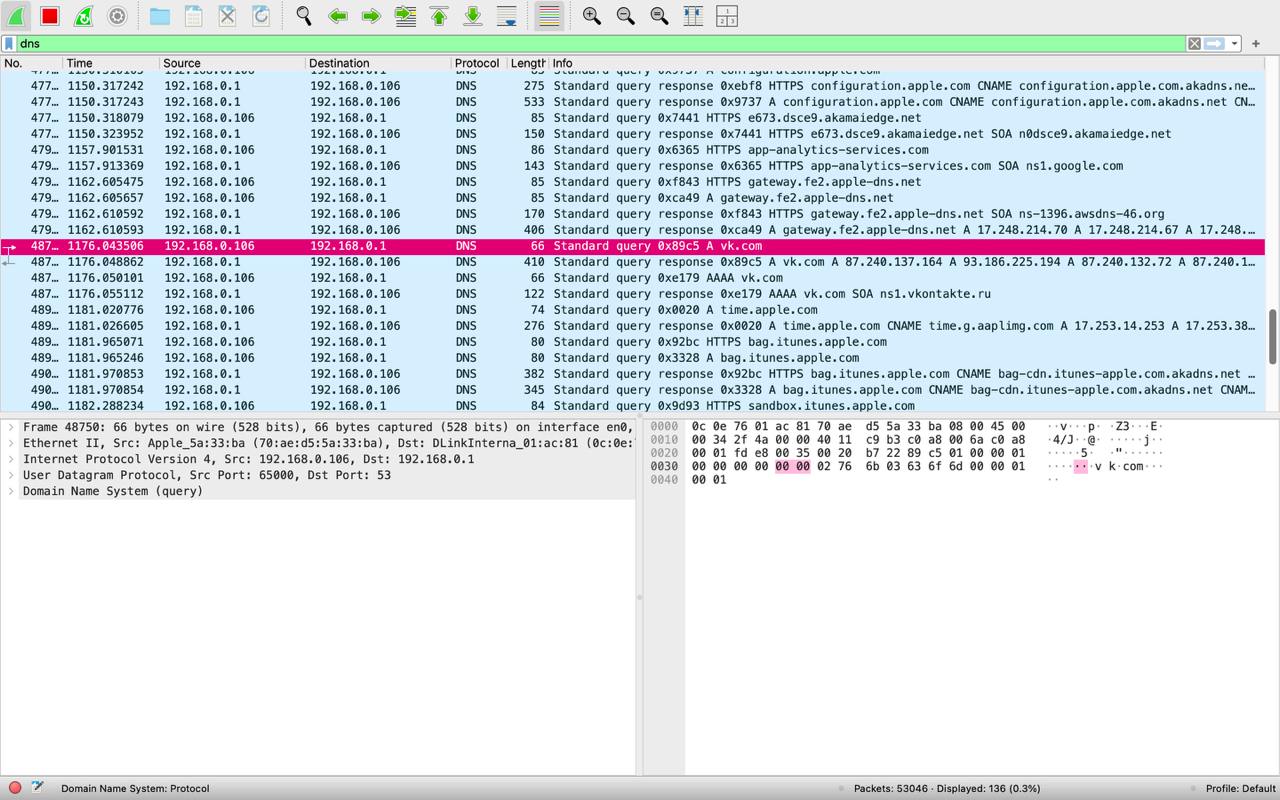
Name: vk.com

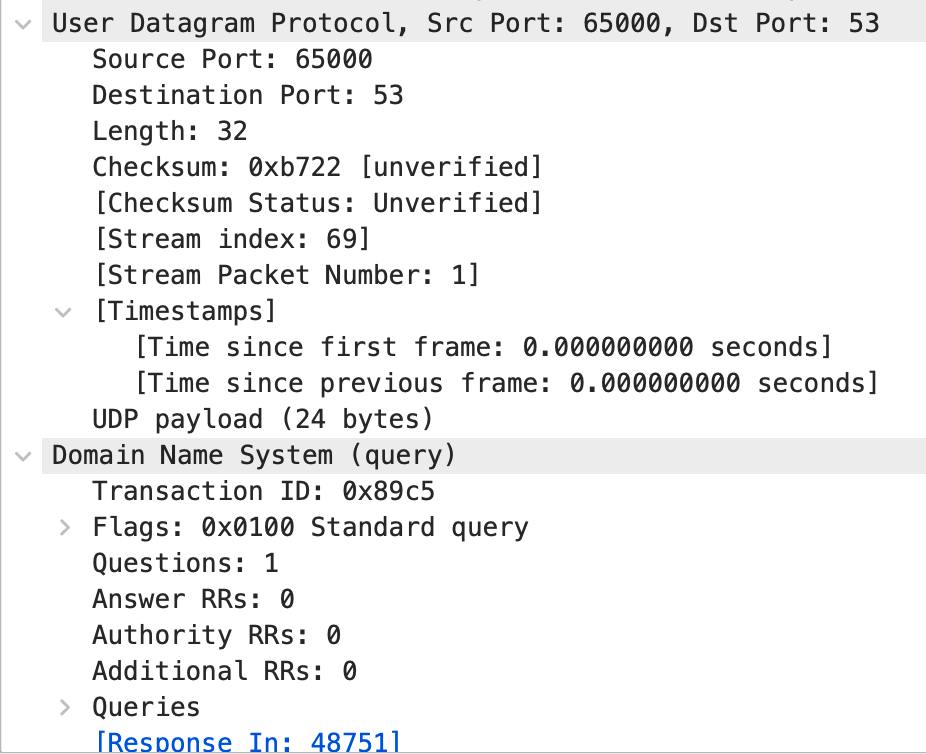
Address: 87.240.132.78

Server: 1.1.1.1 – DNS-сервер, который обработал запрос (в данном случае Cloudflare DNS).

Non-authoritative answer – означает, что полученный ответ пришел не от корневого DNS-сервера vk.com, а от кэшированного или рекурсивного DNS-сервера.

Address: 93.186.225.194 – один из IP-адресов, к которому привязан домен vk.com.  
  






1. Верхний уровень – Протокол UDP (User Datagram Protocol)

Этот запрос использует UDP для передачи данных, так как DNS-запросы по умолчанию отправляются по UDP (порт 53).

**Source Port** (Исходный порт): 65000

→ Это порт, с которого был отправлен запрос. Он назначается динамически операционной системой.

**Destination Por**t (Порт назначения): 53

→ Это стандартный порт DNS-сервера, куда отправляется запрос.

**Length** (Длина): 32

→ Полный размер UDP-пакета (включая заголовок UDP и полезную нагрузку).

**Checksum** (Контрольная сумма): 0xb722 [unverified]

→ Контрольная сумма используется для проверки целостности данных, но в данном случае она не проверена.

**UDP payload** (Полезная нагрузка): 24 bytes

→ Это фактический DNS-запрос.

2. Уровень DNS (Domain Name System)

**Transaction ID** (Идентификатор транзакции): 0x89c5

→ Уникальный идентификатор, который помогает клиенту сопоставить запрос и полученный ответ.

**Flags** (Флаги): 0x0100

→ Это стандартный DNS-запрос (Standard query), который ищет соответствие доменного имени и IP-адреса.

**Questions** (Количество вопросов): 1

→ Запрашивается одна DNS-запись.

**Answer RRs** (Записи ответа): 0

→ Пока ответов нет, так как это исходящий запрос.

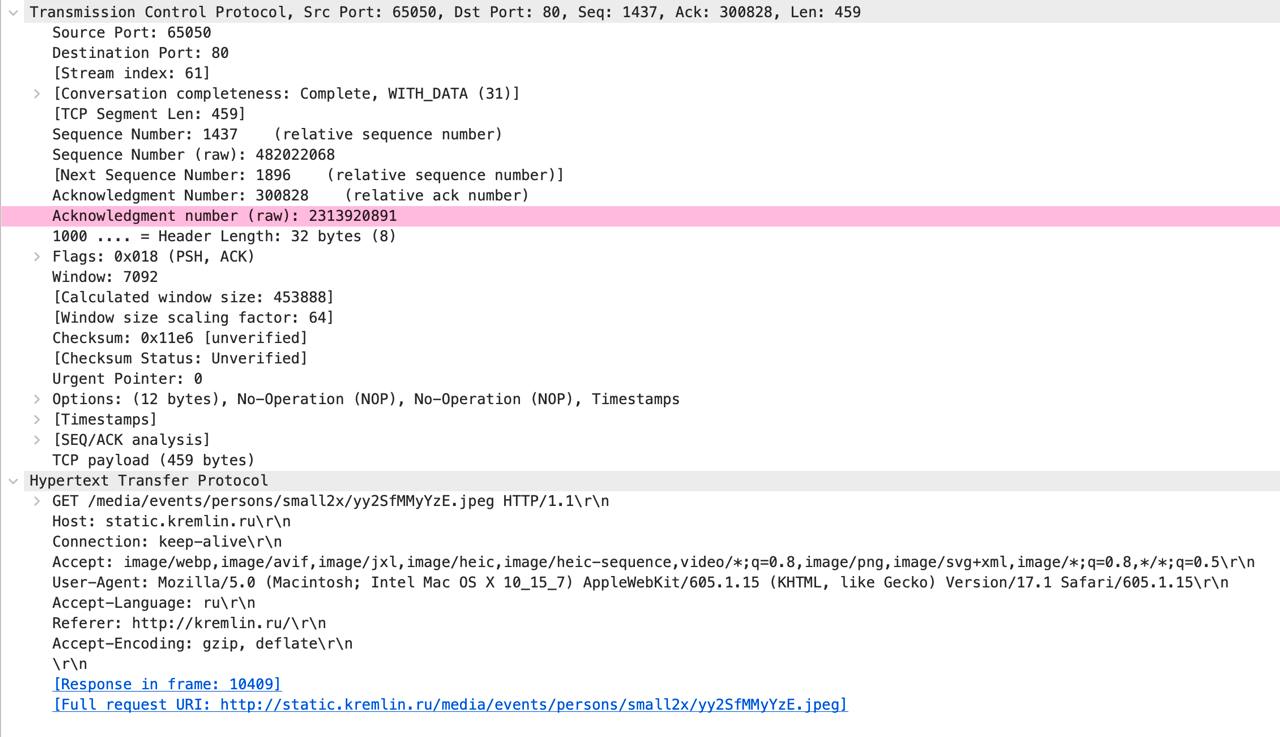
**Authority RRs** (Авторитетные записи): 0

→ Нет записей о том, какие сервера являются авторитетными для запрашиваемого домена.

**Additional RRs** (Дополнительные записи): 0

→ Нет дополнительных записей.

Внизу (Queries)

Содержится информация о том, какой именно домен запрашивается. В данном случае, это, скорее всего, A-запись (IPv4-адрес).  
  


Transmission Control Protocol (TCP): Это протокол транспортного уровня, обеспечивающий надежную передачу данных между устройствами.

Src Port: 65050: Исходный порт, с которого отправляются данные. В данном случае это порт 65050.

Dst Port: 80: Порт назначения, на который отправляются данные. Порт 80 обычно используется для HTTP-трафика.

[Stream index: 61]: Индекс потока, который идентифицирует конкретный поток данных в рамках сессии.

[Conversation completeness: Complete, WITH\_DATA (31)]: Указывает на завершенность разговора и наличие данных.

[TCP Segment Len: 459]: Длина сегмента TCP, которая составляет 459 байт.

Sequence Number: 1437 (relative sequence number): Относительный номер последовательности пакета.

Sequence Number (raw): 432022068: Абсолютный номер последовательности пакета.

[Next Sequence Number: 1896 (relative sequence number)]: Следующий ожидаемый номер последовательности.

Acknowledgement Number: 308028 (relative ack number): Относительный номер подтверждения.

Acknowledgment number (raw): 2313920891: Абсолютный номер подтверждения.

1000 ... = Header Length: 32 bytes (8): Длина заголовка TCP, которая составляет 32 байта (8 слов по 4 байта).

Flags: 0x018 (PSH, ACK): Флаги TCP. В данном случае установлены флаги PSH (Push) и ACK (Acknowledgment).

Window: 7092: Размер окна, который указывает на количество данных, которое может быть отправлено без получения подтверждения.

[Calculated window size: 453888]: Рассчитанный размер окна с учетом масштабирования.

[Window size scaling factor: 64]: Коэффициент масштабирования окна.

Checksum: 0x11e6 [unverified]: Контрольная сумма для проверки целостности данных.

[Checksum Status: Unverified]: Статус проверки контрольной суммы.

Urgent Pointer: 0: Указатель срочности, который используется для обозначения срочных данных.

Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps: Опции TCP. В данном случае используются NOP (No-Operation) и метки времени.

[Timestamps]: Метки времени, используемые для измерения времени передачи данных.

[SEQ/ACK analysis]: Анализ последовательности и подтверждения.

TCP payload (459 bytes): Полезная нагрузка TCP, которая составляет 459 байт.

Hypertext Transfer Protocol: Указывает на то, что полезная нагрузка содержит HTTP-запрос.

GET /media/events/persons/small2x/yy25fWWyYzE.jpeg HTTP/1.1\r\n: HTTP-запрос на получение изображения.

Host: static.kremlin.ru\r\n: Указывает на хост, к которому обращается запрос.

Connection: keep-alive\r\n: Указывает на то, что соединение должно оставаться открытым для последующих запросов.

Accept: image/webp,image/avif,image/jxl,image/helc,image/helc-sequence,video/;q=0.8,image/png,image/svg+xml,image/;q=0.8,/;q=0.5\r\n: Указывает на типы данных, которые клиент может принять.

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.1 Safari/605.1.15\r\n: Accept-Language: ru\r\n: Указывает на предпочитаемый язык клиента.

Referer: http://kremlin.ru/r\n: Указывает на URL, с которого был сделан запрос.

Accept-Encoding: gzip, deflate\r\n: Указывает на методы сжатия, которые клиент может принять.

\r\n: Завершает заголовки HTTP-запроса.

[Response in frame: 10409]: Указывает на кадр, в котором содержится ответ на этот запрос.

[Full request URI: http://static.kremlin.ru/media/events/persons/small2x/yy25fWWyYzE.jpeg]: Полный URI запроса.Информация о браузере и операционной системе клиента.  
  
**HTTP (HyperText Transfer Protocol)** **– это протокол прикладного уровня, который работает поверх TCP.**

TCP – это транспортный протокол: он отвечает за доставку данных.

HTTP – это протокол передачи веб-страниц: он отвечает за формат и структуру запросов/ответов, использует TCP для передачи данных между клиентом и сервером.

Как работает HTTP поверх TCP?

Клиент (браузер) открывает веб-сайт (например, https://example.com).

Устанавливается соединение TCP (через трёхстороннее рукопожатие).

Клиент отправляет HTTP-запрос на сервер (например, GET /index.html).

Сервер обрабатывает запрос и отправляет HTTP-ответ.

TCP передаёт данные по сети, гарантируя их доставку.

После загрузки страницы соединение может закрыться (если используется HTTP/1.1, то соединение может оставаться открытым для следующих запросов).