Лабораторная работа №3

Сетевые технологии

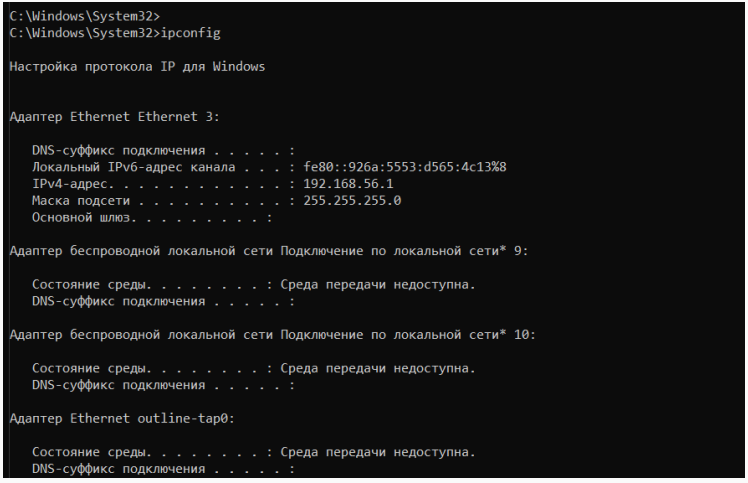
Иванов Сергей Владимирович, НПИбд-01-23

4 октября 2025

Российский университет дружбы народов, Москва, Россия

MAC-адресация

С помощью команды ipconfig для ОС типа Windows выведем информацию о текущем сетевом соединении. (рис. 1).



MAC-адресация

1. Адаптер Ethernet Ethernet 3. (VirtualBox)
2. Адаптер беспроводной локальной сети Подключение по локальной сети* 9. Звёздочка указывает на виртуальный или вспомогательный адаптер. Состояние среды: Среда передачи недоступна. Этот адаптер неактивен.
3. Адаптер беспроводной локальной сети Подключение по локальной сети* 10. Аналогичен предыдущему. Этот адаптер тоже неактивен.
4. Адаптер Ethernet outline-tap0. Название говорит, что это виртуальный адаптер, созданный VPN (Outline VPN). Состояние среды: Среда передачи недоступна. Адаптер отключён, так как VPN выключен.

MAC-адресация

Теперь используем опцию /all команды ipconfig. Команда предоставляет расширенную информацию о конфигурации сетевых адаптеров.

```
Адаптер беспроводной локальной сети Беспроводная сеть:

   DNS-суффикс подключения . . . . . :
   Описание. . . . . . . . . . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
   Физический адрес. . . . . . . . . : 90-E8-68-FA-55-E3
   DHCP включен. . . . . . . . . . . : Да
   Автонастройка включена. . . . . . : Да
   Локальный IPv6-адрес канала . . . : fe80::2fef:1cd:c5e8:217a%14(Основной)
   IPv4-адрес. . . . . . . . . . . . : 172.16.94.216(Основной)
   Маска подсети . . . . . . . . . . : 255.255.254.0
   Аренда получена. . . . . . . . . . : 29 сентября 2025 г. 10:49:21
   Срок аренды истекает. . . . . . . . . . : 29 сентября 2025 г. 15:49:10
   Основной шлюз. . . . . . . . . : 172.16.94.1
   DHCP-сервер. . . . . . . . . . . : 192.168.80.59
   IAID DHCPv6 . . . . . . . . . . . : 496035944
   DUID клиента DHCPv6 . . . . . . . : 00-01-00-01-2D-00-EA-E7-58-11-22-88-F5-69
   DNS-серверы. . . . . . . . . . . : 37.18.92.5
                                       193.232.218.194
   NetBios через TCP/IP. . . . . . . . : Включен

Адаптер Ethernet Сетевое подключение Bluetooth:

   Состояние среды. . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . :
   Описание. . . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Физический адрес. . . . . . . . . : 90-E8-68-FA-55-E2
   DHCP включен. . . . . . . . . . . : Да
   Автонастройка включена. . . . . . : Да
```

MAC-адресация

```
C:\Windows\System32>ipconfig /all

Настройка протокола IP для Windows

   Имя компьютера  . . . . . . . . . : Rtiop
   Основной DNS-суффикс  . . . . . . :
   Тип узла. . . . . . . . . . . . . : Гибридный
   IP-маршрутизация включена . . . . : Нет
   WINS-прокси включен . . . . . . . : Нет

Адаптер Ethernet Ethernet 3:

   DNS-суффикс подключения . . . . . :
   Описание. . . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Физический адрес. . . . . . . . . : 0A-00-27-00-00-08
   DHCP включен. . . . . . . . . . . : Нет
   Автонастройка включена. . . . . . : Да
   Локальный IPv6-адрес канала . . . : fe80::926a:5553:d565:4c13%8(Основной)
   IPv4-адрес. . . . . . . . . . . . : 192.168.56.1(Основной)
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Основной шлюз. . . . . . . . . :
   IAID DHCPv6 . . . . . . . . . . . : 722075687
   DUID клиента DHCPv6 . . . . . . . : 00-01-00-01-2D-00-EA-E7-58-11-22-88-F5-69
   NetBios через TCP/IP. . . . . . . : Включен

Адаптер беспроводной локальной сети Подключение по локальной сети* 9:

   Состояние среды. . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . :
   Описание. . . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Физический адрес. . . . . . . . . : 92-E8-68-FA-55-A3
   DHCP включен. . . . . . . . . . . : Да
   Автонастройка включена. . . . . . : Да
```


Рис. 3: Команда ipconfig /all

MAC-адресация

DNS-суффикс подключения: (пусто). Это может быть связано с динамической настройкой через DHCP.

Описание: MediaTek Wi-Fi 6 MT7921 Wireless LAN Card.

Физический адрес: 90-E8-68-FA-55-E3.

DHCP включён: Да. DHCP включён, IP-адрес и другие параметры сети автоматически выдаются сервером.

Локальный IPv6-адрес канала: fe80::2fef:1cdc:5e8:217a%14. используется для коммуникации внутри локального сегмента сети без маршрутизации.

IPv4-адрес: 172.16.4.1.

MAC-адресация

Маска подсети: 255.255.255.0. Маска подсети /24 определяет, что подсеть содержит до 254 хостов.

Аренда получена: 29 сентября 2025 г. 10:49:21. Срок аренды истекает: 29 сентября 2025 г. 15:49:10.

Основной шлюх: 172.16.4.59. Шлюз, через который трафик направляется за пределы локальной сети.

DHCP-сервер: 192.168.80.59. IP-адрес сервера DHCP, который выдал конфигурацию.

DNS-серверы: 37.18.92.5 193.232.218.194. Два DNS-сервера.

MAC-адресация

Определим MAC-адрес интерфеса Беспроводное соединение (Wi-Fi). Он находится в поле физический адрес. Имеет длину 6 байт. Первые 3 байта — идентификатор организации, который определяет производителя оборудования. Последние 3 байта — серийный номер, назначаемый производителем.

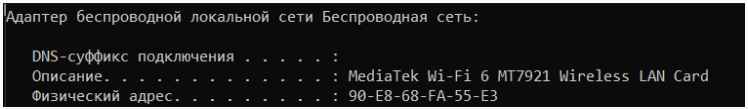


Рис. 4: MAC-адрес

MAC-адресация

90-E8-68 принадлежит компании AzureTechnolody (MediaTek Inc.). Это совпадает с описанием устройства в выводе команды. Проанализируем адрес. Для этого нужно посмотреть на значение первого первого байта адреса в двоичном формате.

Первый байт: 90 (в шестнадцатеричной системе) = 1001 0000 (в двоичной системе).

Нас интересуют два младших бита:

b0 (самый младший бит): Управляет типом адресации. 0 = Индивидуальный (Unicast). 1 = Групповой (Multicast).

b1 (второй бит): Управляет способом администрирования. 0 = Глобально управляемый. 1 = Локально управляемый.

Значит, наш адрес индивидуальный и глобально администрируемый

Анализ кадров канального уровня в Wireshark

Запустим Wireshark. Выберем активный на устройстве сетевой интерфейс и убедимся, что начался процесс захвата трафика. (рис. 5)

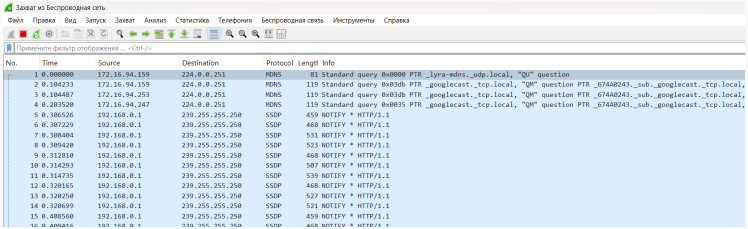


Рис. 5: Захват трафика

На устройстве в консоли определим с помощью команды ipconfig IP-адрес устройства и шлюз по умолчанию. IP: 172.16.94.216, Шлюз: 172.16.94.1 (рис. 6)

```
Адаптер беспроводной локальной сети Беспроводная сеть:

   DNS-суффикс подключения . . . . . :
   Локальный IPv6-адрес канала . . . : fe80::2fef:1cd:c5e8:217a%14
   IPv4-адрес. . . . . . . . . . . . : 172.16.94.216
   Маска подсети . . . . . . . . . . : 255.255.254.0
   Основной шлюз. . . . . . . . . : 172.16.94.1
```

Рис. 6: Определение IP и шлюза

Анализ кадров канального уровня в Wireshark

В консоли с помощью команды ping адрес_шлюза пропингуем шлюз по умолчанию. (рис. 7)

```
C:\Users\1serg>ping 172.16.94.1

Обмен пакетами с 172.16.94.1 по с 32 байтами данных:
Ответ от 172.16.94.1: число байт=32 время=3мс TTL=254
Ответ от 172.16.94.1: число байт=32 время=2мс TTL=254
Ответ от 172.16.94.1: число байт=32 время=4мс TTL=254
Ответ от 172.16.94.1: число байт=32 время=4мс TTL=254

Статистика Ping для 172.16.94.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 4 мсек, Среднее = 3 мсек

C:\Users\1serg>
```

Рис. 7: ping шлюза

Анализ кадров канального уровня в Wireshark

Остановим захват трафика. В строке фильтра пропишем фильтр arp or icmp. Убедимся, что в списке пакетов отобразятся только пакеты ARP или ICMP. (рис. 8)

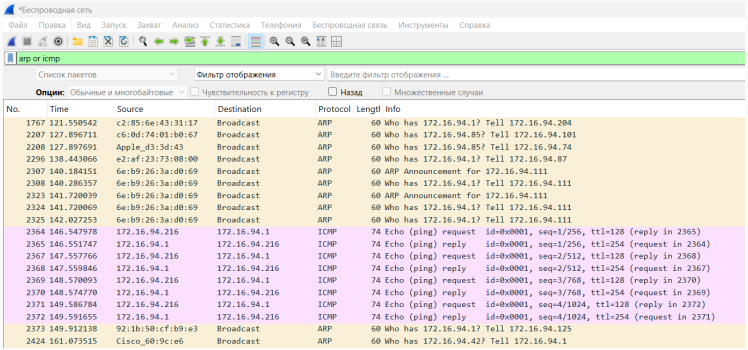


Рис. 8: фильтр arp or icmp

Анализ кадров канального уровня в Wireshark

Изучим эхо-запрос и эхо-ответ ICMP в программе Wireshark:

Эхо-запрос: длина кадра - 74 байта, относится к типу Ethernet (1), MAC-адрес источника - 90:e8:68:fa:55:e3 (тип индивидуальный, глобально администрируемый), MAC-адрес шлюза - 70:18:a7:60:9c:e6 (тип индивидуальный, глобально администрируемый). (рис. 9)

Анализ кадров канального уровня в Wireshark

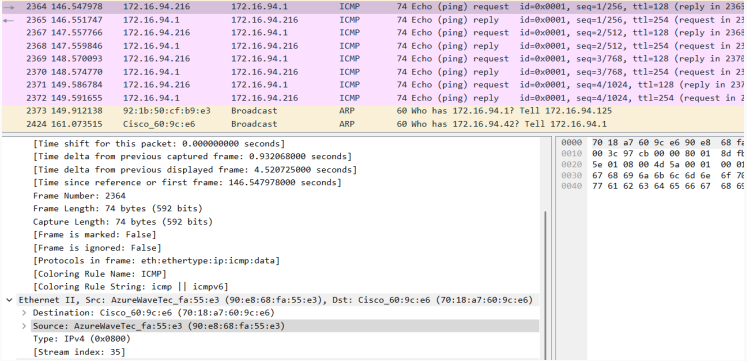


Рис. 9: Эхо запрос

Анализ кадров канального уровня в Wireshark

Эхо-ответ: длина кадра - 74 байта, относится к типу Ethernet (1), MAC-адрес источника - 70:18:a7:60:9c:e6 (тип индивидуальный, глобально администрируемый), MAC-адрес шлюза - 90:e8:68:fa:55:e3 (тип индивидуальный, глобально администрируемый) (рис. 10)

Анализ кадров канального уровня в Wireshark

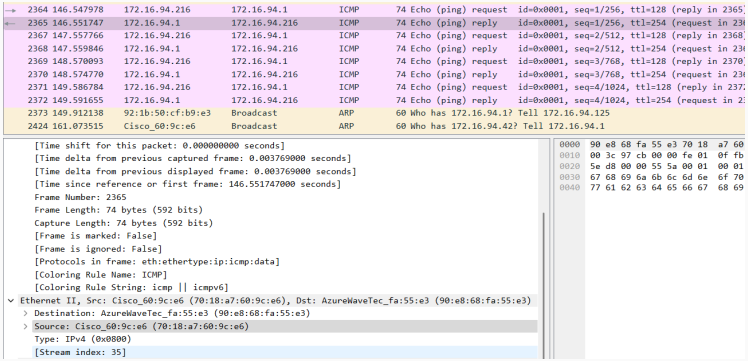


Рис. 10: Эхо ответ

Анализ кадров канального уровня в Wireshark

Изучим кадры данных протокола ARP. Изучим данные в полях заголовка Ethernet II.

MAC-адрес назначения (Destination): ff:ff:ff:ff:ff:ff

Тип адреса: Широковещательный (Broadcast). ARP-запрос отправляется всем узлам в сети, так как отправителю неизвестен MAC-адрес получателя.

MAC-адрес источника (Source): 70:18:a7:60:9c:e6

Тип адреса: Индивидуальный, глобально администрируемый.
Производитель (OUI): 70:18:a7 — Cisco Systems. (рис. 11)

Анализ кадров канального уровня в Wireshark

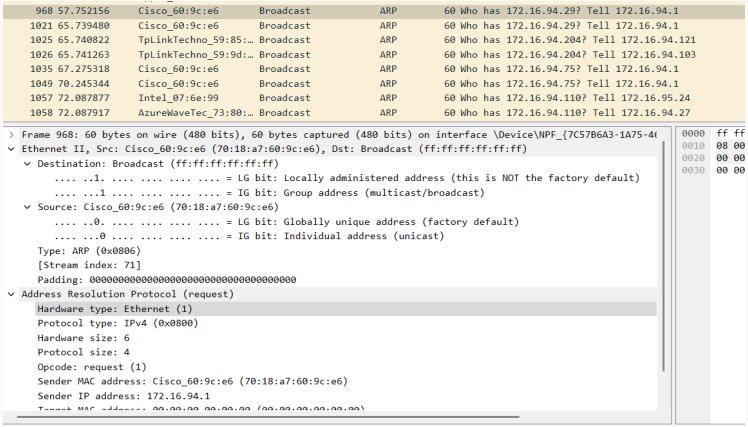


Рис. 11: Протокол ARP

Анализ кадров канального уровня в Wireshark

Начнем новый процесс захвата трафика в Wireshark. На устройстве в консоли пропингуем по имени какой-нибудь известный адрес, я возьму ya.ru (рис. 12)

```
C:\Windows\System32>ping ya.ru

Обмен пакетами с ya.ru [77.88.44.242] с 32 байтами данных:
Ответ от 77.88.44.242: число байт=32 время=32мс TTL=57
Ответ от 77.88.44.242: число байт=32 время=38мс TTL=57
Ответ от 77.88.44.242: число байт=32 время=7мс TTL=57
Ответ от 77.88.44.242: число байт=32 время=3мс TTL=57

Статистика Ping для 77.88.44.242:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 3мсек, Максимальное = 38 мсек, Среднее = 20 мсек

C:\Windows\System32>
```

Рис. 12: Пинг ya.ru

Анализ кадров канального уровня в Wireshark

Остановим захват трафика. Изучим запросы и ответы протоколов ARP и ICMP. Определим MAC-адреса источника и получателя, определим тип MAC-адресов.

Источник данных: IP-адрес: 172.16.94.39

MAC-адрес: 38:fc:98:ea:cf:68. Производитель (OUI): 38:fc:98 — Intel Corporate. Тип MAC-адреса: Индивидуальный, Глобально администрируемый.

Получатель данных (Destination): IP-адрес: 172.16.94.162.

MAC-адрес: ff:ff:ff:ff:ff:ff. Тип MAC-адреса: Широковещательный (Broadcast). Это адрес для отправки кадра всем устройствам в сети.

Устройство с IP 172.16.94.39 (Intel) не знает MAC-адрес устройства с IP 172.16.94.162 и широковещательно запрашивает его у всех в сети. (рис. 13)

Анализ кадров канального уровня в Wireshark

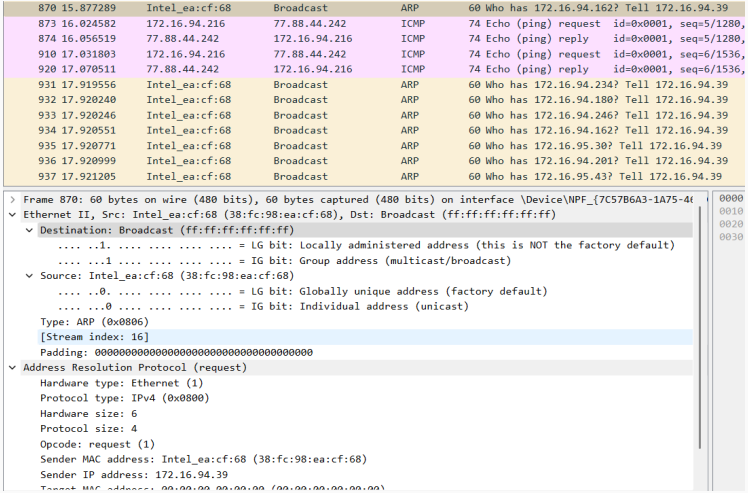


Рис. 13: анализ ARP протокола

Анализ кадров канального уровня в Wireshark

Анализ ICMP-протокола

ICMP (эхо-запрос) это пакет, который отправляется с компьютера на удаленный сервер.

Содержание: 172.16.94.216 -> 77.88.44.242

Источник данных в кадре Ethernet II:

MAC-адрес: 90:e8:68:fa:55:e3 (Это беспроводной адаптер моего компьютера).

Тип MAC-адреса: Индивидуальный, Глобально администрируемый.

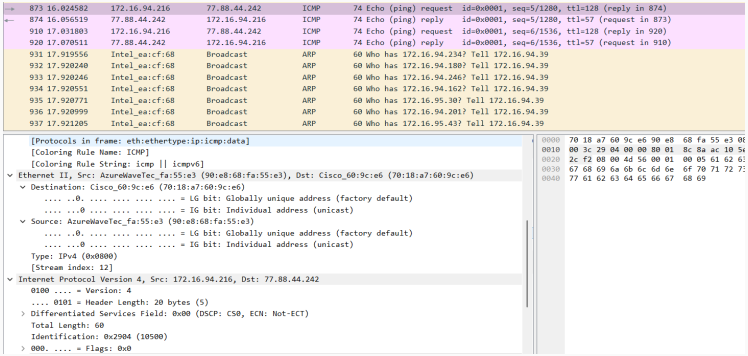
Получатель данных (Destination) в кадре Ethernet II:

MAC-адрес: 70:18:a7:60:9c:e6

Тип MAC-адреса: Индивидуальный, Глобально администрируемый.

Анализ кадров канального уровня в Wireshark

Мой компьютер хочет отправить пакет на внешний IP 77.88.44.242. По правилам маршрутизации, он отправляет пакет на свой основной шлюз. Он уже знает MAC-адрес шлюза, поэтому кадр Ethernet адресован напрямую на MAC-адрес маршрутизатора. (рис. 14)



Анализ кадров канального уровня в Wireshark

Это ответ, который возвращается с удаленного сервера на ваш компьютер.

Содержание: 77.88.44.242 -> 172.16.94.216

Источник данных в кадре Ethernet II:

MAC-адрес: 70:18:a7:60:9c:e6 (Cisco)

Тип MAC-адреса: Индивидуальный, Глобально администрируемый.

Получатель данных (Destination) в кадре Ethernet II:

MAC-адрес: 90:e8:68:fa:55:e3 (мой комп)

Тип MAC-адреса: Индивидуальный, Глобально администрируемый.

Анализ кадров канального уровня в Wireshark

Маршрутизатор получил ответ от сервера и теперь должен доставить его моему компьютеру в локальной сети. Он знает MAC-адрес ПК и отправляет кадр Ethernet напрямую на мой MAC-адрес. (рис. 15)

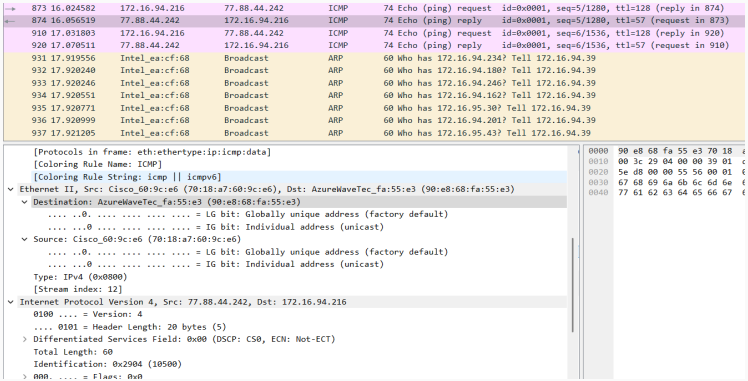


Рис. 15: ICMP эхо-ответ

Анализ протоколов транспортного уровня в Wireshark

Запустим Wireshark. Выберем активный на устройстве сетевой интерфейс. Убедимся, что начался процесс захвата трафика. (рис. 16)

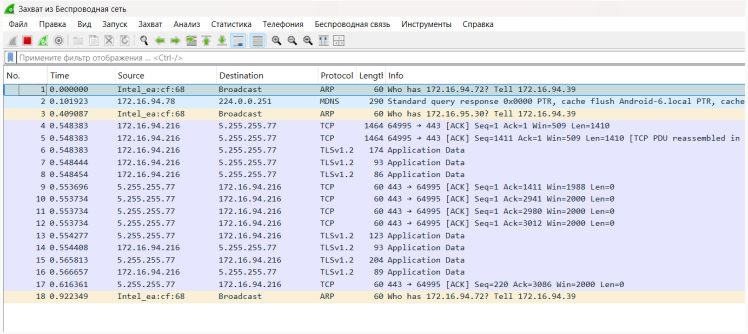


Рис. 16: Захват трафика

В браузере перейдем на сайт, работающий по протоколу HTTP (например, на сайт CERN http://info.cern.ch/). (рис. 17)

Рис. 17: Переход на сайт cern.ch

Анализ протоколов транспортного уровня в Wireshark

В Wireshark в строке фильтра укажем http. Это пакет, в котором компьютер отправляет HTTP-запрос на сервер. Анализируем TCP (запрос)

Порты: Source Port: 65232 — это исходный порт, который случайным образом выбирается компьютером. Destination Port: 80 — это порт назначения

Sequence Number (последовательный номер): Relative (относительный): 1, Raw (абсолютный): 4193937875. Это номер первого байта данных в этом сегменте. Wireshark для удобства показывает относительный номер, начиная с 1.

Acknowledgment Number (номер подтверждения): Relative (относительный): 1, Raw (абсолютный): 2237714506. Это номер следующего байта, который отправитель этого пакета ожидает получить от противоположной стороны. Подтверждает успешное получение всех данных до этого номера.

Flags: PSH, ACK. ACK (Acknowledgment): Установлен, чтобы подтвердить получение предыдущих пакетов от сервера. PSH (Push): Указывает получателю (серверу) немедленно передать данные приложению (веб-серверу), не дожидаясь заполнения буфера.

TCP Segment Len (длина сегмента): 254. (рис. 18)

Анализ протоколов транспортного уровня в Wireshark

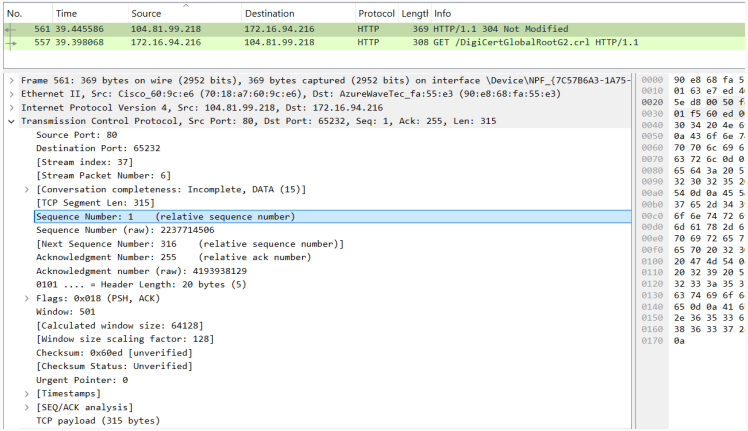


Рис. 18: Анализ TCP (запрос)

Порты: Source Port (порт источника): 80. Destination Port (порт назначения): 65232.

Sequence Number (последовательный номер): Relative (относительный): 1, Raw (абсолютный): 2237714506. Это номер первого байта данных, которые сервер отправляет в этом сегменте.

Acknowledgment Number (номер подтверждения): Relative (относительный): 255, Raw (абсолютный): 4193938129

Flags: PSH, ACK. ACK (Acknowledgment): Подтверждает получение HTTP-запроса от клиента. PSH (Push): Указывает компьютеру немедленно передать данные (HTTP-ответ) приложению (браузеру).

TCP Segment Len (длина сегмента): 315. Размер полезных данных (HTTP-ответа), переносимых в этом TCP-сегменте. (рис. 19)

Анализ протоколов транспортного уровня в Wireshark

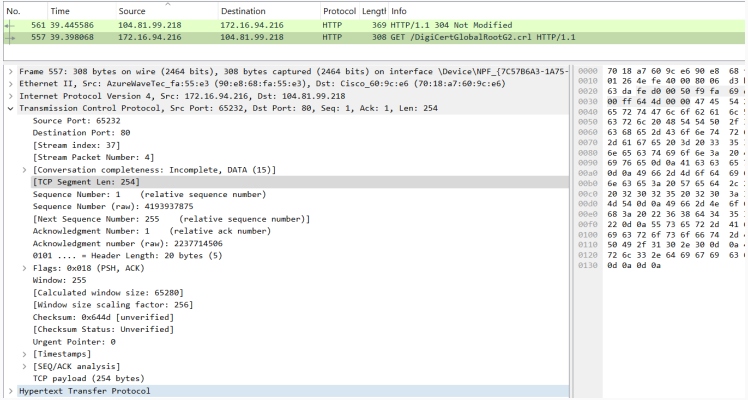


Рис. 19: Анализ TCP (ответ)

UDP в DNS-запросе. Это пакет, в котором компьютер отправляет вопрос DNS-серверу.

Source Port (порт источника): 62966. Destination Port (порт назначения): 53. Это стандартный порт для службы DNS.

Length (длина): 55 байт. Общая длина UDP-датаграммы (заголовок + данные). (рис. 20)

Анализ протоколов транспортного уровня в Wireshark

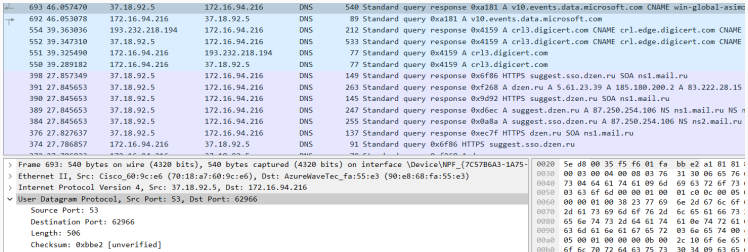


Рис. 20: Анализ UDP (запрос)

UDP в DNS-ответе. Это пакет, в котором DNS-сервер возвращает ответ компьютеру.

Source Port (порт источника): 53. Destination Port (порт назначения): 62966.

Length (длина): 506 байт. Общая длина этой UDP-датаграммы. (рис. 21)

Анализ протоколов транспортного уровня в Wireshark

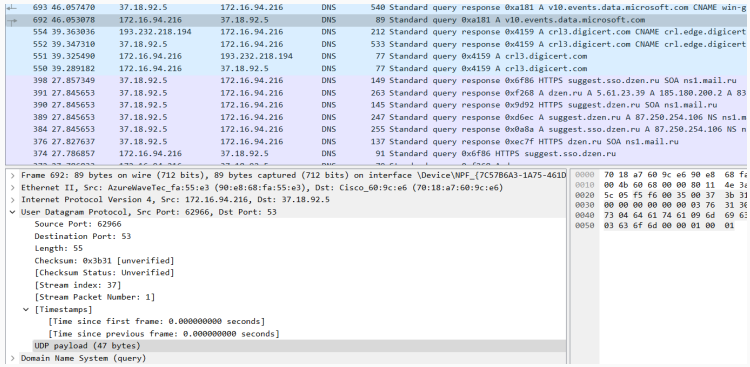


Рис. 21: Анализ UDP (ответ)

Анализ протоколов транспортного уровня в Wireshark

Wireshark в строке фильтра укажем quic и проанализируем информацию по протоколу quic в случае запросов и ответов.

QUIC работает поверх UDP, поэтому в заголовках мы сначала видим Ethernet, затем IP, затем UDP, и только потом — QUIC.

QUIC-пакет от Клиента. Это пакет, который компьютер отправляет на сервер.

Транспорт (UDP): Source Port (порт источника): 62198, Destination Port (порт назначения): 443 (порт QUIC/HTTPS сервера)

QUIC Заголовок:

Destination Connection ID (DCID): f8a9378badb7bea3. Идентификатор соединения назначения. Это уникальный идентификатор, который клиент использует для указания, с каким именно серверным соединением связан этот пакет. Сервер изначально предоставляет этот ID клиенту.

Полезная нагрузка: Remaining Payload: d6e43ad86a11... Основные данные протокола. Как видно из названия пакета в общем списке — “Protected Payload” — эта часть зашифрована. Это одно из ключевых преимуществ QUIC — шифрование, и даже заголовки полей, относящиеся к управлению соединением, шифруются. (рис. 22)

Анализ протоколов транспортного уровня в Wireshark

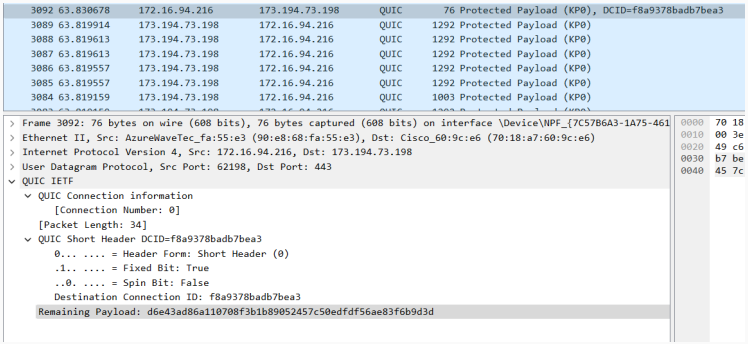


Рис. 22: Анализ QUIC (запрос)

Анализ протоколов транспортного уровня в Wireshark

Транспорт (UDP): Source Port (порт источника): 443, Destination Port (порт назначения): 62198 (сервер отправляет ответ на исходный порт ПК)

QUIC Заголовок:

В ответах сервер будет использовать тот Connection ID, который был предоставлен клиенту (или новый, согласованный в процессе установления соединения).

Полезная нагрузка: Remaining Payload: 3fcea12c11cd… Аналогично клиентскому пакету, полезная нагрузка сервера также является “Protected Payload” (Защищенной) и зашифрована. (рис. 23)

Анализ протоколов транспортного уровня в Wireshark

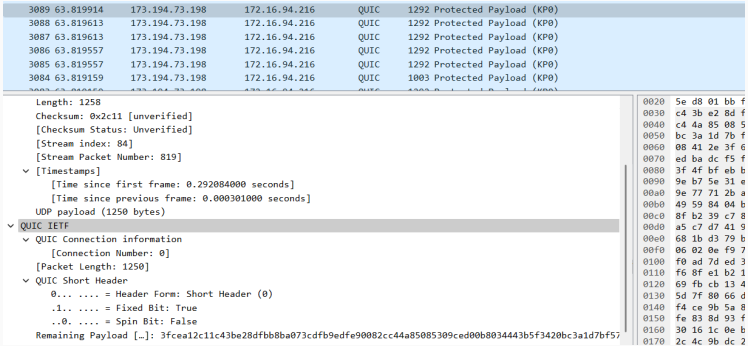


Рис. 23: Анализ QUIC (ответ)

Анализ handshake протокола TCP в Wireshark

Запустим Wireshark. Выберем активный на устройстве сетевой интерфейс. Убедимся, что начался процесс захвата трафика. (рис. 24)

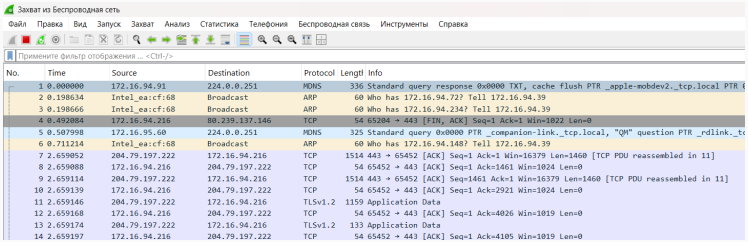


Рис. 24: Захват трафика

Анализ handshake протокола TCP в Wireshark

Использую соединение по HTTP с каким-то сайтом для захвата в Wireshark пакетов TCP. В Wireshark проанализируем handshake протокола TCP.

Шаг 1: SYN (Синхронизация). Клиент инициирует соединение, отправляя серверу специальный пакет.

Ключевые поля TCP:

Sequence Number: 0. Клиент генерирует начальный номер последовательности (ISN).

Flags: SYN (0x002). Установлен только флаг SYN. Это запрос на синхронизацию и начало соединения.

Параметры (Options): MSS=1460 — максимальный размер сегмента, который клиент может принять, WS=256 — фактор масштабирования окна для увеличения его эффективного размера, SACK_PERM — поддержка выборочных подтверждений (Selective Acknowledgements).

Клиент говорит серверу: я хочу установить соединение. Мой начальный номер последовательности — 0, и вот мои параметры. (рис. 25)

Анализ handshake протокола TCP в Wireshark

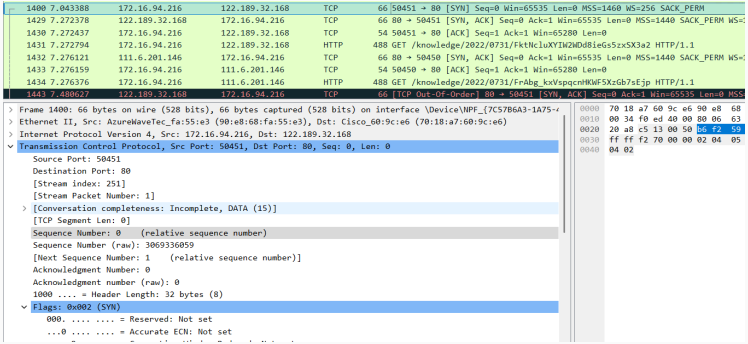


Рис. 25: TCP handshake шаг 1

Шаг 2: SYN-ACK (Синхронизация-Подтверждение). Сервер отвечает, подтверждая запрос клиента и отправляя свой собственный запрос на синхронизацию.

Sequence Number: 0. Сервер генерирует свой собственный начальный номер последовательности (ISN).

Acknowledgment Number: 1. Это поле подтверждения. Сервер подтверждает получение SYN-пакета клиента.

Flags: SYN, ACK (0x012). Установлены флаги SYN (запрос синхронизации от сервера) и ACK (подтверждение пакета клиента).

Сервер отвечает клиенту: Я получил запрос на соединение (ACK=1). Я согласен установить соединение, и мой начальный номер последовательности — 0 (SYN). Вот мои параметры. (рис. 26)

Анализ handshake протокола TCP в Wireshark

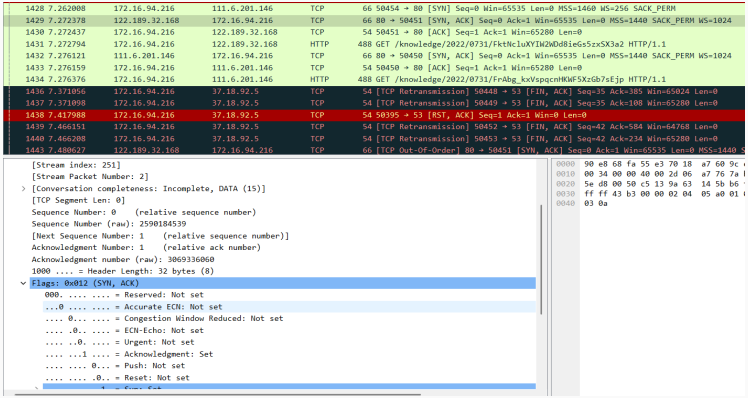


Рис. 26: TCP handshake шаг 2

Шаг 3: ACK (Подтверждение). Клиент завершает рукопожатие, подтверждая SYN-пакет сервера.

Ключевые поля TCP:

Sequence Number (относительный): 1. Номер последовательности клиента теперь 1, так как его SYN-пакет “потребил” номер 0.

Acknowledgment Number (относительный): 1. Это поле подтверждения. Клиент подтверждает получение SYN-пакета сервера. Номер подтверждения равен ISN сервера + 1. Ack=1.

Flags: ACK (0x010). Установлен только флаг ACK.

Клиент говорит серверу: Я получил SYN-пакет. Соединение установлено. (рис. 27)

Анализ handshake протокола TCP в Wireshark

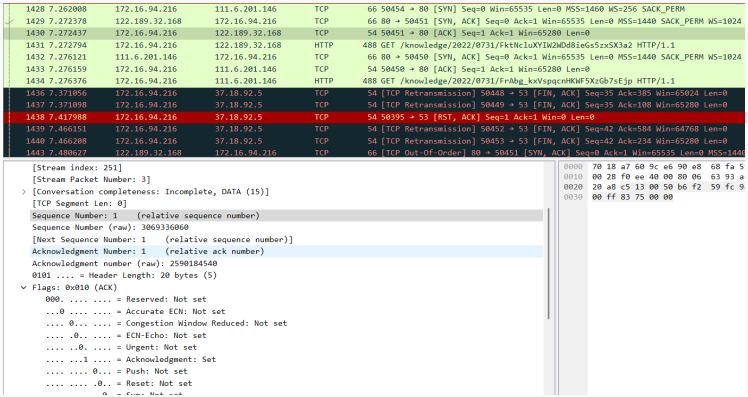


Рис. 27: TCP handshake шаг 3

Вывод

Вывод

В ходе выполнения лабораторной работы мы изучили посредством Wireshark кадры Ethernet, проанализировали PDU протоколы транспортного и прикладного уровней стека TCP/IP.