

Сетевые технологии

Лабораторная работа №3

Тойчубекова Асель Нурлановна

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Задание	7
4	Выполнение лабораторной работы	8
4.1	MAC-адресация	8
4.2	Анализ кадров канального уровня в Wireshark	13
4.3	Анализ протоколов транспортного уровня в Wireshark	21
4.4	Анализ handshake протокола TCP в Wireshark	28
5	Выводы	33
	Список литературы	34

Список иллюстраций

4.1	Сетевые настройки устройства	9
4.2	Сетевые настройки устройства	9
4.3	Информация о сетевых интерфейсах компьютера	11
4.4	Информация о сетевых интерфейсах компьютера	12
4.5	Информация о сетевых интерфейсах компьютера	13
4.6	Установка Wireshark	13
4.7	Установка Wireshark	14
4.8	Сетевые настройки устройства	14
4.9	Проверка связи с Wi-fi	15
4.10	Просмотр пакетов ARP и ICMP	15
4.11	ICMP-запрос	16
4.12	ICMP-ответ	17
4.13	Протокол ARP	18
4.14	Установка связи с habr.com	18
4.15	Протокол ARP	19
4.16	ICMP-запрос	20
4.17	ICMP-ответ	21
4.18	Сайт http://info.cern.ch/	21
4.19	HTTP-запрос	22
4.20	HTTP-ответ	24
4.21	DNS-запрос	25
4.22	DNS-ответ	26
4.23	QUIC -запрос	27
4.24	QUIC -ответ	28
4.25	Сайт Cern	29
4.26	SYN	30
4.27	SYN+ACK	30
4.28	ACK	31
4.29	График Потока	32

Список таблиц

1 Цель работы

В этой лабораторной работе я изучу с помощью Wireshark кадры Ethernet и анализирую PDU протоколов транспортного и прикладного уровней стека TCP/IP.

2 Теоретическое введение

Wireshark — это анализатор сетевого трафика, позволяющий исследовать работу сетевых протоколов и отслеживать обмен данными между устройствами. Он используется для диагностики сетевых неполадок, анализа безопасности и изучения структуры протоколов.

Одним из ключевых протоколов транспортного уровня является TCP (Transmission Control Protocol) — протокол, обеспечивающий надёжную передачу данных между клиентом и сервером. Установление соединения в TCP происходит в три этапа, называемых трёхступенчатым handshake:

Клиент отправляет запрос на соединение (SYN).

Сервер подтверждает запрос и предлагает свои параметры (SYN, ACK).

Клиент подтверждает установку соединения (ACK).

Другим современным транспортным протоколом является QUIC (Quick UDP Internet Connections), разработанный Google. Он работает поверх UDP, но обеспечивает надёжность и безопасность, аналогичную TCP и TLS. QUIC ускоряет установление соединения, объединяя процесс обмена криптографическими и транспортными параметрами, а также поддерживает шифрование каждого пакета и возможность смены сетевого пути без потери соединения.

3 Задание

1. Изучение возможностей команды `ipconfig` для ОС типа Windows (`ifconfig` для систем типа Linux).
2. Определение MAC-адреса устройства и его типа.
3. Установить на домашнем устройстве Wireshark.
4. С помощью Wireshark захватить и проанализировать пакеты ARP и ICMP в части кадров канального уровня.
5. С помощью Wireshark захватить и проанализировать пакеты HTTP, DNS в части заголовков и информации протоколов TCP, UDP, QUIC.
6. С помощью Wireshark проанализировать handshake протокола TCP.

4 Выполнение лабораторной работы

4.1 MAC-адресация

С помощью команды `ipconfig` выведем информацию о текущем сетевом соединении. В выводе видно, что активным является адаптер беспроводной сети (Wi-Fi), так как только у него указаны реальные IP-адреса.

IPv4-адрес: 172.16.48.177 — это адрес устройства в локальной сети.

Маска подсети: 255.255.254.0 — показывает диапазон доступных адресов в сети.

Основной шлюз: 172.16.48.1 — это адрес маршрутизатора, через который осуществляется выход в интернет.

Остальные адаптеры (например, OpenVPN, Ethernet, Bluetooth) находятся в состоянии «Среда передачи недоступна», то есть неактивны и не участвуют в сетевом обмене. (рис. 4.1 и рис. 4.2).


```

C:\Users\aselt>ipconfig

Настройка протокола IP для Windows

Неизвестный адаптер Подключение по локальной сети 3:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Адаптер Ethernet Ethernet 2:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::1e9:81e8:1faf:375c%12
    IPv4-адрес. . . . . : 192.168.56.1
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . :

Неизвестный адаптер Подключение по локальной сети:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Неизвестный адаптер OpenVPN Data Channel Offload:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Неизвестный адаптер Подключение по локальной сети 2:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Неизвестный адаптер OpenVPN Connect DCO Adapter:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Адаптер беспроводной локальной сети Подключение по локальной сети* 1:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

```

Рисунок 4.1: Сетевые настройки устройства

```

Адаптер беспроводной локальной сети Подключение по локальной сети* 2:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Адаптер беспроводной локальной сети Беспроводная сеть:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::e374:c575:84d5:d307%16
    IPv4-адрес. . . . . : 172.16.48.177
    Маска подсети . . . . . : 255.255.254.0
    Основной шлюз. . . . . : 172.16.48.1

Адаптер Ethernet Сетевое подключение Bluetooth:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

C:\Users\aselt>

```

Рисунок 4.2: Сетевые настройки устройства

Далее с помощью команды `ipconfig / all` просмотрим более подробную информацию обо всех сетевых интерфейсах компьютера. Мы видим, что активный сетевой

адаптер (Wi-Fi): F4-6A-DD-79-EC-4D Также есть неактивные виртуальные адаптеры (VirtualBox, OpenVPN, Bluetooth и др.).

Структура MAC-адреса

MAC-адрес состоит из 6 байт (12 шестнадцатеричных цифр): F4-6A-DD | 79-EC-4D

F4-6A-DD — идентификатор производителя (OUI), принадлежит Realtek Semiconductor Corp.

79-EC-4D — уникальный номер сетевого интерфейса, присвоенный устройству производителем.

Определение типа адреса

Чтобы определить тип MAC-адреса, нужно посмотреть первый байт (в примере — F4):

В двоичном виде F4 = 11110100

Последний бит (справа налево второй) показывает, индивидуальный или групповой:

0 - индивидуальный (уникальный для устройства)

1 - групповой (многоадресный, multicast)

Второй бит справа налево показывает, глобально или локально администрируемый:

0 - глобально администрируемый (назначен производителем)

1 - локально администрируемый (изменён пользователем или программно)

Для F4 оба бита равны 0 → адрес индивидуальный и глобально администрируемый. (рис. 4.3, рис. 4.4, рис. 4.5).

```

C:\Users\aselt>ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : LAPTOP-62AN0SVD
Основной DNS-суффикс . . . . . :
Тип узла . . . . . : Гибридный
IP-маршрутизация включена . . . . : Нет
WINS-прокси включен . . . . . : Нет

Неизвестный адаптер Подключение по локальной сети 3:

Состояние среды . . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание . . . . . : TAP-Windows Adapter V9 for OpenVPN Connect
Физический адрес . . . . . : 00-FF-15-70-88-08
DHCP включен . . . . . : Нет
Автонастройка включена . . . . . : Да

Адаптер Ethernet Ethernet 2:

DNS-суффикс подключения . . . . . :
Описание . . . . . : VirtualBox Host-Only Ethernet Adapter
Физический адрес . . . . . : 0A-00-27-00-00-0C
DHCP включен . . . . . : Нет
Автонастройка включена . . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::1e9:81e8:1faf:375c%12(Основной)
IPv4-адрес . . . . . : 192.168.56.1(Основной)
Маска подсети . . . . . : 255.255.255.0
Основной шлюз . . . . . :
IAID DHCPv6 . . . . . : 705298471
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2E-77-7A-8D-F4-6A-DD-79-EC-4D
NetBios через TCP/IP . . . . . : Включен

Неизвестный адаптер Подключение по локальной сети:

Состояние среды . . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание . . . . . : TAP-Windows Adapter V9
Физический адрес . . . . . : 00-FF-51-AC-7F-93
DHCP включен . . . . . : Да
Автонастройка включена . . . . . : Да

```

Рисунок 4.3: Информация о сетевых интерфейсах компьютера

```

Неизвестный адаптер OpenVPN Data Channel Offload:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : OpenVPN Data Channel Offload
Физический адрес. . . . . :
DHCP включен. . . . . : Нет
Автонастройка включена. . . . . : Да

Неизвестный адаптер Подключение по локальной сети 2:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : TAP-Windows Adapter V9 #2
Физический адрес. . . . . : 00-FF-D6-6C-C9-84
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Неизвестный адаптер OpenVPN Connect DCO Adapter:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : OpenVPN Data Channel Offload #2
Физический адрес. . . . . :
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Адаптер беспроводной локальной сети Подключение по локальной сети* 1:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Физический адрес. . . . . : F6-6A-DD-79-EC-4D
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Адаптер беспроводной локальной сети Подключение по локальной сети* 2:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Физический адрес. . . . . : FA-6A-DD-79-EC-4D
DHCP включен. . . . . : Нет
Автонастройка включена. . . . . : Да

```

Рисунок 4.4: Информация о сетевых интерфейсах компьютера

```

Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . :
Описание. . . . . : Realtek RTL8852BE WiFi 6 802.11ax PCIe Adapter
Физический адрес. . . . . : F4-6A-DD-79-EC-4D
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::e374:c575:84d5:d307%16(Основной)
IPv4-адрес. . . . . : 172.16.48.177(Основной)
Маска подсети . . . . . : 255.255.254.0
Аренда получена. . . . . : 10 октября 2025 г. 20:18:47
Срок аренды истекает. . . . . : 11 октября 2025 г. 1:18:47
Основной шлюз. . . . . : 172.16.48.1
DHCP-сервер. . . . . : 192.168.80.59
IAID DHCPv6 . . . . . : 267676381
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2E-77-7A-8D-F4-6A-DD-79-EC-4D
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. . . . . : F4-6A-DD-79-EC-4E
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

C:\Users\aselt>

```

Рисунок 4.5: Информация о сетевых интерфейсах компьютера

4.2 Анализ кадров канального уровня в Wireshark

Установим на нашем компьютере Wireshark. (рис. 4.6).

```

PS C:\WINDOWS\system32> choco install wireshark
Chocolatey v2.5.1
Installing the following packages:
wireshark
By installing, you accept licenses for the packages.
Downloading package from source 'https://community.chocolatey.org/api/v2/'
Progress: Downloading chocolatey-windowsupdate.extension 1.0.5... 100%
chocolatey-windowsupdate.extension v1.0.5 [Approved]
chocolatey-windowsupdate.extension package files install completed. Performing other installation steps.
Installed/updated chocolatey-windowsupdate extensions.
The install of chocolatey-windowsupdate.extension was successful.
Deployed to 'c:\ProgramData\chocolatey\extensions\chocolatey-windowsupdate'
Downloading package from source 'https://community.chocolatey.org/api/v2/'
Progress: Downloading KB2919442 1.0.20160915... 100%
KB2919442 v1.0.20160915 [Approved]
KB2919442 package files install completed. Performing other installation steps.
The package KB2919442 wants to run 'ChocolateyInstall.ps1'.
Note: If you don't run this script, the installation will fail.
Note: To confirm automatically next time, use '-y' or consider:
choco feature enable -n allowGlobalConfirmation
Do you want to run the script?([Y]es/[A]ll scripts/[N]o/[P]rint): A

Skipping installation because this hotfix only applies to Windows 8.1 and Windows Server 2012 R2.
The install of KB2919442 was successful.
Software install location not explicitly set, it could be in package or
default install location of installer.
Downloading package from source 'https://community.chocolatey.org/api/v2/'
Progress: Downloading KB2919355 1.0.20160915... 100%

```

Рисунок 4.6: Установка Wireshark

Запустите Wireshark. Выберем активный на устройстве сетевой интерфейс. Убедемся, что начался процесс захвата трафика. (рис. 4.7).

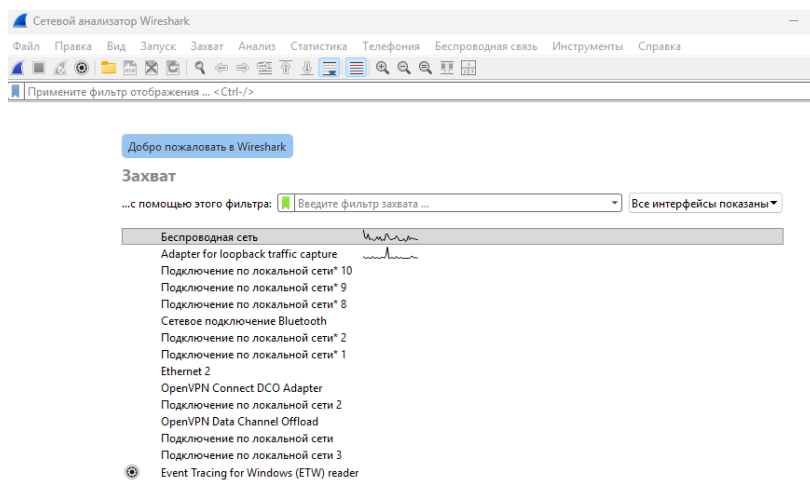


Рисунок 4.7: Установка Wireshark

На вашем устройстве в консоли определим с помощью команды `ipconfig`, IP-адрес нашего устройства и шлюз по умолчанию (default gateway). Мы видим, что наш IP-адрес= 172.16.48.177, а основной шлюз=172.16.48.1. (рис. 4.8).

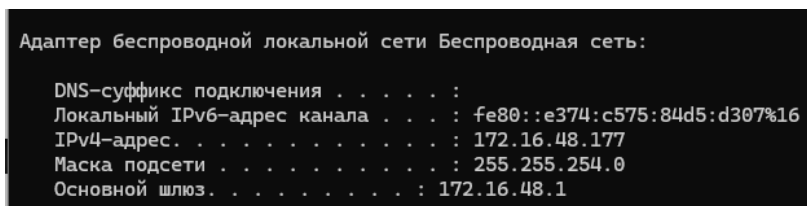


Рисунок 4.8: Сетевые настройки устройства

На нашем устройстве в консоли с помощью команды `ping адрес_шлюза` пропингуем шлюз по умолчанию. (рис. 4.9).

```
C:\Users\asetl>ping 172.16.48.1

Обмен пакетами с 172.16.48.1 по с 32 байтами данных:
Ответ от 172.16.48.1: число байт=32 время=9мс TTL=254
Ответ от 172.16.48.1: число байт=32 время=12мс TTL=254
Ответ от 172.16.48.1: число байт=32 время=13мс TTL=254
Ответ от 172.16.48.1: число байт=32 время=22мс TTL=254

Статистика Ping для 172.16.48.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 9мсек, Максимальное = 22 мсек, Среднее = 14 мсек

C:\Users\asetl>
```

Рисунок 4.9: Проверка связи с Wi-fi

В Wireshark остановим захват трафика. В строке фильтра пропишем фильтр `arp or icmp`. Убедимся, что в списке пакетов отобразились только пакеты ARP или ICMP, в частности пакеты, которые были сгенерированы с помощью команды `ping`, отправленной с устройства на шлюз по умолчанию. (рис. 4.10).

No.	Time	Source	Destination	Protocol	Length	Info
37	0.385329	ar100(d0:3e:62:c1)	Broadcast	ARP	60	Who has 172.16.48.1? Tell 172.16.48.155
375	4.365855	Intel_af:bereb	Broadcast	ARP	60	Who has 172.16.48.107? Tell 172.16.48.155
394	5.388396	Intel_af:bereb	Broadcast	ARP	60	Who has 172.16.48.107? Tell 172.16.48.155
397	5.864708	172.16.48.177	172.16.48.1	ICMP	74	Echo (ping) request id=0x0001, seq=38/9728, ttl=128 (reply in 399)
399	5.873435	172.16.48.1	172.16.48.177	ICMP	74	Echo (ping) reply id=0x0001, seq=38/9728, ttl=254 (request in 397)
454	6.871812	172.16.48.177	172.16.48.1	ICMP	74	Echo (ping) request id=0x0001, seq=39/9984, ttl=128 (reply in 455)
455	6.875331	172.16.48.1	172.16.48.177	ICMP	74	Echo (ping) reply id=0x0001, seq=39/9984, ttl=254 (request in 454)
477	7.875718	172.16.48.177	172.16.48.1	ICMP	74	Echo (ping) request id=0x0001, seq=40/10240, ttl=128 (reply in 478)
478	7.884445	172.16.48.1	172.16.48.177	ICMP	74	Echo (ping) reply id=0x0001, seq=40/10240, ttl=254 (request in 477)
715	8.878244	172.16.48.177	172.16.48.1	ICMP	74	Echo (ping) request id=0x0001, seq=41/10496, ttl=128 (reply in 716)
716	8.884956	172.16.48.1	172.16.48.177	ICMP	74	Echo (ping) reply id=0x0001, seq=41/10496, ttl=254 (request in 715)
781	11.021877	Apple_8e:58:1b	Broadcast	ARP	60	Who has 172.16.48.141? (ARP Probe)
782	11.328400	Apple_8e:58:1b	Broadcast	ARP	60	Who has 172.16.48.141? (ARP Probe)
783	12.148176	92:ea:38:f4:a5:0d	Broadcast	ARP	60	ARP Announcement for 172.16.48.200
816	12.058988	Apple_8e:58:1b	Broadcast	ARP	60	ARP Announcement for 172.16.48.141
817	12.059565	Apple_8e:58:1b	Broadcast	ARP	60	Who has 172.16.48.1? Tell 172.16.48.141
938	13.588659	92:ea:38:f4:a5:0d	Broadcast	ARP	60	ARP Announcement for 172.16.48.200
1139	13.888358	92:ea:38:f4:a5:0d	Broadcast	ARP	60	Who has 172.16.48.1? Tell 172.16.48.200
1140	13.888395	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.27? Tell 172.16.48.18
1141	13.889643	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.11? Tell 172.16.48.18
1142	13.890278	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.27? Tell 172.16.48.18
1143	13.890381	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.11? Tell 172.16.48.18
1144	13.890381	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.160? Tell 172.16.48.18
1145	13.890317	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.172? Tell 172.16.48.18
1146	13.890965	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.154? Tell 172.16.48.18
1147	13.990392	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.154? Tell 172.16.48.18
1149	13.990722	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.27? Tell 172.16.48.18
1150	13.991521	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.235? Tell 172.16.48.18
1151	13.991539	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.34? Tell 172.16.48.18
1152	13.991539	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.34? Tell 172.16.48.18
1153	13.992947	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.34? Tell 172.16.48.18
1154	13.992966	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.235? Tell 172.16.48.18
1155	13.993084	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.34? Tell 172.16.48.18
1156	13.993628	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.235? Tell 172.16.48.18
1157	13.993628	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.34? Tell 172.16.48.18
1158	13.993641	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.34? Tell 172.16.48.18
1159	13.993649	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.235? Tell 172.16.48.18
1160	13.993676	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.235? Tell 172.16.48.18
1161	13.994389	XiaomiMobile_d4:38:..	Broadcast	ARP	60	Who has 172.16.48.27? Tell 172.16.48.18

Рисунок 4.10: Просмотр пакетов ARP и ICMP

Просмотрим эхо-запрос ICMP в программе Wireshark.

Данные пакета (из панели сведений)

Длина кадра (Frame Length): 74 bytes (на проводе и захвачено).

Тип Ethernet: Ethernet II, Type: IPv4 (0x0800).

IP-адреса: источник 172.16.48.177, назначение (шлюз) 172.16.48.1.

MAC-адреса

MAC источника (ваш компьютер): f4:6a:dd:79:ec:4d (отмечено как LiteonTechno_79:ec:4d).

MAC назначения (шлюз/маршрутизатор): 70:18:07:60:9c:f8 (в Wireshark показан как устройство Cisco).

Определение типа MAC-адресов (коротко и как проверять)

Берём первый байт каждого MAC и смотрим его два младших бита (в двоичной записи):

Источник f4 - F4 hex = 1111 0100₂

LSB (бит 0) = 0 - индивидуальный (unicast)

бит 1 (U/L) = 0 - глобально администрируемый (назначен производителем)-
f4:6a:dd:79:ec:4d — индивидуальный, глобально администрируемый.

Назначение 70 - 70 hex = 0111 0000₂

LSB = 0 - индивидуальный (unicast)

бит 1 = 0 - глобально администрируемый - 70:18:07:60:9c:f8 — индивидуальный, глобально администрируемый. (рис. 4.11).

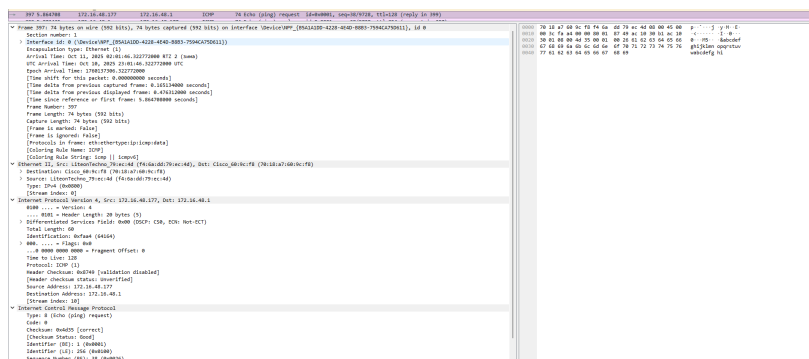


Рисунок 4.11: ICMP-запрос

Теперь посмотрим ICMP-ответ.

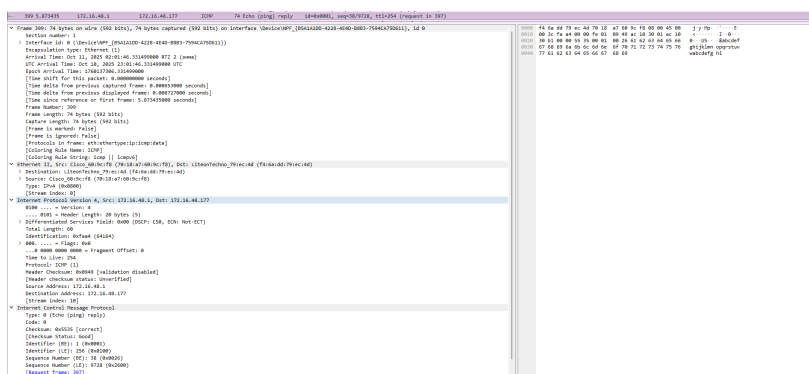
Данные пакета

Frame length: 74 bytes (на проводе и захвачено).

Тип Ethernet: Ethernet II, Type: IPv4 (0x0800).

IP-адреса:

MAC назначения (ваш компьютер): f4:6a:dd:79:ec:4d (LiteonTechno) - f4 (hex \rightarrow 111100₂) -индивидуальный,глобально администрируемый. (рис. 4.12).



Тип MAC-адресов: индивидуальные (у источника), широковещательный (у назначения)

Назначение кадра: запрос ARP, цель — определить MAC-адрес устройства с IP 172.16.48.107

Пояснение:

В ARP-запросе источник знает только IP назначения, поэтому отправляет кадр на Broadcast.

MAC-адрес источника уникален и глобально администрируемый (первые три байта f4:7b:09 идентифицируют производителя Intel).

MAC-адрес назначения — широковещательный, потому что ARP-запрос адресован всем устройствам в локальной сети. (рис. 4.13).

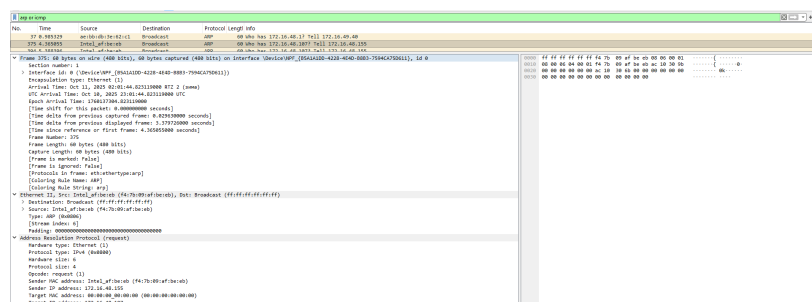


Рисунок 4.13: Протокол ARP

Начнем новый процесс захвата трафика в Wireshark. На устройстве в консоли пропингуем по имени какой-нибудь известный вам адрес, habr.com. (рис. 4.14).

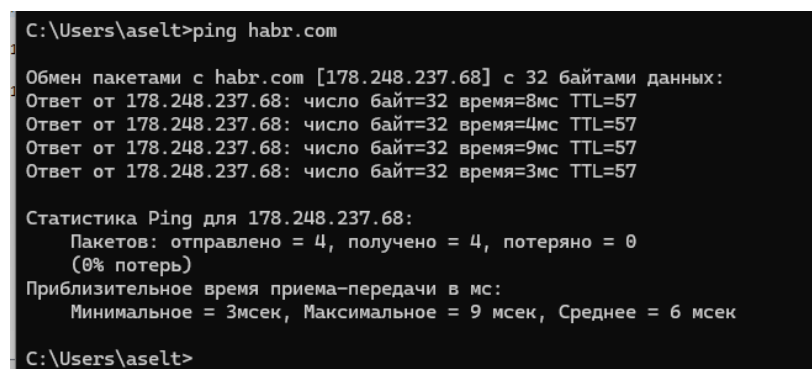


Рисунок 4.14: Установка связи с habr.com

В Wireshark остановим захват трафика. Изучим протокол ARP.

Данные кадра

Номер кадра: 148

Длина кадра (Frame Length): 42 bytes (336 bits)

Тип Ethernet: Ethernet II, Type: ARP (0x0806)

IP-адрес отправителя: 172.16.48.51

IP-адрес цели (запрашиваемый): 172.16.48.146

MAC-адреса

MAC источника (Sender MAC): 20:04:84:63:46:95 (Wireshark показывает как Apple_63:46:95)-индивидуальный, глобально администрируемый.

MAC назначения (Destination): ff:ff:ff:ff:ff:ff — Broadcast (широковещательный) - широковещательный (broadcast)

Кадр 148 — это ARP-запрос: устройство с MAC 20:04:84:63:46:95 и IP 172.16.48.51 посылает широковещательный запрос Who has 172.16.48.146? Tell 172.16.48.51, чтобы узнать MAC-адрес хоста с IP 172.16.48.146. MAC отправителя — индивидуальный и глобально администрируемый; MAC назначения — широковещательный (групповой). (рис. 4.15).

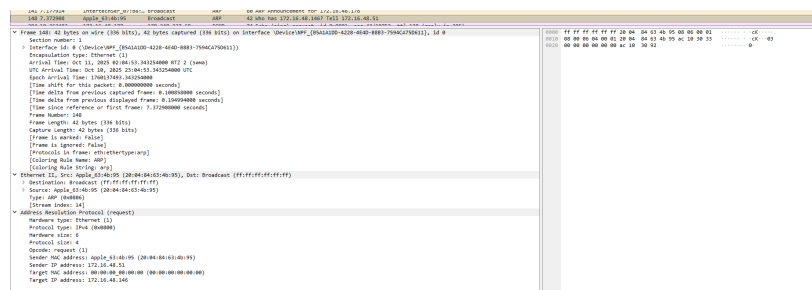


Рисунок 4.15: Протокол ARP

Изучим запросы протокола ICMP.

Основные данные пакета

Номер кадра: 204

Длина кадра (Frame Length): 74 bytes (592 bits)

Тип Ethernet: Ethernet II, Type: IPv4 (0x0800)

MAC назначения (шлюз/маршрутизатор): 70:18:27:60:9c:f8 (помечен как Cisco_60:9c:f8) — индивидуальный, глобально администрируемый. (рис. 4.16).

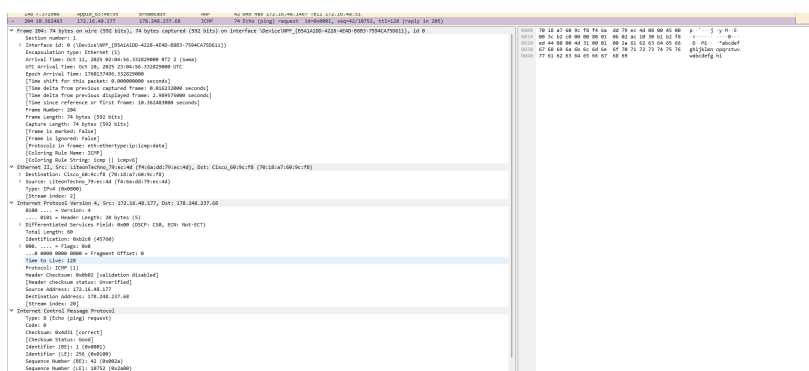


Рисунок 4.16: ICMP-запрос

MAC назначения: f4:6a:dd:79:ec:4d (Wireshark показывает как LiteonTechno_79:ec:4d) — это MAC вашего компьютера. - индивидуальные (unicast) и глобально администрируемые. (рис. 4.17).

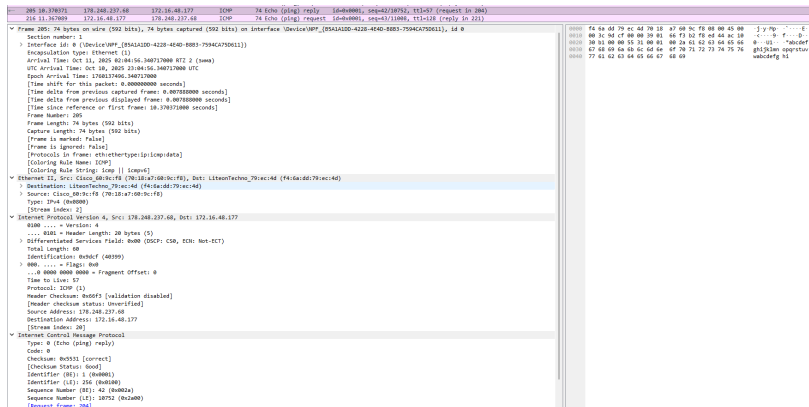


Рисунок 4.17: ICMP-ответ

4.3 Анализ протоколов транспортного уровня в Wireshark

Выберим активный на устройстве сетевой интерфейс. Убедимся, что начался процесс захвата трафика. На устройстве в браузере перейдем на сайт, работающий по протоколу HTTP, <http://info.cern.ch/>. По перемещаемся по ссылкам или разделам сайта в браузере. (рис. 4.18).

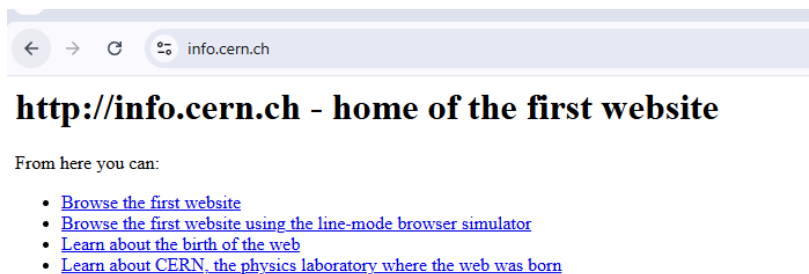


Рисунок 4.18: Сайт <http://info.cern.ch/>

В Wireshark в строке фильтра укажем http и проанализируем информацию по протоколу TCP в случае запросов.

Кадр 751 (HTTP-запрос по протоколу TCP)

Длина кадра: 652 байта

Теперь проанализируем информацию по протоколу TCP в случае ответов.

Кадр 770 (HTTP-ответ по протоколу TCP)

Длина кадра: 276 байт

Тип Ethernet: Ethernet II (IPv4 – 0x0800)

MAC-адрес источника: 70:18:a7:60:9c:f8 (Cisco_60:9c:f8)

MAC-адрес получателя: f4:6a:dd:79:ec:4d (LiteonTechno_79:ec:4d)

Тип MAC-адресов: индивидуальные, глобально администрируемые

Информация по TCP:

Протокол уровня транспорта: TCP (6)

Порт источника: 80 (HTTP)

Порт назначения: 62398

Флаги: PSH, ACK — данные передаются и подтверждаются

Номер последовательности (Seq): 2921

Номер подтверждения (Ack): 599

Размер окна: 31872

Длина TCP-сегмента: 222 байта

Тип данных: HTTP-ответ HTTP/1.1 200 OK (text/html)

Кадр представляет собой TCP-сегмент с HTTP-ответом от сервера (IP: 188.184.67.127) клиенту (IP: 172.16.48.177). Использование флага PSH указывает на немедленную передачу данных приложения (тело ответа HTTP). ACK подтверждает получение предыдущих сегментов TCP. Этот сегмент является частью установленного TCP-соединения для передачи HTTP-данных. (рис. 4.20).

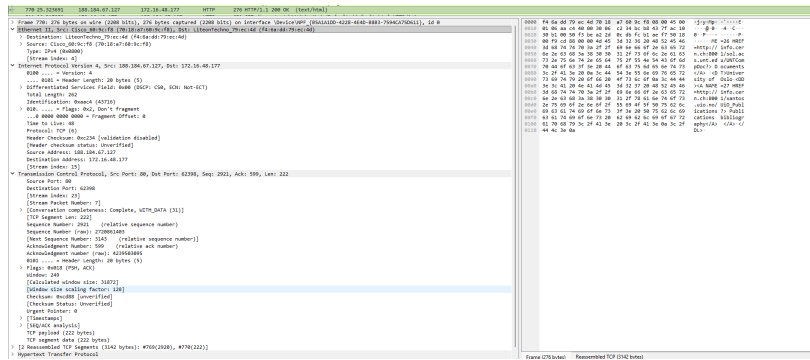


Рисунок 4.20: HTTP-ответ

В Wireshark в строке фильтра укажем dns и проанализируем информацию по протоколу UDP в случае запросов.

Кадр 419 (DNS-запрос по протоколу UDP)

Длина кадра: 79 байт

Тип Ethernet: Ethernet II (IPv4 – 0x0800)

MAC-адрес источника: f4:6a:dd:79:ec:4d (LiteonTechno_79:ec:4d)

MAC-адрес получателя: 70:18:a7:60:9c:f8 (Cisco_60:9c:f8)

Тип MAC-адресов: индивидуальные, глобально администрируемые

Информация по UDP:

Протокол уровня транспорта: UDP (17)

Порт источника: 64394

Порт назначения: 53 (DNS)

Длина UDP-пакета: 45 байт

Информация по DNS:

Тип запроса: стандартный DNS-запрос

Запрашиваемое доменное имя: accounts.google.com

Тип записи: A (IP-адрес)

Назначение запроса: разрешение доменного имени в IP-адрес

Кадр представляет собой DNS-запрос от клиента (IP: 172.16.48.177) к DNS-серверу (IP: 37.18.92.5) по UDP. Клиент запрашивает IP-адрес для домена accounts.google.com.

Использование UDP позволяет быстро передавать небольшие запросы без установки соединения, что характерно для протокола DNS. (рис. 4.21).

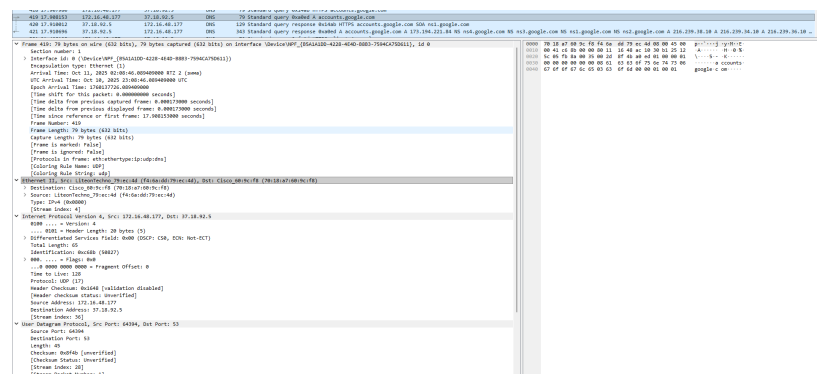


Рисунок 4.21: DNS-запрос

Проанализируем информацию по протоколу UDP в случае ответов.

Кадр 420 (DNS-ответ по протоколу UDP)

Длина кадра: 129 байт

Тип Ethernet: Ethernet II (IPv4 – 0x0800)

MAC-адрес источника: 70:18:37:60:9c:f8 (Cisco_60:9c:f8)

MAC-адрес получателя: f4:6a:dd:79:ec:4d (LiteonTechno_79:ec:4d)

Тип MAC-адресов: индивидуальные, глобально администрируемые

Информация по UDP:

Протокол уровня транспорта: UDP (17)

Порт источника: 53 (DNS)

Порт назначения: 51234

Длина UDP-пакета: 95 байт

Информация по DNS:

Тип ответа: стандартный DNS-ответ

Ответ на запрос домена: accounts.google.com

Типы записей:

A-запись: 173.194.221.84 (IP-адрес)

NS-запись: ns4.google.com

Цель ответа: разрешение доменного имени в IP-адрес для клиента

Кадр представляет собой DNS-ответ от сервера (IP: 37.18.92.5) клиенту (IP: 172.16.48.177). Сервер возвращает IP-адрес и данные NS для запрошенного домена accounts.google.com. Использование UDP позволяет передавать быстрые ответы без установления соединения. (рис. 4.22).

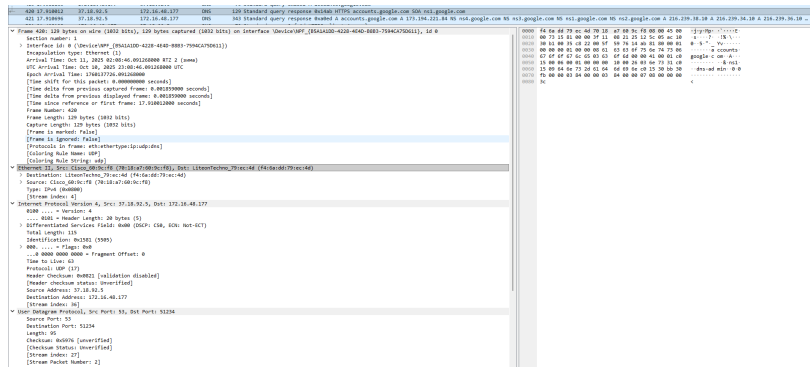


Рисунок 4.22: DNS-ответ

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

Кадр 617 — QUIC-запрос:

Длина кадра: 1292 байта

MAC-адрес источника: f4:6a:dd:79:ec:4d (LiteonTechno_79:ec:4d)

MAC-адрес получателя: 70:18:27:60:9c:f8 (Cisco_60:9c:f8)

Тип MAC-адресов: индивидуальные, глобально администрируемые

IP-адрес источника: 172.16.48.177

IP-адрес получателя: 142.250.74.142

Протокол уровня транспорта: UDP (17)

Порт источника: 54703

Порт назначения: 443 (HTTPS/QUIC)

Тип пакета QUIC: Initial

Содержимое: CRYPTO, PING, PADDING, DCID, PIN — инициирование защищённого соединения, обмен криптографическими данными, подтверждение доступности.

(рис. 4.23).

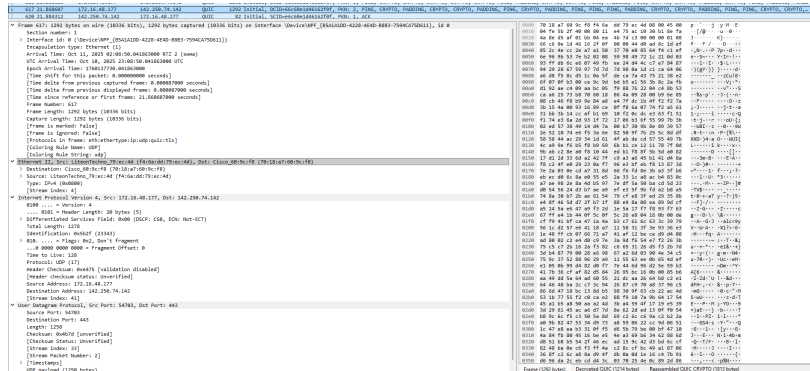


Рисунок 4.23: QUIC -запрос

Проанализируем информацию по протоколу quic в случае ответов.

Кадр 620 — QUIC-ответ (Initial, ACK):

Длина кадра: 82 байта

MAC-адрес источника: 70:18:a7:60:9c:f8 (Cisco_60:9c:f8)

MAC-адрес получателя: f4:6a:dd:79:ec:4d (LiteonTechno_79:ec:4d)

IP-адрес источника: 142.250.74.142

IP-адрес получателя: 172.16.48.177

Протокол транспорта: UDP (17)

Порт источника: 443

Порт назначения: 54703

Содержимое QUIC: Initial пакет с ACK, содержит SCID (Server Connection ID) и PKN=1 — подтверждение получения первого пакета от клиента, начало обмена ключами.

Кадр 621 — QUIC-ответ (Initial, ACK, PADDING):

Длина кадра: 1292 байта

MAC-адрес источника: 70:18:a7:60:9c:f8 (Cisco_60:9c:f8)

MAC-адрес получателя: f4:6a:dd:79:ec:4d (LiteonTechno_79:ec:4d)

IP-адрес источника: 142.250.74.142

IP-адрес получателя: 172.16.48.177

Протокол транспорта: UDP (17)

Порт источника: 443

Порт назначения: 54703

Содержимое QUIC: Initial пакет с ACK и PADDING, PKN=2 — подтверждение второго шага и выравнивание пакета для защиты от анализа трафика, продолжение криптографического обмена.

QUIC использует UDP для передачи зашифрованного трафика между клиентом и сервером HTTPS.

Кадры 620 и 621 — ответы сервера на запрос клиента, включающие подтверждения приёма и продолжение безопасного обмена данными. (рис. 4.24).

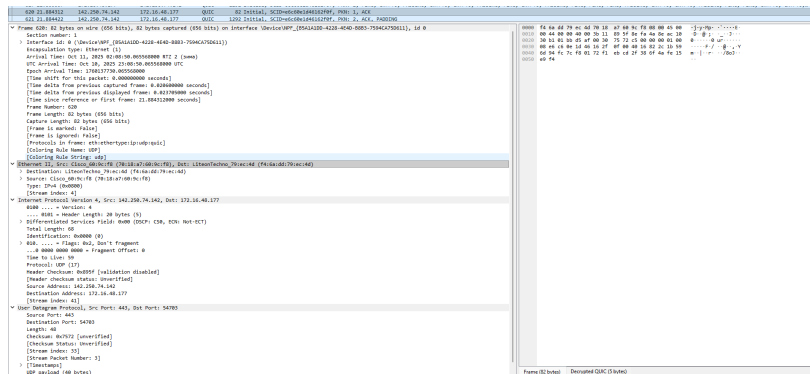


Рисунок 4.24: QUIC -ответ

4.4 Анализ handshake протокола TCP в Wireshark

Выберем активный на устройстве сетевой интерфейс. Убедимся, что начался процесс захвата трафика.

На нашем устройстве в браузере перейдем вновь на сайт CERN <http://info.cern.ch/>, работающий по протоколу http, для захвата в Wireshark пакетов TCP. (рис. 4.25).

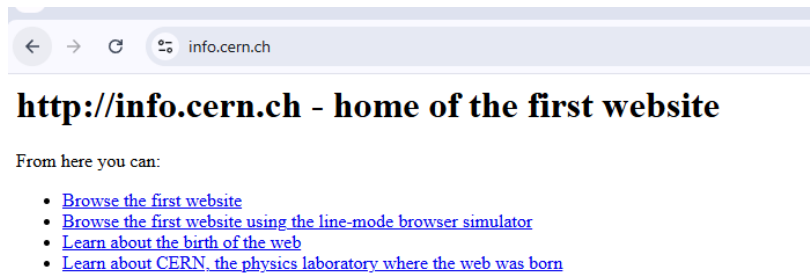


Рисунок 4.25: Сайт Cern

В Wireshark проанализируем handshake протокола TCP.

Кадр 307 — SYN (инициализация соединения от клиента)

Источник: 172.16.48.177

Назначение: 188.184.67.127

Порт источника: 56113

Порт назначения: 80

Флаги TCP: SYN (0x002)

Последовательный номер (Seq): 0

Размер окна (Window): 65535

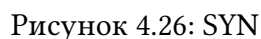
Опции TCP:

MSS=1468 — максимальный размер сегмента

WS=256 — масштаб окна

SACK permitted — разрешение SACK

Смысл: Клиент инициирует соединение, сообщая серверу свой начальный Seq номер. (рис. 4.26).



Источник: 188.184.67.127

Назначение: 172.16.48.177

Порт источника: 80

Порт назначения: 62101 (соответствует клиентскому порту + NAT/локальный)

Флаги TCP: SYN, ACK (0x012)

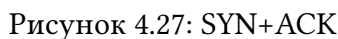
Seq сервера: 0

Ask: 1 — подтверждение Seq клиента + 1

Размер окна: 32120

Опции TCP: MSS=1460, WS=128, SACK permitted

Смысл: Сервер принимает запрос клиента и подтверждает его Seq, одновременно отправляя свой SYN для установления двустороннего соединения. (рис. 4.27).



Кадр 309 — ACK (подтверждение клиентом)

Источник: 172.16.48.177

Назначение: 188.184.67.127

Порт источника: 62101

Порт назначения: 80

Флаги TCP: ACK (0x010)

Seq: 1 — следующий Seq клиента

Ask: 1 — подтверждение Seq сервера + 1

Смысл: Клиент подтверждает получение SYN+ACK от сервера. (рис. 4.28).

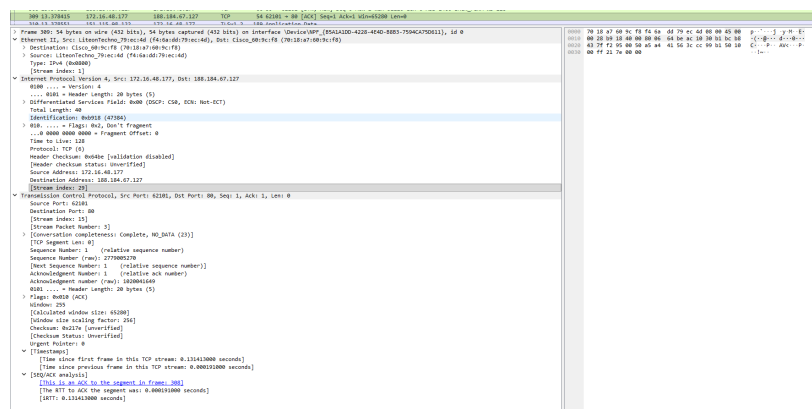


Рисунок 4.28: ACK

В Wireshark в меню «Статистика» выберем «График Потока». Рассмотрим процесс установлении соединения по TCP.

Seq и Ack показывают согласование номеров последовательностей, обеспечивая надежную доставку данных.

Флаги SYN/ACK изменяются от SYN → SYN+ACK → ACK, что является стандартной трехсторонней рукопожатой процедурой TCP.

Размер окна (Window) указывает на емкость буфера приема каждого участника и может масштабироваться (WS) для высокопроизводительных соединений.

SYN (клиент → сервер)

Сообщение: TCP 56448 → 80 [SYN] Seq=0 Win=65535 Len=0

ACK: отсутствует, так как это первый сегмент.

Win: 65535 — размер окна, сколько байт клиент готов принять.

SYN-ACK (сервер → клиент)

Сообщение: TCP 80 → 56448 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0

ACK: 1 — подтверждает получение SYN от клиента.

Win: 8192 — сколько байт сервер готов принять от клиента.

ACK (клиент → сервер)

Сообщение: TCP 56448 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0

ACK: 1 — подтверждает получение SYN сервера.

Win: 65280 — обновленный размер окна, сколько клиент готов принять. (рис. 4.29).

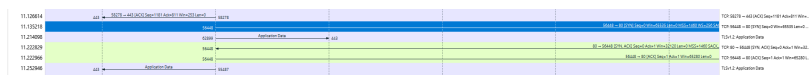


Рисунок 4.29: График Потока

5 Выводы

В ходе выполнения лабораторной работы №3 я изучила с помощью Wireshark кадры Ethernet и проанализировала PDU протоколов транспортного и прикладного уровней стека TCP/IP.

Список литературы

1. Barr D. Common DNS Operational and Configuration Errors: RFC / RFC Editor. —02/1996. — DOI: 10.17487/rfc1912.
2. Security-Enhanced Linux. Linux с улучшенной безопасностью: руководство пользователя / М. McAllister, S. Radvan, D. Walsh, D. Grift, E. Paris, J. Morris. — URL: https://docs-old.fedoraproject.org/ru-RU/Fedora/13/html/Security-Enhanced_Linux/index.html.
3. Systemd. — 2015. — URL: <https://wiki.archlinux.org/index.php/Systemd>.
4. Костромин В. А. Утилита lsof — инструмент администратора. — URL: <http://ruslinux.net/kos.php?name=/papers/lsof/lsof.html>