

Сетевые технологии

Лабораторная работа №3

Тойчубекова Асель Нурлановна

2025-10-11

Содержание I

1. Информация
2. Цель работы
3. Теоретическое введение
4. Задание
5. Выполнение лабораторной работы
6. Выводы
7. Список литературы

Раздел 1

1. Информация

1.1 Докладчик

► Тойчубекова Асель Нурлановна

1.1 Докладчик

- ▶ Тойчубекова Асель Нурлановна
- ▶ Студент 3 курса

1.1 Докладчик

- ▶ Тойчубекова Асель Нурлановна
- ▶ Студент 3 курса
- ▶ факультет физико-математических и естественных наук

1.1 Докладчик

- ▶ Тойчубекова Асель Нурлановна
- ▶ Студент 3 курса
- ▶ факультет физико-математических и естественных наук
- ▶ Российский университет дружбы народов им. П. Лумумбы

1.1 Докладчик

- ▶ Тойчубекова Асель Нурлановна
- ▶ Студент 3 курса
- ▶ факультет физико-математических и естественных наук
- ▶ Российский университет дружбы народов им. П. Лумумбы
- ▶ 1032235033@rudn.ru

Раздел 2

2. Цель работы

2.1 Цель работы

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

Раздел 3

3. Теоретическое введение

3.1 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.

3.2 Теоретическое введение

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).

3.3 Теоретическое введение

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. Q

Раздел 4

4. Задание

4.1 Задание

1. Изучение возможностей команды `ipconfig` для ОС типа Windows (`ifconfig` для систем типа Linux).

4.1 Задание

1. Изучение возможностей команды `ipconfig` для ОС типа Windows (`ifconfig` для систем типа Linux).
2. Определение MAC-адреса устройства и его типа.

4.1 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.

4.1 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.

4.1 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.

4.1 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.

Раздел 5

5. Выполнение лабораторной работы

5.1 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.

5.2 MAC-адресация

```
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 :

5.3 MAC-адресация

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 2: Сетевые настройки устройства

5.4 MAC-адресация

Далее с помощью команды `ipconfig / all` посмотрим 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.

5.5 MAC-адресация

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.

5.6 MAC-адресация

```
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 . . . . . :
```

5.7 MAC-адресация

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 :

5.8 MAC-адресация

```
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\ase<...>
```

Рисунок 5: Информация о сетевых интерфейсах компьютера

5.9 Анализ кадров канального уровня в Wireshark

Установим на нашем компьютере Wireshark.

```
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%

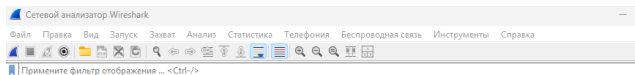
KB2919442 v1.0.20160915 [Approved]
KB2919442 package files install completed. Performing other installation steps.
The package KB2919442 wants to run 'ChocolateyInstall.ps1'.
Note: If you don't run this script, the installation will fail.
Note: To confirm automatically next time, use '-y' or consider:
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 6: Установка Wireshark

5.10 Анализ кадров канального уровня в Wireshark



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



Добро пожаловать в Wireshark

Захват

...с помощью этого фильтра: Все интерфейсы показаны ▾

Беспроводная сеть	
Adapter for loopback traffic capture	
Подключение по локальной сети* 10	
Подключение по локальной сети* 9	
Подключение по локальной сети* 8	
Сетевое подключение Bluetooth	
Подключение по локальной сети* 2	
Подключение по локальной сети* 1	
Ethernet 2	
OpenVPN Connect DCO Adapter	
Подключение по локальной сети 2	
OpenVPN Data Channel Offload	
Подключение по локальной сети	
Подключение по локальной сети 3	
<input checked="" type="radio"/> Event Tracing for Windows (ETW) reader	

5.11 Анализ кадров канального уровня в 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.

```
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
```

Рисунок 8: Сетевые настройки устройства

5.12 Анализ кадров канального уровня в Wireshark

На нашем устройстве в консоли с помощью команды ping адрес_шлюза пропингуем шлюз по умолчанию.

```
C:\Users\aselt>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\aselt>
```

Рисунок 9: Проверка связи с Wi-fi

5.13 Анализ кадров канального уровня в Wireshark

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.

arp or icmp					
No.	Time	Source	Destination	Protocol	Length Info
37	0.985329	ae:bb:db:3e:62:c1	Broadcast	ARP	60 Who has 172.16.48.1? Tell 172.16.48.40
375	4.361955	Intel_afib:eb	Broadcast	ARP	60 Who has 172.16.48.187? Tell 172.16.48.155
394	5.388396	Intel_afib:eb	Broadcast	ARP	60 Who has 172.16.48.187? Tell 172.16.48.155
397	5.864788	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	7.875710	172.16.48.177	172.16.48.1	ICMP	74 Echo (ping) request id=0x0001, seq=40/10240, ttl=128 (reply in 478)
478	7.884645	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	8.884056	172.16.48.1	172.16.48.177	ICMP	74 Echo (ping) reply id=0x0001, seq=41/10496, ttl=254 (request in 715)
781	11.801877	Apple_Be:58:1b	Broadcast	ARP	60 Who has 172.16.48.141? (ARP Probe)
782	11.528400	Apple_Be:58:1b	Broadcast	ARP	60 Who has 172.16.48.141? (ARP Probe)
783	12.148176	92:ea:38:f4:a5:8d	Broadcast	ARP	60 ARP Announcement for 172.16.48.200
816	12.658908	Apple_Be:58:1b	Broadcast	ARP	60 ARP Announcement for 172.16.48.141
817	12.659565	Apple_Be:58:1b	Broadcast	ARP	60 Who has 172.16.48.1? Tell 172.16.48.141
930	13.508659	92:ea:38:f4:a5:8d	Broadcast	ARP	60 ARP Announcement for 172.16.48.200
1139	13.888358	92:ea:38:f4:a5:8d	Broadcast	ARP	60 Who has 172.16.48.1? Tell 172.16.48.200
1140	13.888395	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.48.277? Tell 172.16.48.18
1141	13.889643	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.49.117? Tell 172.16.48.18
1142	13.890278	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.48.277? Tell 172.16.48.18
1143	13.890301	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.49.117? Tell 172.16.48.18
1144	13.890301	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.48.160? Tell 172.16.48.18
1145	13.890317	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.48.172? Tell 172.16.48.18
1146	13.890905	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.48.154? Tell 172.16.48.18
1147	13.990132	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.48.194? Tell 172.16.48.18
1149	13.990722	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.48.277? Tell 172.16.48.18
1150	13.991521	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.48.235? Tell 172.16.48.18
1151	13.991539	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.49.34? Tell 172.16.48.18
1152	13.991539	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.49.34? Tell 172.16.48.18
1153	13.992947	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.49.34? Tell 172.16.48.18
1154	13.992966	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.48.235? Tell 172.16.48.18
1155	13.993604	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.49.34? Tell 172.16.48.18
1156	13.993628	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.48.235? Tell 172.16.48.18
1157	13.993628	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.49.34? Tell 172.16.48.18
1158	13.993641	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.49.34? Tell 172.16.48.18
1159	13.993649	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.48.235? Tell 172.16.48.18
1160	13.993676	XiaomiMobile_dd:38:1e	Broadcast	ARP	60 Who has 172.16.48.235? Tell 172.16.48.18

5.14 Анализ кадров канального уровня в Wireshark

Посмотрим 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). - F4 hex = 1111 0100₂- индивидуальный, глобально администрируемый.

MAC назначения (шлюз/маршрутизатор): 70:18:07:60:9c:f8 (в Wireshark показан как устройство Cisco). - 70 hex = 0111 0000₂ - индивидуальный, глобально администрируемый.

5.15 Анализ кадров канального уровня в Wireshark

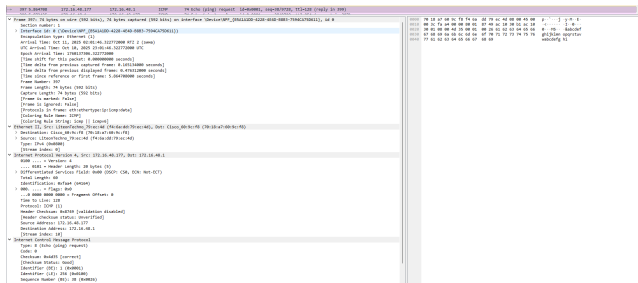


Рисунок 11: ICMP-запрос

5.16 Анализ кадров канального уровня в Wireshark

Теперь посмотрим ICMP-ответ.

Данные пакета

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

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

IP-адреса:

Источник (шлюз): 172.16.48.1

Назначение (ваш компьютер): 172.16.48.177

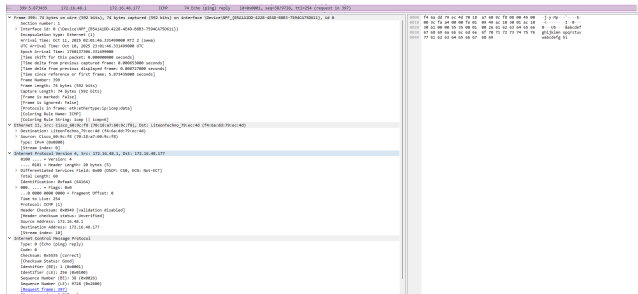
MAC-адреса

MAC источника (шлюз): 70:18:a7:60:9c:f8 (Cisco) - 70 (hex → 0111 0000₂) -

индивидуальный, глобально администрируемый

MAC назначения (ваш компьютер): f4:6a:dd:79:ec:4d (LiteonTechno) - f4 (hex → 1111 0100₂) - индивидуальный, глобально администрируемый.

Рисунок 12: ICMP-ответ



5.18 Анализ кадров канального уровня в Wireshark

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

Кадр ARP (Frame 375):

Длина кадра: 60 байт (480 бит)

Тип Ethernet: Ethernet II

MAC-адрес источника: f4:7b:09:af:be:eb (сетевой интерфейс отправителя)

MAC-адрес назначения: ff:ff:ff:ff:ff:ff (широковещательный — Broadcast)

Протокол в кадре: ARP (0x0806)

IP-адрес источника: 172.16.48.155

IP-адрес назначения: 172.16.48.107

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

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

5.19 Анализ кадров канального уровня в Wireshark

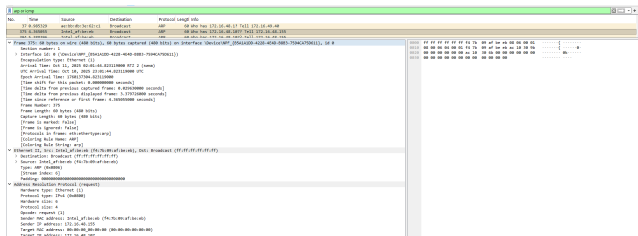


Рисунок 13: Протокол ARP

5.20 Анализ кадров канального уровня в Wireshark

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

```
C:\Users\aselt>ping habr.com

Обмен пакетами с habr.com [178.248.237.68] с 32 байтами данных:
Ответ от 178.248.237.68: число байт=32 время=8мс TTL=57
Ответ от 178.248.237.68: число байт=32 время=4мс TTL=57
Ответ от 178.248.237.68: число байт=32 время=9мс TTL=57
Ответ от 178.248.237.68: число байт=32 время=3мс TTL=57

Статистика Ping для 178.248.237.68:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
        Минимальное = 3мсек, Максимальное = 9 мсек, Среднее = 6 мсек

C:\Users\aselt>
```

Рисунок 14: Установка связи с `habr.com`

5.21 Анализ кадров канального уровня в Wireshark

В Wireshark остановим захват трафика. Изучим протокол ARP.

Кадр 148(Длина кадра (Frame Length): 42 bytes (336 bits))— 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).

5.22 Анализ кадров канального уровня в Wireshark

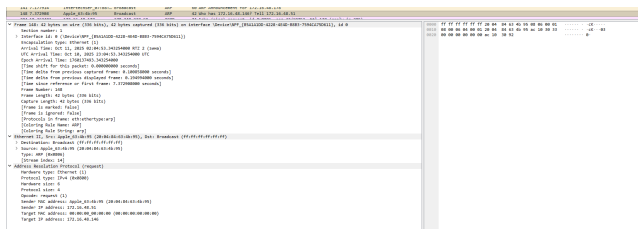


Рисунок 15: Протокол ARP

5.23 Анализ кадров канального уровня в Wireshark

Изучим запросы протокола ICMP.

Номер кадра: 204

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

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

IP-адреса: источник 172.16.48.177, назначение 178.248.237.68 (пинг наружному хосту)

MAC-адреса (Ethernet II)

MAC источника (ваш компьютер): f4:6a:dd:79:ec:4d (Wireshark показывает как LiteonTechno_79:ec:4d)- — индивидуальный, глобально администрируемый.

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

5.24 Анализ кадров канального уровня в Wireshark

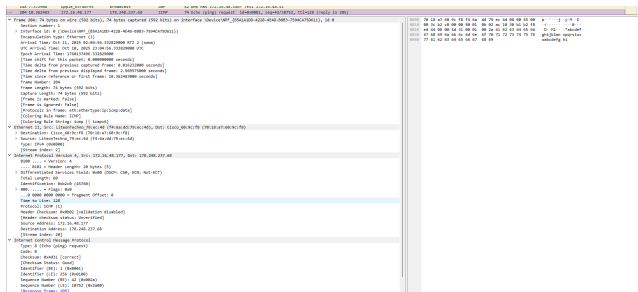


Рисунок 16: ICMP-запрос

5.25 Анализ кадров канального уровня в Wireshark

Изучим ответы протокола ICMP.

Длина кадра (Frame Length): 74 bytes.

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

IP-адреса: источник 178.248.237.68, назначение 172.16.48.177.

MAC-адреса (Ethernet II)

MAC источника: 70:18:37:60:9c:f8 (Wireshark показывает как Cisco_60:9c:f8) — это MAC шлюза/маршрутизатора/удалённого устройства, от которого пришёл ответ. - индивидуальные (unicast) и глобально администрируемые.

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

5.26 Анализ кадров канального уровня в Wireshark

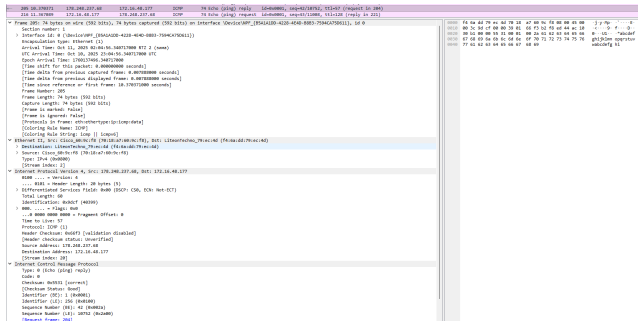


Рисунок 17: ICMP-ответ

5.27 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.



Рисунок 18: Сайт <http://info.cern.ch/>

5.28 Анализ протоколов транспортного уровня в Wireshark

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

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

5.29 Анализ протоколов транспортного уровня в Wireshark

Информация по TCP:

Протокол уровня транспорта: TCP (6)

Порт источника: 62398

Порт назначения: 80 (HTTP)

Флаги: PSN, ACK — данные передаются и подтверждаются

Номер последовательности (Seq): 1

Номер подтверждения (Ack): 1

Размер окна: 65280

Длина TCP-сегмента: 598 байт

Тип данных: HTTP-запрос GET /hypertext/DataSources/byOrganisation/Overview.html
HTTP/1.1

5.30 Анализ протоколов транспортного уровня в Wireshark

175.26.20944	172.16.48.177	188.184.47.127	HTTP	852 B[1] / Hypertext Transfer Protocol [application/javascript] [87591.1]
177.26.12169	188.184.47.127	172.16.48.177	HTTP	278 B[7913.1.200 OK (text/html)]
1 frame 261: 852 bytes on wire (5118 bits), 852 bytes captured (5118 bits) on interface DeviceNPF {8541A500-4218-404B-B805-750AC4750611}, id 0				
↳ Ethernet II, Src: VMwareNet0:08:00:27:00:00:00:00, Dest: Cisco48:63:FC:3B:39:3E:08:00:27:00:00:00:00				
1 Destination: Cisco48:63:FC:3B:39:3E (78:18:ad:ab:bc:fe)				
1 Source: VMwareNet0:08:00:27:00:00:00:00 (18:ad:ab:bc:fe:ad)				
Type: IPv4 (Internet)				
[Screen Index: 4]				
1 Internet Protocol Version 4, Src: 172.16.48.177, Dest: 188.184.47.127				
8000 ... > Version: 4				
... > Header Length: 20 bytes (5)				
1 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)				
Total Length: 656				
Identification: 66044 (X2707)				
1 8000 ... > Flags: 0x0, No S Fragment				
... > 8 0000 0000 - Fragment Offset: 0				
Time to Live: 128				
Protocol: TCP (6)				
Header Checksum: 0x02af [validation failed]				
[Header checksum status: invalid]				
Source Address: 172.16.48.177				
Destination Address: 188.184.47.127				
[Screen Index: 11]				
1 Transmission Control Protocol, Src Port: 82398, Dest Port: 80, Seq: 1, Len: 308				
Source Port: 82398				
Destination Port: 80				
[Screen Index: 23]				
1 [Sequence completion]: Complete, WTR_RSTA (13)				
[TCP Sequence Number: 1]				
[Sequence Number: 1 (relative sequence number)]				
Sequence Number (raw): 623982097				
[Next sequence number: 599 (relative sequence number)]				
Acknowledgment Number: 1 (relative ack number)				
Acknowledgment Number (raw): 570959403				
6561 ... > Header Length: 20 bytes (5)				
1 Flags: 0x02 (PSH, ACK)				
Window: 285				
[Unlabeled window size: 65536]				
Window size scaling factor: 216				
Checksum: 0x0210 [validation failed]				
[Checksum status: invalid]				
Urgent Pointer: 0				
1 [Timestamp]				
1 [Sequence Number]				
TCP payload (308 bytes)				
1 Hypertext Transfer Protocol				
68800	78.28.47.68	78.28.47.68	44739	44739
68801	78.28.47.68	78.28.47.68	44739	44739
68802	78.28.47.68	78.28.47.68	44739	44739
68803	78.28.47.68	78.28.47.68	44739	44739
68804	78.28.47.68	78.28.47.68	44739	44739
68805	78.28.47.68	78.28.47.68	44739	44739
68806	78.28.47.68	78.28.47.68	44739	44739
68807	78.28.47.68	78.28.47.68	44739	44739
68808	78.28.47.68	78.28.47.68	44739	44739
68809	78.28.47.68	78.28.47.68	44739	44739
68810	78.28.47.68	78.28.47.68	44739	44739
68811	78.28.47.68	78.28.47.68	44739	44739
68812	78.28.47.68	78.28.47.68	44739	44739
68813	78.28.47.68	78.28.47.68	44739	44739
68814	78.28.47.68	78.28.47.68	44739	44739
68815	78.28.47.68	78.28.47.68	44739	44739
68816	78.28.47.68	78.28.47.68	44739	44739
68817	78.28.47.68	78.28.47.68	44739	44739
68818	78.28.47.68	78.28.47.68	44739	44739
68819	78.28.47.68	78.28.47.68	44739	44739
68820	78.28.47.68	78.28.47.68	44739	44739
68821	78.28.47.68	78.28.47.68	44739	44739
68822	78.28.47.68	78.28.47.68	44739	44739
68823	78.28.47.68	78.28.47.68	44739	44739
68824	78.28.47.68	78.28.47.68	44739	44739
68825	78.28.47.68	78.28.47.68	44739	44739
68826	78.28.47.68	78.28.47.68	44739	44739
68827	78.28.47.68	78.28.47.68	44739	44739
68828	78.28.47.68	78.28.47.68	44739	44739
68829	78.28.47.68	78.28.47.68	44739	44739
68830	78.28.47.68	78.28.47.68	44739	44739
68831	78.28.47.68	78.28.47.68	44739	44739
68832	78.28.47.68	78.28.47.68	44739	44739
68833	78.28.47.68	78.28.47.68	44739	44739
68834	78.28.47.68	78.28.47.68	44739	44739
68835	78.28.47.68	78.28.47.68	44739	44739
68836	78.28.47.68	78.28.47.68	44739	44739
68837	78.28.47.68	78.28.47.68	44739	44739
68838	78.28.47.68	78.28.47.68	44739	44739
68839	78.28.47.68	78.28.47.68	44739	44739
68840	78.28.47.68	78.28.47.68	44739	44739
68841	78.28.47.68	78.28.47.68	44739	44739
68842	78.28.47.68	78.28.47.68	44739	44739
68843	78.28.47.68	78.28.47.68	44739	44739
68844	78.28.47.68	78.28.47.68	44739	44739
68845	78.28.47.68	78.28.47.68	44739	44739
68846	78.28.47.68	78.28.47.68	44739	44739
68847	78.28.47.68	78.28.47.68	44739	44739
68848	78.28.47.68	78.28.47.68	44739	44739
68849	78.28.47.68	78.28.47.68	44739	44739
68850	78.28.47.68	78.28.47.68	44739	44739
68851	78.28.47.68	78.28.47.68	44739	44739
68852	78.28.47.68	78.28.47.68	44739	44739
68853	78.28.47.68	78.28.47.68	44739	44739
68854	78.28.47.68	78.28.47.68	44739	44739
68855	78.28.47.68	78.28.47.68	44739	44739
68856	78.28.47.68	78.28.47.68	44739	44739
68857	78.28.47.68	78.28.47.68	44739	44739
68858	78.28.47.68	78.28.47.68	44739	44739
68859	78.28.47.68	78.28.47.68	44739	44739
68860	78.28.47.68			

5.31 Анализ протоколов транспортного уровня в Wireshark

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

5.32 Анализ протоколов транспортного уровня в Wireshark

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)

5.33 Анализ протоколов транспортного уровня в Wireshark

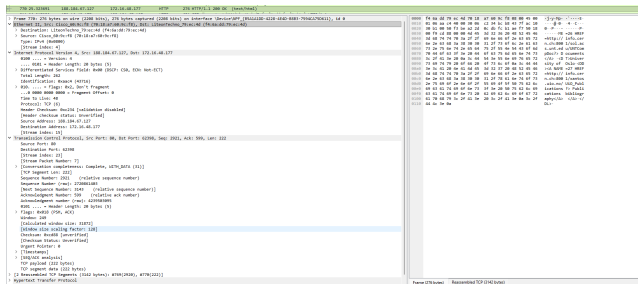


Рисунок 20: HTTP-ответ

5.34 Анализ протоколов транспортного уровня в Wireshark

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

5.35 Анализ протоколов транспортного уровня в Wireshark

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

Рисунок 21: DNS-запрос



5.37 Анализ протоколов транспортного уровня в Wireshark

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

5.38 Анализ протоколов транспортного уровня в Wireshark

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

Рисунок 22: DNS-ответ

5.40 Анализ протоколов транспортного уровня в Wireshark

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

5.41 Анализ протоколов транспортного уровня в Wireshark

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.

Рисунок 23: QUIC -запрос

5.43 Анализ протоколов транспортного уровня в Wireshark

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)

5.44 Анализ протоколов транспортного уровня в Wireshark

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.

5.45 Анализ протоколов транспортного уровня в Wireshark

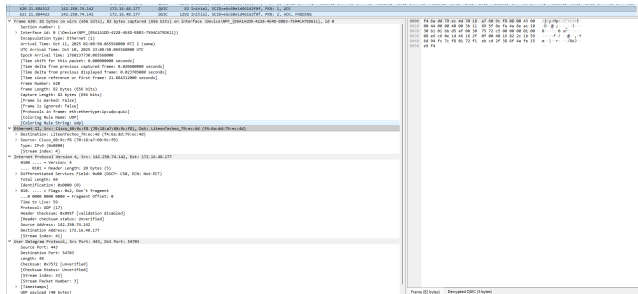


Рисунок 24: QUIC -ответ

5.46 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.

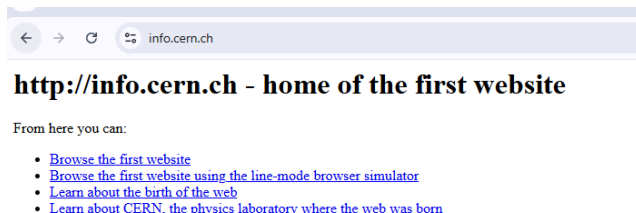


Рисунок 25: Сайт Cern

5.47 Анализ handshake протокола TCP в Wireshark

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.

5.48 Анализ handshake протокола TCP в Wireshark

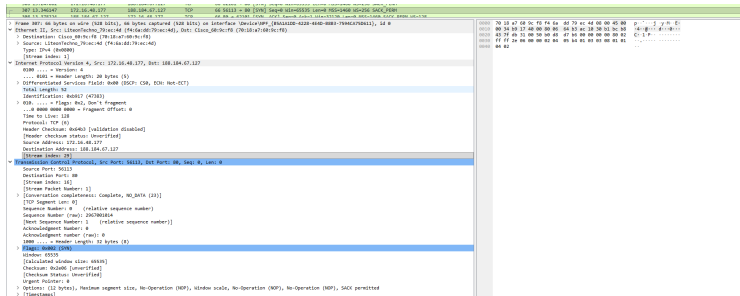


Рисунок 26: SYN

5.49 Анализ handshake протокола TCP в Wireshark

Кадр 308 — SYN+ACK (ответ сервера)

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

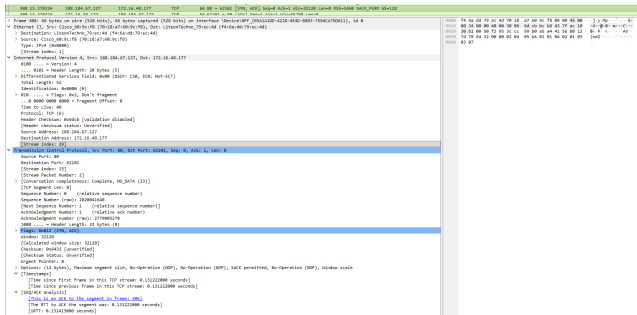
Ask: 1 — подтверждение Seq клиента + 1

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. =

Рисунок 27: SYN+ACK



5.51 Анализ handshake протокола TCP в Wireshark

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

Ack: 1 — подтверждение Seq сервера + 1

Смысл: Клиент подтверждает получение SYN+ACK от сервера.

5.52 Анализ handshake протокола TCP в Wireshark

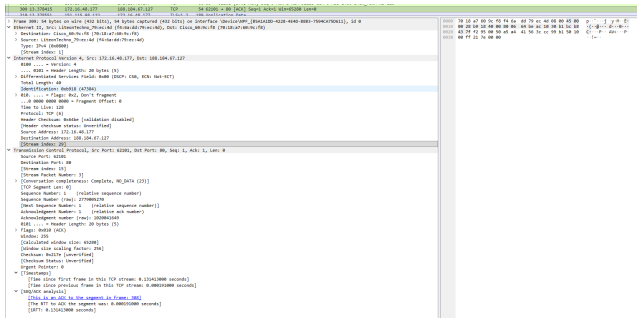


Рисунок 28: ACK

5.53 Анализ handshake протокола TCP в Wireshark

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

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.

5.54 Анализ handshake протокола TCP в Wireshark

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.

5.55 Анализ handshake протокола TCP в Wireshark

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.

5.56 Анализ handshake протокола TCP в Wireshark

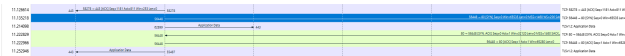


Рисунок 29: График Потока

Раздел 6

6. Выводы

6.1 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.

Раздел 7

7. Список литературы

7.1 Список литературы

1. Barr D. Common DNS Operational and Configuration Errors: RFC / RFC Editor. —02/1996. — DOI: 10.17487/rfc1912.

7.1 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 / M. 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.

7.1 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 / M. 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>.

7.1 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 / M. 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>