

# **Лабораторная работа №3**

**Анализ трафика в Wireshark**

Газизянов Владислав Альбертович

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>7</b>
3.1	MAC-адресация . . . . .	7
3.2	Анализ кадров канального уровня в Wireshark . . . . .	8
3.3	Анализ протоколов транспортного уровня . . . . .	11
<b>4</b>	<b>Выводы</b>	<b>14</b>

# Список иллюстраций

3.1	Вывод команды <code>ipconfig /all</code> . . . . .	7
3.2	Структура MAC-адреса . . . . .	8
3.3	Запуск Wireshark и выбор интерфейса . . . . .	9
3.4	Выполнение <code>ping</code> команды . . . . .	9
3.5	Фильтрация ARP и ICMP пакетов . . . . .	9
3.6	Анализ ICMP-запроса . . . . .	10
3.7	Анализ ICMP-ответа . . . . .	10
3.8	Анализ ARP пакетов . . . . .	11
3.9	Захват TCP трафика . . . . .	12
3.10	TCP handshake анализ . . . . .	12
3.11	График потока TCP . . . . .	13

## **Список таблиц**

# 1 Цель работы

Изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.

## 2 Задание

1. Изучить MAC-адресацию сетевых интерфейсов
2. Проанализировать кадры канального уровня в Wireshark
3. Исследовать протоколы транспортного уровня
4. Проанализировать handshake протокола TCP

## 3 Выполнение лабораторной работы

### 3.1 MAC-адресация

#### 3.1.1 Вывод команды ipconfig /all

Выполнена команда `ipconfig /all` для получения информации о сетевых интерфейсах.

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

Настройка протокола IP для Windows

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

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::45ca:6cd8:ba02:f0cb%12(Основной)
IPv4-адрес. . . . . : 192.168.56.1(Основной)
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . :
IAID DHCPv6 . . . . . : 537526311
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2E-B6-C0-87-3C-18-A0-C8-8D-52
NetBios через TCP/IP. . . . . : Включен
```

Рисунок 3.1: Вывод команды `ipconfig /all`

В результате получена информация о всех сетевых адаптерах. Основные

параметры: - Основной рабочий интерфейс: Беспроводная сеть - IP-адрес: 192.168.0.101 - Шлюз по умолчанию: 192.168.0.1

### 3.1.2 Определение MAC-адресов

Определены MAC-адреса всех сетевых интерфейсов: - VirtualBox Host-Only: 0A-00-27-00-00-0C - Основной Wi-Fi адаптер: C0-BF-BE-CF-C4-CE - Дополнительные Wi-Fi адаптеры: C2-BF-BE-CF-94-9E, C2-BF-BE-CF-E4-EE - Bluetooth адаптер: C0-BF-BE-CF-C4-CF

### 3.1.3 Анализ структуры MAC-адреса

Проанализирована структура основного MAC-адреса C0-BF-BE-CF-C4-CE: - OUI (первые 3 байта): C0-BF-BE - производитель MediaTek Inc. - Идентификатор интерфейса: CF-C4-CE - Тип адреса: индивидуальный (unicast) - Администрирование: глобально администрируемый

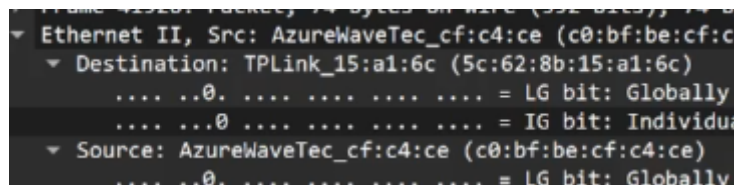


Рисунок 3.2: Структура MAC-адреса

## 3.2 Анализ кадров канального уровня в Wireshark

### 3.2.1 Захват ARP и ICMP пакетов

Запущен Wireshark, выбран интерфейс «Беспроводная сеть» и начат захват трафика.



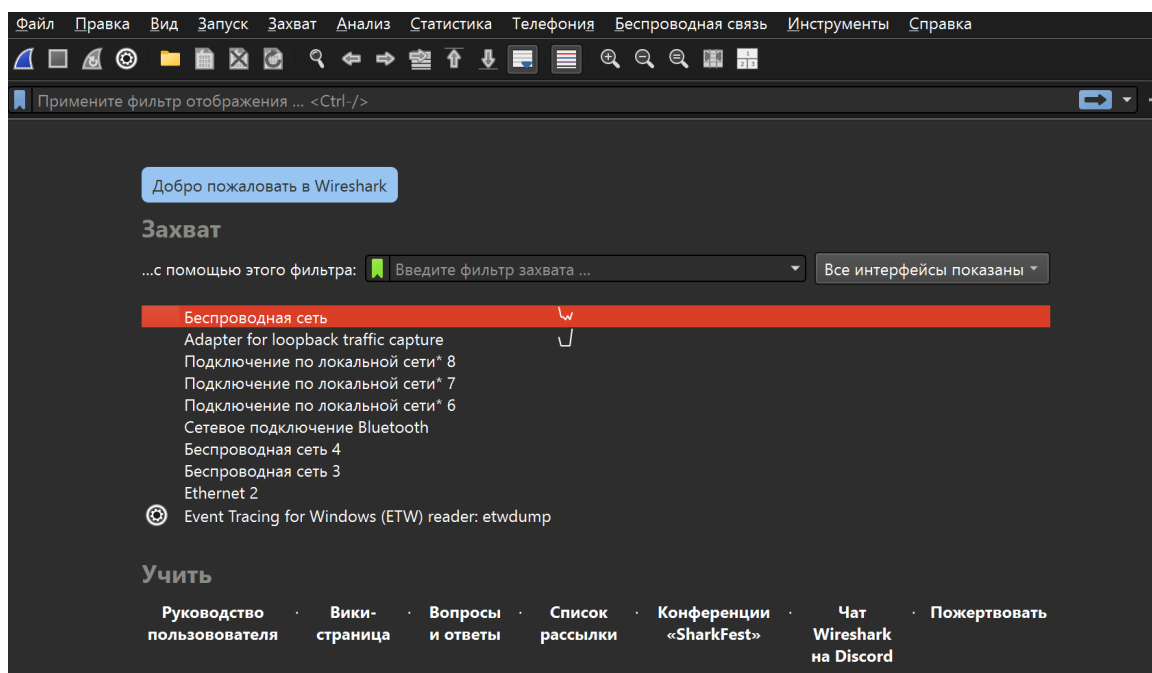


Рисунок 3.3: Запуск Wireshark и выбор интерфейса

Выполнена команда `ping 192.168.0.1 -n 4` для генерации ICMP трафика.

```
C:\Windows\System32>ping 192.168.0.1

Обмен пакетами с 192.168.0.1 по 32 байтами данных:
Ответ от 192.168.0.1: число байт=32 время=3мс TTL=64
Ответ от 192.168.0.1: число байт=32 время=6мс TTL=64
Ответ от 192.168.0.1: число байт=32 время=8мс TTL=64
Ответ от 192.168.0.1: число байт=32 время=7мс TTL=64

Статистика Ping для 192.168.0.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 3мсек, Максимальное = 8 мсек, Среднее = 6 мсек
```

Рисунок 3.4: Выполнение ping команды

После остановки захвата применен фильтр `arp or icmp` для отображения только ARP и ICMP пакетов.



Рисунок 3.5: Фильтрация ARP и ICMP пакетов

### 3.2.2 Анализ ICMP-запроса

Исследован ICMP-запрос (Echo request): - Длина кадра: 74 байта - MAC назначения: TPLink\_15:al:6c (5c:62:8b:15:al:6c) - шлюз - MAC источника: AzureWaveTec\_cf:c4:ce (c0:bf:be:cf:c4:ce) - компьютер - Тип Ethernet: Ethernet II

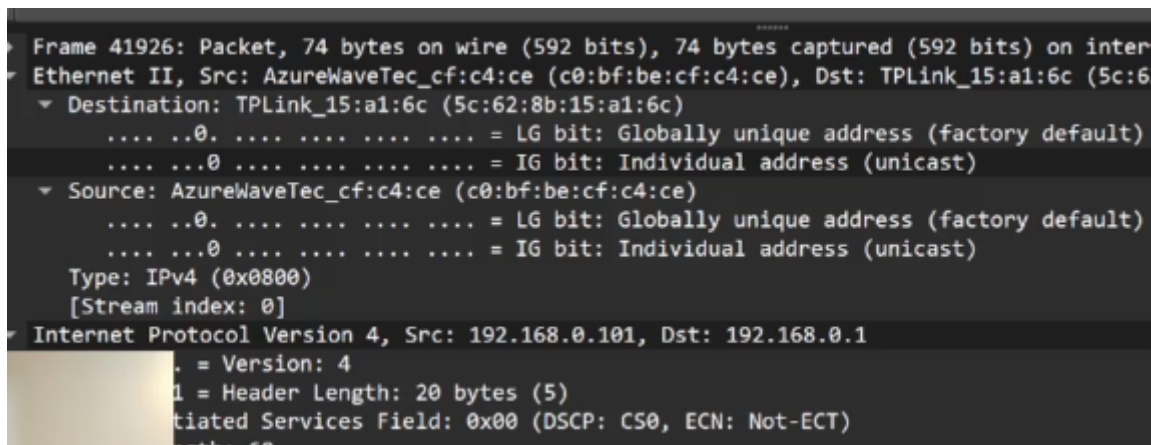


Рисунок 3.6: Анализ ICMP-запроса

### 3.2.3 Анализ ICMP-ответа

Исследован ICMP-ответ (Echo reply): - Длина кадра: 74 байта - MAC назначения: AzureWaveTec\_cf:c4:ce (c0:bf:be:cf:c4:ce) - компьютер - MAC источника: TPLink\_15:al:6c (5c:62:8b:15:al:6c) - шлюз - Тип Ethernet: Ethernet II

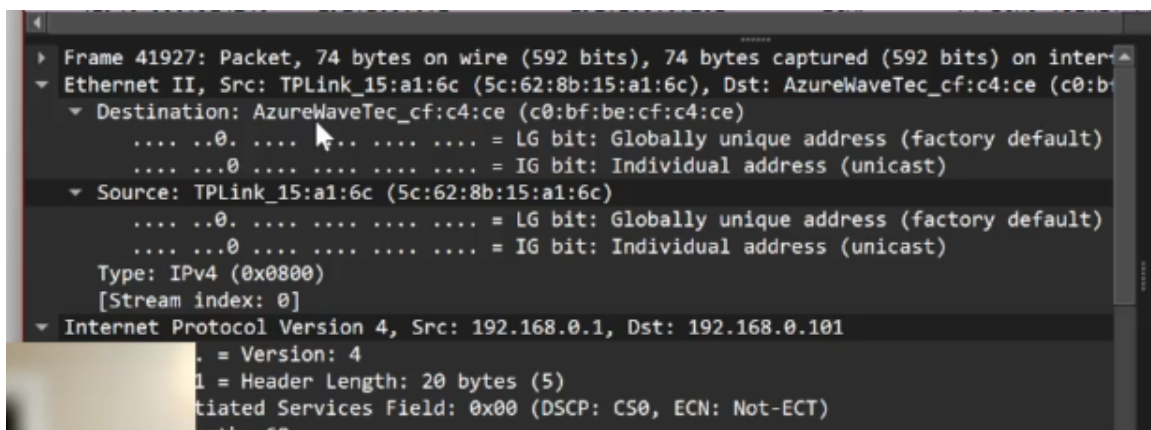


Рисунок 3.7: Анализ ICMP-ответа

### 3.2.4 Анализ ARP пакетов

Исследованы ARP запросы и ответы:

**ARP запрос:** - Отправитель MAC: TPLink\_15:a1:6c (шлюз) - Отправитель IP: 192.168.0.1 - Целевой MAC: 00:00:00:00:00:00 (неизвестен) - Целевой IP: 192.168.0.101

**ARP ответ:** - Отправитель MAC: AzureWaveTec\_cf:c4:ce (компьютер) - Отправитель IP: 192.168.0.101 - Целевой MAC: TPLink\_15:a1:6c (шлюз) - Целевой IP: 192.168.0.1

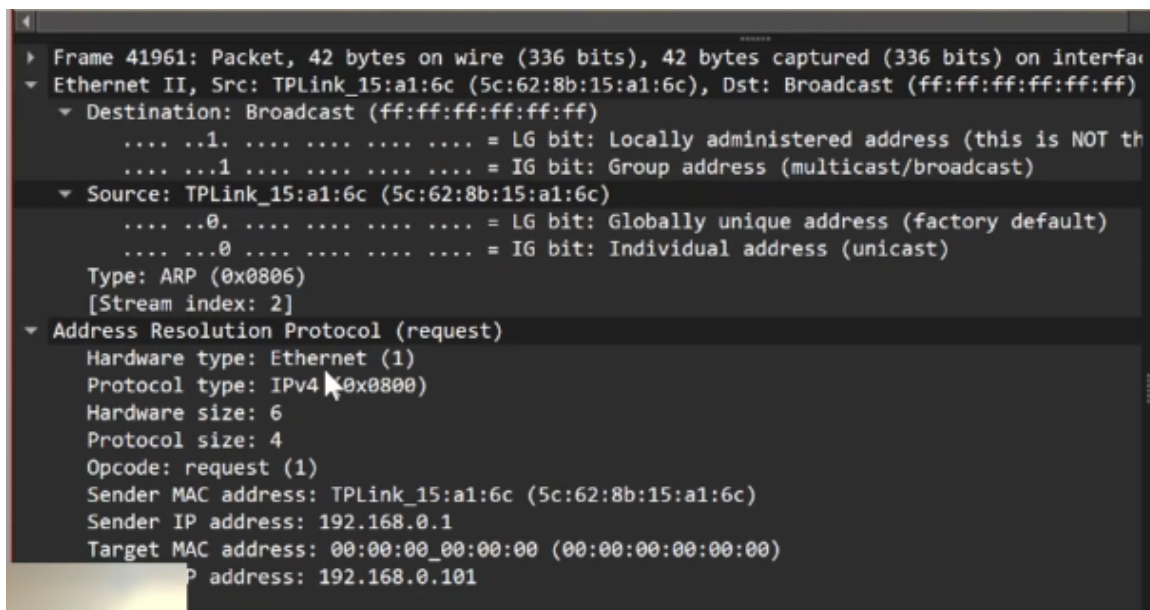


Рисунок 3.8: Анализ ARP пакетов

## 3.3 Анализ протоколов транспортного уровня

### 3.3.1 Захват TCP трафика

Выполнен захват TCP трафика при обращении к веб-сайтам. Применен фильтр для отображения TCP пакетов.

No.	Time	Source	Destination	Protocol	Length	Info
645	27.719773	192.168.0.101	146.75.118.172	HTTP	342	GET /msdownload/update/v3/static/trusteddr
653	27.759038	146.75.118.172	192.168.0.101	HTTP	257	HTTP/1.1 304 Not Modified
659	27.792098	192.168.0.101	64.233.164.94	HTTP	254	GET /r/r1.crl HTTP/1.1
662	27.808025	64.233.164.94	192.168.0.101	PKIX-C...	347	Certificate Revocation List
670	27.849813	192.168.0.101	104.76.25.39	HTTP	281	GET / HTTP/1.1
672	27.872898	104.76.25.39	192.168.0.101	HTTP	317	HTTP/1.1 304 Not Modified
673	27.879927	192.168.0.101	64.233.164.94	HTTP	256	GET /r/gsr1.crl HTTP/1.1
674	27.895900	64.233.164.94	192.168.0.101	HTTP	276	HTTP/1.1 304 Not Modified
675	27.908101	192.168.0.101	64.233.164.94	HTTP	254	GET /r/r4.crl HTTP/1.1
677	27.928284	64.233.164.94	192.168.0.101	PKIX-C...	1296	Certificate Revocation List
678	27.937400	192.168.0.101	146.75.118.172	HTTP	336	GET /msdownload/update/v3/static/trusteddr
680	27.976954	146.75.118.172	192.168.0.101	HTTP	256	HTTP/1.1 304 Not Modified
682	27.986091	192.168.0.101	146.75.118.172	HTTP	336	GET /msdownload/update/v3/static/trusteddr
684	28.025166	146.75.118.172	192.168.0.101	HTTP	257	HTTP/1.1 304 Not Modified
958	34.172853	192.168.0.101	146.75.118.172	HTTP	342	GET /msdownload/update/v3/static/trusteddr
960	34.213483	146.75.118.172	192.168.0.101	HTTP	257	HTTP/1.1 304 Not Modified
961	34.220932	192.168.0.101	146.75.118.172	HTTP	336	GET /msdownload/update/v3/static/trusteddr
969	34.260783	146.75.118.172	192.168.0.101	HTTP	256	HTTP/1.1 304 Not Modified

Рисунок 3.9: Захват TCP трафика

### 3.3.2 Анализ TCP handshake

Обнаружен и проанализирован трехэтапный handshake TCP:

**Пакет 26:** [SYN] - инициация соединения - Seq=0

**Пакет 30:** [SYN, ACK] - подтверждение от сервера - Seq=0, Ack=1

**Пакет 34:** [ACK] - завершение handshake - Seq=1, Ack=1

No.	Time	Source	Destination	Protocol	Length	Info
26	2.760229	192.168.0.101	192.168.0.1	TCP	66	49703 → 53 [SYN] Seq=0 Win=65535 Len=0 MS
30	2.764080	192.168.0.1	192.168.0.101	TCP	66	53 → 49703 [SYN, ACK] Seq=0 Ack=1 Win=292
34	2.764208	192.168.0.101	192.168.0.1	TCP	54	49703 → 53 [ACK] Seq=1 Ack=1 Win=65280 Le
36	2.764281	192.168.0.101	192.168.0.1	TCP	56	49703 → 53 [PSH, ACK] Seq=1 Ack=1 Win=652
37	2.764328	192.168.0.101	192.168.0.1	DNS	88	Standard query 0x8957 A gator.volces.com
40	2.768452	192.168.0.1	192.168.0.101	TCP	54	53 → 49703 [ACK] Seq=1 Ack=3 Win=29312 Le
41	2.768452	192.168.0.1	192.168.0.101	TCP	54	53 → 49703 [ACK] Seq=1 Ack=37 Win=29312 L
44	2.768452	192.168.0.1	192.168.0.101	DNS	1111	Standard query response 0x8957 A gator.vc
46	2.768733	192.168.0.101	192.168.0.1	TCP	54	49703 → 53 [FIN, ACK] Seq=37 Ack=1058 Win
49	2.772888	192.168.0.1	192.168.0.101	TCP	54	53 → 49703 [FIN, ACK] Seq=1058 Ack=38 Win
51	2.772976	192.168.0.101	192.168.0.1	TCP	54	49703 → 53 [ACK] Seq=38 Ack=1059 Win=6425

Рисунок 3.10: TCP handshake анализ

### 3.3.3 График потока TCP

Построен график потока TCP через меню Statistics → Flow Graph.

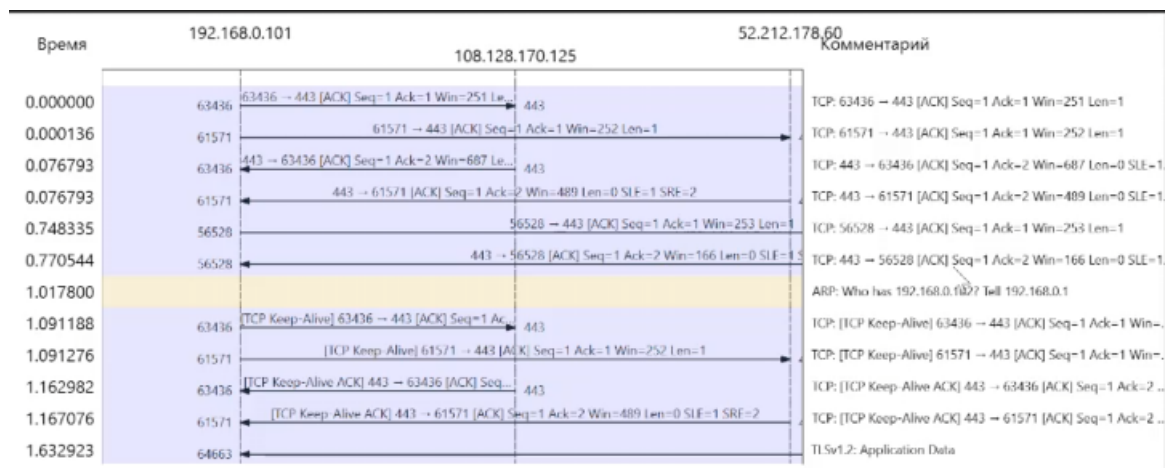


Рисунок 3.11: График потока TCP

На графике четко видны три этапа установления соединения и последующая передача данных.

## 4 Выводы

В ходе лабораторной работы успешно изучены принципы анализа сетевого трафика с помощью Wireshark. Освоены методы захвата и анализа кадров Ethernet, исследованы протоколы канального уровня (ARP, ICMP) и транспортного уровня (TCP). Практически подтвержден механизм трехэтапного handshake TCP. Полученные навыки позволяют проводить диагностику сетевых соединений и анализировать структуру сетевых пакетов на различных уровнях стека TCP/IP.