Лабораторная работа №3

Анализ трафика в Wireshark

Газизянов Владислав Альбертович

Содержание

Список иллюстраций

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.

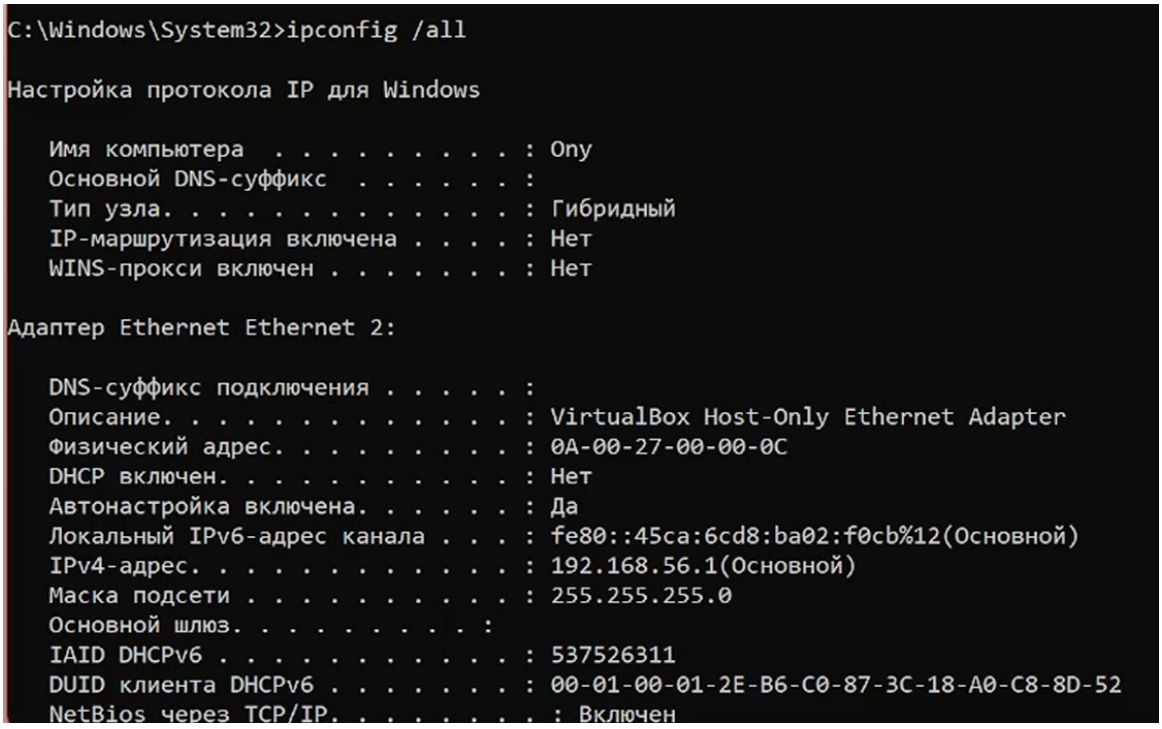

Рисунок 3.1: Вывод команды ipconfig /all

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

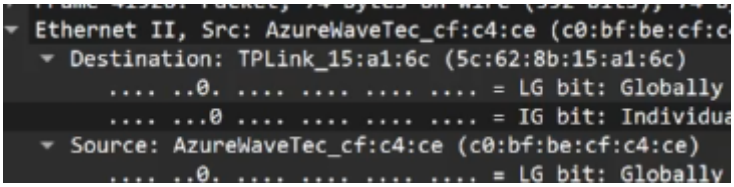

Рисунок 3.2: Структура MAC-адреса

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.

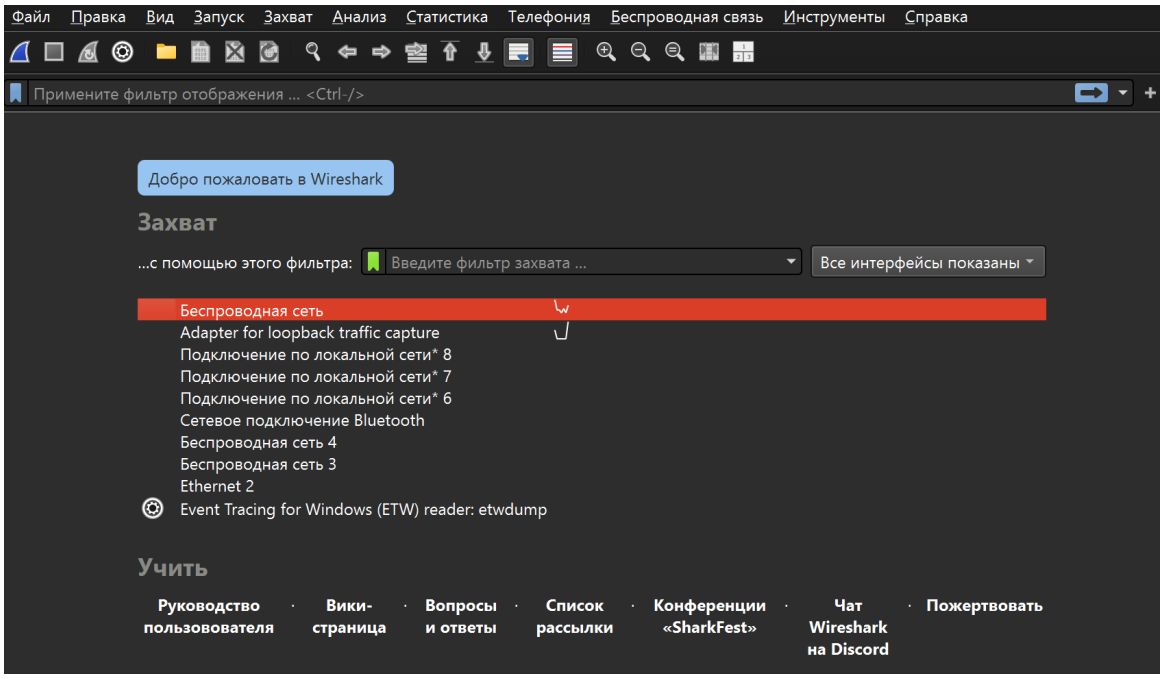

Рисунок 3.3: Запуск Wireshark и выбор интерфейса

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

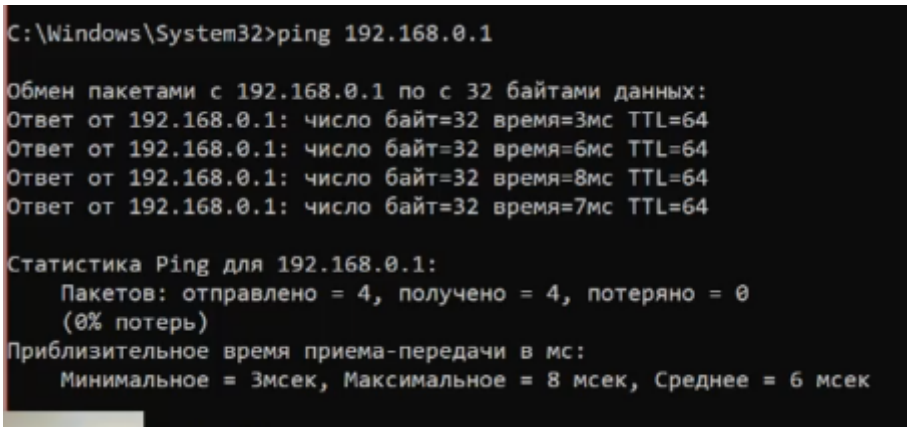

Рисунок 3.4: Выполнение ping команды

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

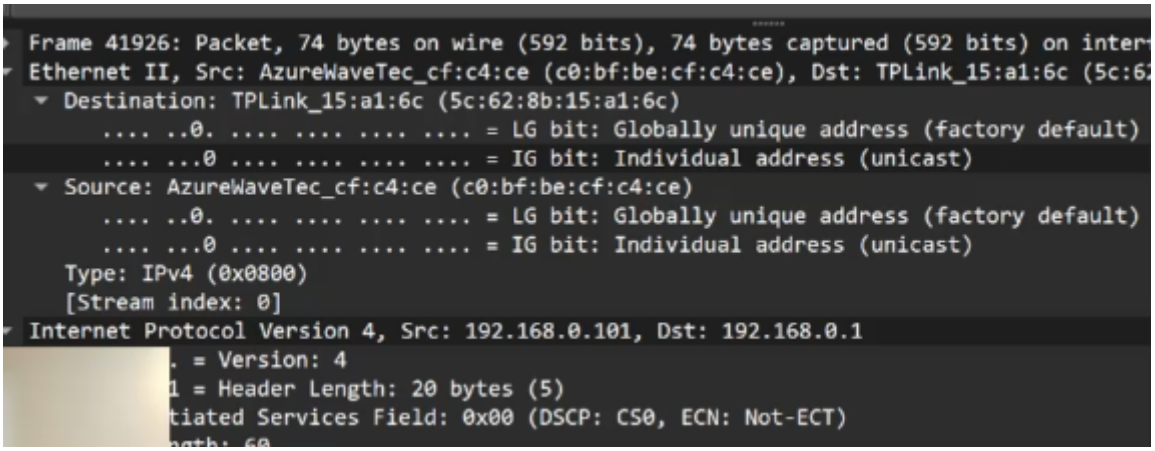

Рисунок 3.6: Анализ ICMP-запроса

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

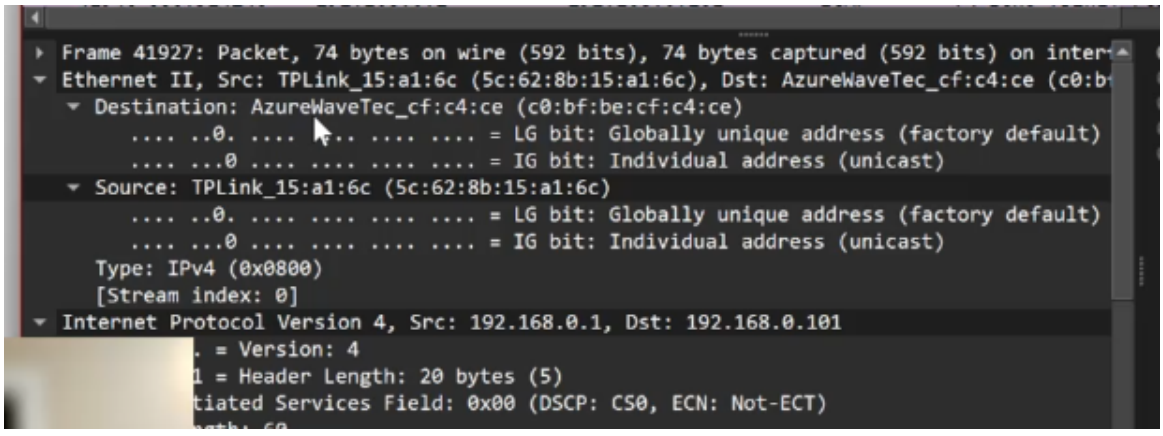

Рисунок 3.7: Анализ ICMP-ответа

3.2.4 Анализ ARP пакетов

Исследованы ARP запросы и ответы:

ARP запрос: - Отправитель MAC: TPlink_15:al: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:al:6c (шлюз) - Целевой IP: 192.168.0.1

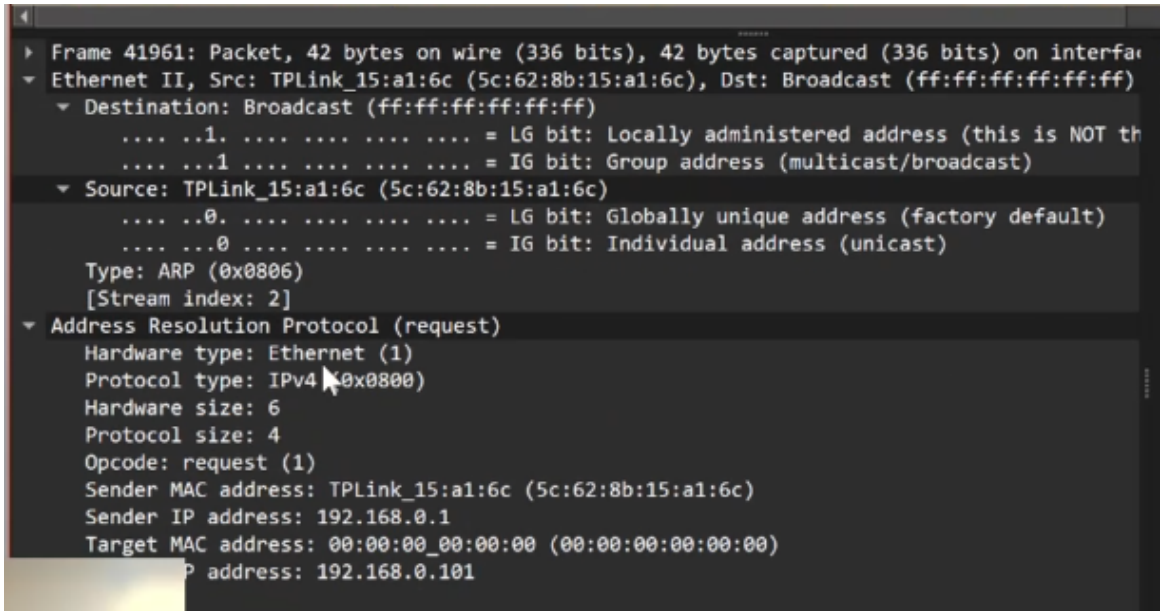

Рисунок 3.8: Анализ ARP пакетов

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.

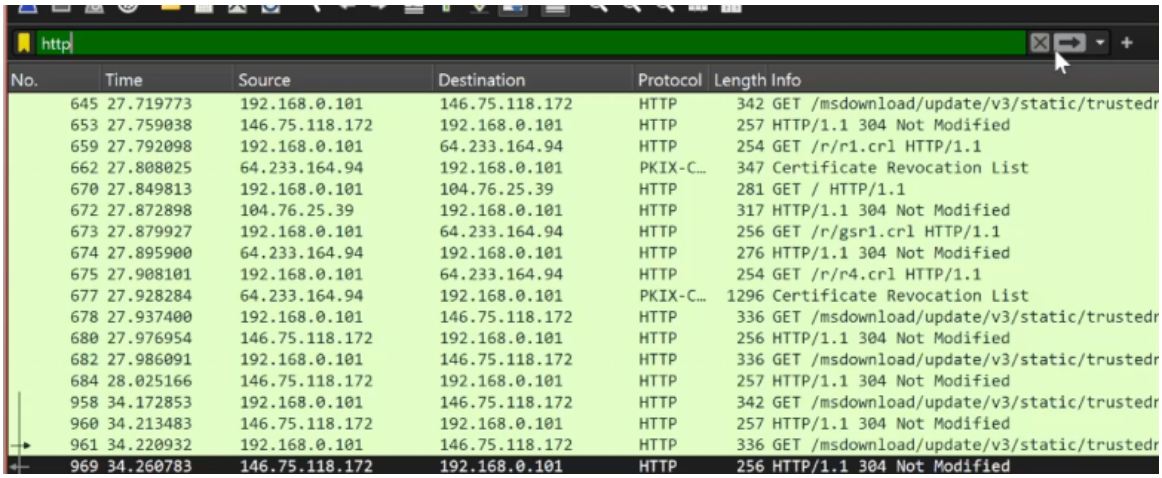

Рисунок 3.9: Захват TCP трафика

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

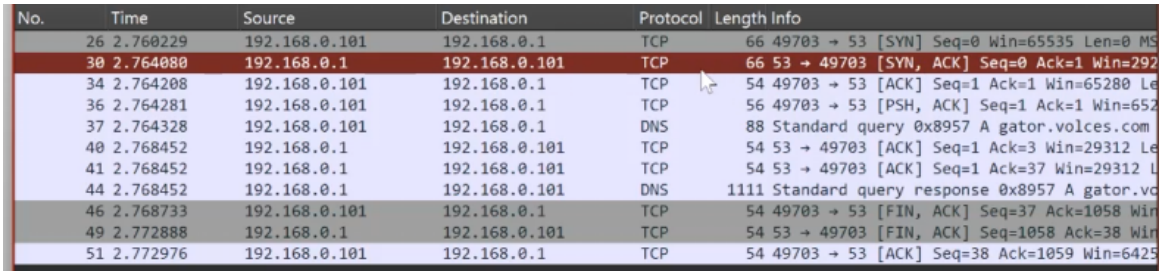

Рисунок 3.10: TCP handshake анализ

3.3.3 График потока TCP

Построен график потока TCP через меню Statistics → Flow Graph.

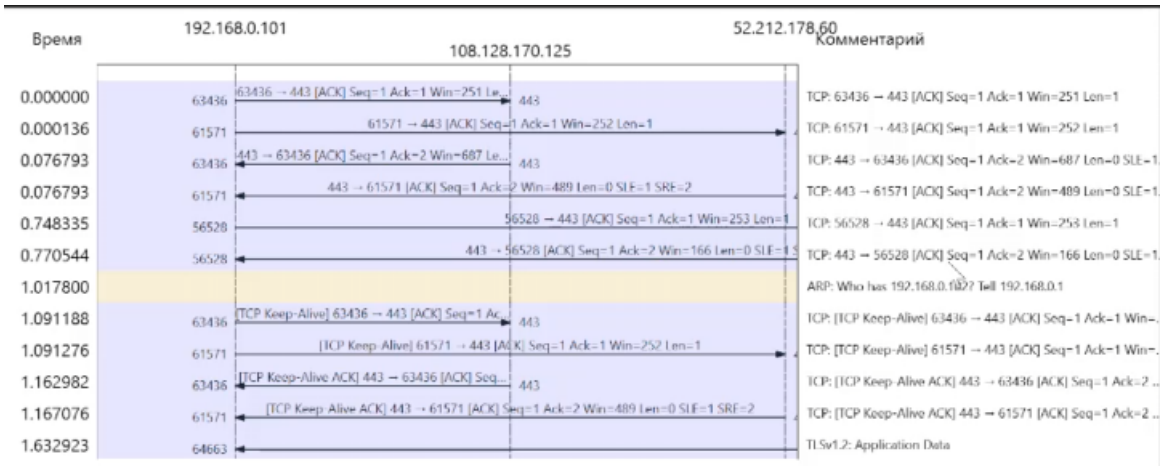

Рисунок 3.11: График потока TCP

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.