Лабораторная работа №3

Анализ трафика в Wireshark

Лисовская А. В.

18 декабря 2025

Российский университет дружбы народов, Москва, Россия

Докладчик

:::::::::::::: {.columns align=center} ::: {.column width=“70%”}

- Лисовская Арина Валерьевна
- Студент учебной группы
- Российский университет дружбы народов

::: ::: {.column width=“30%”}

Цель работы

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

Задачи

1. Изучить сетевые настройки ОС (`ipconfig`, `getmac`).
2. Проанализировать работу протоколов ICMP и ARP.
3. Исследовать структуру HTTP-трафика.
4. Провести анализ процесса установления соединения (handshake) TCP.

Выполнение работы: Сетевые настройки

Изучение конфигурации IP

Команда `ipconfig /all` выводит детальную информацию о сетевых интерфейсах: имя компьютера, настройки DHCP и IPv6-адрес канала.

```
PS C:\Users\Арина> ipconfig /all

Настройка протокола IP для Windows

   Имя компьютера  . . . . . . . . . : LAPTOP-5GUQC0PM
   Основной DNS-суффикс  . . . . . . :
   Тип узла. . . . . . . . . . . . . : Гибридный
   IP-маршрутизация включена . . . . : Нет
   WINS-прокси включен . . . . . . . : Нет
   Порядок просмотра суффиксов DNS . : rudn.ru

Адаптер Ethernet Ethernet 2:

   DNS-суффикс подключения . . . . . :
   Описание. . . . . . . . . . . . . : VirtualBox Host-Only Ethe
rnet Adapter
   Физический адрес. . . . . . . . . : 0A-00-27-00-00-03
   DHCP включен. . . . . . . . . . . : Нет
   Автонастройка включена. . . . . . : Да
   Локальный IPv6-адрес канала . . . : fe80::154b:8e54:709f:48cf
```

Определение MAC-адресов

С помощью утилиты GETMAC были определены физические адреса сетевых адаптеров и их текущее состояние (подключен/отключен).

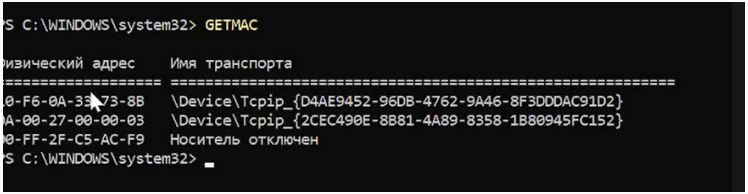
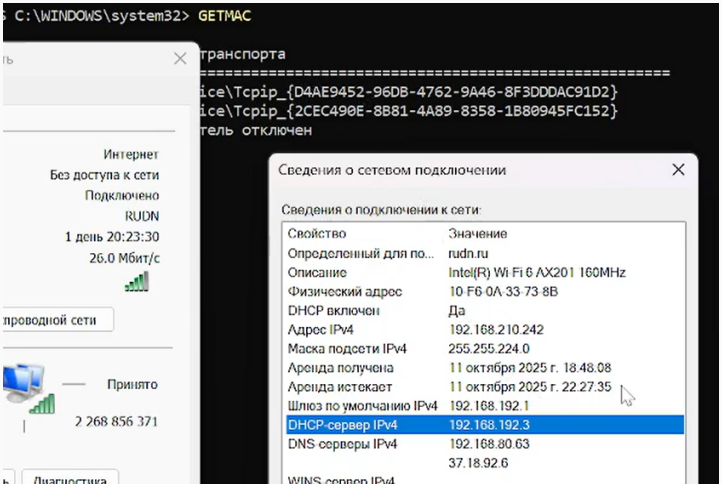


Рис. 2: Вывод GETMAC

Сведения о подключении (GUI)

Параметры сетевого адаптера Intel Wi-Fi и адрес шлюза (192.168.192.1) подтверждены через графический интерфейс ОС Windows.



Выполнение работы: Анализ трафика

Захват ICMP-пакетов

В Wireshark проанализирована структура кадра Ethernet II. На скриншоте виден эхо-запрос от клиента к шлюзу и ответный пакет.

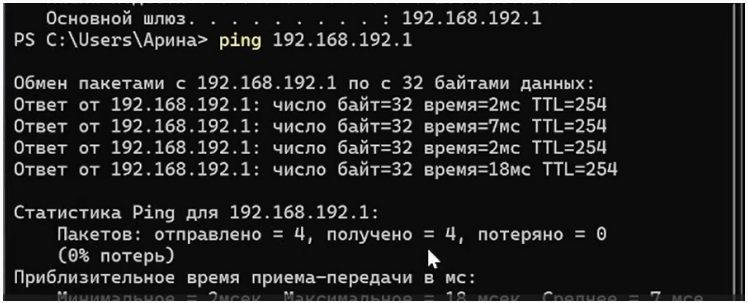


Рис. 4: Анализ ICMP в Wireshark

Пинг внешнего ресурса

Выполнен запрос к домену `rudn.ru`. IP-адрес узла — 192.168.80.63. Это действие позволило зафиксировать процесс разрешения имен.

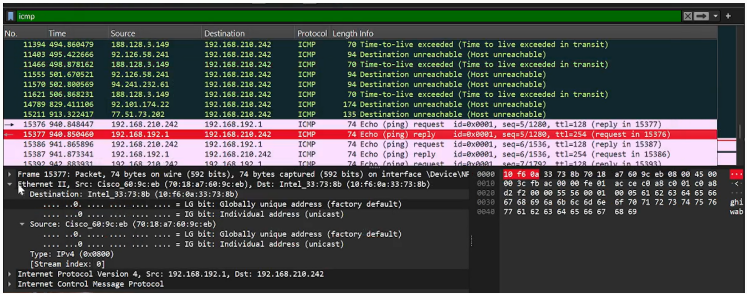


Рис. 5: Пинг rudn.ru

Анализ ARP-пакетов

Пример широковещательного ARP-пакета (Gratuitous ARP). Использовался для обновления информации о физическом адресе в локальной сети.

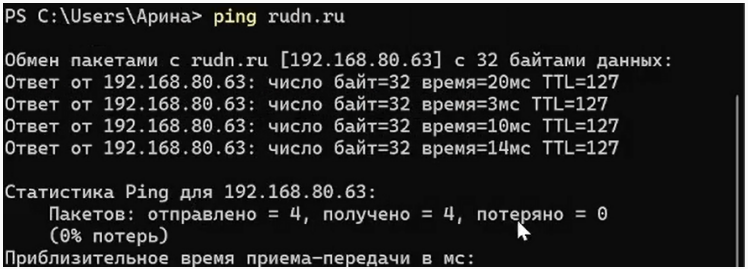


Рис. 6: Захват ARP

Выполнение работы: TCP и HTTP

Работа с протоколом HTTP

Для генерации трафика прикладного уровня осуществлен переход на сайт `info.cern.ch`. Зафиксированы GET-запросы и ответы сервера.

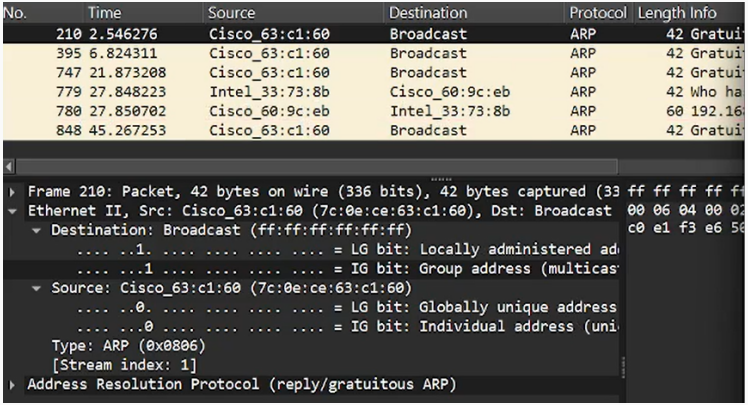


Рис. 7: Сайт info.cern.ch

Анализ TCP Handshake

Наглядная иллюстрация установления соединения. Видны флаги SYN от клиента, SYN-ACK от сервера и завершающий ACK от клиента.

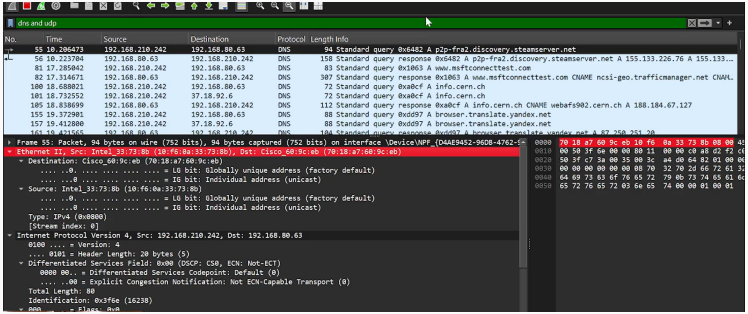


Рис. 8: TCP Handshake

Выводы

- Освоены практические навыки работы в Wireshark.
- Изучена структура кадров канального и пакетов сетевого уровней.
- Проанализирован процесс «трехступенчатого рукопожатия» TCP.
- Научился определять OUI производителя по MAC-адресу.