Отчёт по лабораторной работе 3

Анализ трафика в Wireshark

Цвелев С.А. НПИбд-02-22

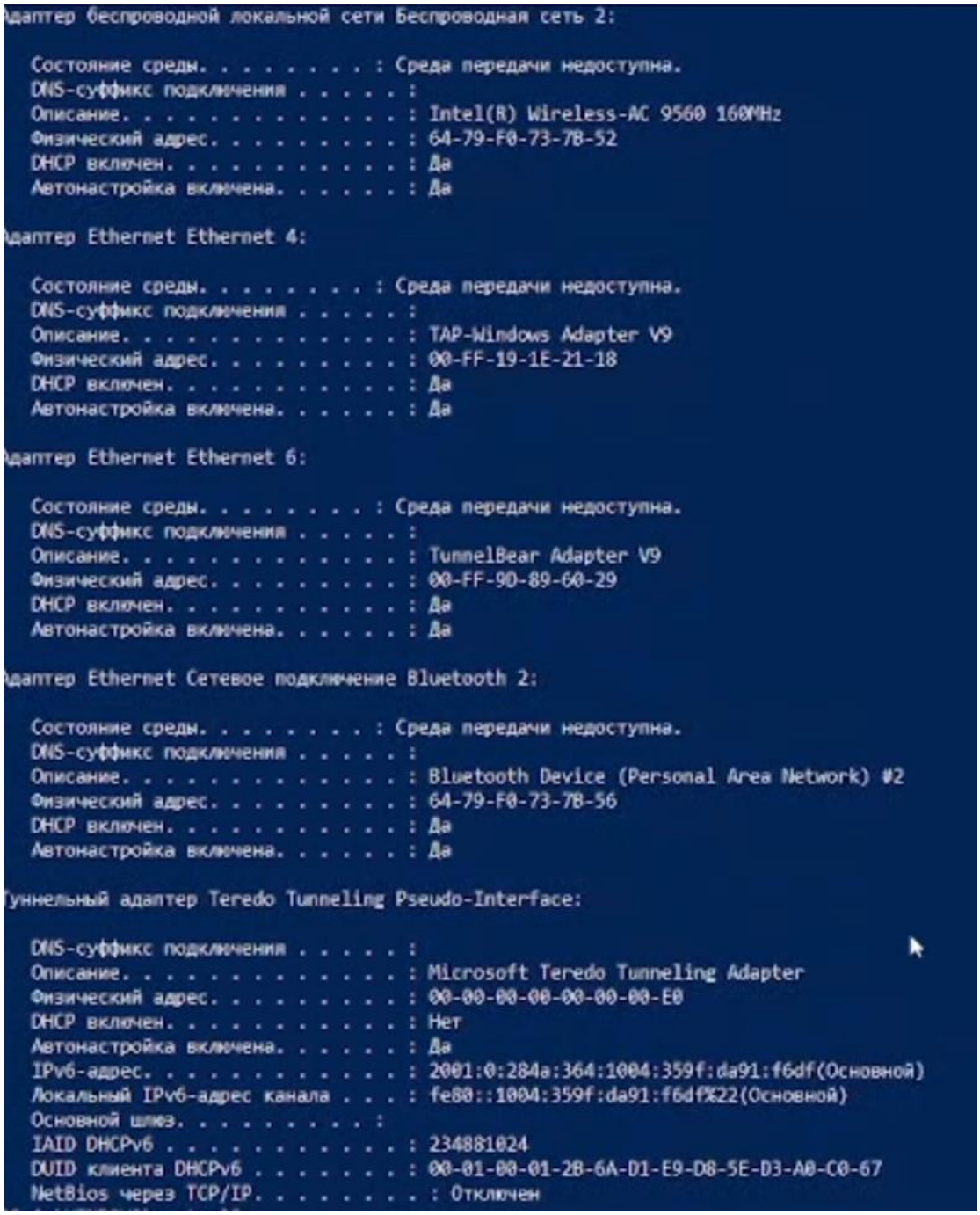
Содержание

1 Цель работы

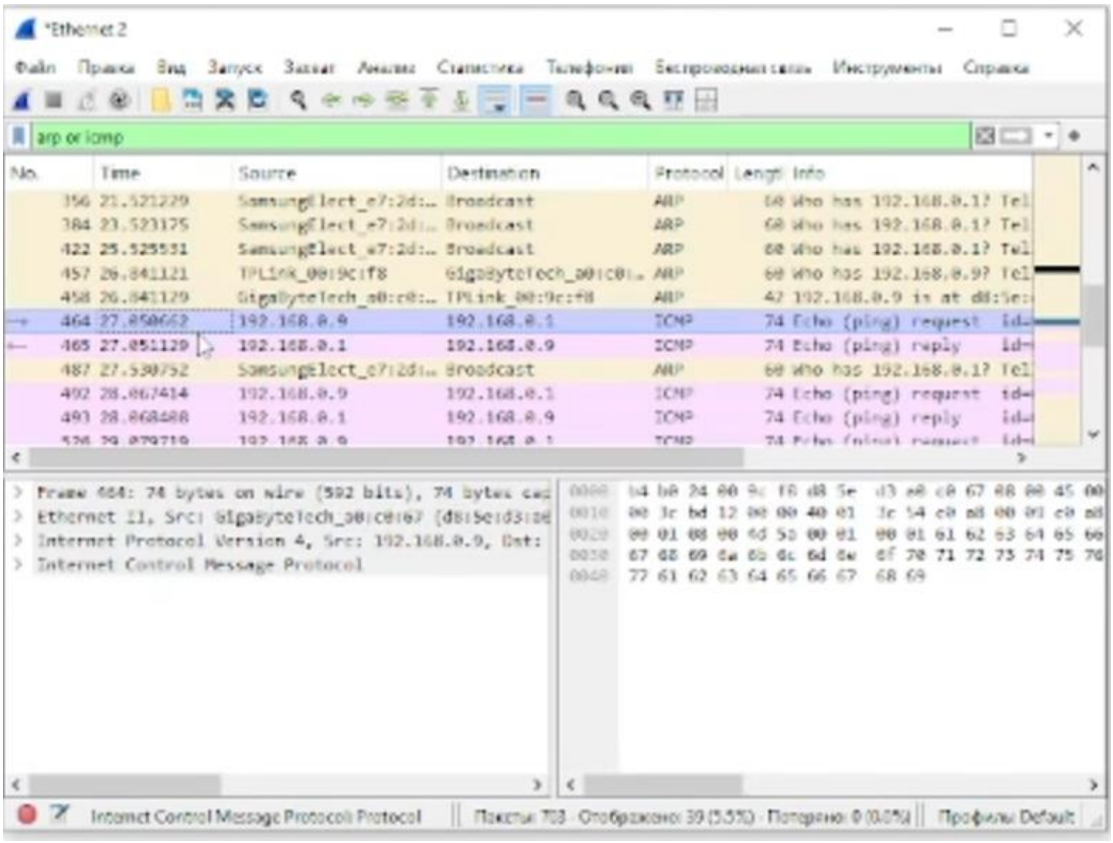
Изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.

2 Ход работы

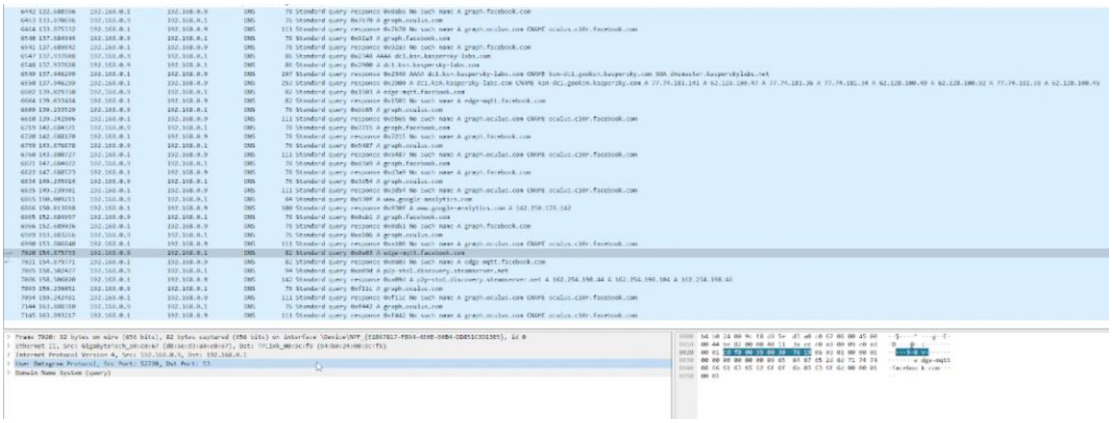
Мы вводим команду ipconfig, которая показывает информацию о текущих сетевых соединениях. Добавив /all, мы узнаем ещё больше информации. Вместе с этим, мы определяем MAC-адрес.



Закончив, мы переходим к Wireshark. Он был предварительно установлен, и нам требовалось лишь начать захват трафика. С помощью ipconfig мы находим адрес активного сетевого подключения и пропинговываем его. Помимо этого, мы ещё и пропингуем какой-то известный нам адрес (я взял адрес yandex.ru).



Мы начинаем новый захват трафика. Заходим на какой-либо из сайтов с протоколом HTTP (поначалу это сайт CERN, в дальнейших заданиях я заходил на сайт правительства России). В Wireshark мы анализируем информацию по этим запросам.



Напоследок, нам требовалось проанализировать handshake протокола TCP. К сожалению, эти самые handshake у меня не отображались...

3 Вывод

Мы изучили посредством Wireshark кадры Ethernet, проанализировали PDU протоколы транспортного и прикладного уровней стека TCP/IP.