

# 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.

```

Адаптер беспроводной локальной сети Беспроводная сеть 2:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Intel(R) Wireless-AC 9560 160MHz
Физический адрес. . . . . : 64-79-F8-73-78-52
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Адаптер Ethernet Ethernet 4:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : TAP-Windows Adapter V9
Физический адрес. . . . . : 00-FF-19-1E-21-18
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Адаптер Ethernet Ethernet 6:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : TunnelBear Adapter V9
Физический адрес. . . . . : 00-FF-90-89-60-29
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Адаптер Ethernet Сетевое подключение Bluetooth 2:

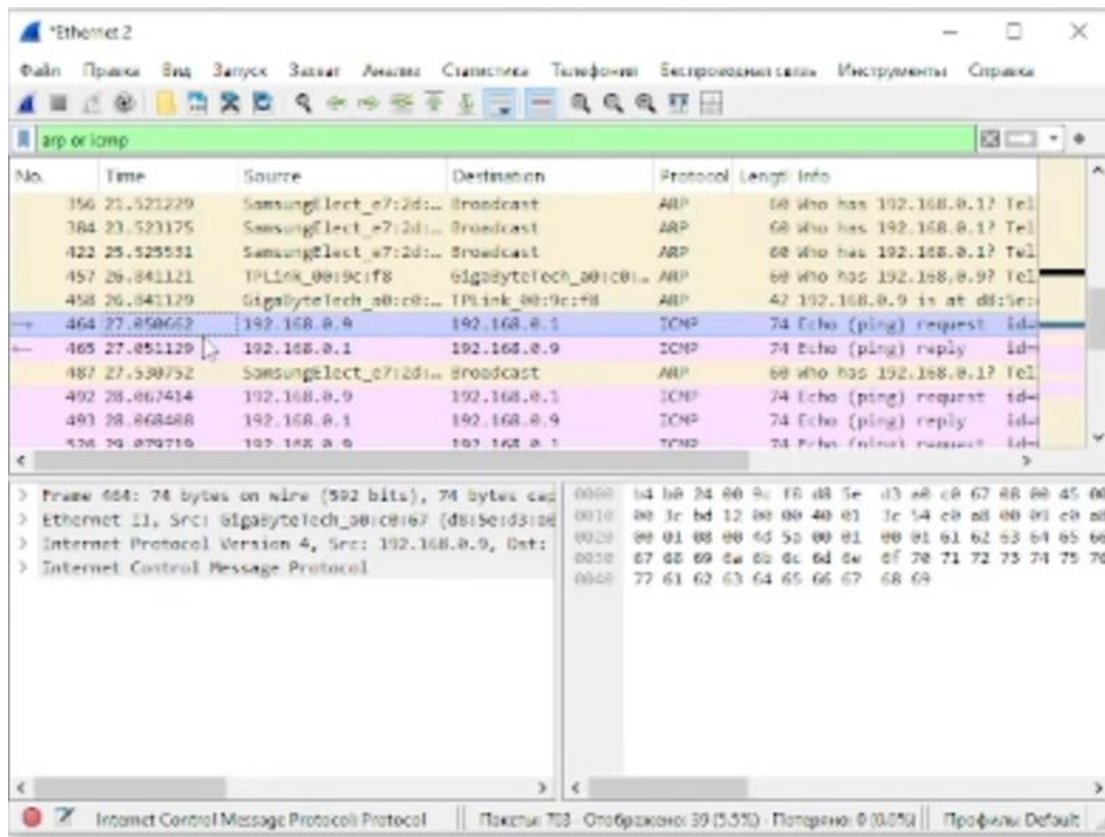
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Bluetooth Device (Personal Area Network) #2
Физический адрес. . . . . : 64-79-F8-73-78-56
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Туннельный адаптер Teredo Tunneling Pseudo-Interface:

DNS-суффикс подключения . . . . . :
Описание. . . . . : Microsoft Teredo Tunneling Adapter
Физический адрес. . . . . : 00-00-00-00-00-00-E0
DHCP включен. . . . . : Нет
Автонастройка включена. . . . . : Да
IPv6-адрес. . . . . : 2001:0:284a:364:1004:359f:da91:f6df(Основной)
Локальный IPv6-адрес канала . . . : fe80::1004:359f:da91:f6df%22(Основной)
Основной шлюз. . . . . :
IAID DHCPv6 . . . . . : 234881024
DUID клиента DHCPv6 . . . . . : 00-01-00-01-28-6A-D1-E9-D8-5E-D3-A0-C0-67
NetBios через TCP/IP. . . . . : Отключен

```

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.

