Лабораторная работа. Использование программы Wireshark для просмотра сетевого трафика

Цель работы:

Научиться собирать и анализировать данные протокола ICMP в программе Wireshark при передаче данных в локальной сети и при передаче данных в удаленную сеть.

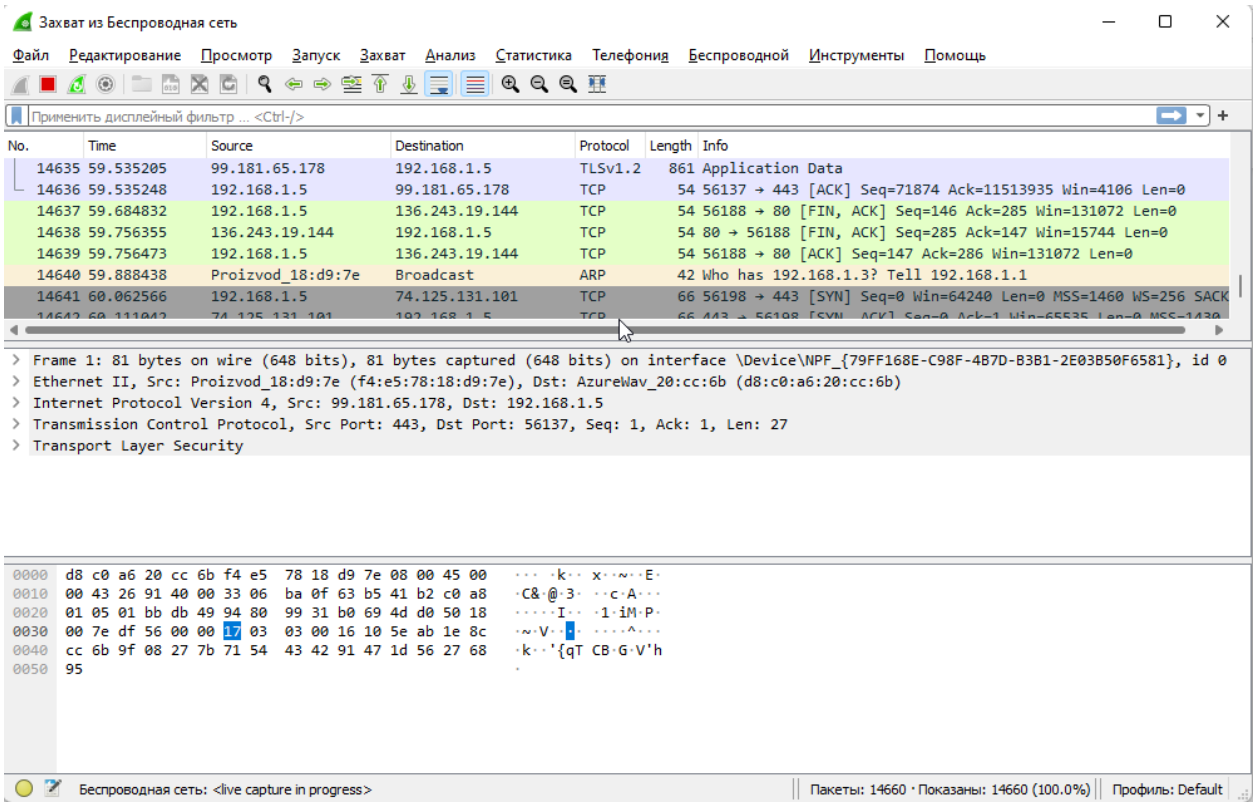
Ход работы:

Часть 1. Сбор и анализ данных протокола ICMP в программе Wireshark при передаче данных в локальной сети.

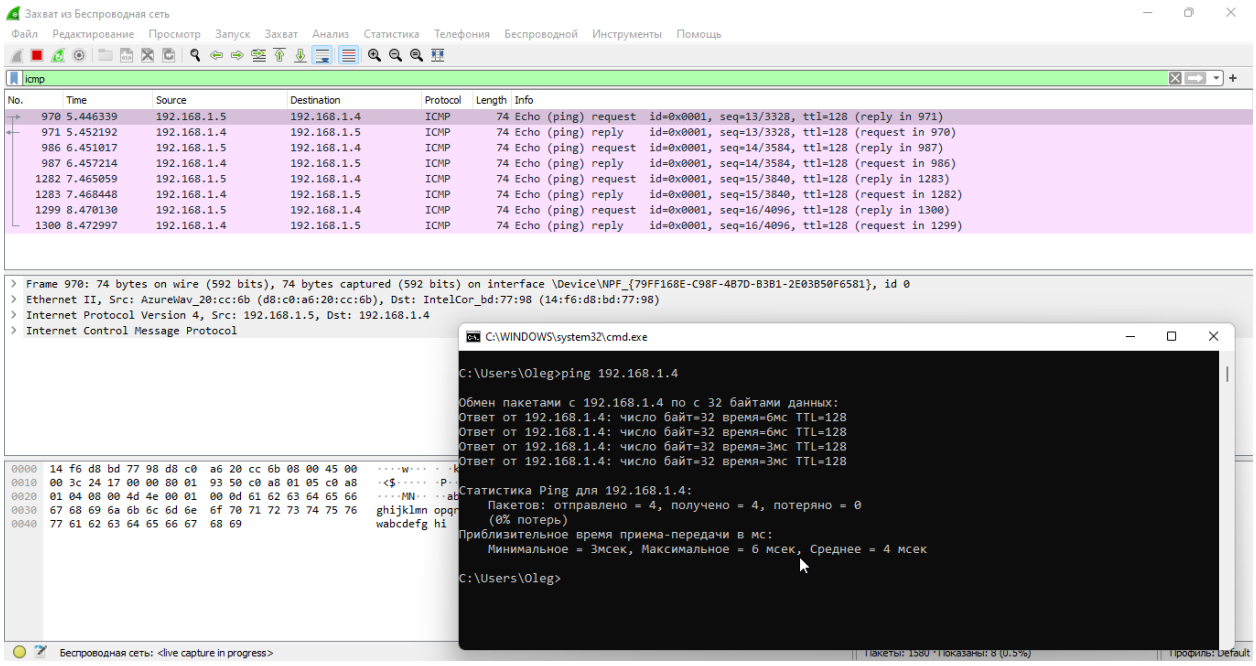
Определим адреса интерфейсов ПК, с помощью команды ipconfig /all

```
DNS-суффикс подключения . . . . . :
Описание. . . . . . . . . . . . . : Realtek RTL8723DE 802.11b/g/n PCIe Adapter
Физический адрес. . . . . . . . . : D8-C0-A6-20-CC-6B
DHCP включен. . . . . . . . . . . : Да
Автонастройка включена. . . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::3d8a:4da4:bb5c:56eb%10(Основной)
IPv4-адрес. . . . . . . . . . . . : 192.168.1.5(Основной)
Маска подсети . . . . . . . . . . : 255.255.255.0
```

Предварительно загрузив и установив, запустим программу Wireshark. Выберем интерфейс и убедившись в его правильности запустим захват данных.



Применим фильтр для того, чтобы видеть только единицы данных протокола ICMP. Затем отправим ping на IP-адрес другого компьютера.



Остановим захват и проанализируем данные.
Выбрав кадр отправки пакета (request) и открыв вкладку Ethernet II и ответим на поставленные вопросы.

Совпадает ли MAC-адрес источника с интерфейсом вашего компьютера? **Да**

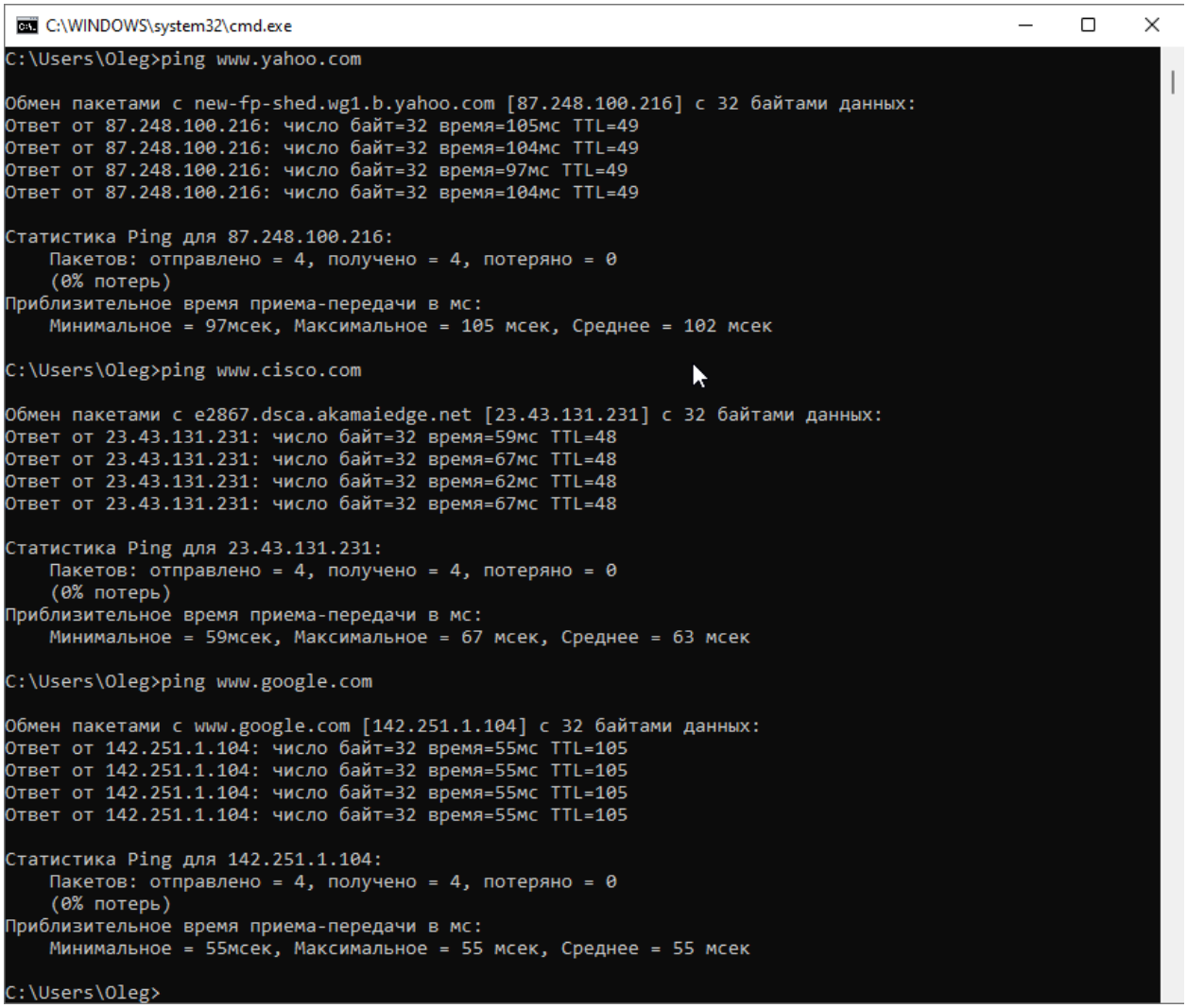
Совпадает ли MAC-адрес назначения в программе Wireshark с MAC-адресом другого учащегося? **Да**

Как ваш ПК определил MAC-адрес другого ПК, на который был отправлен эхо-запрос с помощью команды ping? **При помощи протокола ARP. Для того, чтобы обменяться данными по сети Ethernet компьютерам нужно знать MAC адрес друг друга, так как сеть Ethernet не работает с IP-адресами. При запросе компьютер №1 обращается по IP к компьютеру №2, сообщает свой MAC-адрес и запрашивает MAC-адрес компьютера №2.**

Часть 2. Сбор и анализ данных протокола ICMP в программе Wireshark при передаче данных в удаленную сеть

Активируем захват данных и отправим эхо-запрос с помощью команды ping на три URL-адреса, указанных веб-сайтов:

1) www.yahoo.com
2) www.cisco.com
3) www.google.com



Остановим захват данных, проанализируем и ответим на поставленные вопросы:

a. Указать IP- и MAC-адреса для трех веб-сайтов:

1) IP: 87.248.100.216 MAC: f4:e5:78:18:d9:7e

2) IP: 23.43.131.231 MAC: f4:e5:78:18:d9:7e

3) IP: 142.251.1.104 MAC: f4:e5:78:18:d9:7e

b. Какова существенная особенность этих данных?

Все адреса имеют одинаковый MAC-адрес.

c. Как эта информация отличается от данных, полученных в результате эхо-запросов локальных узлов в части 1?

В первой части показывается MAC-адрес компьютера находящегося в локальной сети, во второй части отображается MAC-адрес сетевого шлюза.

d. Почему программа Wireshark показывает фактические MAC-адреса локальных узлов, но не показывает фактические MAC-адреса удаленных узлов?

Потому что IP-адрес на который отправляется ping находится в другой сети доступ к которой осуществляется через локальный узел.