

Использование программы Wireshark для просмотра сетевого трафика

Отчет по лабораторной работе

ФИО: Вакарчук Арсений Александрович

Группа: АТ-12

Академическая группа: РИ-230914

Преподаватель: Присяжный Алексей Владимирович, Ваулин Сергей Степанович

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

Шаг 1: Определите адреса интерфейсов вашего ПК.

- а. Откройте окно командной строки, введите команду **ipconfig /all** и нажмите клавишу ввода. Добавьте скриншот окна командной строки с результатом работы команды.

```
Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . : IGD_Rostelecom
Описание. . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Физический адрес. . . . . : 98-59-7A-E7-E9-9C
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
IPv4-адрес. . . . . : 192.168.0.4(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 9 марта 2025 г. 21:15:15
Срок аренды истекает. . . . . : 10 марта 2025 г. 1:15:15
Основной шлюз. . . . . : 192.168.0.1
DHCP-сервер. . . . . : 192.168.0.1
DNS-серверы. . . . . : 192.168.0.1
                        0.0.0.0
                        0.0.0.0
NetBios через TCP/IP. . . . . : Включен
```

- б. Запишите IP-адрес интерфейса ПК и MAC-адрес (физический адрес).

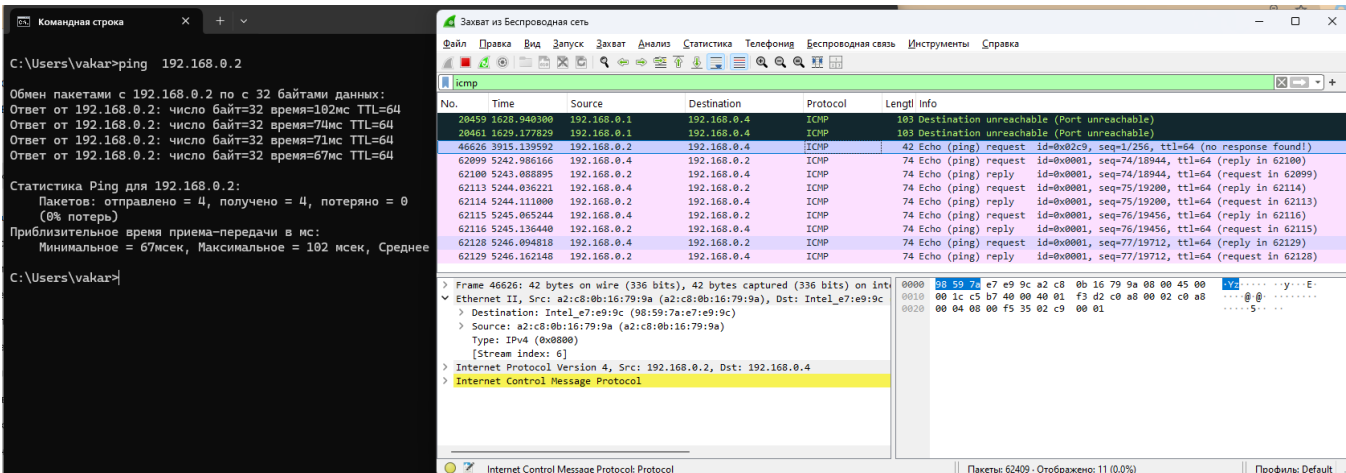
IP-адрес	192.168.0.4
MAC-адрес	98-59-7A-E7-E9-9C

- с. Обменяйтесь IP-адресами ПК с другими учащимися, но пока что не сообщайте им свой MAC-адрес. Или определите IP-адрес другого Вашего устройства (например, смартфона). Узел должен быть подключен к той же локальной сети. Добавьте скриншот.

Интерфейс: 192.168.0.4 --- 0x5		
адрес в Интернете	Физический адрес	Тип
192.168.0.1	68-13-e2-2c-9d-90	динамический
192.168.0.2	a2-c8-0b-16-79-9a	динамический
192.168.0.8	04-7c-16-a4-c9-2d	динамический
192.168.0.255	ff-ff-ff-ff-ff-ff	статический
224.0.0.2	01-00-5e-00-00-02	статический
224.0.0.22	01-00-5e-00-00-16	статический
224.0.0.251	01-00-5e-00-00-fb	статический
224.0.0.252	01-00-5e-00-00-fc	статический
239.255.255.250	01-00-5e-7f-ff-fa	статический
255.255.255.255	ff-ff-ff-ff-ff-ff	статический

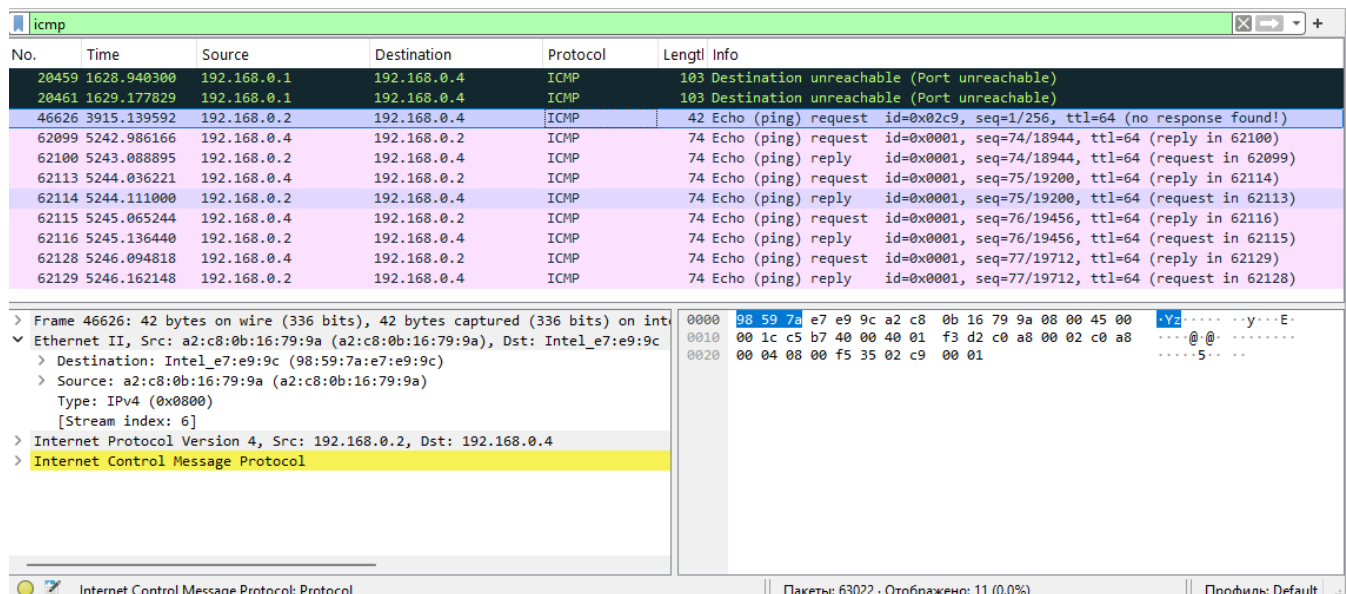
Шаг 2: Запустите программу Wireshark и начните сбор данных.

Начните сбор данных в программе Wireshark. Примените фильтр для отображения единиц данных протокола ICMP. Откройте окно командной строки и отправьте эхо-запрос на IP-адрес устройства, указанного в шаг 1, пункт с. Добавьте скриншот программы Wireshark и командной строки.



Шаг 3: Изучите полученные данные.

Выберите кадр PDU первого запроса ICMP. Нажмите на символ + слева от строки «Ethernet II», чтобы увидеть MAC-адреса источника и назначения. Добавьте скриншот окна Wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
20459	1628.940300	192.168.0.1	192.168.0.4	ICMP	103	Destination unreachable (Port unreachable)
20461	1629.177829	192.168.0.1	192.168.0.4	ICMP	103	Destination unreachable (Port unreachable)
46626	3915.139592	192.168.0.2	192.168.0.4	ICMP	42	Echo (ping) request id=0x02c9, seq=1/256, ttl=64 (no response found!)
62099	5242.986166	192.168.0.4	192.168.0.2	ICMP	74	Echo (ping) request id=0x0001, seq=74/18944, ttl=64 (reply in 62100)
62100	5243.088895	192.168.0.2	192.168.0.4	ICMP	74	Echo (ping) reply id=0x0001, seq=74/18944, ttl=64 (request in 62099)
62113	5244.036221	192.168.0.4	192.168.0.2	ICMP	74	Echo (ping) request id=0x0001, seq=75/19200, ttl=64 (reply in 62114)
62114	5244.111000	192.168.0.2	192.168.0.4	ICMP	74	Echo (ping) reply id=0x0001, seq=75/19200, ttl=64 (request in 62113)
62115	5245.065244	192.168.0.4	192.168.0.2	ICMP	74	Echo (ping) request id=0x0001, seq=76/19456, ttl=64 (reply in 62116)
62116	5245.136440	192.168.0.2	192.168.0.4	ICMP	74	Echo (ping) reply id=0x0001, seq=76/19456, ttl=64 (request in 62115)
62128	5246.094818	192.168.0.4	192.168.0.2	ICMP	74	Echo (ping) request id=0x0001, seq=77/19712, ttl=64 (reply in 62129)
62129	5246.162148	192.168.0.2	192.168.0.4	ICMP	74	Echo (ping) reply id=0x0001, seq=77/19712, ttl=64 (request in 62128)

> Frame 46626: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: a2:c8:0b:16:79:9a (a2:c8:0b:16:79:9a), Dst: Intel_e7:e9:9c: (98:59:7a:e7:e9:9c)
> Destination: Intel_e7:e9:9c (98:59:7a:e7:e9:9c)
> Source: a2:c8:0b:16:79:9a (a2:c8:0b:16:79:9a)
Type: IPv4 (0x0800)
[Stream index: 6]
> Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.4
> Internet Control Message Protocol

0000 98 59 7a e7 e9 9c a2 c8 0b 16 79 9a 08 00 45 00 ...y...E-
0010 00 1c c5 b7 40 00 40 01 f3 d2 c0 a8 00 02 c0 a8 ...@.@:
0020 00 04 08 00 f5 35 02 c9 00 015...

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?

Сначала он отправил **ARP-запрос** (Address Resolution Protocol). Получив ответ, добавил MAC-адрес в ARP-кеш.

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

Шаг 1: Запустите захват данных в интерфейсе.

Активировав захват данных, отправьте эхо-запрос с помощью команды ping на следующие три URL-адреса веб-сайтов:

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

Добавьте скриншот командной строки с результатом выполнения эхо-запросов.

```
C:\Users\vakar>ping www.yahoo.com
```

```
Обмен пакетами с me-uscpi-cf-www.g06.yahoodns.net [87.248.119.252] с 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
```

```
Статистика Ping для 87.248.119.252:
```

```
Пакетов: отправлено = 4, получено = 0, потеряно = 4
(100% потерь)
```

```
C:\Users\vakar>ping www.cisco.com
```

```
Обмен пакетами с e2867.dsca.akamaiedge.net [23.52.86.15] с 32 байтами данных:
```

```
Ответ от 23.52.86.15: число байт=32 время=60мс TTL=55
```

```
Ответ от 23.52.86.15: число байт=32 время=53мс TTL=55
```

```
Ответ от 23.52.86.15: число байт=32 время=56мс TTL=55
```

```
Ответ от 23.52.86.15: число байт=32 время=55мс TTL=55
```

```
Статистика Ping для 23.52.86.15:
```

```
Пакетов: отправлено = 4, получено = 4, потеряно = 0
(0% потерь)
```

```
Приблизительное время приема-передачи в мс:
```

```
Минимальное = 53мсек, Максимальное = 60 мсек, Среднее = 56 мсек
```

```
C:\Users\vakar>ping www.google.com
```

```
Обмен пакетами с www.google.com [173.194.73.106] с 32 байтами данных:
```

```
Ответ от 173.194.73.106: число байт=32 время=48мс TTL=106
```

```
Ответ от 173.194.73.106: число байт=32 время=48мс TTL=106
```

```
Ответ от 173.194.73.106: число байт=32 время=46мс TTL=106
```

```
Ответ от 173.194.73.106: число байт=32 время=46мс TTL=106
```

```
Статистика Ping для 173.194.73.106:
```

```
Пакетов: отправлено = 4, получено = 4, потеряно = 0
(0% потерь)
```

```
Приблизительное время приема-передачи в мс:
```

```
Минимальное = 46мсек, Максимальное = 48 мсек, Среднее = 47 мсек
```

Шаг 2: Изучите и проанализируйте данные, полученные от удаленных узлов.

- а. Просмотрите собранные данные в программе Wireshark и изучите IP- и MAC-адреса трех веб-сайтов, на которые вы отправили эхо-запросы. Ниже в оставленном месте укажите IP- и MAC-адреса назначения для всех трех веб-сайтов.

1-й адрес: IP не удалось получить ответ от адреса MAC не удалось получить ответ от адреса

2-й адрес: IP: 23.52.86.15 MAC: 68:13:e2:2c:9d:90

3-й адрес: IP: 173.194.73.106 MAC: 68:13:e2:2c:9d:90

- б. Какова существенная особенность этих данных?

У всех удаленных узлов (веб-сайтов) MAC-адрес одинаковый (68:13:e2:2c:9d:90).

Это MAC-адрес роутера (шлюза), через который отправляются пакеты в интернет.

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

Локальные узлы (ПК в одной сети) → MAC-адреса принадлежат конечным устройствам.

Удаленные узлы (веб-сайты) → Wireshark видит только MAC-адрес роутера, а не серверов сайтов.

Вопросы для повторения (на каждый вопрос необходим подробный ответ)

Для чего в компьютерных сетях используются IP- и MAC-адреса?

IP-адрес (логический) → используется для маршрутизации данных между сетями (локальными и глобальными).

MAC-адрес (физический) → нужен для передачи данных внутри одной сети (например, в Wi-Fi или Ethernet).

В локальной сети устройства обмениваются MAC-адресами через протокол ARP.

При выходе в интернет данные передаются через маршрутизатор, и его MAC-адрес подставляется в кадры.

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

В локальной сети ПК может напрямую узнать MAC-адрес другого устройства с помощью ARP-запроса.

При отправке данных в интернет кадры доходят только до роутера, а дальше передаются на основе IP-адресов.

Поэтому Wireshark показывает MAC-адрес роутера, а не конечного сервера.





Схематично* представьте пути прохождения данных при передаче в локальной сети и при отправке в удаленную сеть. Подпишите узлы. Добавьте к изображениям краткие пояснения.

1. В локальной сети

 Телефон ↔ (MAC) ↔  Ноутбук

MAC-адреса используются для передачи данных между устройствами напрямую.

2. В интернете

 Твой ноут → (MAC роутера) →  Роутер →  Интернет-провайдер →  Сервер Google

MAC-адреса меняются на каждом шаге.

В конечную точку данные доходят по IP-адресу.

* для рисования схемы можно воспользоваться инструментом <https://app.diagrams.net/>