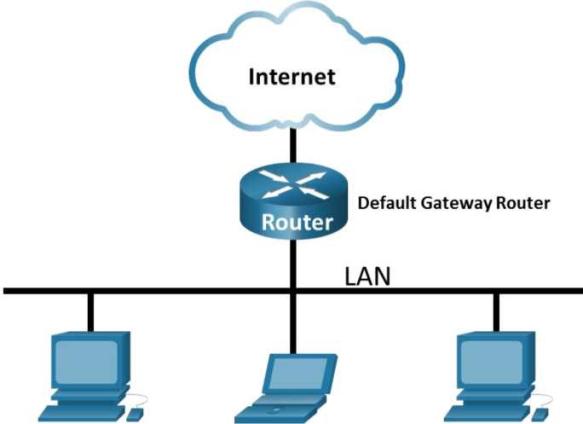
**Лабораторная работа**

**Анализ кадров Ethernet и просмотр сетевого трафика с помощью программы Wireshark**

**Топология**



**Задачи**

**Часть 1**. Изучение полей кадра Ethernet II

**Часть 2**. Захват и анализ данных протокола ICMP в локальной сети с помощью программы Wireshark

**Часть 3**. Захват и анализ данных протокола ICMP для удаленных узлов с помощью программы Wireshark

**Общие сведения**

При взаимодействии устройств по сети, данные приложений проходя уровни модели взаимодействия открытых систем (OSI), инкапсулируются в единицы данных протокола (PDU) канального уровня (кадры). Структура кадра зависит от типа среды передачи данных и метода доступа к ней. При изучении процесса функционирования канального уровня будет полезно проанализировать данные полей кадров. В первой части лабораторной работы необходимо изучить поля кадра Ethernet II. Во второй и третьей части требуется перехватить и проанализировать поля кадра Ethernet II для локального и удаленного трафика ICMP с помощью программы Wireshark.

Wireshark — это полезный инструмент для анализа трафика (анализатор кадров), который используется для поиска неполадок в сети, анализа, разработки программного обеспечения и протоколов, а также обучения. При передаче данных по среде передачи, Wireshark захватывает каждый кадр канального уровня и декодирует его содержимое согласно документам RFC или другим спецификациям.

**Необходимые ресурсы**

* Компьютер с ОС Windows, доступом в Интернет и установленной программой Wireshark
* Дополнительный компьютер (оконечное устройство) в той же локальной сети.

# Часть 1. Изучение полей в кадре Ethernet II

В этой части необходимо изучить поля кадра Ethernet II, перехваченного программой Wireshark, их размер и назначение.

**Шаг 1. Изучите размер и назначение полей кадров Ethernet II.**

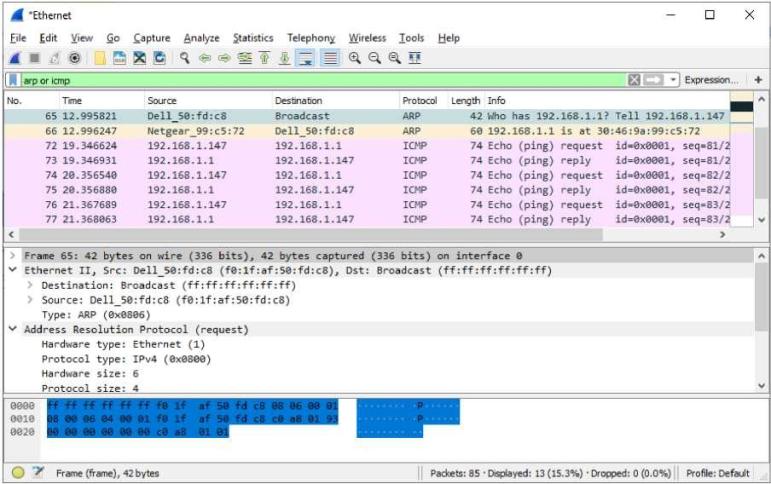


**Шаг 2. Изучите кадры Ethernet, перехваченные программой Wireshark.**

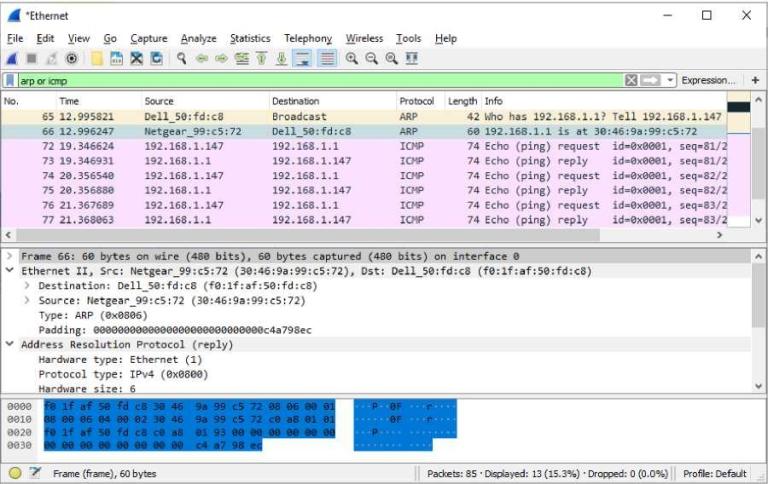
Приведенный ниже пример перехвата данных программой Wireshark отображает кадры, содержащие эхо-запросы, которые были созданы с помощью команды **ping**, и отправлены с компьютера на **основной шлюз**

(**шлюз по умолчанию**). В программе Wireshark установлен фильтр для просмотра только трафика протоколов ARP и ICMP. Протокол разрешения адресов (ARP), используется для сопоставления MAC-адреса с IP-адресом. Передача начинается с ARP-запроса МАС-адреса основного шлюза, за которым следуют четыре эхо-запроса и ответа.

На этом снимке экрана показаны сведения о кадре ARP-запроса.



На этом снимке экрана показаны сведения о кадре ARP-ответа.



**Шаг 3. Изучите содержимое полей кадра Ethernet II.**

В приведенной ниже таблице выбран кадр 65 из примера выше, перехваченный программой Wireshark, и приведены данные в полях этого кадра Ethernet II.

|  |  |  |
| --- | --- | --- |
| **Поле** | **Значение** | **Описание** |
| Преамбула | Не отображается при перехвате данных | В этом поле содержатся биты синхронизации, обработанные сетевой платой. |
| Адрес назначения          Адрес источника | Адрес широковещательной рассылки (FF:FF:FF:  FF:FF:FF)    Netgear\_99:C5:72  (30:46:9A:99:C5:72) | Адреса канального уровня (физический адрес). Длина каждого адреса составляет 48 бит (6 октетов), представленных 12 шестнадцатеричными цифрами: 0-9, A-F. Обычный формат записи — 12:34:56:78:90:AB. Первые 6 шестнадцатеричных цифр определяют производителя сетевой платы, а последние — ее серийный номер.  Адрес назначения может быть адресом широковещательной или одноадресной рассылки. Адрес источника всегда является адресом одноадресной рассылки. |
| Тип кадра | 0x0806 | Это поле содержит шестнадцатеричное значение, которое указывает данные какого протокола верхнего уровня содержатся в поле **Данные** кадра Ethernet II. Ethernet II поддерживает множество протоколов верхнего уровня. Наиболее распространены следующие типы кадров. Значение Описание  0x0800 IPv4 Protocol  0x0806 Address Resolution Protocol (ARP) |
| Данные | ARP | Содержит инкапсулированную PDU протокола верхнего уровня. Поле данных имеет размер в диапазоне от 46 до 1500 байт. |
| FCS | Не отображается при перехвате данных | Контрольная последовательность кадра (FCS), которая используется сетевой платой для обнаружения ошибок при передаче данных. Значение поля вычисляется устройством-  отправителем и проверяется устройством-получателем. |

Что можно сказать о данных, содержащихся в поле **Адрес назначения** приведенного примера?

|  |  |  |
| --- | --- | --- |
| Выполняется отправка широкого вещания | | |
| Почему перед первым эхо-запросом широковещательную рассылку ARP? | компьютер | отправляет |
| Запрос MAC-адреса | | |

Назовите физический адрес источника в приведенном для примера кадре.

|  |
| --- |
| Netgear\_99:C5:72 (30:46:9A:99:C5:72) |

Назовите идентификатор производителя (OUI) сетевой интерфейсной платы источника в ответе ARP (кадр 66 примера)?

|  |
| --- |
| Netgear\_99:C5:72 |

Какая часть физического адреса соответствует идентификатору производителя?

|  |
| --- |
| Первые 3 Байта |

Назовите серийный номер сетевой интерфейсной платы (NIC) источника (кадр 66 примера).

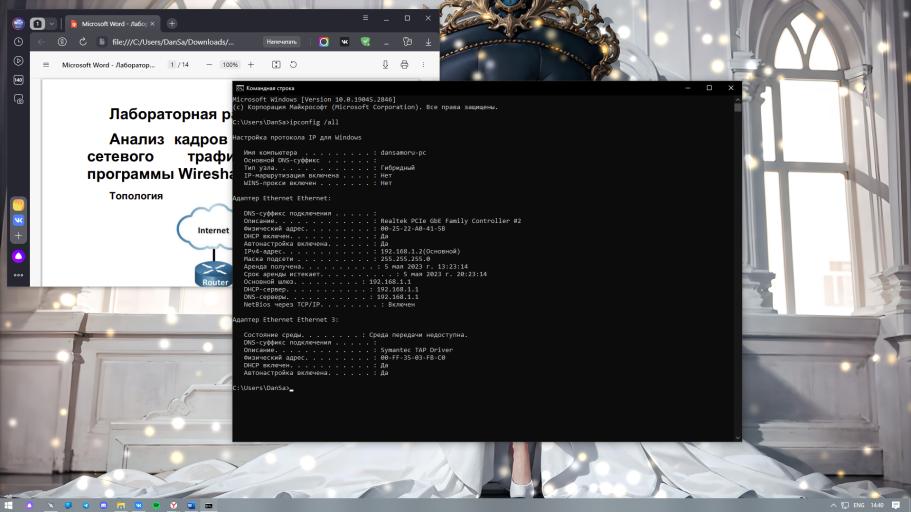
|  |
| --- |
| 99:C5:72 |

# Часть 2. Захват и анализ данных протокола ICMP в локальной сети с помощью программы Wireshark

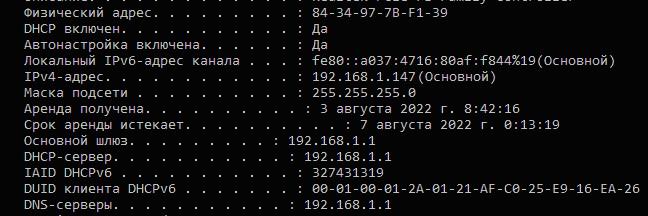
В этой части лабораторной работы необходимо осуществить перехват ICMP-запросов и ответов в локальной сети с помощью программы Wireshark. Кроме этого, требуется найти и проанализировать информацию в захваченных кадрах. Этот анализ позволит понять, как используются поля кадров при передаче данных по локальной сети.

**Шаг 1. Определите параметры интерфейсов своего компьютера и IP-адрес основного шлюза.**

В данном шаге необходимо узнать IP-адрес компьютера, физический адрес (MAC-адрес) сетевой интерфейсной платы (NIC) и IP-адрес основного шлюза.

1. В окне командной строки ОС Windows введите команду **ipconfig /all** 

чтобы узнать IP-адрес интерфейса компьютера, его описание, физический адрес, а также IP-адрес основного шлюза.



Назовите IP-адрес этого компьютера.

|  |
| --- |
| 192.168.1.2 |

Назовите IP-адрес основного шлюза.

|  |
| --- |
| 192.168.1.1 |

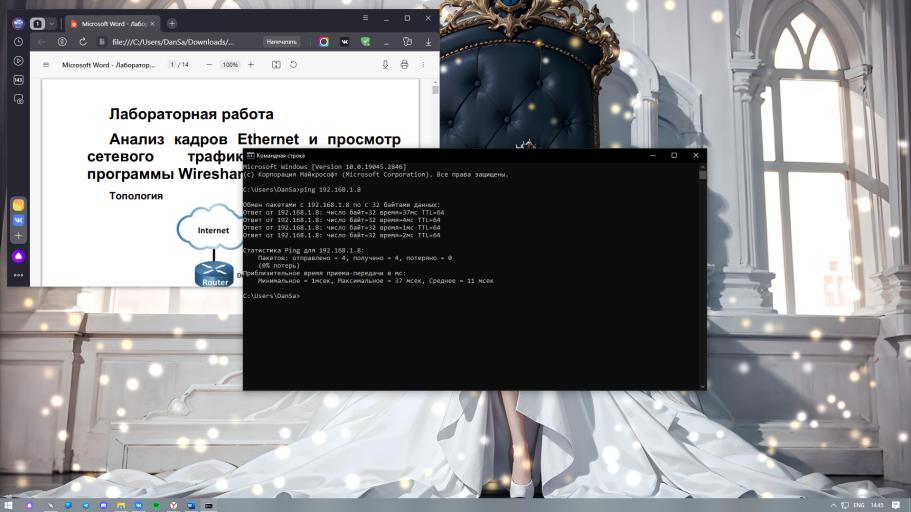
Назовите физический адрес сетевой интерфейсной платы этого компьютера.

|  |
| --- |
| 00-25-22-A0-41-5B |

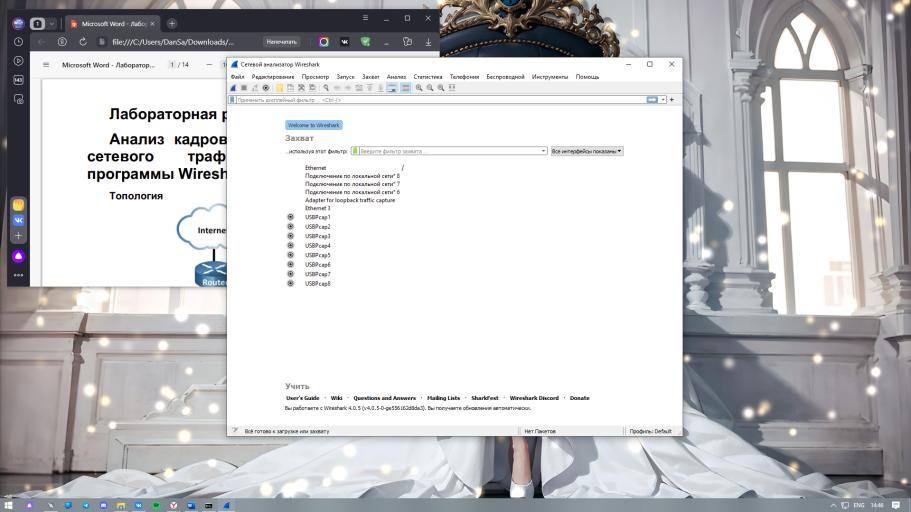
Назовите физический адрес основного шлюза.

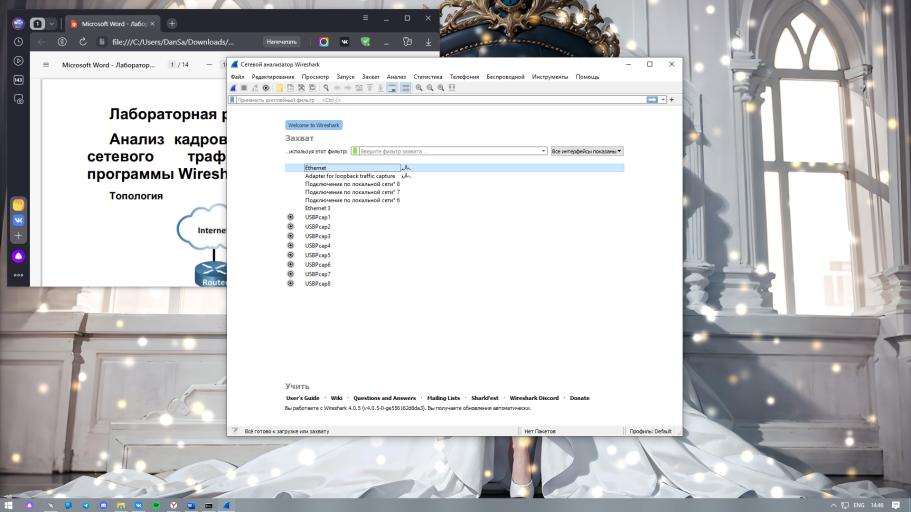
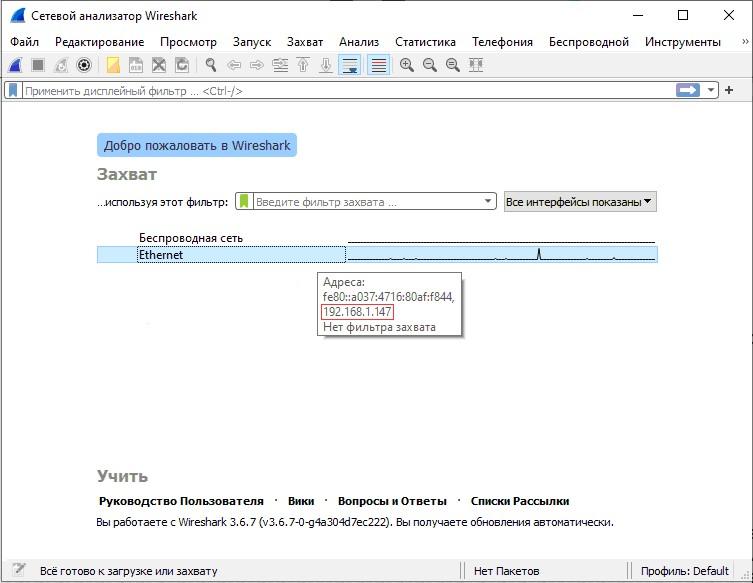
|  |
| --- |
| 50-ff-20-4c-8b-32 |

1. Узнайте IP-адрес другого компьютера (устройства), **находящегося**

**в той же подсети**. 

**Шаг 2. Запустите программу Wireshark и начните захват данных.**

1. Запустите программу Wireshark. 
2. В списке интерфейсов выберите необходимый интерфейс.

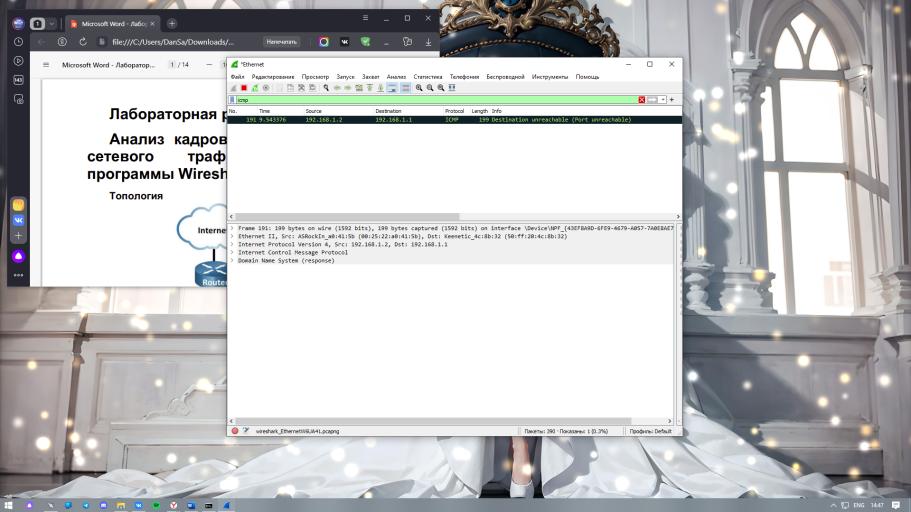


**Примечание**. Если указано несколько интерфейсов, убедитесь в том, что IP-адрес выбранного интерфейса **соответствует тому, что вы узнали в шаге 1a**.

В верхней части окна программы Wireshark должна выводиться информация. Цвет строк данных, выводимых Wireshark зависит от протокола, к которому они относятся.

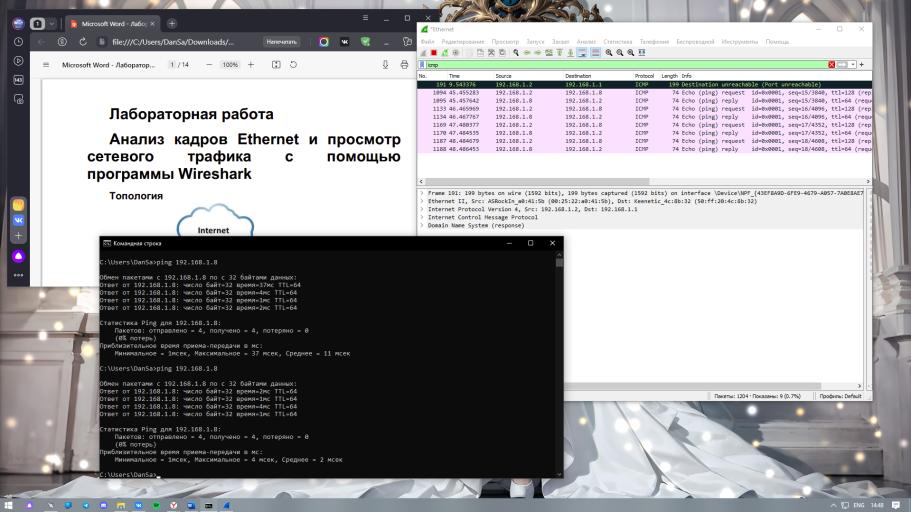
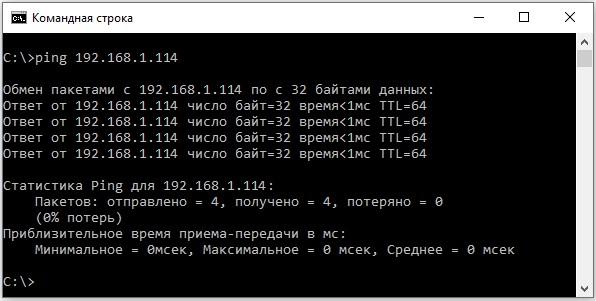
**Шаг 3. Применение фильтров программы Wireshark для отображения на экране только нужного трафика.**

Информация на экране может выводиться очень быстро. Скорость вывода зависит от многих факторов. Чтобы облегчить поиск и анализ данных, захваченных программой Wireshark, применяют фильтры, скрывающие ненужный трафик. Фильтр лишь отображает нужный трафик на экране, но не блокирует захват других кадров. В этой лабораторной работе анализируются только единицы данных протокола ICMP, полученные с помощью команды **ping**.

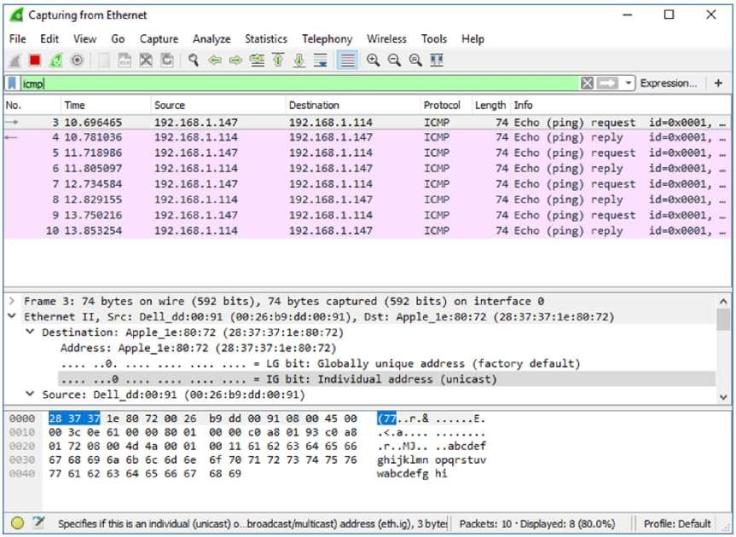
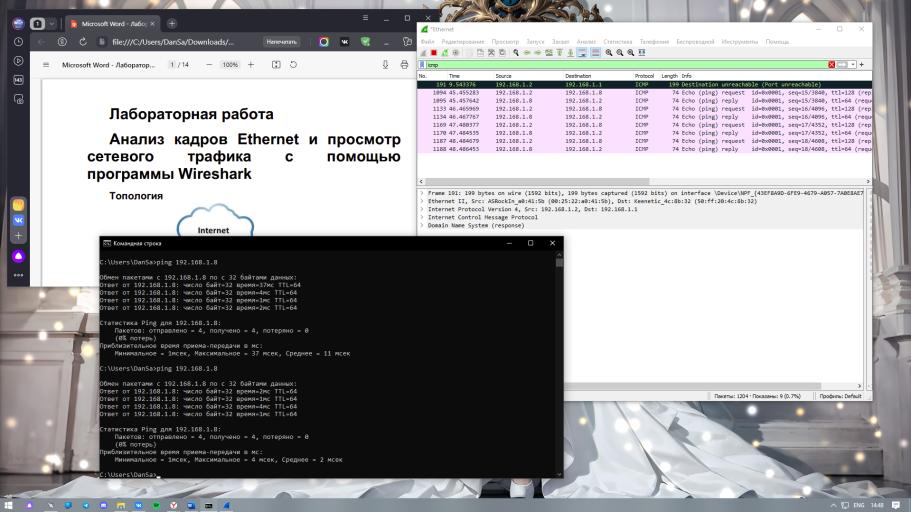
1. В поле **Фильтр** в верхней части окна программы Wireshark введите icmp, чтобы на экран выводились только сведения о кадрах, содержащих единицы данных протокола ICMP. При правильном задании фильтра, указанное поле станет зеленым. После этого, нажмите клавишу **Ввод** или кнопку **Применить** , чтобы применить фильтр. 

После этого верхняя часть окна программы Wireshark очистится от данных, однако захват трафика в интерфейсе продолжится.

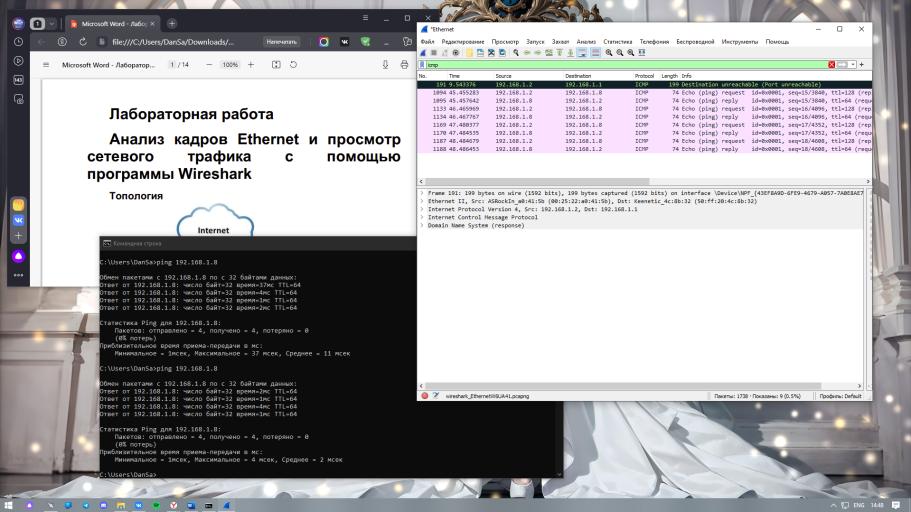
1. Откройте окно командной строки ОС Windows на компьютере и отправьте с помощью команды **ping** эхо-запрос на IP-адрес компьютера, полученный в шаге 1, пункт **b** (**находящегося в той же подсети**).



1. В верхней части окна программы Wireshark должны снова появиться данные.

**Примечание**. Если компьютер из той же подсети не отвечает на эхо-запросы, то возможно, их блокирует межсетевой экран. Чтобы обеспечить пропуск трафика ICMP через межсетевой экран на компьютере с ОС Windows, воспользуйтесь **Приложением А**. Пропуск трафика ICMP через межсетевой экран.

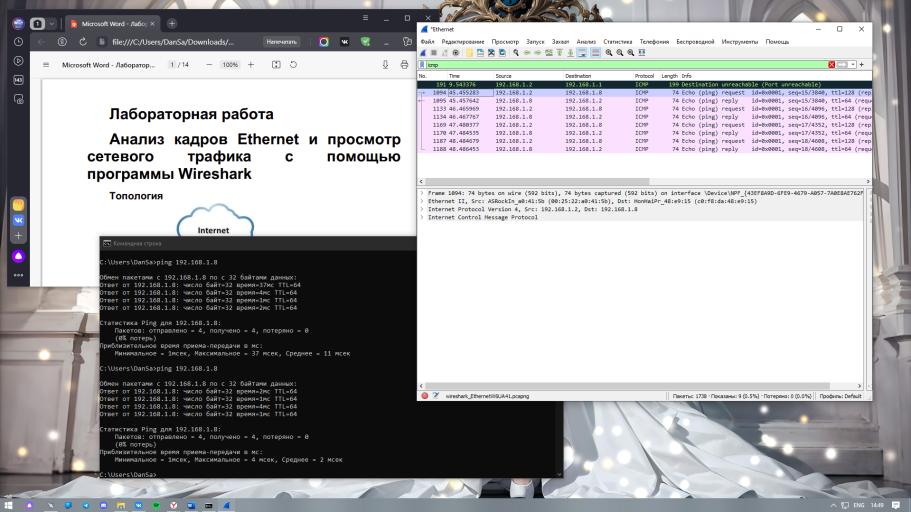
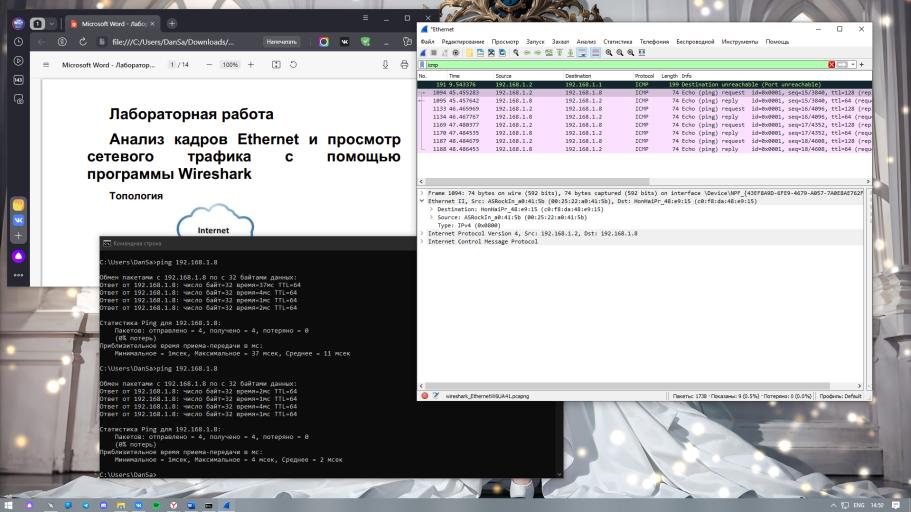
1. Нажмите на значок **Остановить захват пакетов**  , чтобы остановить захват кадров. 

**Шаг 4. Проанализируйте полученные данные.**

На шаге 4 необходимо изучить данные, сформированные эхо-запросами на компьютер в той же подсети. Окно программы Wireshark состоит из трех частей: в верхней части отображается список полученных кадров и общая

информация о них; в средней части приводится информация о кадре, **выбранном в**

**верхней части экрана**; в нижней части отображаются декодированные данные верхних уровней, как в шестнадцатеричном представлении, так и в кодировке ASCII.

1. Выделите кадр первого запроса ICMP в верхней части окна программы Wireshark. В столбце Source (Источник) должен быть указан IP-адрес вашего компьютера, а в столбце Destination (Назначение) — IP-адрес компьютера в той же подсети, на который вы отправили эхо-запрос. 
2. Не меняя выделенный кадр в верхней части окна, перейдите в среднюю часть. Нажмите значок  слева от строки Ethernet II, чтобы просмотреть физические адреса источника и назначения. 

Совпадает ли физический адрес источника с физическим адресом сетевого интерфейса вашего компьютера?

|  |
| --- |
| Да |

Совпадает ли физический адрес назначения с физическим адресом другого компьютера в той же подсети, на который вы отправили эхо-запрос?

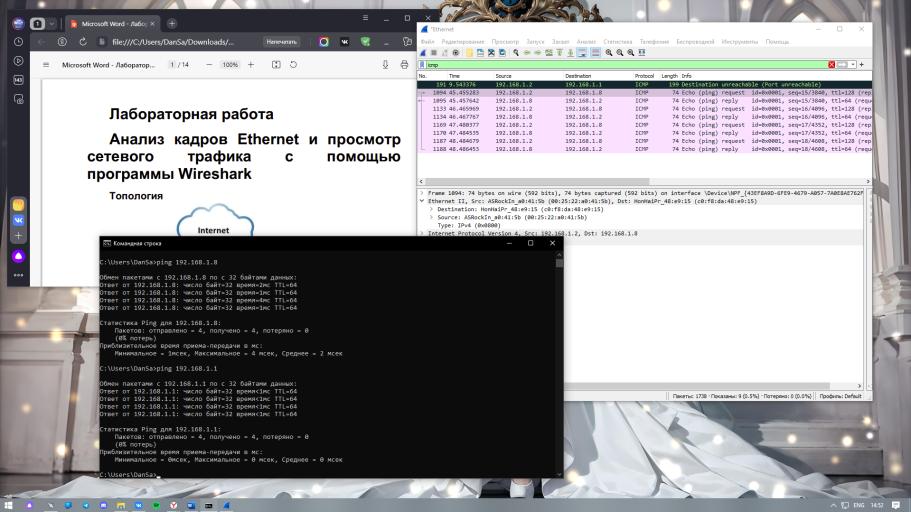
|  |
| --- |
| Неизвестно, адрес не был проанализирован заранее |

Как ваш компьютер определил физический адрес другого компьютера в той же подсети, на который он отправил эхо-запрос с помощью команды **ping**?

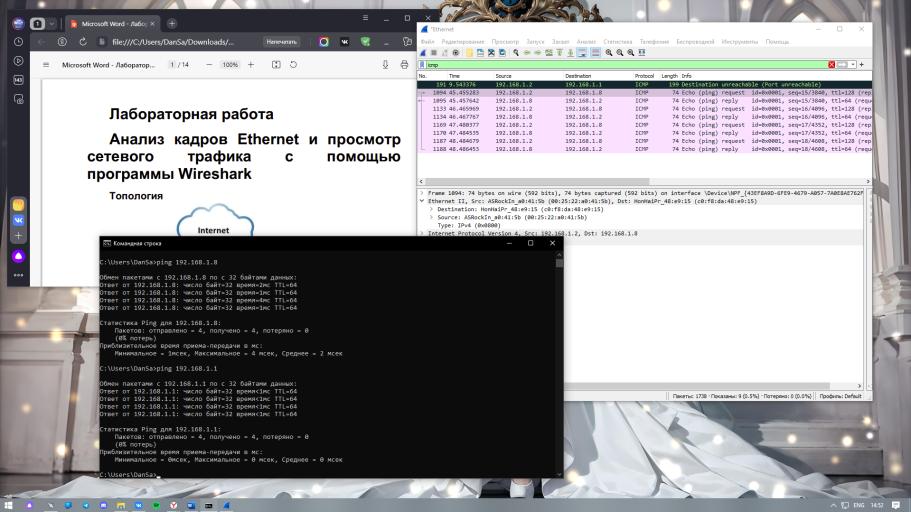
|  |
| --- |
| ARP |

**Примечание**. В показанном примере перехваченного кадра, данные протокола ICMP инкапсулируются в пакет IPv4, который затем инкапсулируется в кадр Ethernet II для передачи по локальной сети.

**Шаг 5. Из окна командной строки компьютера отправьте эхо-запрос на основной шлюз.**

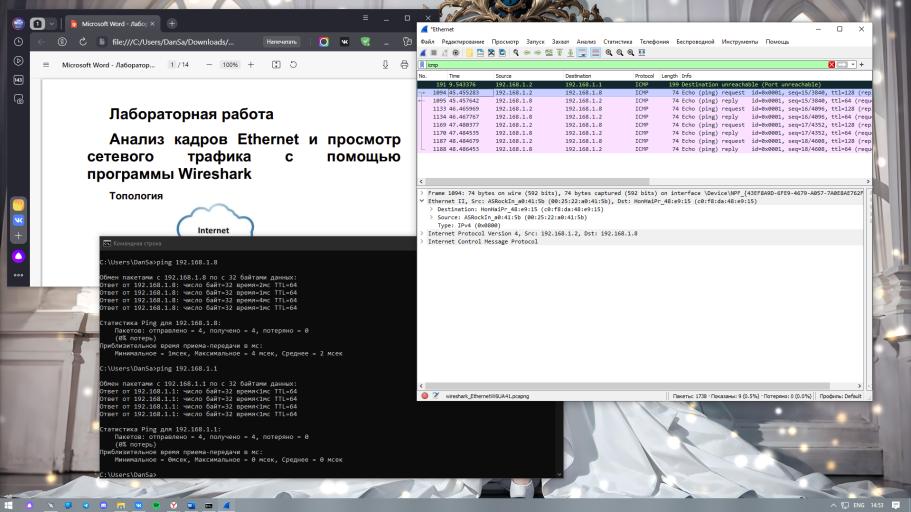
Из окна командной строки ОС Windows компьютера отправьте с помощью команды **ping** эхо-запрос на основной шлюз, используя IP-адрес, записанный в шаге 1, пункт **a**. 

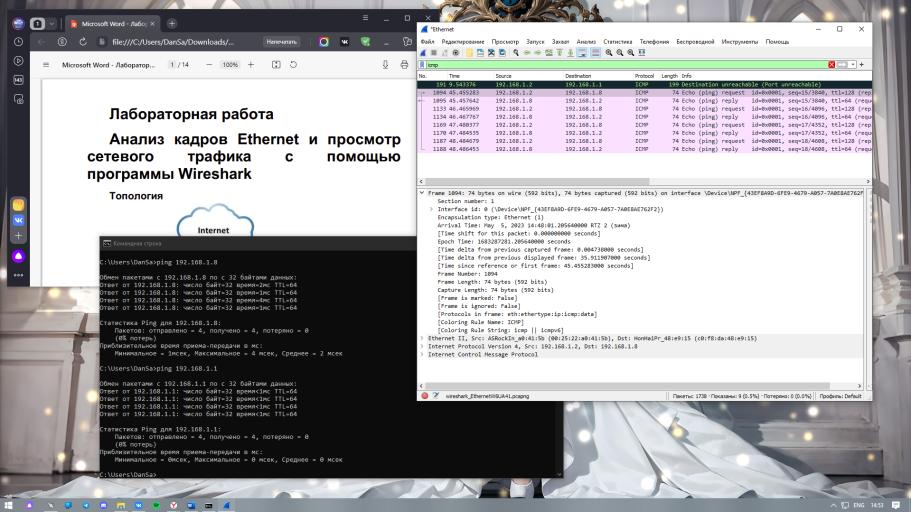
**Шаг 6. Остановите захват кадров программой Wireshark.**

Нажмите значок **Остановить захват пакетов** , чтобы остановить захват кадров. 

**Шаг 7. Изучите первый эхо-запрос в программе**

**Wireshark.**

1. На панели списка кадров (верхняя часть) выделите необходимый кадр. В столбце Info должно быть указано Echo (ping) request (Эхо-запрос с помощью команды **ping**). 
2. Изучите в панели сведений о кадре в средней части экрана первую

строку. В этой строке показана длина кадра. 

1. Вторая строка в панели сведений о кадре показывает, что это кадр Ethernet II. Здесь же отображаются физические адреса источника и назначения.

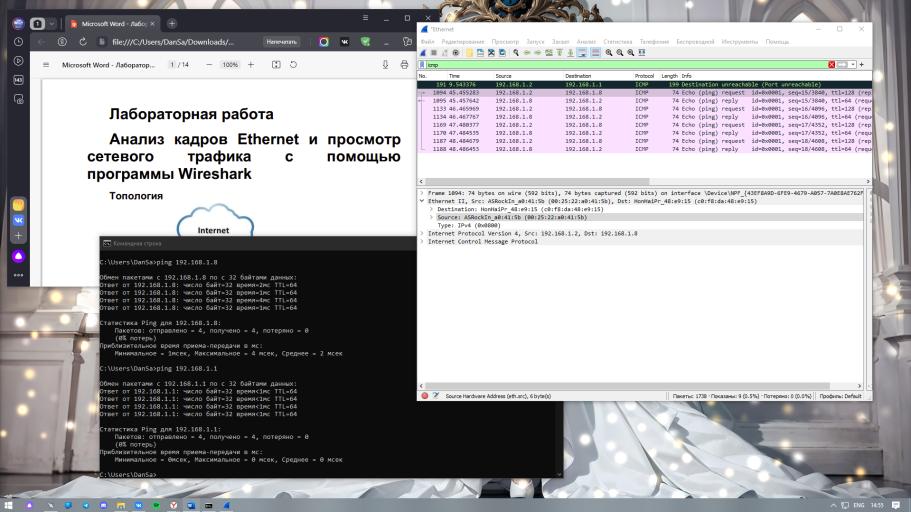
Назовите физический адрес сетевой интерфейсной платы этого компьютера.

|  |
| --- |
| 00:25:22:a0:41:5b |

Назовите физический адрес основного шлюза.

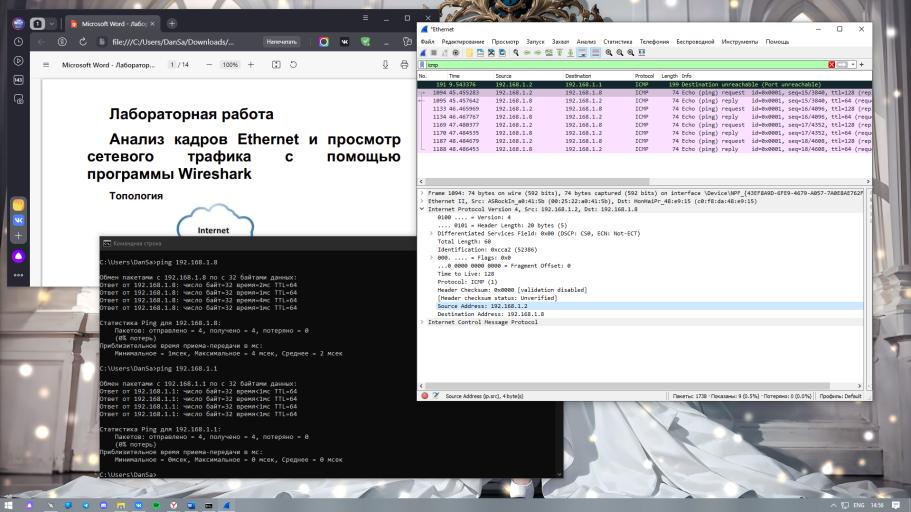
|  |
| --- |
| 50-ff-20-4c-8b-32 |

1. Вы можете щелкнуть значок  в начале второй строки, чтобы

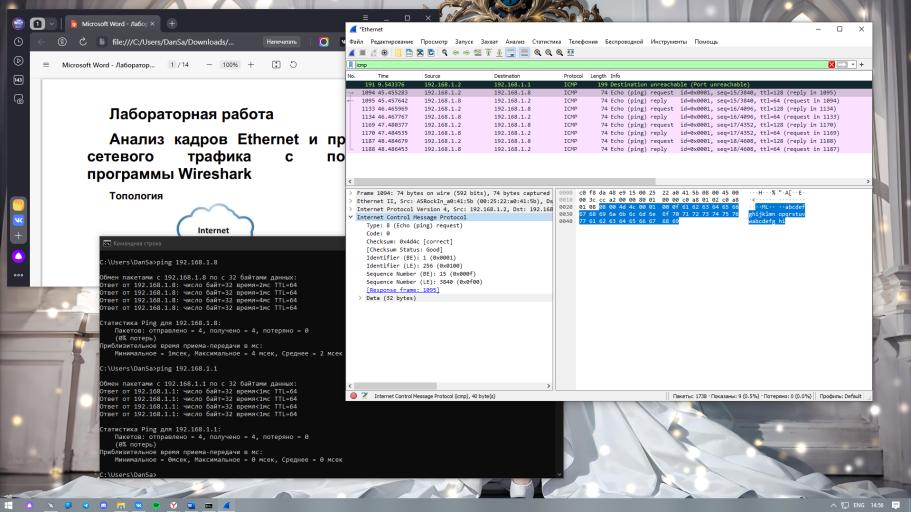
получить развернутую информацию о кадре Ethernet II. Назовите тип текущего кадра. 

|  |
| --- |
| 0x0800 |

|  |
| --- |
|  |

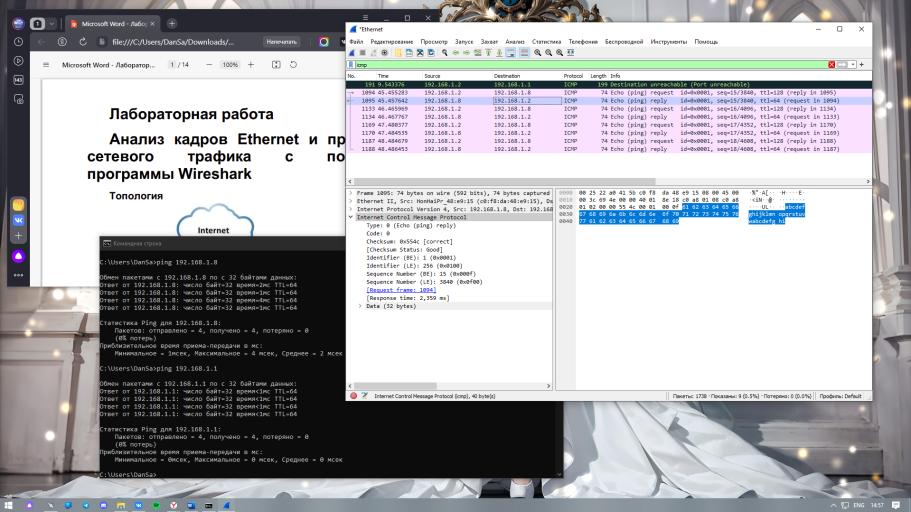
1. Последние две строки среднего раздела содержат информацию о поле данных кадра. В рассматриваемом примере, данные содержат IPv4-адреса источника и назначения.  Назовите IP-адрес источника. Назовите IP-адрес назначения.

|  |
| --- |
| 192.168.1.2 192.168.1.8 |

1. Для того, чтобы выделить часть кадра (в шестнадцатеричной системе и в кодировке ASCII) в нижней части окна программы Wireshark, необходимо щелкнуть по любой строке в средней части. Щелкните по строке Internet Control Message Protocol в средней части и посмотрите, что будет выделено в нижней части. 

Какое слово образуют последние два выделенных октета?

|  |
| --- |
| hi |

1. Нажмите **следующий** кадр в верхней части и изучите кадр эхо-ответа. Физические адреса источника и назначения **поменялись местами**, т. к. основной шлюз, отправил этот кадр в ответ на первый эхо-запрос. 

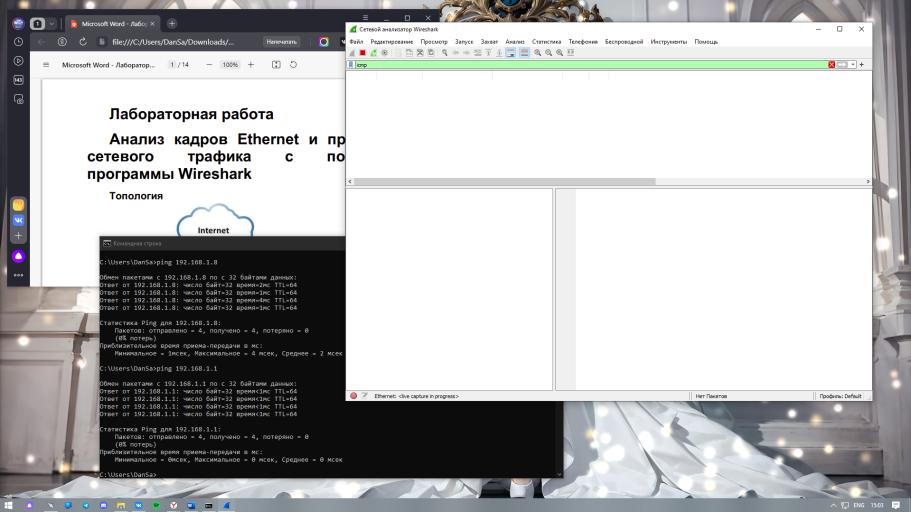
Какое устройство и какой физический адрес показаны в качестве адреса назначения?

|  |
| --- |
| 00:25:22:a0:41:5b |

# Часть 3. Захват и анализ данных протокола ICMP для удаленных узлов с помощью программы Wireshark

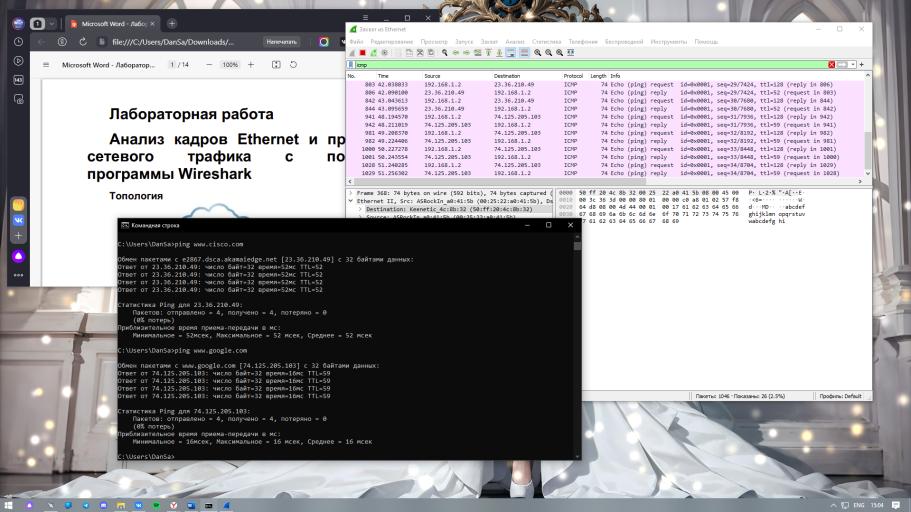
В части 3 необходимо отправить с помощью команды **ping** эхо-запросы на удаленные узлы (расположенные за пределами локальной сети) и изучить данные, сформированные этими запросами. Затем необходимо определить различия между этими данными и данными, полученными в части 2.

**Шаг 1. Запустите захват данных в программой Wireshark.**

1. Нажмите значок **Перезапустить текущий захват** , чтобы начать новый перехват кадров в программе Wireshark. Откроется всплывающее окно с предложением сохранить перед началом нового перехвата предыдущие перехваченные кадры в файл. Сохранять данные необязательно. Нажмите **Продолжить без сохранения**. 
2. Отправьте из командной строки ОС Windows с помощью команды

**ping** эхо-запросы на следующие URL-адреса узлов:

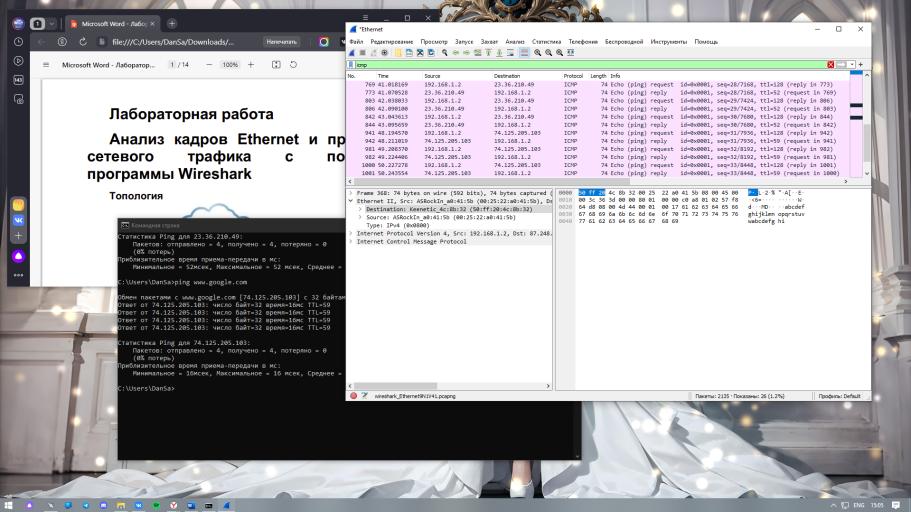
1. www.yahoo.com
2. www.cisco.com
3. www.google.com

**Примечание**. При отправке эхо-запросов с помощью команды **ping** на указанные URL-адреса, служба доменных имен (DNS) сопоставляет адрес URL и IP-адрес.

Запишите IP-адреса, сопоставленные службой доменных имен каждому URL-адресу.

|  |
| --- |
| 87.248.100.216  23.36.210.49  74.125.205.103 |

**c**. Остановите захват кадров, нажав на значок **Остановить захват**

**пакетов** . 

**Шаг 2. Проанализируйте данные, полученные от удаленных узлов.**

Просмотрите перехваченные кадры в программе Wireshark. Укажите IP- и физические адреса назначения для всех узлов. IP-адрес для www.yahoo.com: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 87.248.100.216

Физический адрес для www.yahoo.com: \_4950:ff:20:4c:8b:32\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IP-адрес для www.cisco.com: \_\_23.36.210. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Физический адрес для www.cisco.com: \_\_4950:ff:20:4c:8b:32\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IP-адрес для www.google.com: \_\_\_\_\_ 74.125.205.103\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Физический адрес для www.google.com: \_\_4950:ff:20:4c:8b:32\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Проанализируйте IP- и физические адреса узлов, на которые были отправлены эхо-запросы. Какова существенная особенность этих данных?

|  |
| --- |
| IP меняется, MAC остаётся |

Почему IP-адрес назначения изменяется, а физический адрес назначения остается прежним?

|  |
| --- |
| Роутер отвечает на разные IP, но на один MAC |

Как эти данные отличаются от данных, полученных в результате эхо-запросов, отправленных на локальные узлы в части 2?

|  |
| --- |
| Там MAC менялся |

# Вопросы для повторения

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

|  |
| --- |
| Запрашиваемое устройство находится в другой локальной сети и его MAC недоступен |

Программа Wireshark не отображает поле преамбулы заголовка кадра. Что содержит преамбула?

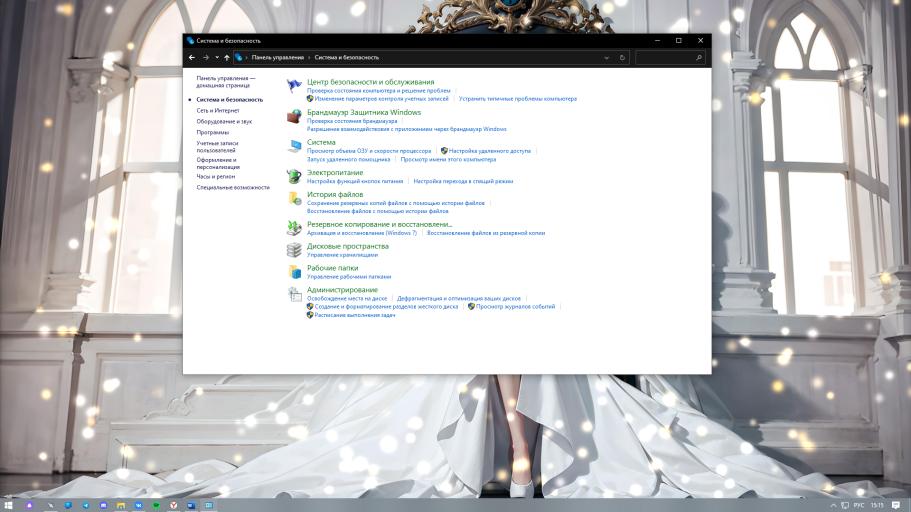
|  |
| --- |
| Шаблон синхронизации |

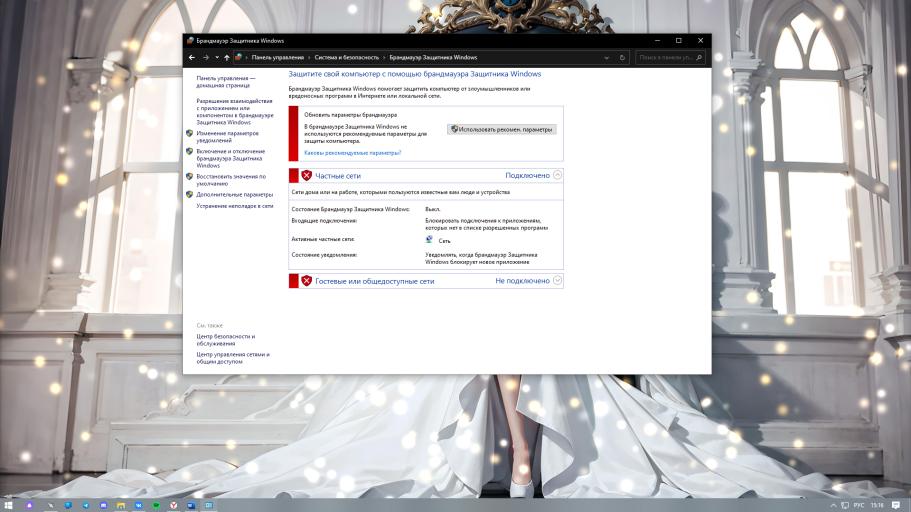
**Приложение А. Пропуск трафика протокола ICMP через межсетевой экран**

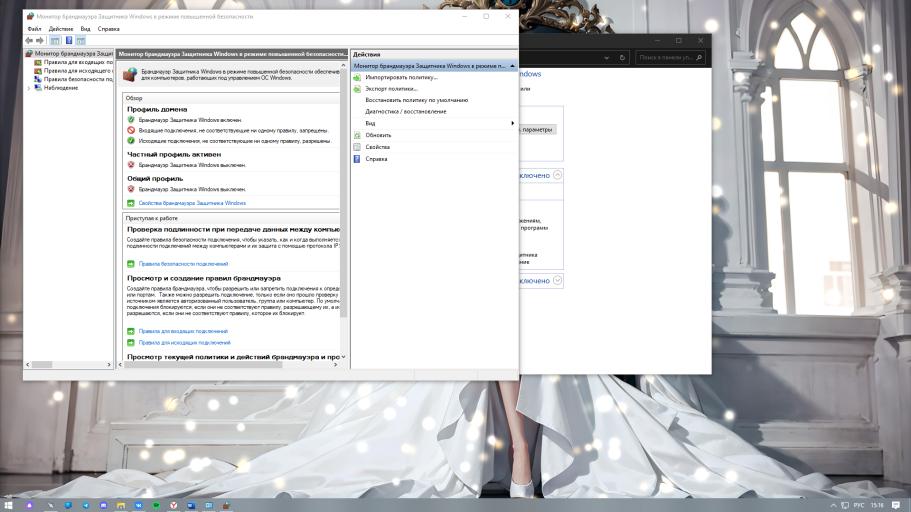
Если эхо-запросы, отправленные с помощью команды **ping** с других компьютеров не достигают вашего компьютера, возможно, их блокирует межсетевой экран. В этом приложении объясняется, как обеспечить прохождение эхо-запросов через межсетевой экран, а также как отменить это по завершении лабораторной работы.

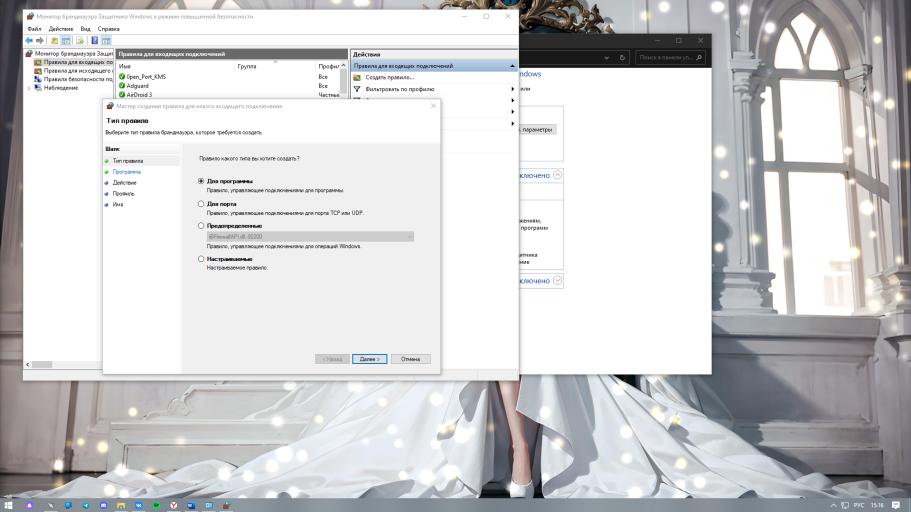
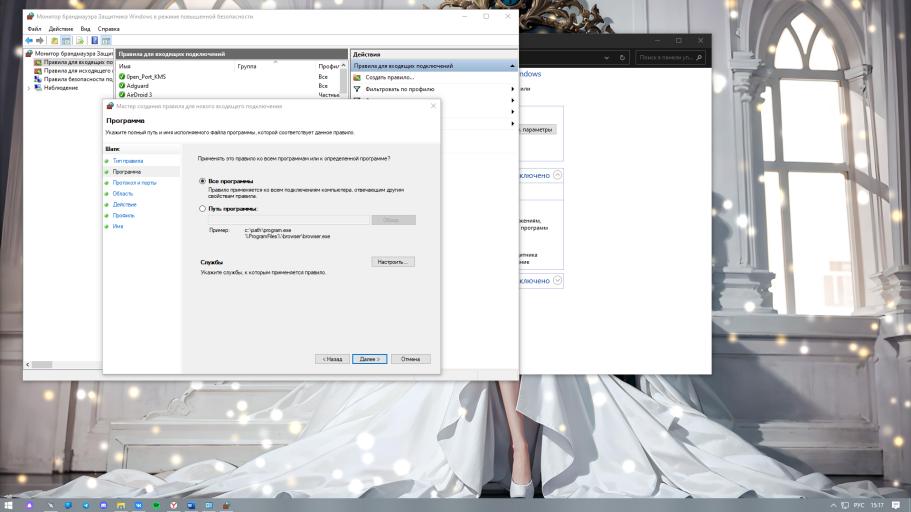
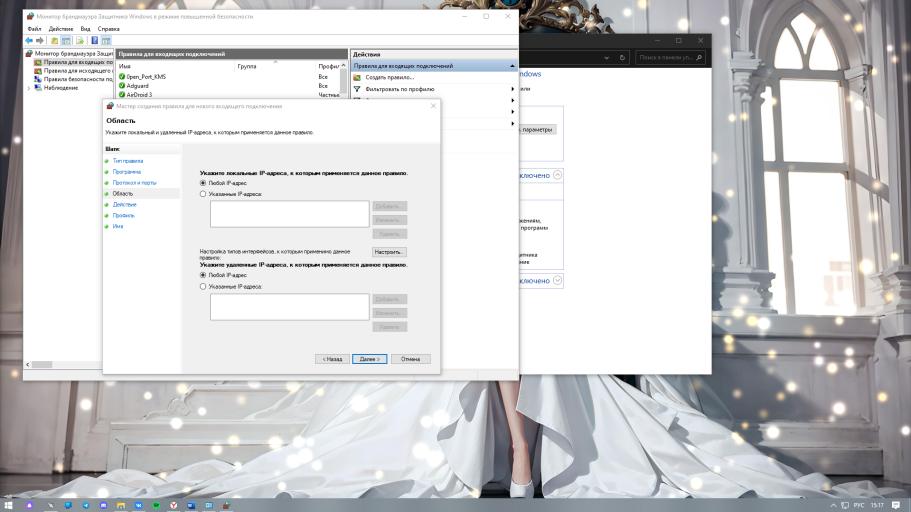
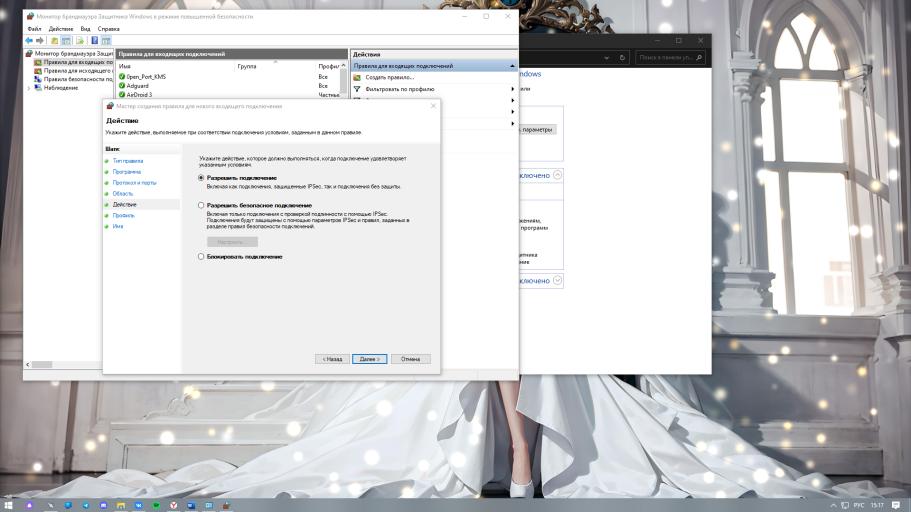
**Часть 1. Создание нового правила, разрешающего прохождение трафика ICMP через межсетевой экран.**

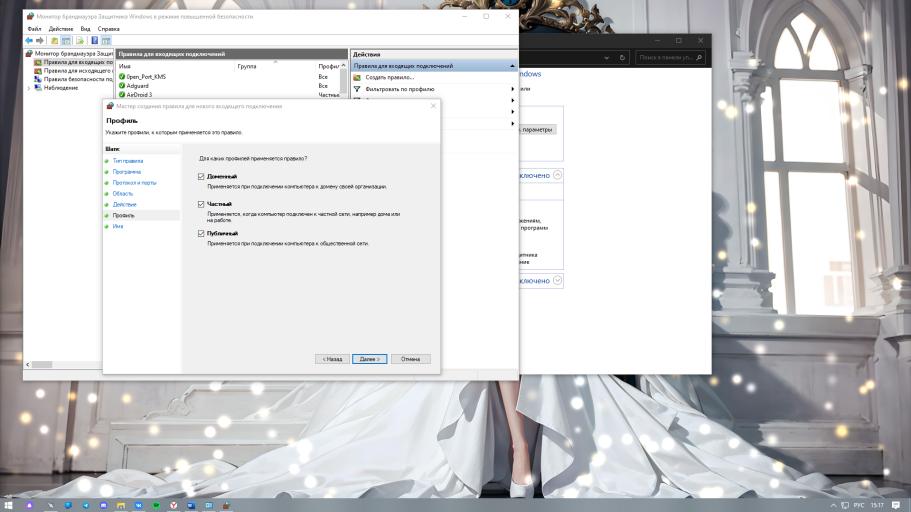
1. Перейдите в **Панель управления** и выберите параметр **Система и**

**безопасность** в представлении **Категория**. 

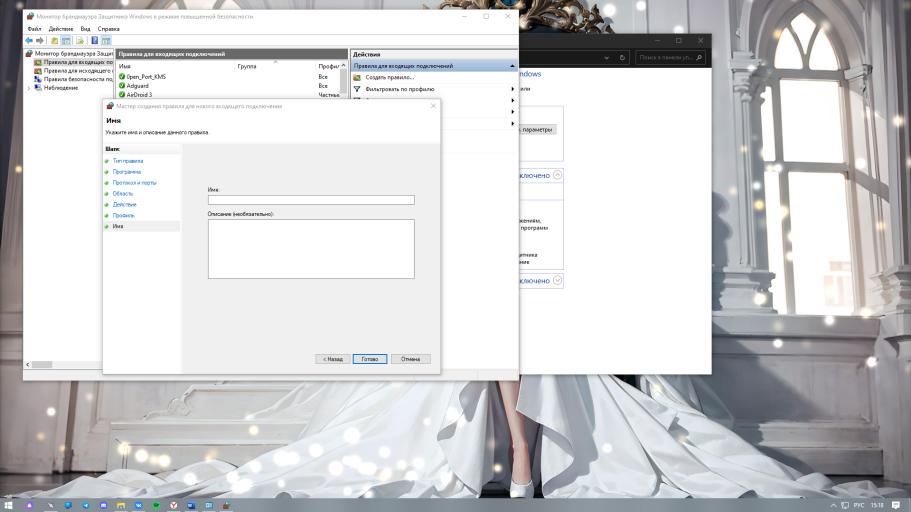
1. В окне System and Security (Система и информационная безопасность) выберите Windows Defender Firewall или Windows Firewall. 
2. В левой части окна Windows Firewall или Windows Defender Firewall

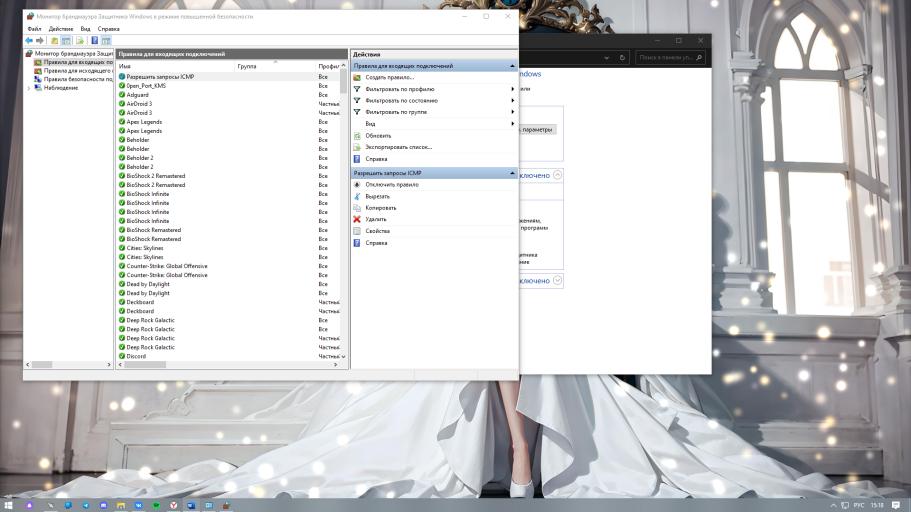
выберите Advanced settings (Дополнительные параметры). 

1. В окне Advanced Security (Расширенные функции безопасности) выберите параметр Inbound Rules (Правила для входящих подключений) на левой боковой панели, а затем щелкните New Rule... (Создать правило...) на правой боковой панели. 
2. Откроется Мастер создания новых правил для входящих подключений. На экране Rule Type (Тип правила) нажмите селективную кнопку Custom (Настраиваемые) и нажмите Next (Далее). 
3. На левой панели щелкните параметр Protocol and Ports (Протокол и порты) и выберите ICMPv4 из раскрывающегося меню Protocol Type (Тип протокола), затем щелкните Next (Далее). 
4. Убедитесь, что выбран любой IP-адрес для локальных и удаленных IP-адресов. Для продолжения нажмите кнопку Next (Далее). 
5. Выберите **Разрешить подключение**. Для продолжения нажмите

кнопку Next (Далее). 

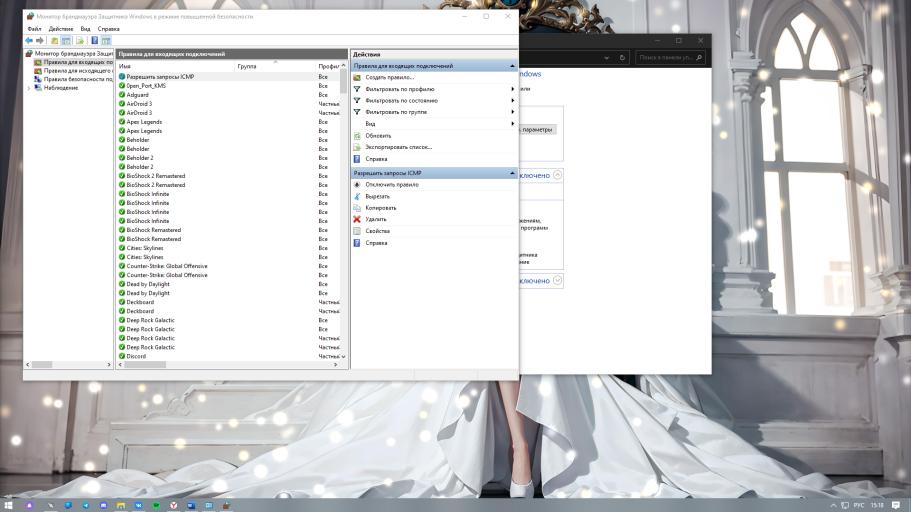
1. По умолчанию это правило применяется ко всем профилям. Для

продолжения нажмите кнопку Next (Далее). 

1. Назовите правило **Разрешить запросы ICMP**. Нажмите **Готово**, чтобы продолжить. Созданное правило позволит другим устройствам сети получать эхо-отклики с вашего компьютера. 

**Часть 2. Отключение или удаление нового правила.**

По завершении лабораторной работы отключите или удалите правило, созданное в части 1, пункт **j**.

1. В левой части окна Advanced Security (Расширенные функции безопасности) выберите Inbound Rules и найдите правило, созданное ранее в части 1, пункт **j**. 
2. Щелкните правой кнопкой мыши правило ICMP и выберите пункт **Отключить правило** или **Удалить**. Выбор пункта **Отключить правило** позволит снова включить его, если это снова станет необходимо. Выбор пункта **Удалить** позволит навсегда удалить правило для входящих подключений из списка. Если после этого снова потребуется разрешить запросы ICMP, правило нужно будет создавать заново. 