Федеральное государственное образовательное бюджетное

учреждение высшего образования

**«Финансовый университет при Правительстве Российской Федерации»**

**(Финансовый университет)**

Колледж информатики и программирования

Специальность 09.02.03 «Программирование в компьютерных системах»

**ОТЧЕТ**

**ПО УЧЕБНОЙ ПРАКТИКЕ**

Профессиональный модуль ПМ.02 Инфокоммукационные системы и сети

*(наименование профессионального модуля)*

Выполнил:

студент группы № 3ПКС-220

А. А. Кравцова

*(И.О. Фамилия)*

Проверил:

руководитель практики от колледжа:

И. В. Сиберев

*(И.О. Фамилия)*

**Москва**

**20­­­­23**

Оглавление

[Работа №1. Работа с командами ipconfig, ping, tracert, hostname. 3](#_Toc136983015)

# Работа №1. Работа с командами ipconfig, ping, tracert, hostname.

Цель работы: ознакомиться со средствами диагностики сети и поиска неисправностей стека TCP/IP.

Практическая часть

Для начала просмотрим настройки активного логического сетевого адаптера. Для этого в командной строке пишем «ipconfig».

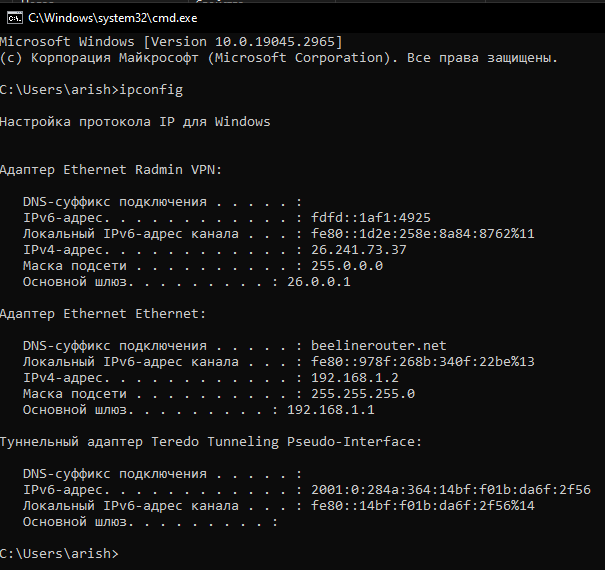


Рисунок 1. Настройки активного логического сетевого адаптера

Ethernet Radmin VPN не активнен, так как у него нет DNS суффикса подключения.

Проверим активность Ethernet Ethernet, необходимо просмотреть основной шлюз с помощью команды «ping 192.168.1.1».

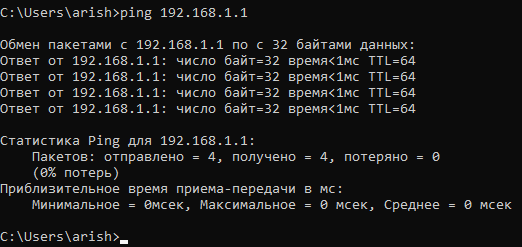


Рисунок 2. Проверка активности

Следующим шагом проверим доступ к интернету командой «ping [www.dzen.ru»](http://www.dzen.ru). Все выполнено без потер, подключение к интернету имеется.

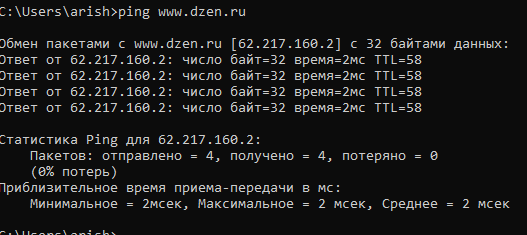


Рисунок 3. Проверка доступа к интернету

Теперь добавим в браузер расширение Browsec VPN и проверим доступность сайтов из разных стран.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ссылка на сайт | Доступ в Нидерландах | Доступ в Сингапуре | Доступ в США | Доступ в Великобритании |
| <https://www.youtube.com/> | Есть | Есть | Есть | Есть |
| <https://stackoverflow.com/questions/5898011/jquery-javascript-filtering-html-object-from-ajax-response> | Есть | Есть | Есть | Есть |
| <https://ru.pinterest.com/> | Есть | Есть | Есть | Есть |
| <https://www.twitch.tv/terablade> | Есть | Есть | Есть | Есть |
| <https://w4.cuevana3.ai/> | Есть | Есть | Есть | Есть |
| <https://kip.eljur.ru/journal-messages-action> | Есть | Есть | Есть | Есть |
| <http://translit-online.ru/> | Есть | Есть | Есть | Есть |
| <https://dev.1c-bitrix.ru/community/webdev/user/16002/blog/479/> | Есть | Есть | Есть | Есть |
| <https://www.youtube.com/watch?v=ZECkSAuy6sg&ab_channel=%D0%A2%D0%B5%D0%BB%D0%B5%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%AE> | Нет | Нет | Нет | Нет |
| <https://cloud.mail.ru/public/QaCU/7uQUyPrGD> | Есть | Есть | Есть | Есть |
| <https://ananasprint.ru/spm/#/> | Есть | Есть | Есть | Есть |
| <https://mail.rambler.ru/> | Есть | Есть | Есть | Есть |
| <https://www.mozilla.org/ru/firefox/> | Есть | Есть | Есть | Есть |
| <https://www.yahoo.com/> | Есть | Есть | Есть | Есть |
| <https://github.com/IvanSibirevV2/KipFin_Lab_2023_v0_Git0/blob/main/%D0%A3%D0%BF_02_3%D0%9F%D0%9A%D0%A1_120_220/> | Есть | Есть | Есть | Есть |
| <https://rutube.ru/video/9eec837c57f774773da9afb1aad1cf93/> | Есть | Есть | Есть |  |

Следующим шагом определим пути пактов до сайтов dzen.ru и yandex.ru. определим, до какого сайта наибольшее/наименьшее время пинга и количество узлов с помощью команды tracert.

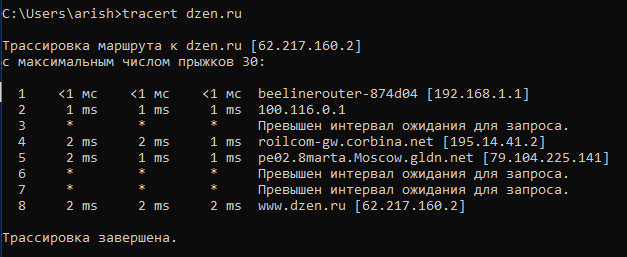


Рисунок 4. Трассировка маршрута к dzen.ru

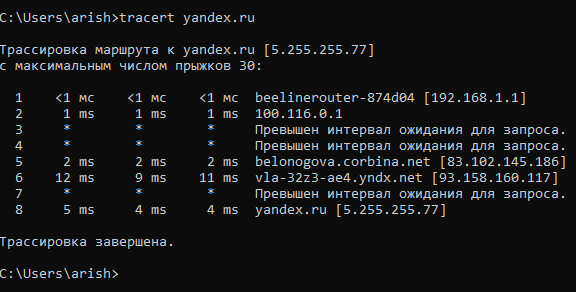


Рисунок 5. Трассировка маршрута к yandex.ru

Согласно полученным результатам, до сайта dzen.ru время пинга наименьшее, а количество узлов у обоих сайтов одинаковое.

На следующем этапе выведем перечень сетевых соединений и прослушиваемых потоков локального узла, используя команду «netstat». Также отдельно получим список активных TCP-соединителей локального компьютера, TCP-соединителей локального компьютера без преобразования адресов в символьные имена DNS и список прослушиваемых компьютером портов TCP и UDP без преобразования адресов в символьные имена DNS.

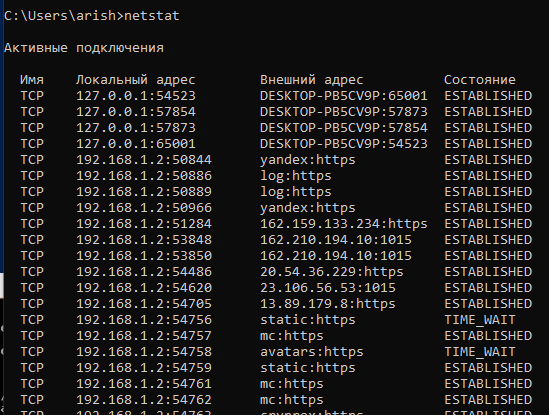


Рисунок 6. Активные подключения

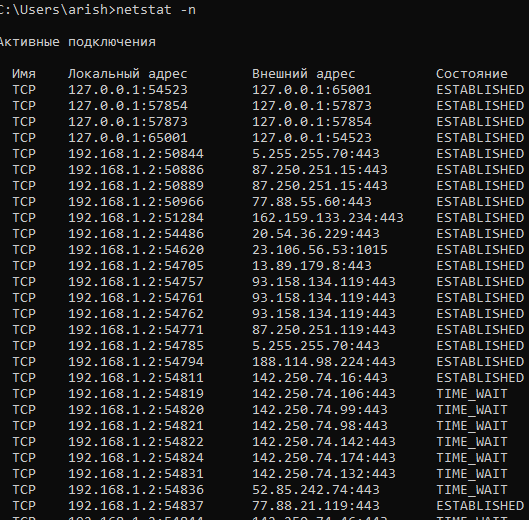


Рисунок 7. Список активных TCP-соединителей локального компьютера

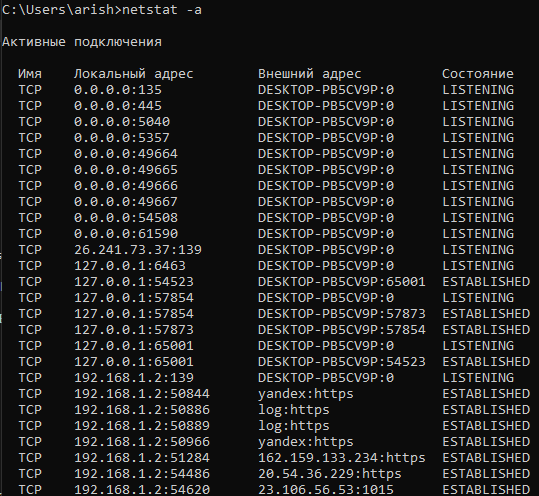


Рисунок 8. Список TCP-соединителей локального компьютера без преобразования адресов в символьные имена DNS

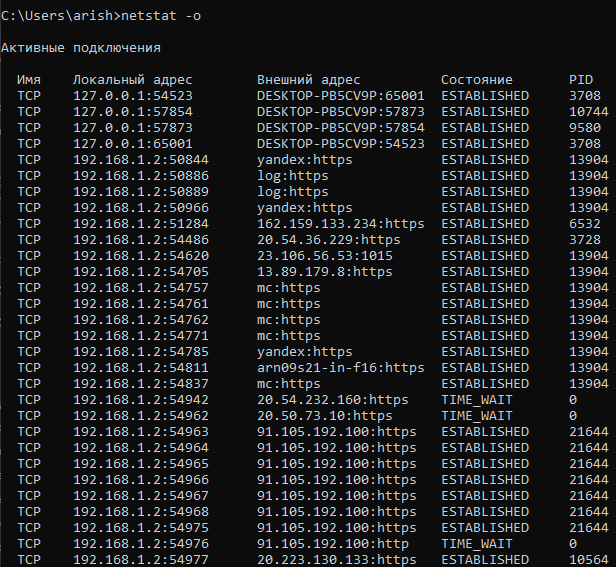


Рисунок 9. Список прослушиваемых компьютером портов TCP и UDP без преобразования адресов в символьные имена DNS

Следующим шагом необходимо получить сведения о маршрутизации нашего компьютера.

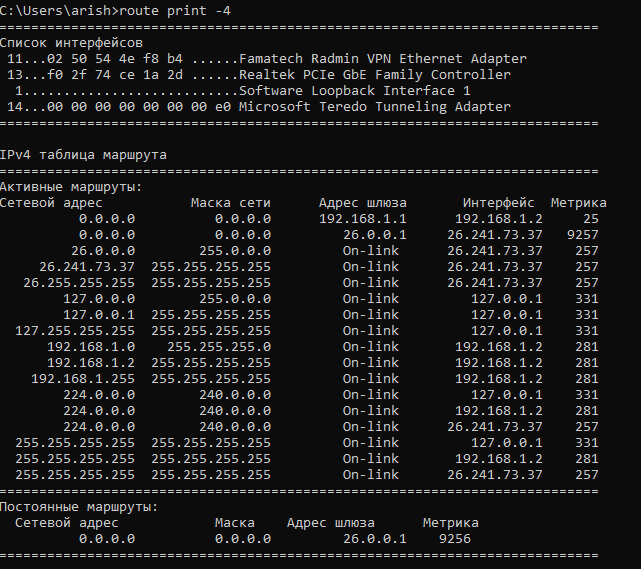


Рисунок 10. Таблица маршрутизаци

Просмотрим текущие ARP-записи, применив команду «arp – a».

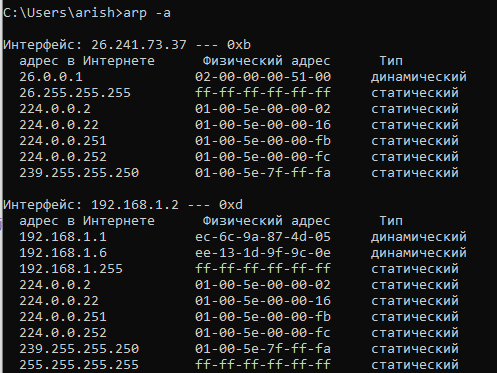


Рисунок 11. Текущие ARP-записи.

Вывод: в ходе работы я ознакомилась со средствами диагностики сети и поиска неисправностей стека TCP/IP, проверила команды на своем компьютере.

# Работа № 3.

Часть 1.

Шаг 1. Выводим все необходимые данные

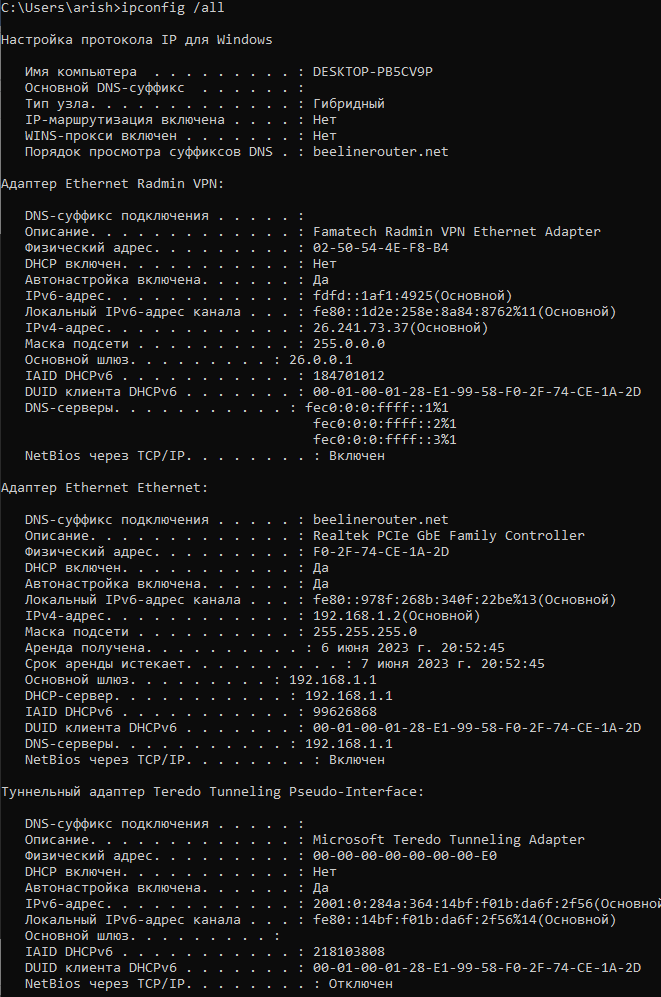


Рисунок 12. Команда ipconfig /all

Шаг 2. Строки данных из захваченного пакета

В программе Wireshark выводим строки данных из захваченного сетевого пакета.

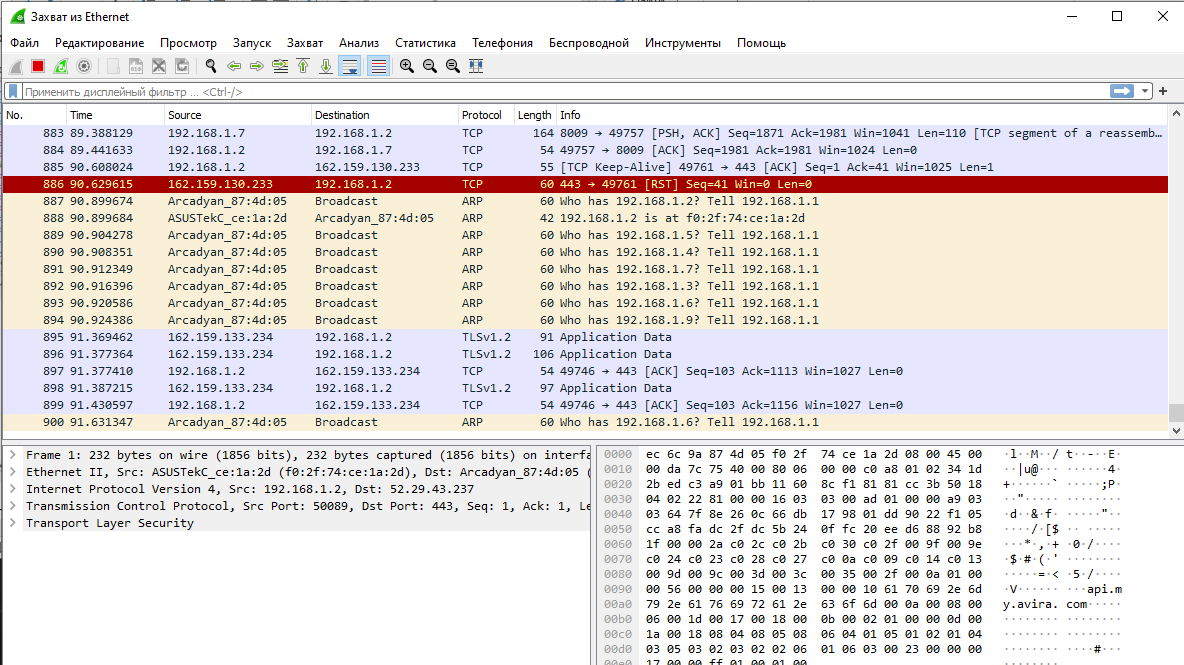


Рисунок 13. Данные из захваченного сетевого пакета

Далее используем фильтр под единицы данных icmp и смотрим обновленный список.

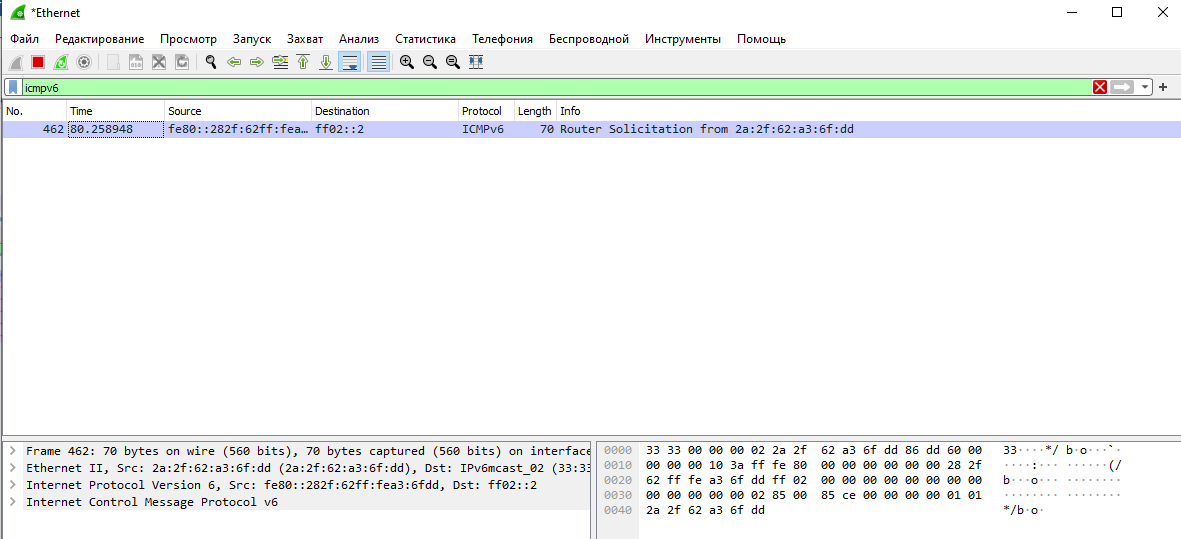


Рисунок 14. Фильтр данных icmp

Вопросы:

1. ***Совпадает ли MAC-адрес источника с интерфейсом компьютера?***



Ответ: нет

1. ***Совпадает ли MAC-адрес назначения в программе Wireshark с MAC-адресом другого участника рабочей группы?***

Ответ: да

1. ***Как ваш ПК определил MAC-адрес другого ПК, на который был отправлен эхо-запрос с помощью команды ping?***

Ответ: когда вы отправляете эхо-запрос с помощью команды ping, ваш компьютер отправляет пакет данных на указанный IP-адрес. В этом пакете данных содержится MAC-адрес вашего компьютера и IP-адрес компьютера, на который отправляется запрос. Когда пакет данных достигает целевого компьютера, он отвечает на запрос и отправляет ответный пакет данных обратно на ваш компьютер. В этом ответном пакете данных также содержится MAC-адрес целевого компьютера и IP-адрес вашего компьютера. Ваш компьютер использует эту информацию, чтобы определить MAC-адрес целевого компьютера.

Часть 2.

Шаг 1.

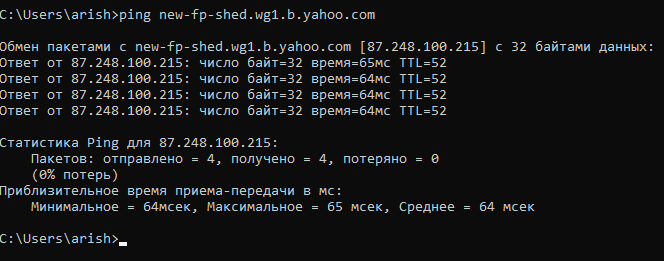


Рисунок 15. Проверка потери пакетов с сайтом new-fp-shed.wg1.b.yahoo.com

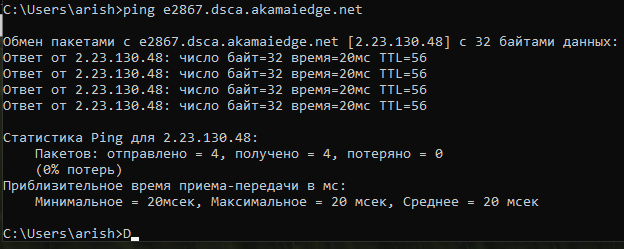


Рисунок 16. Проверка потери пакетов с сайтом e2867.dsca.akamaiedge.net

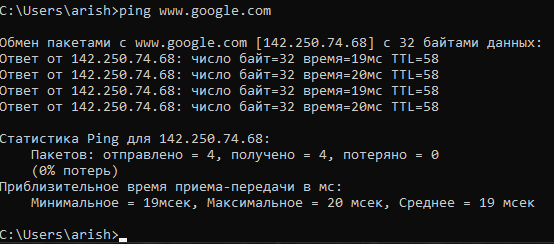
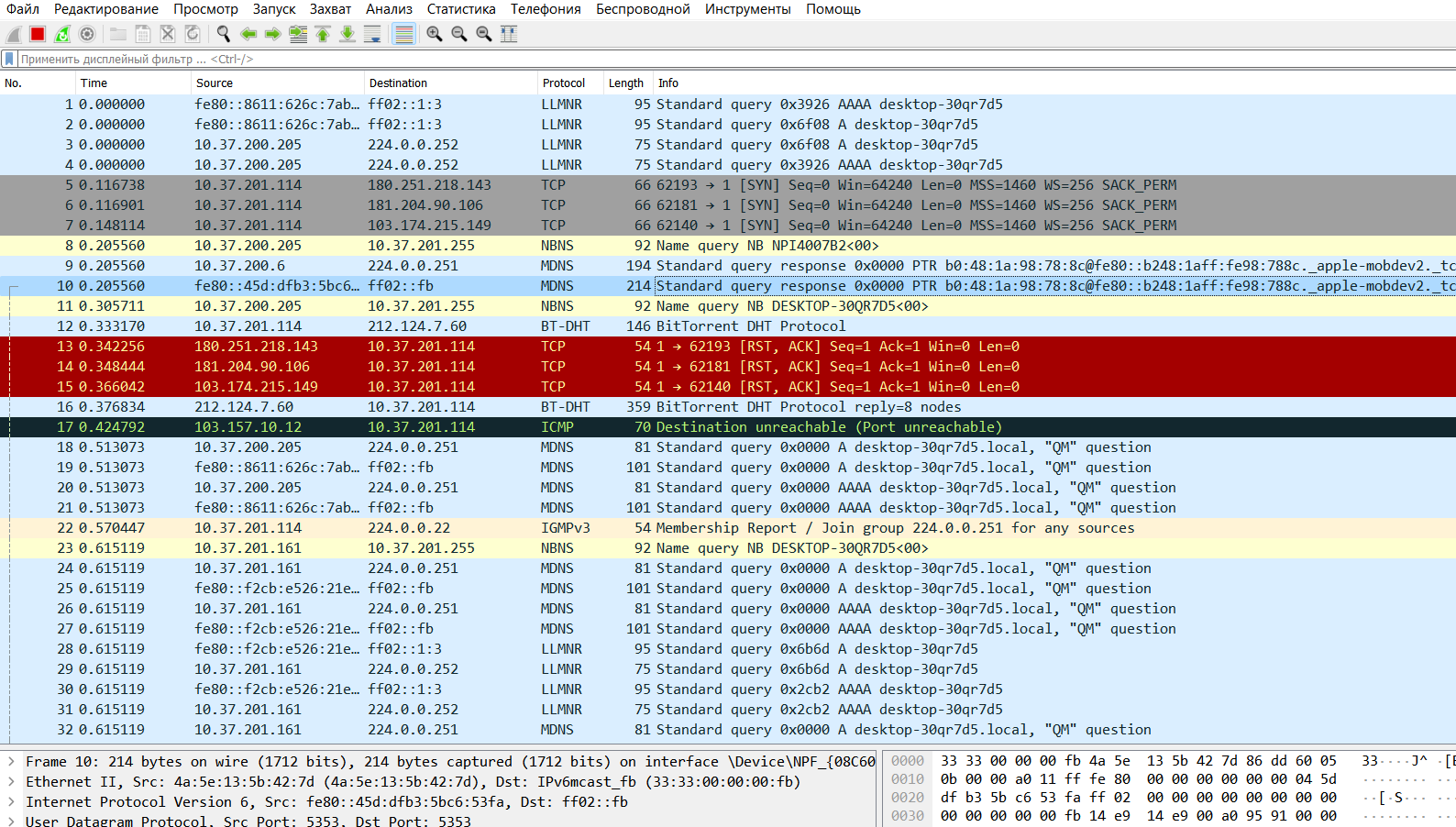


Рисунок 17. Проверка потери пакетов с сайтом www.google.com

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Шаг 2.



Вопросы:

1. ***Какова существенная особенность этих данных?***

Ответ: Все адреса имеют одинаковый MAC-адрес.

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

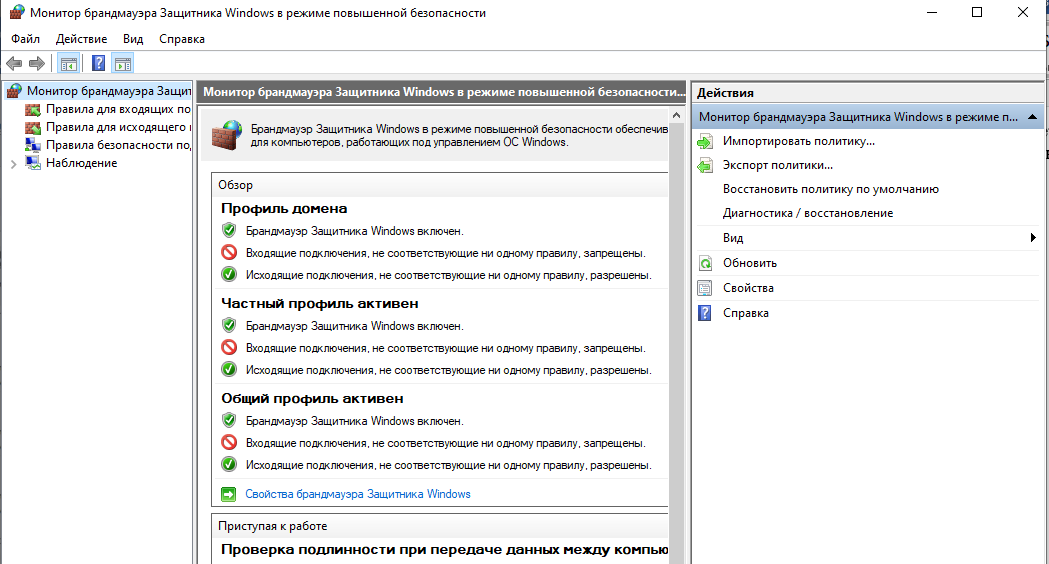
Ответ: В первой части показывается МАС-адрес компьютера  
находящегося в локальной сети, во второй части отображается МАС-  
адрес сетевого шлюза.

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

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

Часть 3.

Открываем монитор брандмауэра защитника в режиме повышенной безопасности.



Следующим шагом указываем путь к браузеру и нажимаем «Разрешить запросы ICMP».

***Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание***

***Изображение выглядит как снимок экрана, текст, программное обеспечение, веб-страница

Автоматически созданное описание***

Затем удаляем это правило.

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание