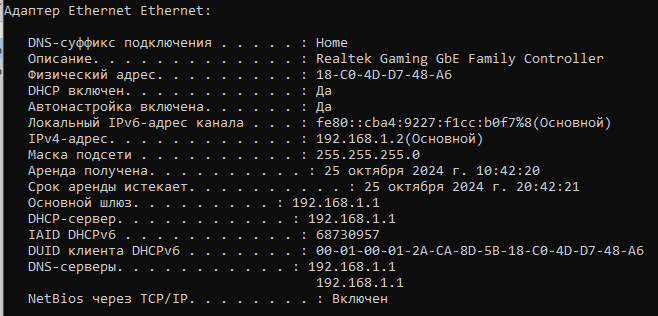
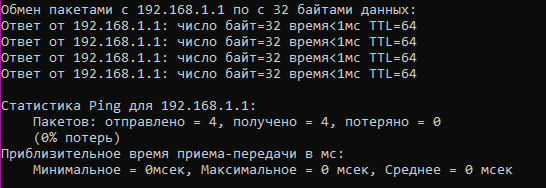
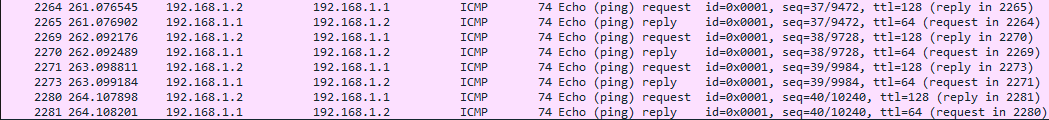
Лабораторная работа 2. Использование программы Wireshark для просмотра сетевого трафика

1. Сбор и анализ данных протокола ICMP по локальным узлам в программе Wireshark
   1. Узнайте адреса интерфейсов своего ПК.

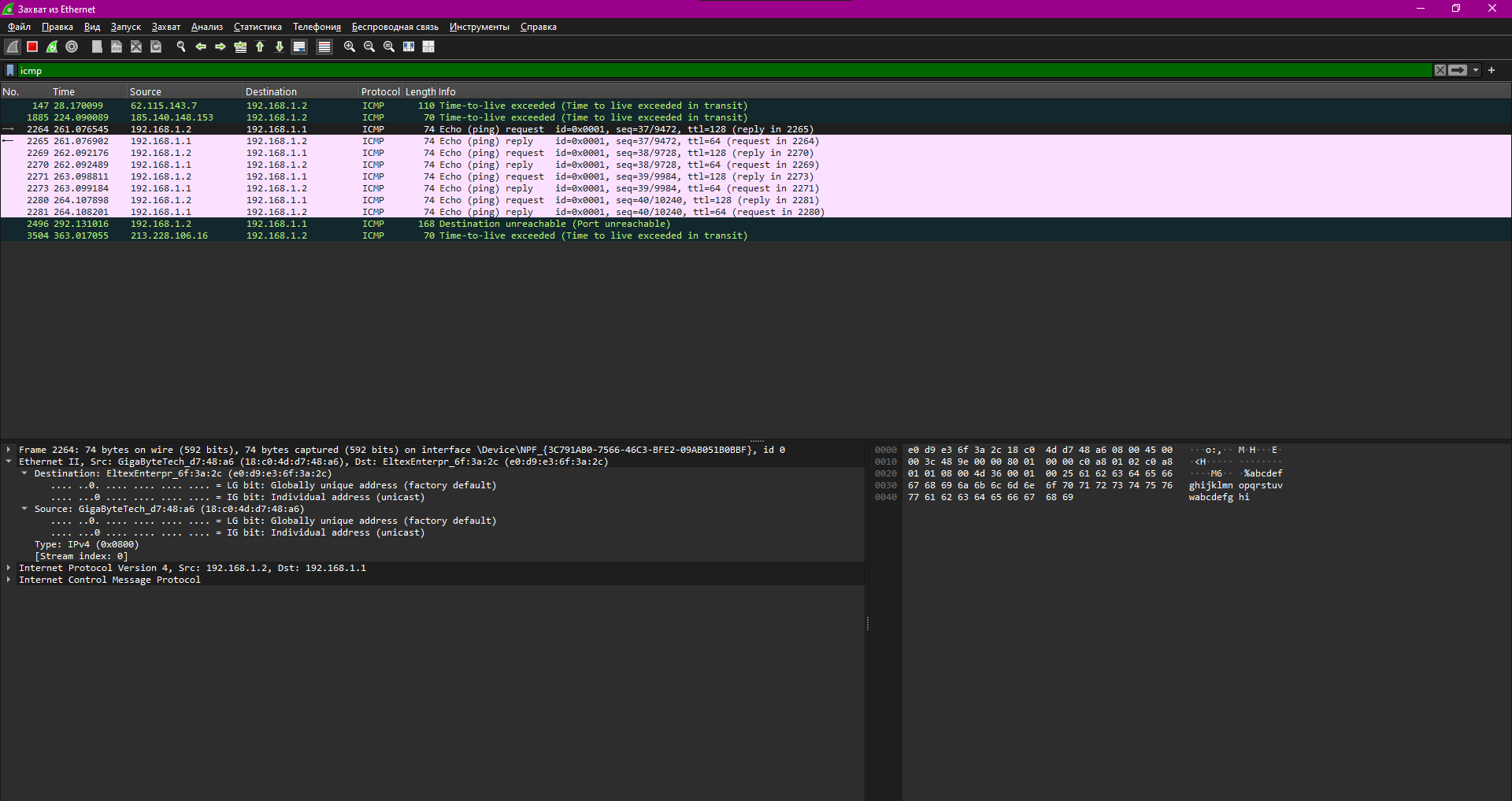


* 1. Запустите программу Wireshark и начните сбор данных.





* 1. Изучите полученные данные.



Соответствует ли MAC-адрес источника интерфейсу вашего ПК (показанному на шаге 1Б)? \_\_Да\_\_

Совпадает ли MAC-адрес назначения в программе Wireshark с MAC-адресом другого участника рабочей группы? \_\_Да\_

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

\_ПК отправляет ARP запрос, содержащий IP-адрес, для которого нужно узнать MAC, все устройства в локальной сети получают этот запрос, устройство с соответствующим IP отвечает на него своим MAC адресом\_

1. Сбор и анализ данных протокола ICMP по удаленным узлам в программе Wireshark

В части 2 вы должны будете отправить эхо-запросы с помощью команды ping на удаленные узлы (расположенные за пределами локальной сети) и изучить данные, сформированные этими запросами. Затем вам нужно будет определить различия между этими данными и данными, которые вы изучали в части 1.

* 1. Запустите захват данных в интерфейсе.
     + 1. www.mail.ru
       2. www.yandex.ru
       3. www.omgtu.ru
  2. Изучите и проанализируйте данные, полученные от удаленных узлов.
     1. Просмотрите собранные данные в программе Wireshark и изучите IP- и MAC-адреса трех веб-сайтов, на которые вы отправили ping-запросы. Ниже в оставленном месте укажите IP- и MAC-адреса назначения для всех трех веб-сайтов.

1-й адрес: IP: 217.69.139.70 MAC: e0:d9:e3:6f:3a:2c

2-й адрес: IP: 77.88.55.88 MAC: e0:d9:e3:6f:3a:2c

3адрес: IP: 185.129.102.137 MAC: e0:d9:e3:6f:3a:2c

* + 1. Какова существенная особенность этих данных?

\_Полученный MAC адрес является MAC адресом маршрутизатора локальной сети ПК с которого отправляется запрос\_

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

\_В 1 части мы получали фактические MAC адреса устройств, подключенных к одной локальной сети, в этом случае был получен MAC адрес маршрутизатора\_\_\_

1. Вопросы для повторения

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

\_Потому что в случае с удалёнными узлами Wireshark может анализировать только трафик, проходящий через маршрутизатор\_