МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение   
высшего профессионального образования

«УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных Систем и Технологий

Кафедра «Информационные системы»

Дисциплина «Информационная безопасность»

**ОТЧЕТ**

**по лаборатороной работе № 3**

Тема Захват и анализ сетевого трафика

Выполнил студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_Кузнецов В. И.\_\_\_\_\_\_\_/

подпись инициалы, фамилия

Курс\_\_\_\_\_\_\_\_\_\_4\_\_\_\_\_\_\_\_\_\_\_\_\_ Группа\_\_\_\_\_\_\_ПИбд-41\_\_\_\_\_\_\_\_\_\_

Направление/специальность\_\_\_09.03.04. Программная инженерия\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель Мытарев П.В.

должность, ученая степень, ученое звание

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

фамилия, имя, отчество

Дата сдачи:

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_201\_\_г.

Дата защиты:

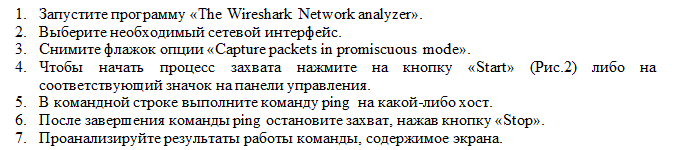
«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_201\_\_г.

Оценка: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ульяновск

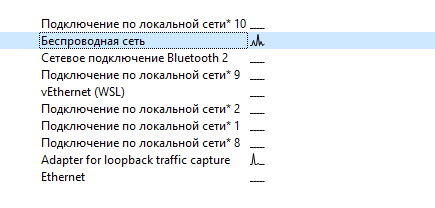
2020 г.

**Первая часть задания.**

****

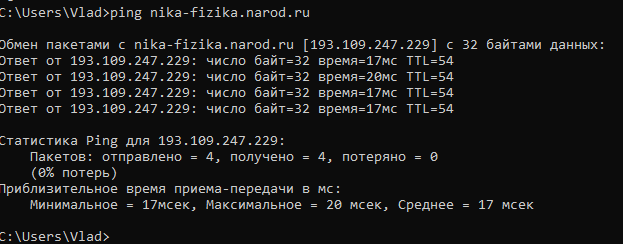
**Выполнение задания:**

Для перехвата сетевого трафика выберем сетевой интерфейс беспроводной сети:

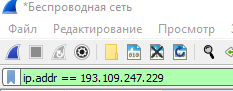


Для просмотра сетевого трафика попробуем сначала пропинговать сайт <http://nika-fizika.narod.ru/>

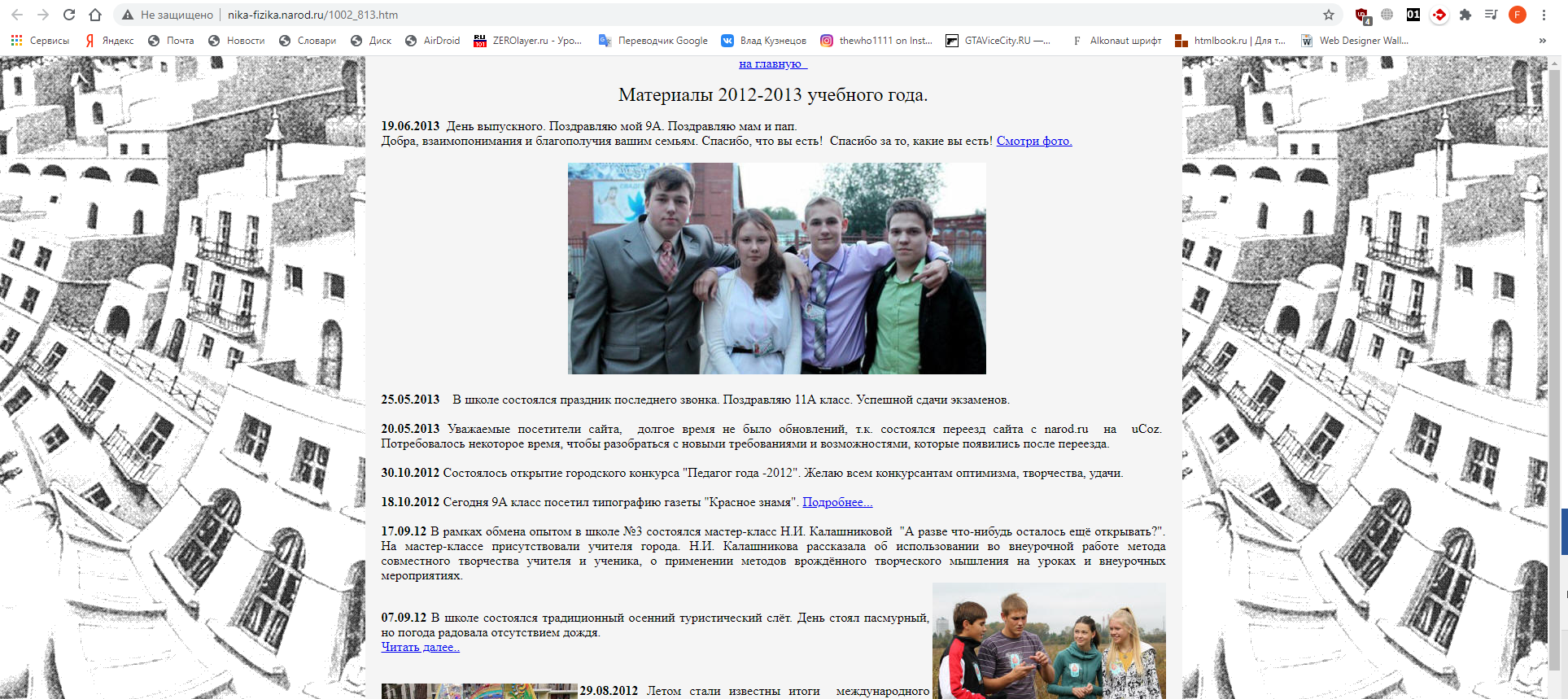
, для того чтобы узнать ip адрес сервера и применить фильтр по адресу в поле фильтров.



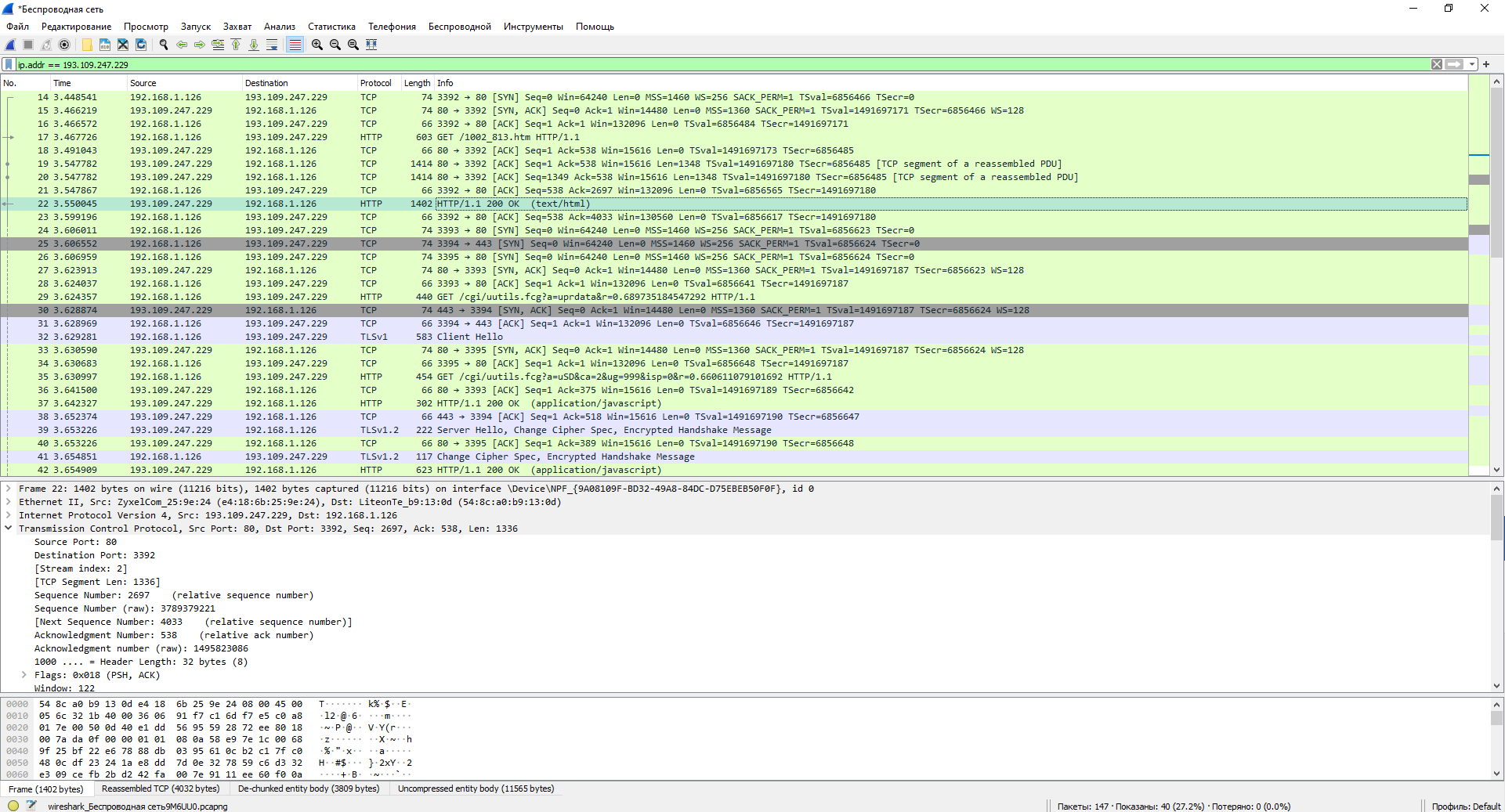
Применим фильтр.



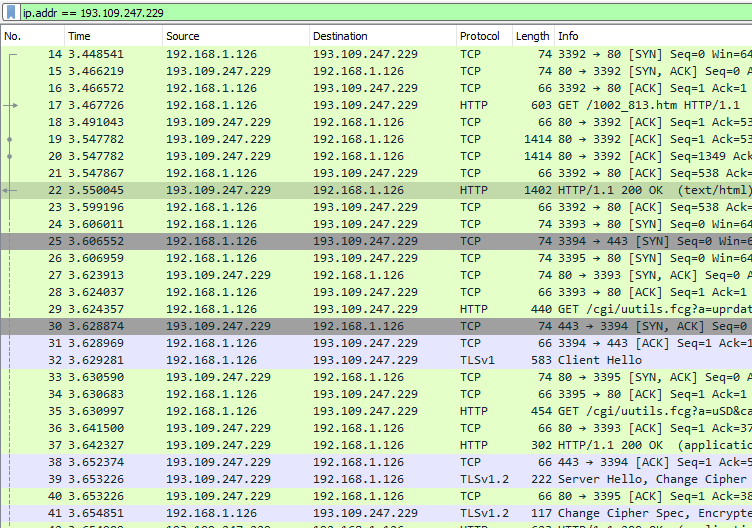
Откроем сайт в браузере.



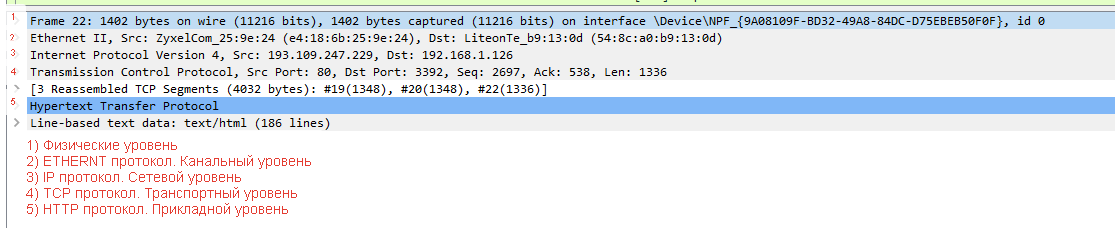
Остановим сканирование.



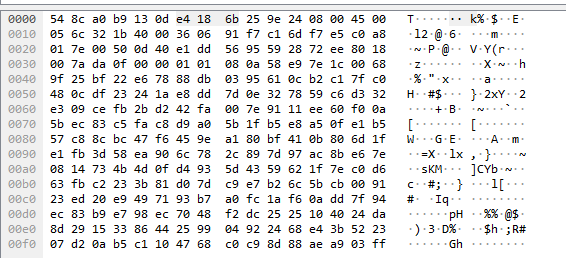
На экране мы видим все сетевые пакеты (удв. фильтру), отправленные в сеть с адресом получателя, отправителя, протоколом, размером пакета и т.д.



В средней секции видим представление пакета на разных уровнях модели OSI



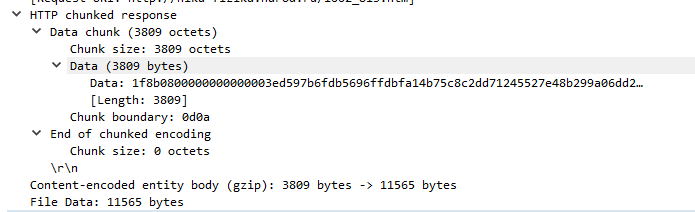
Внизу мы видим шестнадцатеричное представление пакета, в котором они бегают по сети.



Рассмотрим ответа сервера по протоколу HTTP:



Видим, что страница html записана чанками, общей длиной 11565 байт и упакована в gzip:



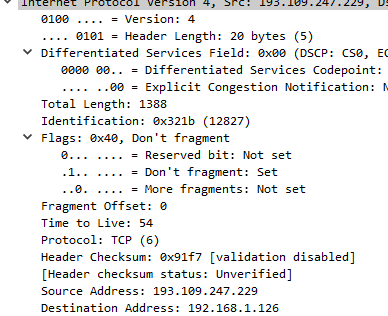
Рассмотрим распакованную страницу:



На транспортном уровне можем увидеть порты клиента и сервера:

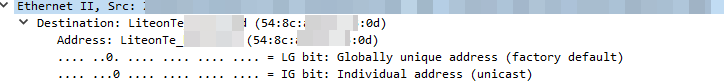


На сетевом уровне можем увидеть ip адреса клиента и сервера:

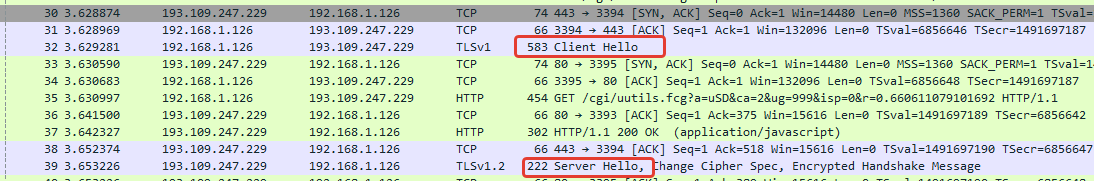


На канальном уровне можно увидеть mac-адреса устройств:

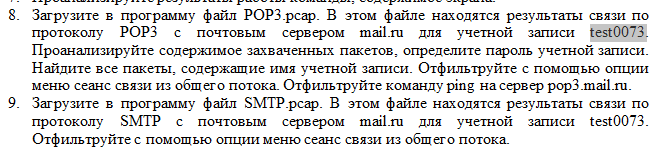




Также можно увидеть TLS рукопожатие:



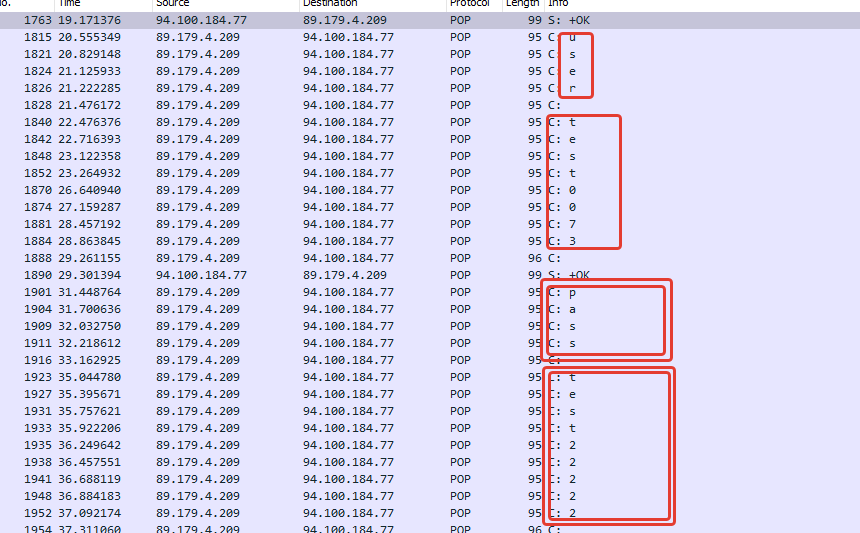
**Задание второе.**

****

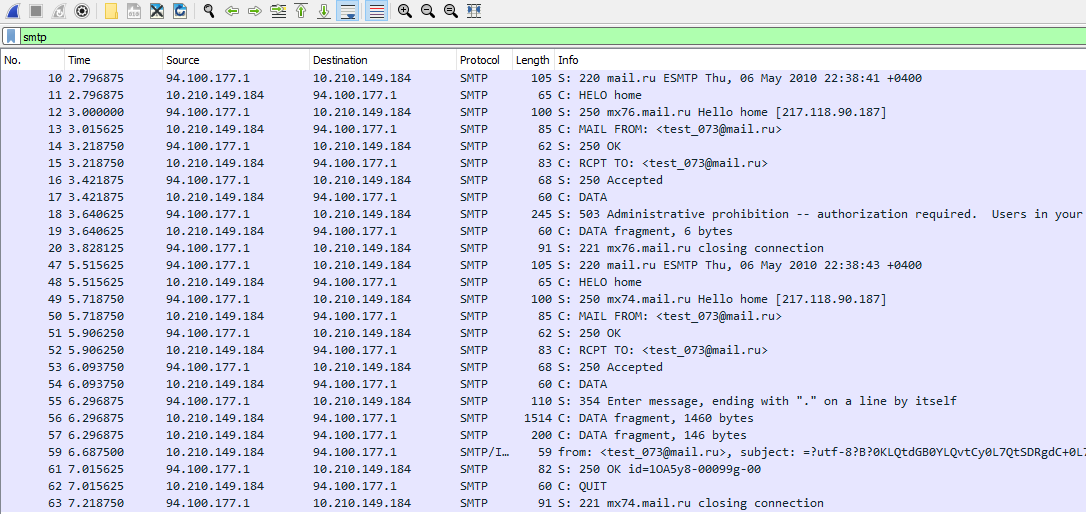
Применяем фильтр по протоколу pop.

****

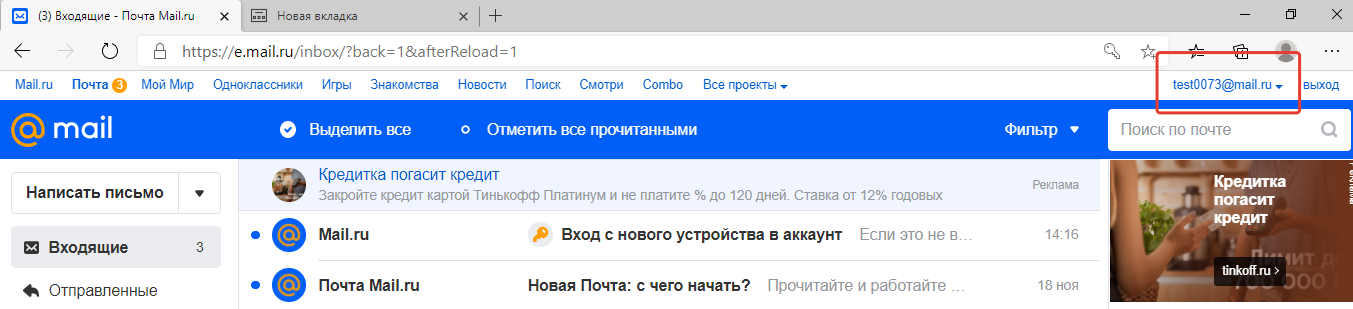
Находим POP3 команды USER … и PASS …

****

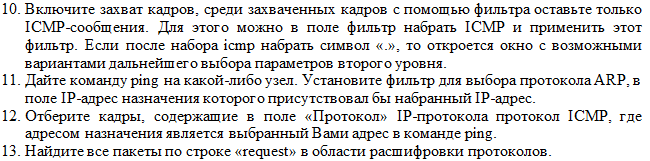
Фильтрация по протоколу smtp:



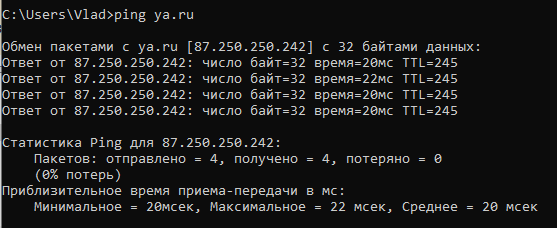
Выполняем вход в аккаунт:



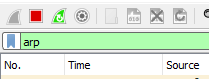
**Задание третье.**



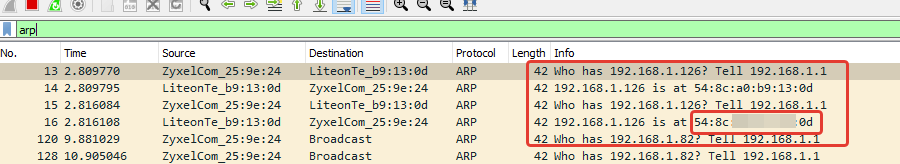
Пингуем сервер Яндекс:



Применяем фильтр arp.

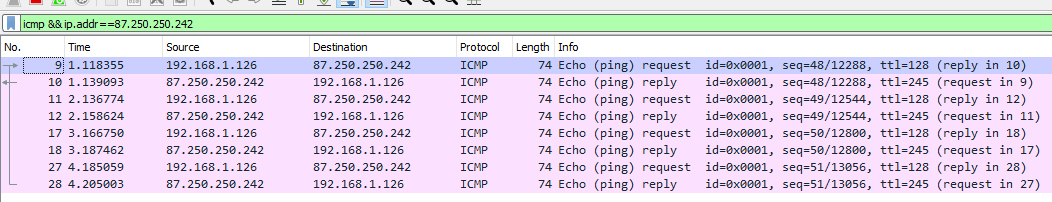


Находим mac-адрес и сверяем его с тем адресом, который записан в конфигах ОС.

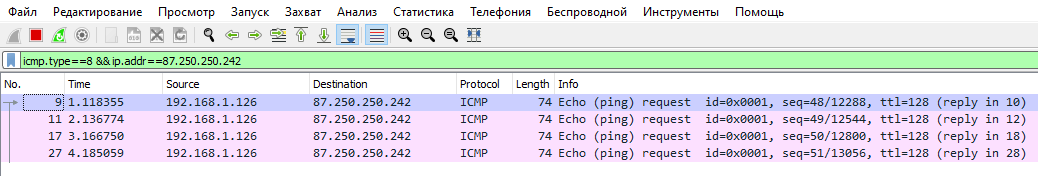




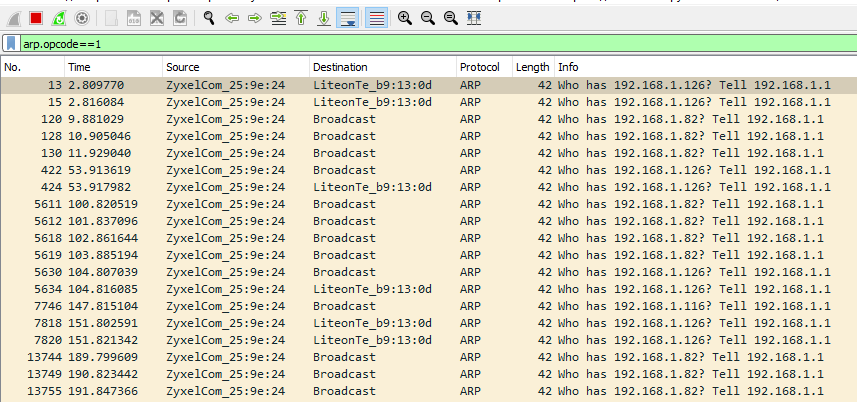
Находим все пакеты icmp-протокола, содержащие ip адрес сервера.



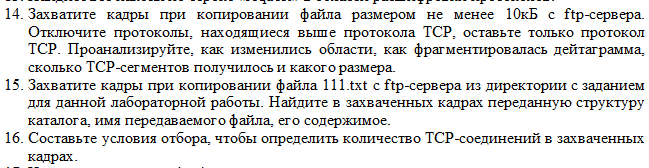
Находим все пакеты icmp-протокола, содержащие ip адрес сервера, по типу request



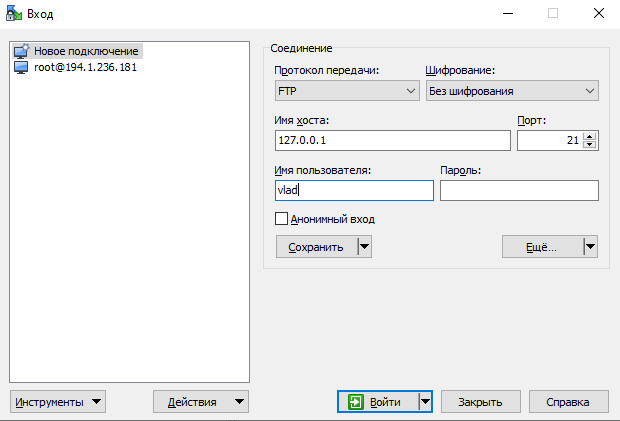
Находим все пакеты arp-протокола, по типу request

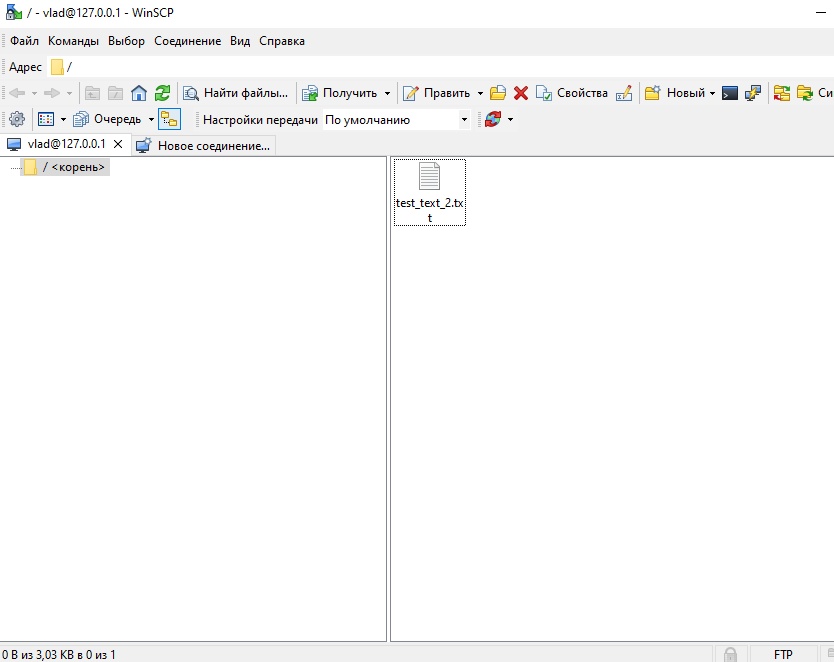


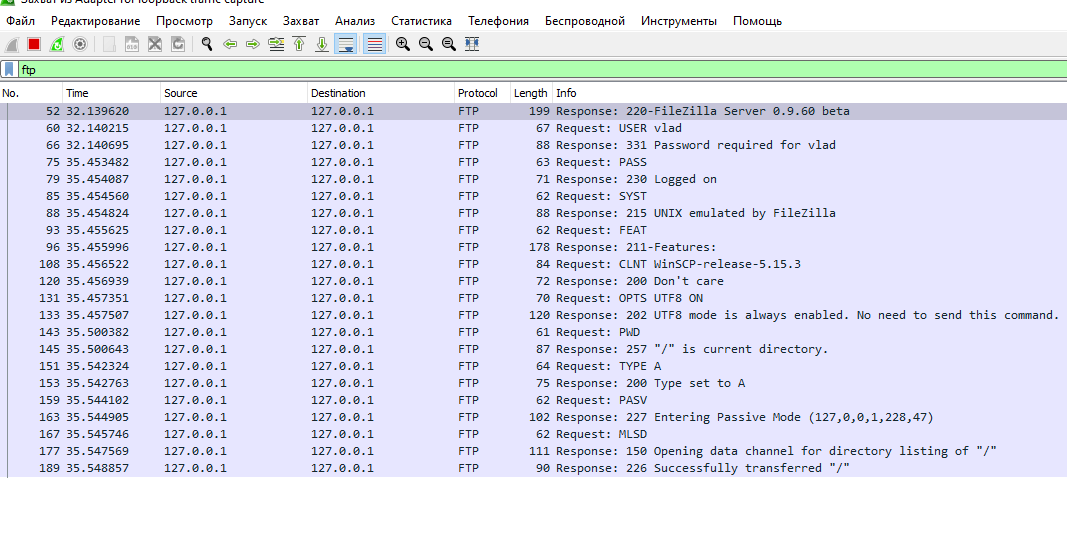
**Задание четвертое**



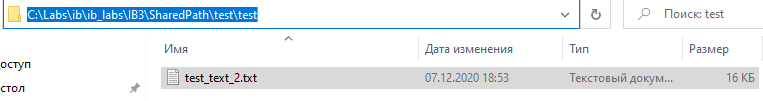
В отсутствии открытых ftp-серверов, поднял свой локальный, на кастомном порту.

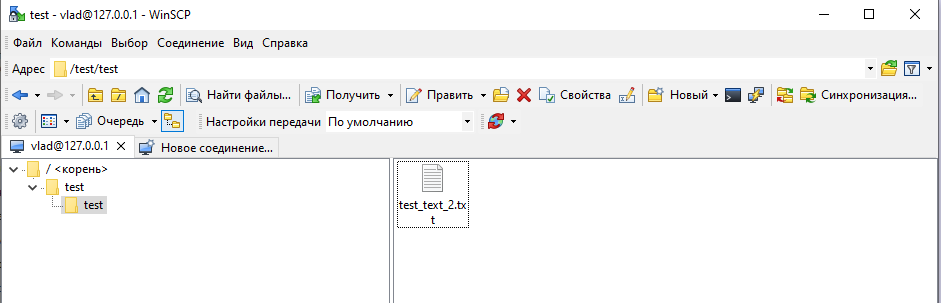






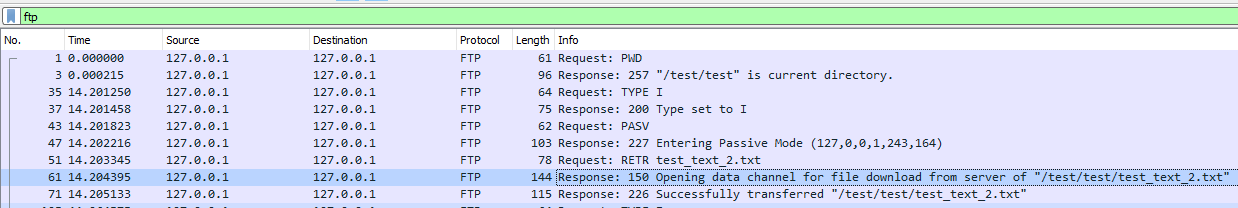
Корневая директория SharedPath с файлом вложенным в папки ./test/test

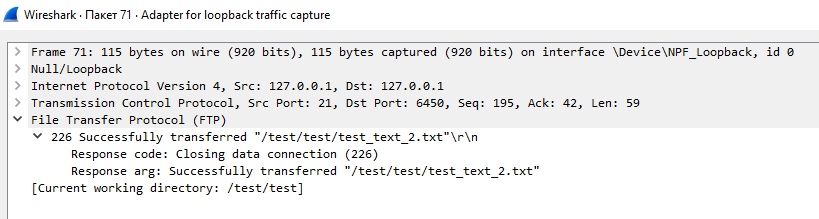




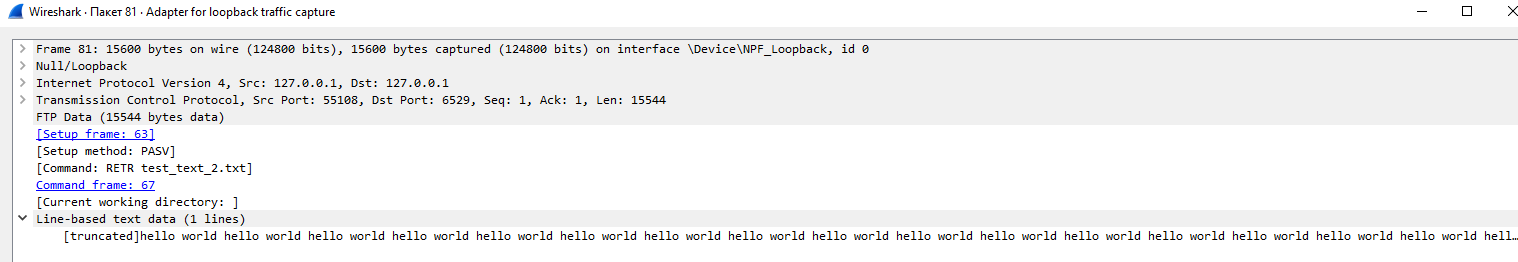
Копируем файл 16 кб с ftp сервера в папку хоста.

Видим расположение файла на сервере, путь до него.



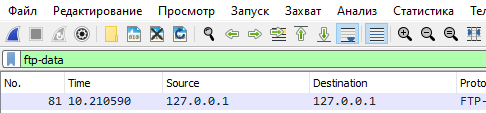


Содержимое файла.

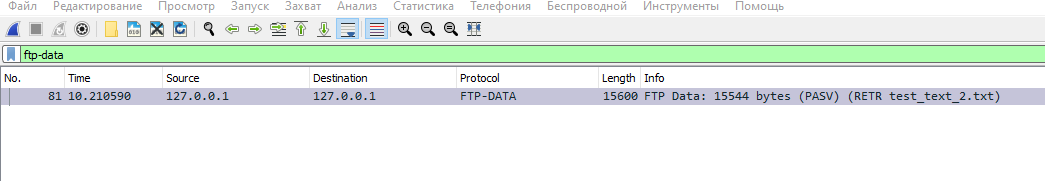


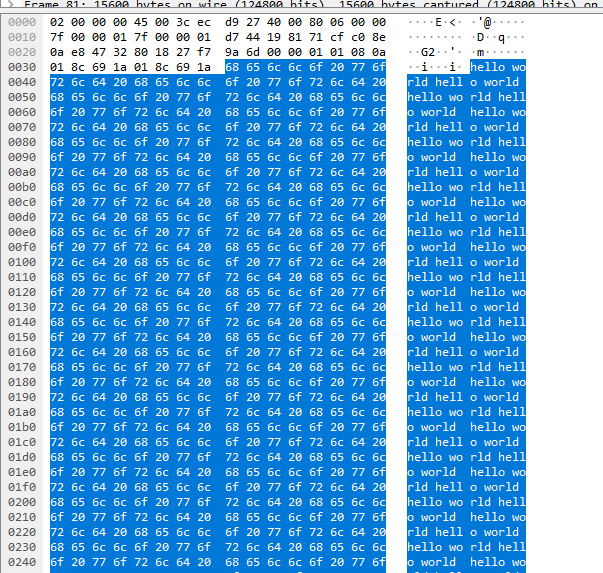
Файл отправился одним пакетом.

Используем фильтр по протоколу ftp-data.



Дейтаграмма равна 15600 байтам из которых 15544 заняты под данные.





Статистика:

