МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт цифровых технологий, электроники и физики

Кафедра вычислительной техники и электроники (ВТиЭ)

Лабораторная работа № 7

**Доступность информации. Анализ сетевого трафика. Снифферы.**

Выполнил студент 595 гр.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Лаптев

Проверил:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ П.С. Ладыгин

Лабораторная работа защищена

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2023 г.

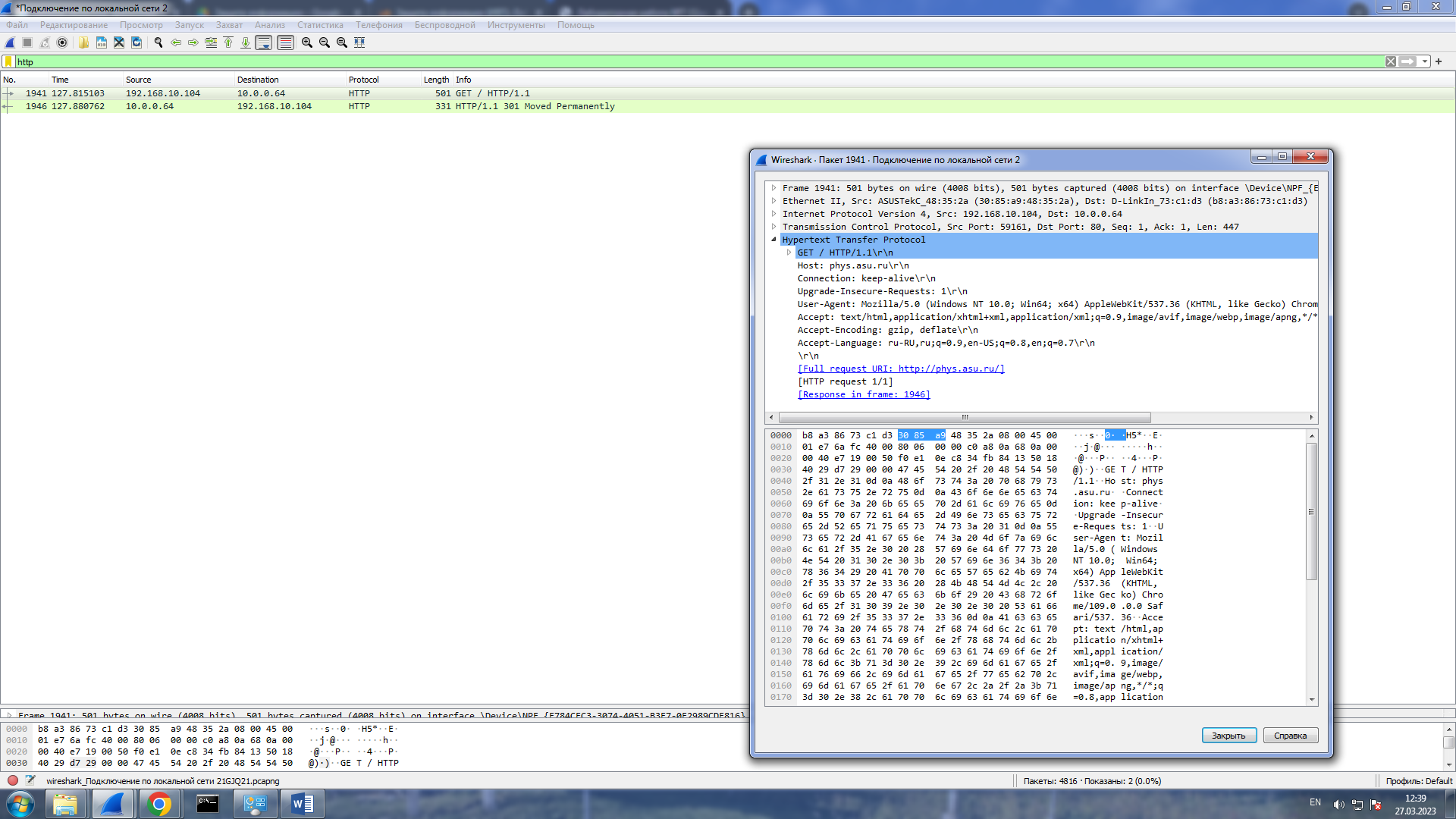
Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Цель работы:** рассмотрение методов обеспечения доступности информации, а также возможности анализа сетевого трафика на примере снифферов.

**Задачи:**

1. Работа с Wireshark.
   1. Запустите анализатор трафика Wireshark.
   2. Включите захват пакетов на вашей рабочей станции.
   3. Зайдите на сайт с HTTP соединением, например <http://phys.asu.ru>.
   4. Проанализируйте полученный трафик, найдите пакеты протокола HTTP.
   5. Вставьте в отчет скриншот одного из пакетов. В каком виде передаются данные?

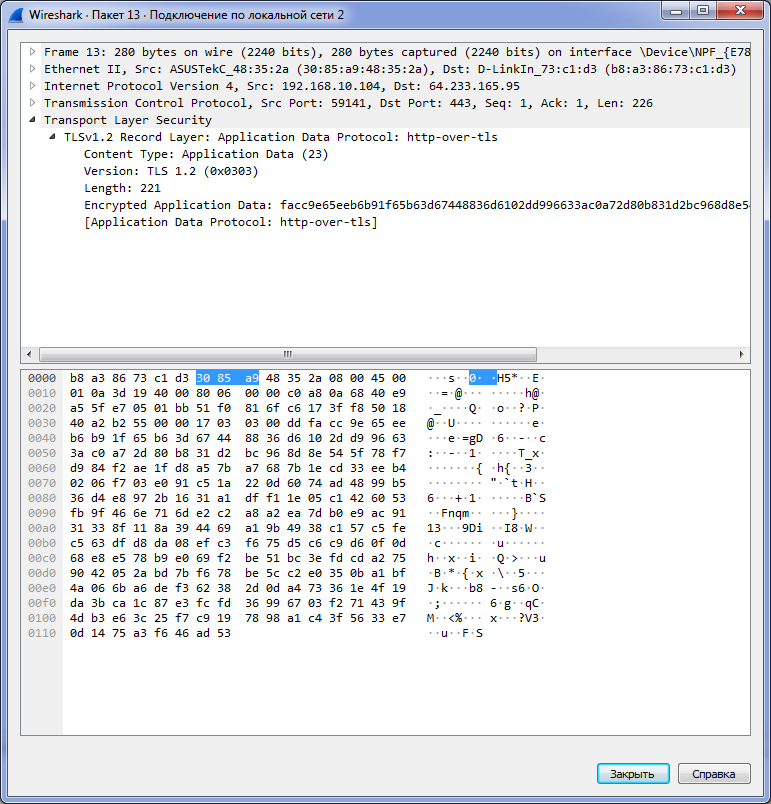
В протоколе HTTP данные передаются в незашифрованном формате.



*Рис. 1. Содержимое HTTP-пакета.*

* 1. Перейдите на сайт с HTTPS соединением.
  2. Вставьте в отчет скриншот одного из пакетов. В каком виде передаются данные?

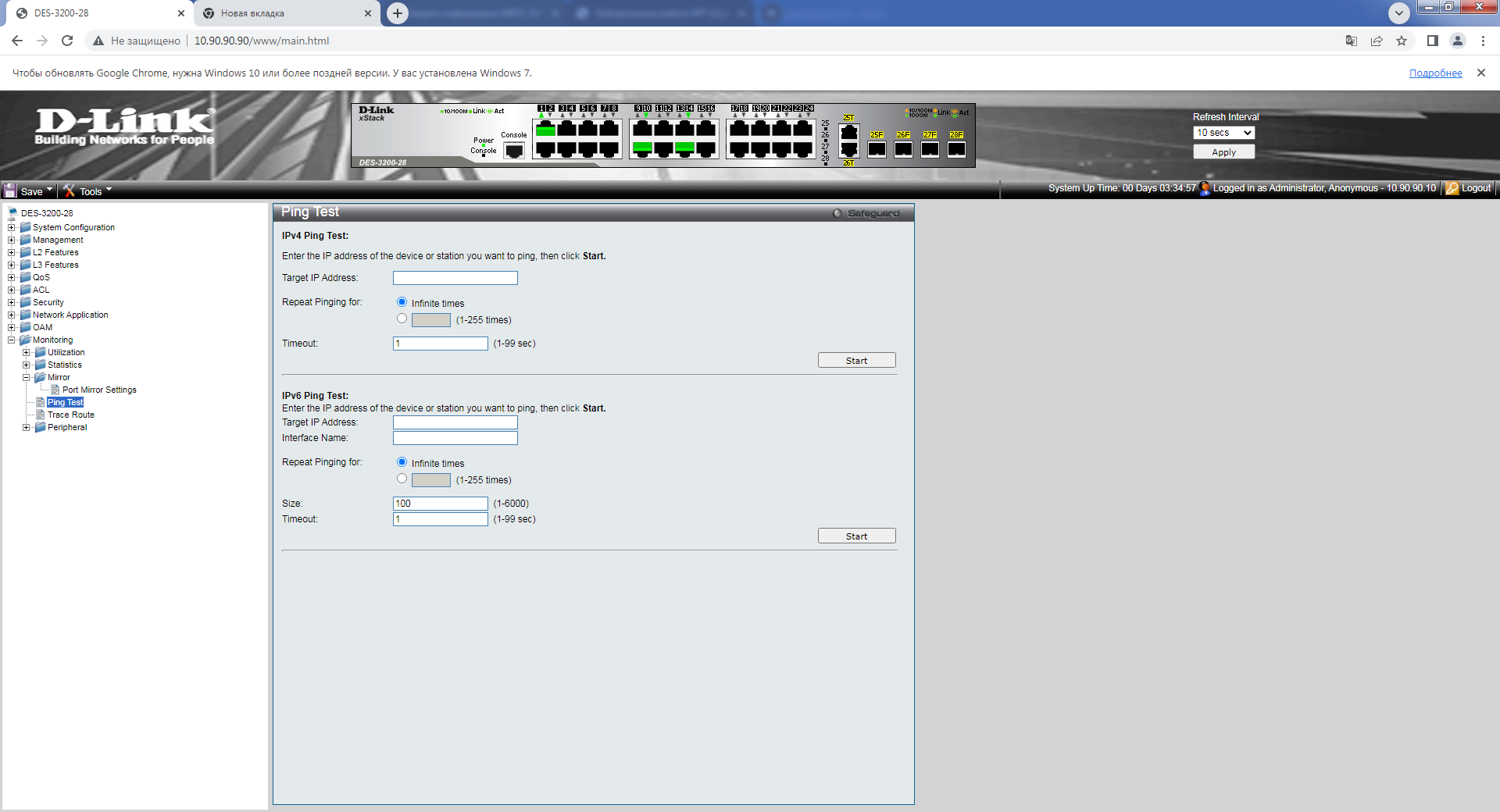
В протоколе HTTPS данные передаются в зашифрованном виде.



*Рис. 2. Содержимое HTTPS-пакета.*

1. Работа с коммутатором.
   * 1. Зайдите через браузер в web-интерфейс коммутатора D-Link DES 3200. По умолчанию коммутатор имеет IP адрес 10.90.90.90. Первоначально дайте своему компьютеру адрес в диапазоне 10.90.90.1-255 с маской подсети 255.255.255.0.
     2. Изучите настройки коммутатора, вставьте в отчет описание не менее двух пунктов меню со скриншотами.

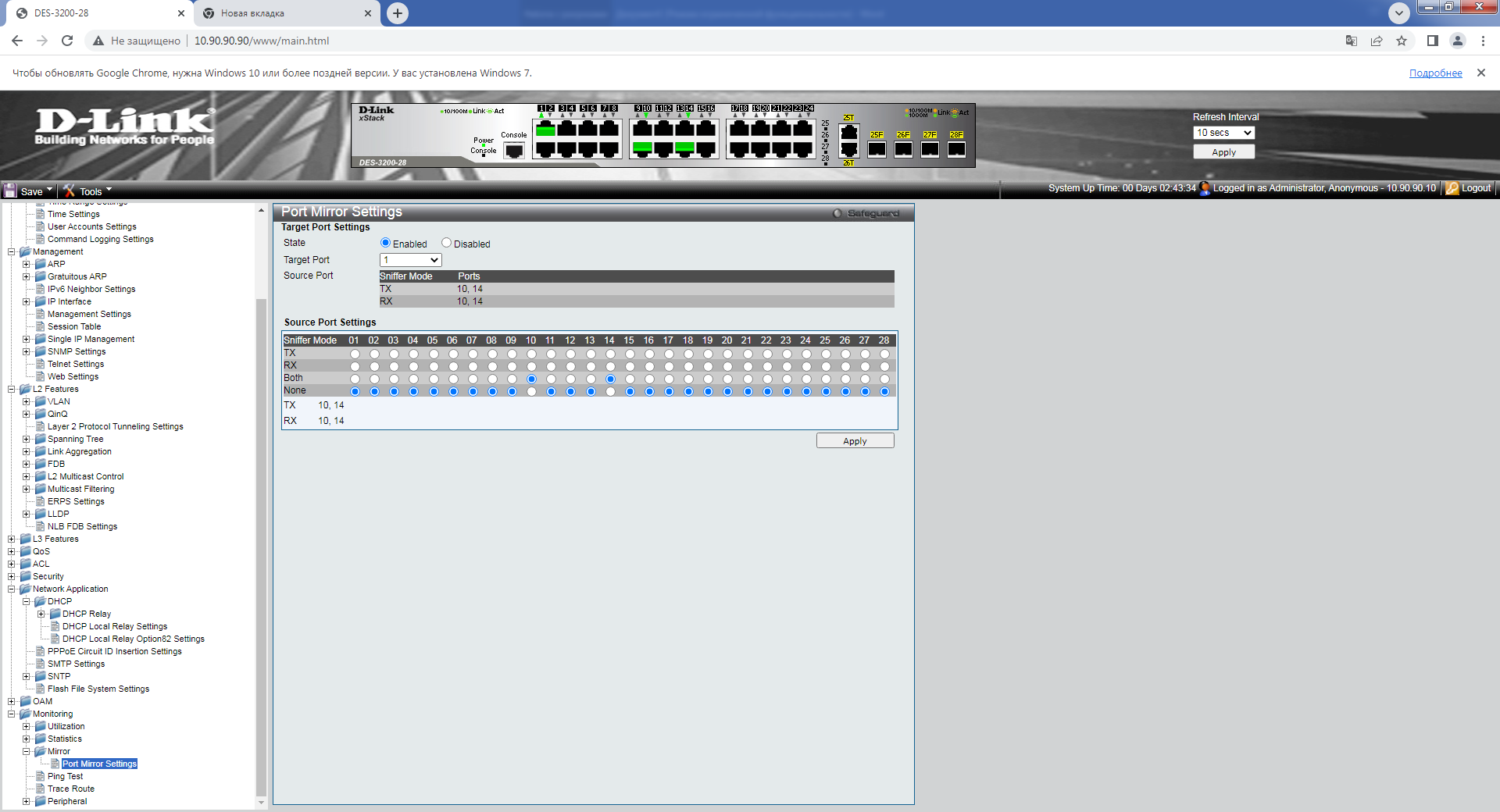
Один из пунктов меню – Ping Test. Он нужен для проверки соединения между ПК в одной сети.



*Рис. 3. Пункт меню – Ping Test.*

В верхнее поле вводим IP-адрес, к которому хотим постучаться. Ниже устанавливаем количество пакетов для передачи и таймаут передачи.

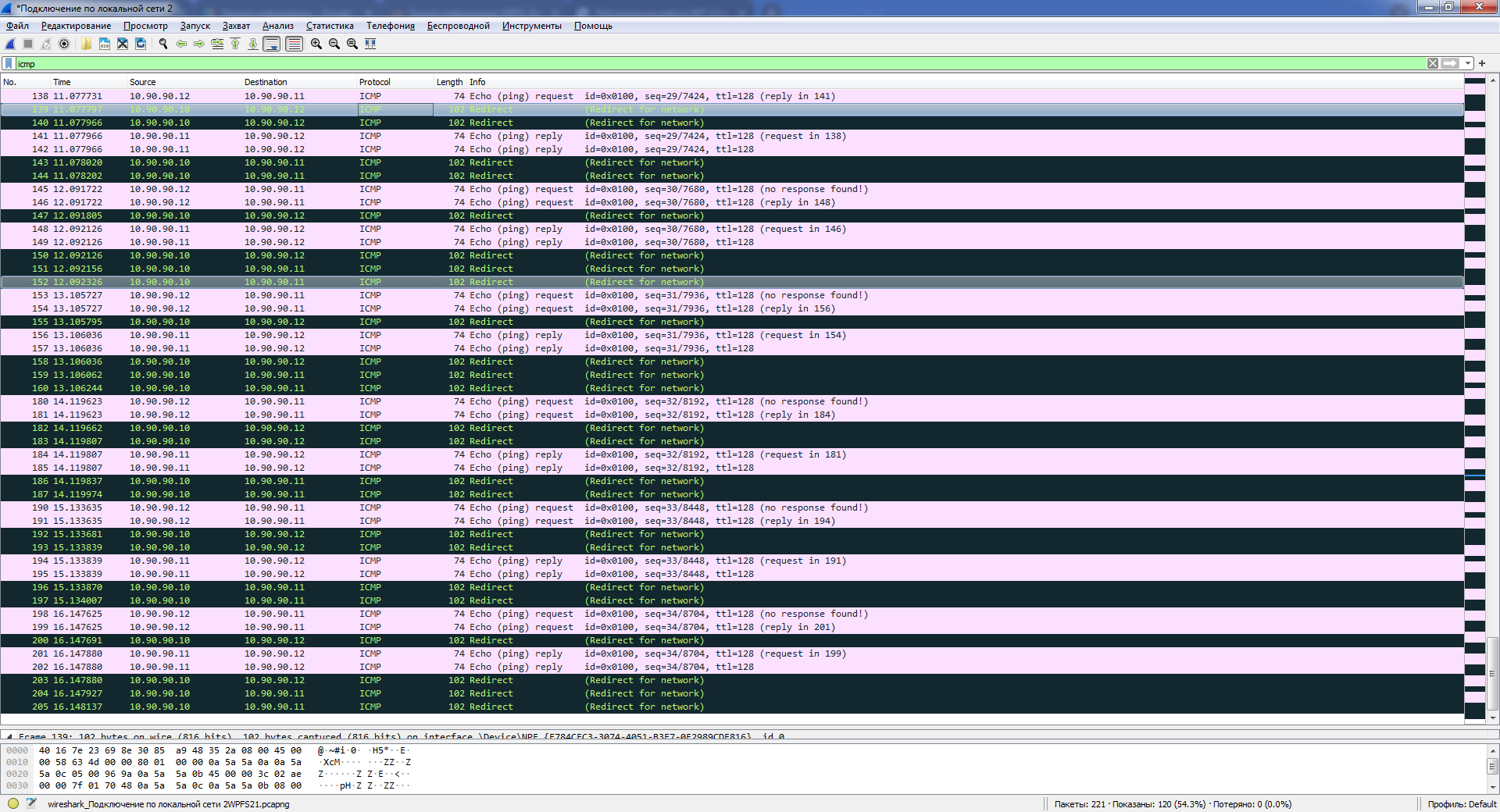
Еще один пункт меню – настройка зеркалирования.



*Рис. 4. Пункт меню – настройка зеркалирования.*

Здесь выбираем порт, который будет зеркалом (выпадающий список). И выбираем номера портов, с которых будет перехватываться трафик.

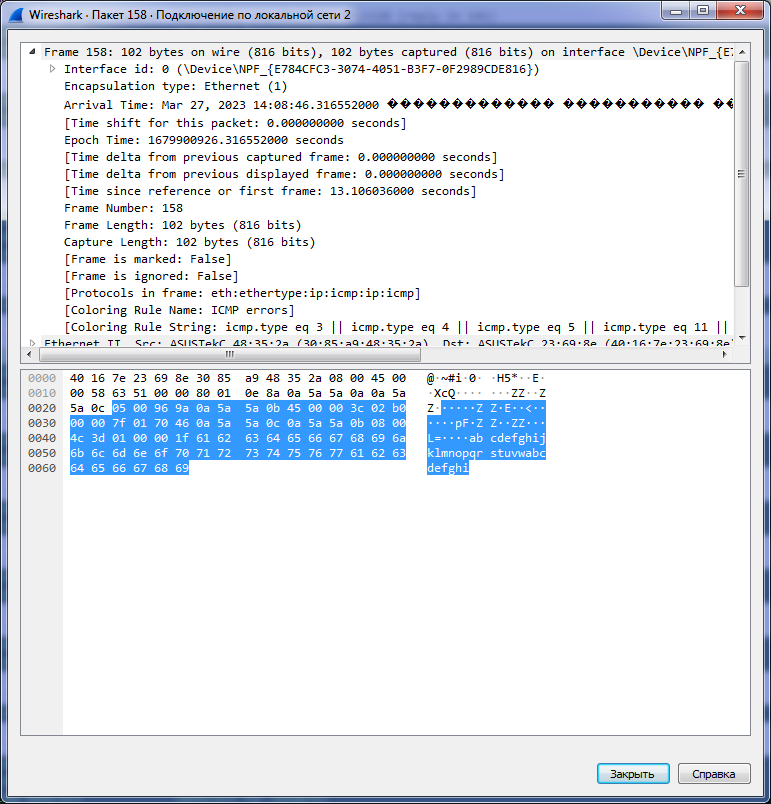
* + 1. Подключите к коммутатору ещё два компьютера, присвойте им адреса из того же диапазона.
    2. Настройте на первый ПК «зералирование», например, подключившись к нему через консоль (возможна команда telnet), можно попробовать настройку через Web-интерфейс.
    3. Включите на первом ПК Wireshark.
    4. На втором ПК попробуйте команду ping к третьему ПК.
    5. Проследите за появлением новых пакетов в программе Wireshark. Пакеты какого протокола захвачены анализатором? Вставьте скриншот в отчёт.



*Рис. 5. Пакеты, захваченные Wireshark.*

В результате перехвата были захвачены пакеты ICMP (на приведенном скриншоте применен фильтр, поэтому видны только эти пакеты).

Ниже приведен пример содержимого таких пакетов.



*Рис. 6. Пример содержимого ICMP-пакета.*

**Вывод:** в ходе выполнения лабораторной работы были рассмотрены методы обеспечения доступности информации, а также возможности анализа сетевого трафика на примере снифферов.

**Ответы на контрольные вопросы:**

1. «Человек посередине» — это кто?

О: «Человек посередине» — вид [атаки](https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%B0%D0%BA%D0%B0_%D0%BF%D0%BE_%D1%81%D1%82%D0%BE%D1%80%D0%BE%D0%BD%D0%BD%D0%B8%D0%BC_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%B0%D0%BC) в [криптографии](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F) и [компьютерной безопасности](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C), когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом.

Является методом [компрометации](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%80%D0%BE%D0%BC%D0%B5%D1%82%D0%B0%D1%86%D0%B8%D1%8F_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)) [канала связи](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB_%D1%81%D0%B2%D1%8F%D0%B7%D0%B8_%D0%B2_%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9_%D1%81%D0%B5%D1%82%D0%B8), при котором взломщик, подключившись к каналу между контрагентами, осуществляет вмешательство в протокол передачи, удаляя или искажая информацию.

1. Какие снифферы бывают?

О: Снифферы пакетов, снифферы Wi-Fi, снифферы сетевого трафика и снифферы пакетов IP.

1. Возможен ли перехват трафика в беспроводной сети?

О: Да, конечно. Для этого существует специальный вид снифферов – Wi-Fi снифферы.