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 _____

Барнаул 2023

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

Задачи:

1. Работа с Wireshark.

1.1. Запустите анализатор трафика Wireshark.
1.2. Включите захват пакетов на вашей рабочей станции.
1.3. Зайдите на сайт с HTTP соединением, например http://phys.asu.ru.
1.4. Проанализируйте полученный трафик, найдите пакеты протокола HTTP.
1.5. Вставьте в отчет скриншот одного из пакетов. В каком виде передаются данные?
В протоколе HTTP данные передаются в незашифрованном формате.

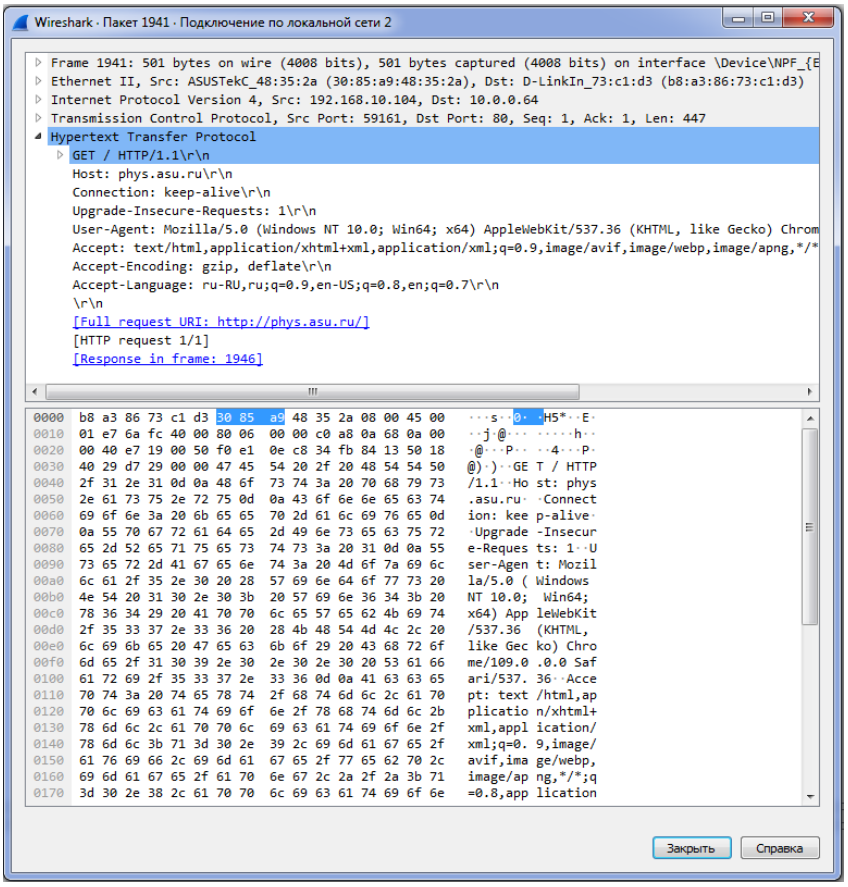

Рис. 1. Содержимое HTTP-пакета.

1.6. Перейдите на сайт с HTTPS соединением.
1.7. Вставьте в отчет скриншот одного из пакетов. В каком виде передаются данные?
В протоколе HTTPS данные передаются в зашифрованном виде.

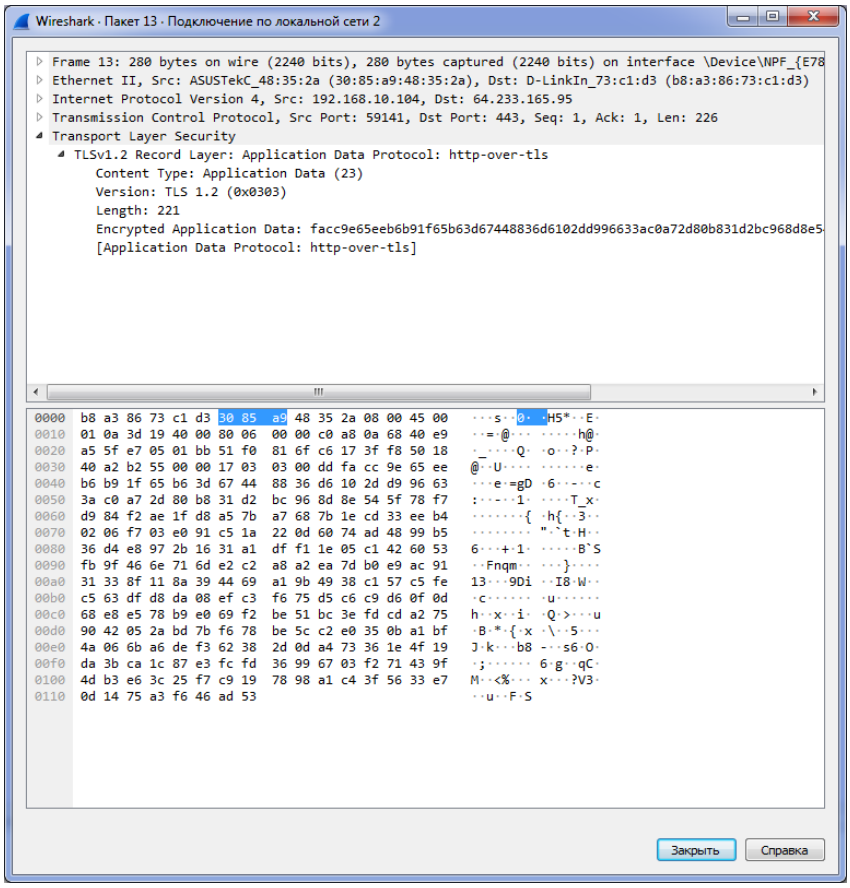

Рис. 2. Содержимое HTTPS-пакета.

2. Работа с коммутатором.

2.1. 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.

2.2. 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.

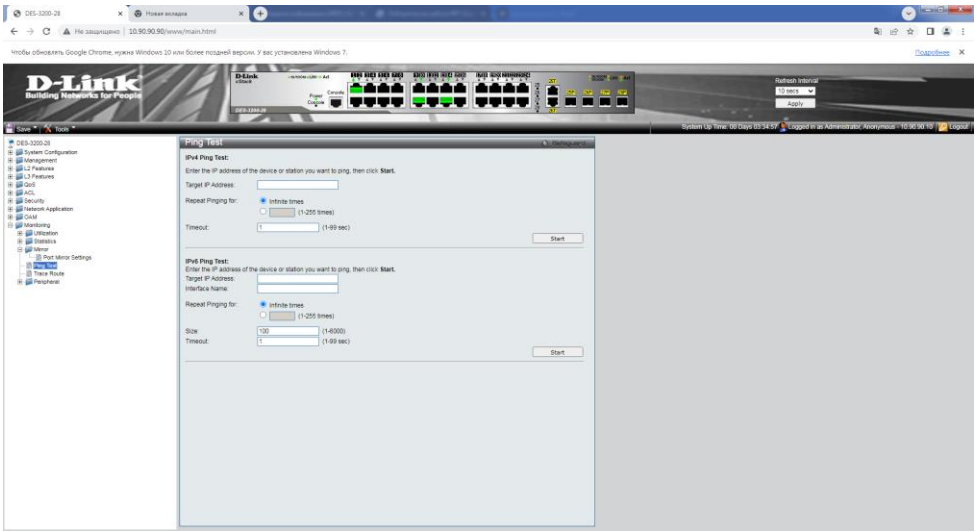

Рис. 3. Пункт меню – Ping Test.

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.

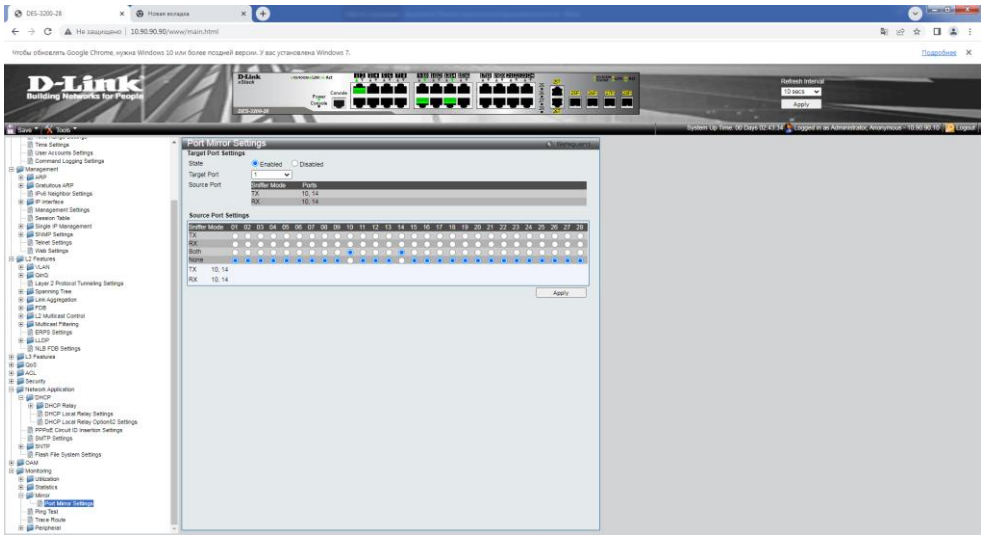

Рис. 4. Пункт меню – настройка зеркалирования.

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

2.3. Подключите к коммутатору ещё два компьютера, присвойте им адреса из того же диапазона.

2.4. Настройте на первый ПК «зералирование», например, подключившись к нему через консоль (возможна команда telnet), можно попробовать настройку через Web-интерфейс.

2.5. Включите на первом ПК Wireshark.

2.6. На втором ПК попробуйте команду ping к третьему ПК.

2.7. Проследите за появлением новых пакетов в программе Wireshark. Пакеты какого протокола захвачены анализатором? Вставьте скриншот в отчёт.

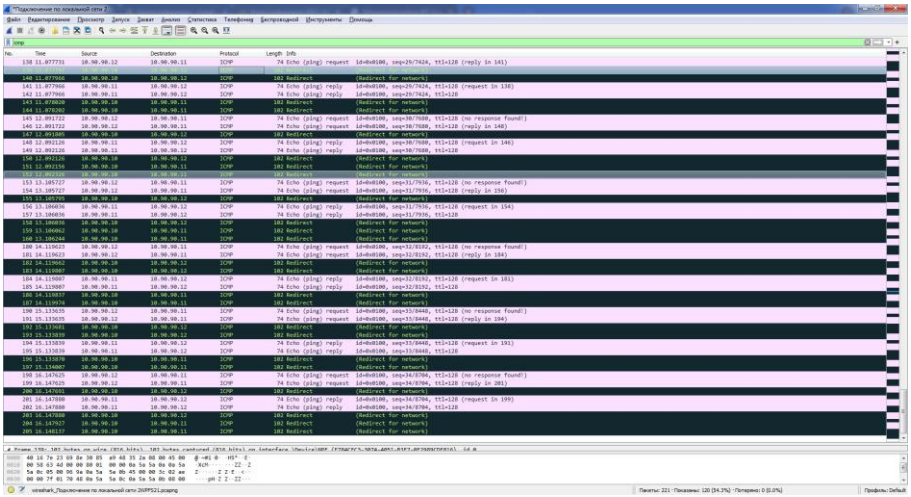

Рис. 5. Пакеты, захваченные Wireshark.

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

Ниже приведен пример содержимого таких пакетов.

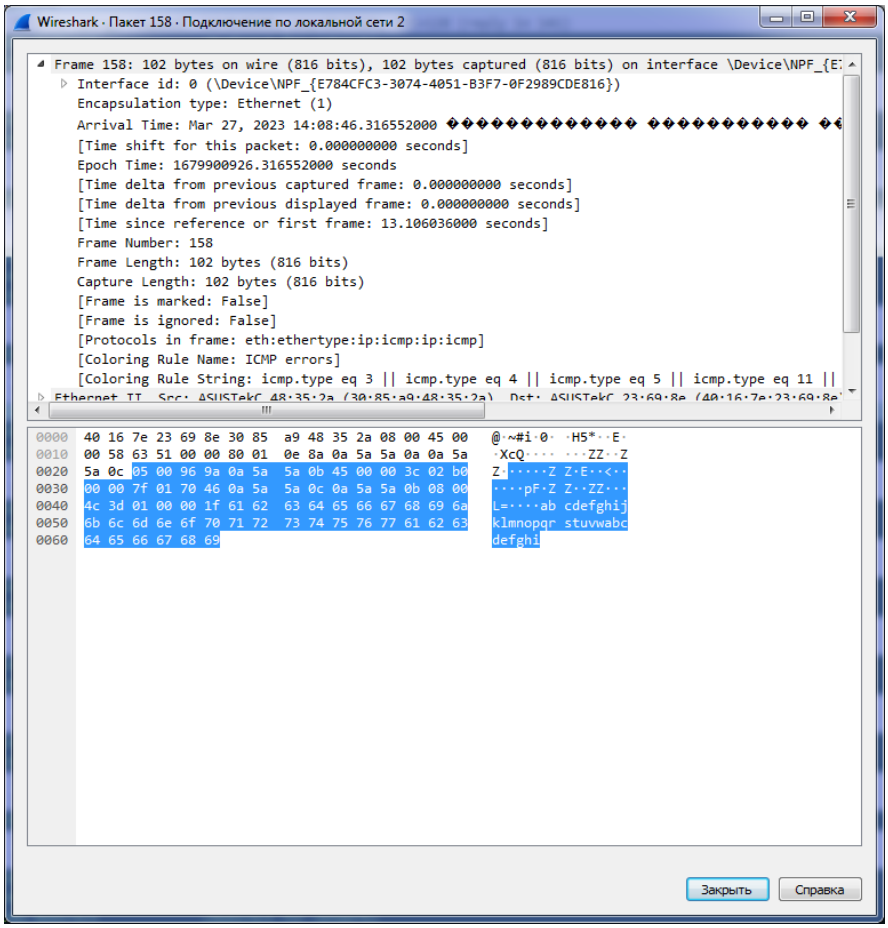

Рис. 6. Пример содержимого ICMP-пакета.

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 в криптографии и компьютерной безопасности, когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом.
   Является методом компрометации канала связи, при котором взломщик, подключившись к каналу между контрагентами, осуществляет вмешательство в протокол передачи, удаляя или искажая информацию.
2. Какие снифферы бывают?
   О: Снифферы пакетов, снифферы Wi-Fi, снифферы сетевого трафика и снифферы пакетов IP.
3. Возможен ли перехват трафика в беспроводной сети?

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