МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ

«Брестский государственный технический университет»

Кафедра «Интеллектуальные информационные технологии»

Лабораторная работа №3

По дисциплине «Аппаратное и программное обеспечение сетей»

Тема: «АНАЛИЗ СЕТЕВОГО ТРАФИКА И ПРОТОКОЛОВ НА

БАЗЕ WIRESHARK»

Выполнил:

студент 3 курса

группы ИИ-23

Романюк А. П.

Проверил:

Степанчук В.И.

Брест 2024

**Цель работы:** изучить программу wireshark, научиться перехватывать пакеты.

**Задание 1**

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

Автоматически созданное описаниеЗапустив Wireshark на захват, выполнить загрузку доступной в

лабораторных условиях страницы (bstu.by, iit.bstu.by или др.).

Остановить и сохранить захват. Для захваченных пакетов определить

статистические данные:

* процентное соотношение трафика разных протоколов в сети;
* среднюю скорость кадров/сек;
* среднюю скорость байт/сек;
* минимальный, максимальный и средний размеры пакета;
* степень использования полосы пропускания канала (загрузку сети)

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

Автоматически созданное описаниеИзображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Изображение выглядит как текст, диаграмма, линия, График

Автоматически созданное описание

**Задание 2**

Отфильтровать в захвате IP пакеты. Определить статистические

данные:

* процентное соотношение трафика разных протоколов стека tcp/ip в сети;
* средний, минимальный, максимальный размеры пакета.

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

Автоматически созданное описание

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

Автоматически созданное описаниеИзображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

Изображение выглядит как текст, линия, График, диаграмма

Автоматически созданное описание

**Задание 3**

Запустив Wireshark на захват, выполнить команду ping для IP адреса соседней рабочей станции в лаборатории (предварительно определив ее адрес с помощью ipconfig

). Сохранить результат. Сформировав нужный фильтр, отфильтровать пакеты, относящиеся к выполнению команды ping. На базе полученных пакетов и значений их полей интерпретировать результат работы утилиты ping. Описать все протоколы, используемые утилитой. Составить диаграмму взаимодействия машин при работе утилиты ping. Примечание. Данная утилита использует протокол ICMP (RFC 792 и RFC 960).

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

Автоматически созданное описание

Компьютер А отправляет компьютеру В данные, которые нужно отправить обратно. Они идут через сетевые устройства с некоторой задержкой, утилита ping замеряет эту задержку.

Структура протокола ICMP:

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

**Задание 4**

Запустив Wireshark на захват, выполнить разработанный в предыдущей лабораторной работе TCP-сервер и TCP-клиент. Сохранить результат. Сформировав нужный фильтр, отфильтровать пакеты данного сеанса. На примере любого TCP-сегмента указать структуру протокола TCP. Отметить поля заголовка, описать их и интерпретировать их значения. Составить диаграмму взаимодействия TCP-сервера и TCP-клиента.

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

Автоматически созданное описание

**Задание 5**

Запустив Wireshark на захват, выполнить разработанный в предыдущей лабораторной работе UDP-сервер и UDP-клиент. Сохранить результат. Сформировав нужный фильтр, отфильтровать пакеты данного сеанса. На примере любого UDP-сегмента указать структуру протокола UDP. Отметить поля заголовка, описать их и интерпретировать их значения.

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

Автоматически созданное описание

**Задание 6**

Выполнить анализ ARP-протокола по примеру из методических указаний.

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

Автоматически созданное описание

**Вывод:** изучил программу wireshark, научился перехватывать пакеты данных с разными протоколами передачи, изучил структуры некоторых протоколов.