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-21(1)

Романко Н.А.

Проверил:

Степанчук В.И.

Брест 2023

Цель: изучить приёмы работы с Wireshark, типы фильтрации трафика, правила построения фильтров, приёмы статистической обработки сетевого трафика в Wireshark.

Задания:

1. Изучить краткие теоретические сведения по возможностям, приемам работы с программой Wireshark (файл netWS.pdf).

2. Изучить: типы фильтрации трафика, правила построения фильтров, приемы статистической обработки сетевого трафика в Wireshark

3. Запустив 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).

Запустив Wireshark на захват, выполнить загрузку доступной в лабораторных условиях страницы (bstu.by, iit.bstu.by или др.). Остановить и сохранить захват. Изображение выглядит как текст, снимок экрана, документ, меню

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, График, линия

Автоматически созданное описание

Изображение выглядит как текст, число, Шрифт, линия

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

4)Отфильтровать в захвате IP пакеты. Определить статистические данные: • процентное соотношение трафика разных протоколов стека tcp/ip в сети; • средний, минимальный, максимальный размеры пакета. На примере любого IP-пакета указать структуры протоколов Ethernet и IP. Отметить поля заголовков и описать их и интерпретировать их значения.

Изображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

Изображение выглядит как текст, Шрифт, число, снимок экрана

Автоматически созданное описание

5. 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, снимок экрана, Шрифт, число

Автоматически созданное описание

Изображение выглядит как текст, линия, График, Параллельный

Автоматически созданное описание

6. 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, Шрифт, число

Автоматически созданное описание

Изображение выглядит как текст, линия, Шрифт, число

Автоматически созданное описание

7.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, снимок экрана, Шрифт, алгебра

Автоматически созданное описание

8. Выполнить анализ ARP-протокола по примеру из методических указаний.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Вывод: изучил приёмы работы с Wireshark, типы фильтрации трафика, правила построения фильтров, приёмы статистической обработки сетевого трафика в Wireshark.