|  |
| --- |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждениевысшего образования**«МИРЭА  Российский технологический университет»** **РТУ МИРЭА**  |

Институт информационных технологий

Кафедра Корпоративных Информационных Систем

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №5**

**по дисциплине**

«Разработка клиент-серверных приложений»

**Тема: «Отладка клиент-серверных приложений»**

|  |  |  |
| --- | --- | --- |
| Выполнил студент группы ИКБО-08-18 ИНБО-01-17 |  | Валяев Д.А. |
| Принял старший преподаватель |  | Мирзоян Д.И. |
| Лабораторная работа выполнена | «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_2020г. | *(подпись студента)* |
| «Зачтено» | «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_2020г. | *(подпись руководителя)* |

Москва 2020

# Задание

Произвести отладку и мониторинг сетевого обмена приложений из списка. Выполнить сравнительный анализ характеристик трафика — среднее количество соединений, средняя скорость передачи на соединение, среднее время жизни соединения, средний объем данных, переданных через соединение, географическое распределение. Составить таблицу.

# Теоретическая часть

Анализ сетевого трафика производится с помощью специальных программ, называемых снифферами. Снифферами называют приложения, перехватывающие сетевые пакеты, фильтрующие их по определенным правилам и отображающим их содержимое в более-менее понятном пользователю виде. Необходимость фильтрации пакетов обусловлена большим количеством фоновых, ненужных для анализа в данном конкретном случае соединений и призвана уменьшить количество анализируемого пользователем шума.

Основными снифферами, которые используются при анализе трафика, являются tcpdump и Wireshark. tcpdump — это консольное приложение для Unix систем. Wireshark — это кроссплаформенное приложение с графическим интерфейсом, которое облегчает процесс анализа сетевого трафика.

# Практическая часть

Для перехвата трафика из приложения веб-браузера, необходимо настроить фильтр на перехват http пакетов. В Wireshark данный фильтр называется http.



Рисунок 1 — HTTP трафик в Wireshark

Выполнив запрос на сайт <http://termilab.ru/mirea/> можно отследить HTTP пакеты, которыми обмениваются веб-сервер сайта и компьютер.

Применив фильтр tcp.port == 80 можно найти среди множества пакетов характерные для TCP тройного рукопожатия.



Рисунок 2 — TCP: тройное рукопожатие

С помощью средств Wireshark определим показатели:

1. Средняя длина пакетов: 314.2

2. Средняя скорость передачи: 0.0015 мс.

3. Всего пакетов: 471

Запустим анализ трафика и напишем сообщение в месенджере Telegram. Пакеты Telegram можно найти по пакетам протокола TLS.



Рисунок 3 — Трафик месенджера Telegram

Во время анализа HTTP пакетов, с помощью Wireshark была возможность собрать передаваемую страницу с помощью утилиты Follow. Попробуем восстановить передаваемое сообщение в Telegram.



Рисунок 4 — Восстановленное сообщение от Telegram

Видно, что восстановить и проверить содержимое сообщения не удалось, благодаря шифрованию.

Определим показатели:

1. Средняя длина пакета: 341.27

2. Средняя скорость передачи: 0.0153 мс

3. Всего пакетов: 97

Попробуем отследить сетевой трафик веб-браузера Tor и зайдём на сайт <http://termilab.ru/mirea/>.

Загрузив сайт и применив фильтр http, видим следующее.



Рисунок 5 — HTTP пакеты Tor

Определим показатели:

1. Средняя длина пакета: 910.52

2. Средняя скорость передачи: 0.107

3. Всего пакетов: 546

|  |  |  |  |
| --- | --- | --- | --- |
|  | Веб-браузер | Telegram | Tor |
| Длина пакета | 314.2 | 341.27 | 910.52 |
| Скорость передачи | 0.0016 | 0.0153 | 0.107 |
| Всего пакетов | 471 | 97 | 546 |

**Вывод**

В данной лабораторной работе была освоена работа с программой Wireshark и произведен анализ трафика сетевых приложений. Определены пакеты, используемые для передачи данных приложением и просмотрено их содержимое.