Уральский федеральный университет

имени первого Президента России Б. Н. Ельцина

Кафедра «Интеллектуальные информационные технологии»

**ЛАБОРАТОРНАЯ РАБОТА 2**

ОТЧЁТ

Дисциплина «Web-программирование»

Преподаватель:

Д.В. Свинцов

Студент:

гр. РИ-380022

Борисова В. Б.

Екатеринбург, 2020

**Лабораторная работа 2**

**Работа с протоколом HTTPS через openssl**

1. Задание подключиться по openssl к <https://wikipedia.org> и отправить запрос:
2. Ход работы

Подключиться по openssl к <https://wikipedia.org>.

С помощью следующей команды:

$ openssl s\_client -connect wikipedia.org:443

Получаем следующий ответ:

В первых строчках ответа можно увидеть, что соединение было установлено. (рисунок 1, рисунок 2)

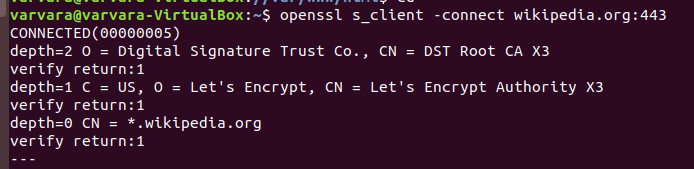


Рисунок 1 — Серверный сертификат

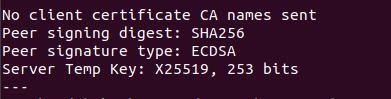


Рисунок 2 — Информация о сертификате

Вывод серверного сертификата со слова BEGIN (рисунок 3).



Рисунок 3 — Вывод серверное сертификата

Вывод информации об используемом алгоритме шифрования AES\_256 и версии протокола TLS 1.3 (рисунок 4).

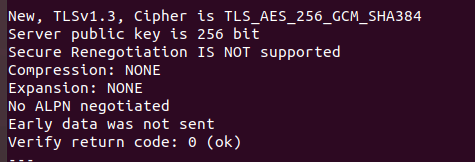


Рисунок 4 — Алгоритм шифрования и протокол TLS

Чтобы мы могли возобновлять сеансы без сохранения состояния сервера, был выпущен session\_id и TLS session ticket (рисунок 5).

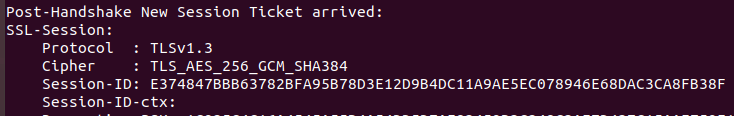


Рисунок 5 — session\_id

Дальше отправим следующий запрос (рисунок 6):



Рисунок 6 — GET-запрос

Ответ на запрос код состояния 301.

URL, который был запрошен, перенесен на адрес, хранящийся в поле Location (рисунок 7).

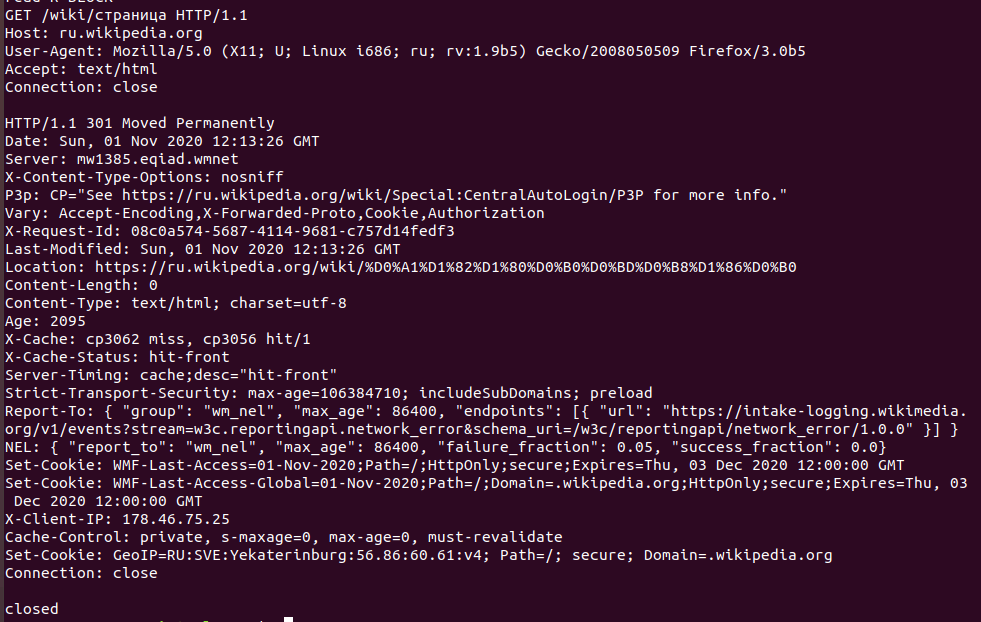


Рисунок 7 — Ответ на GET-запрос