# Министерство образования Республики Беларусь

Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Кафедра интеллектуальных информационных технологий

**Отчет по лабораторной работе №3**

**по курсу «СиМОИБ»**

на тему: «Наблюдение за стеком TCP/IP.»

|  |  |
| --- | --- |
| Выполнил студент группы 421701: | Бобр И.А. |
| Проверил: | Захаров В.В. |

МИНСК

18.11.16

**1 ЗАДАНИЕ**

Ознакомиться со средствами мониторинга сетевой активности.

**2 ВЫПОЛНЕНИЕ РАБОТЫ**

1. Установка инструментальных средств

Для выполнения лабораторной работы использовался следующий софт:

### - HTTP Analyzer

### - Smart sniff

### - Firebug для Firefox

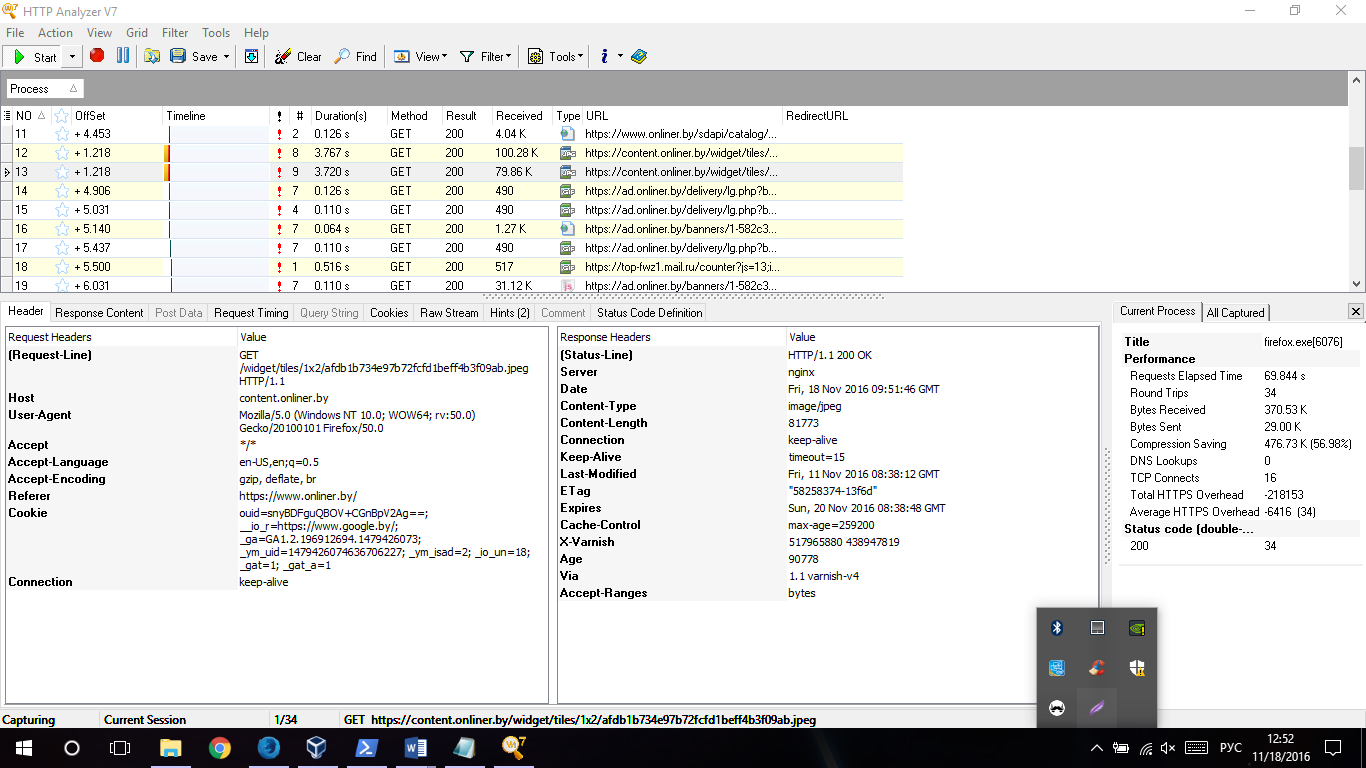
### 2. Анализ трафика

### 

Рисунок 1 – Анализ трафика при помощи HTTP Analyzer

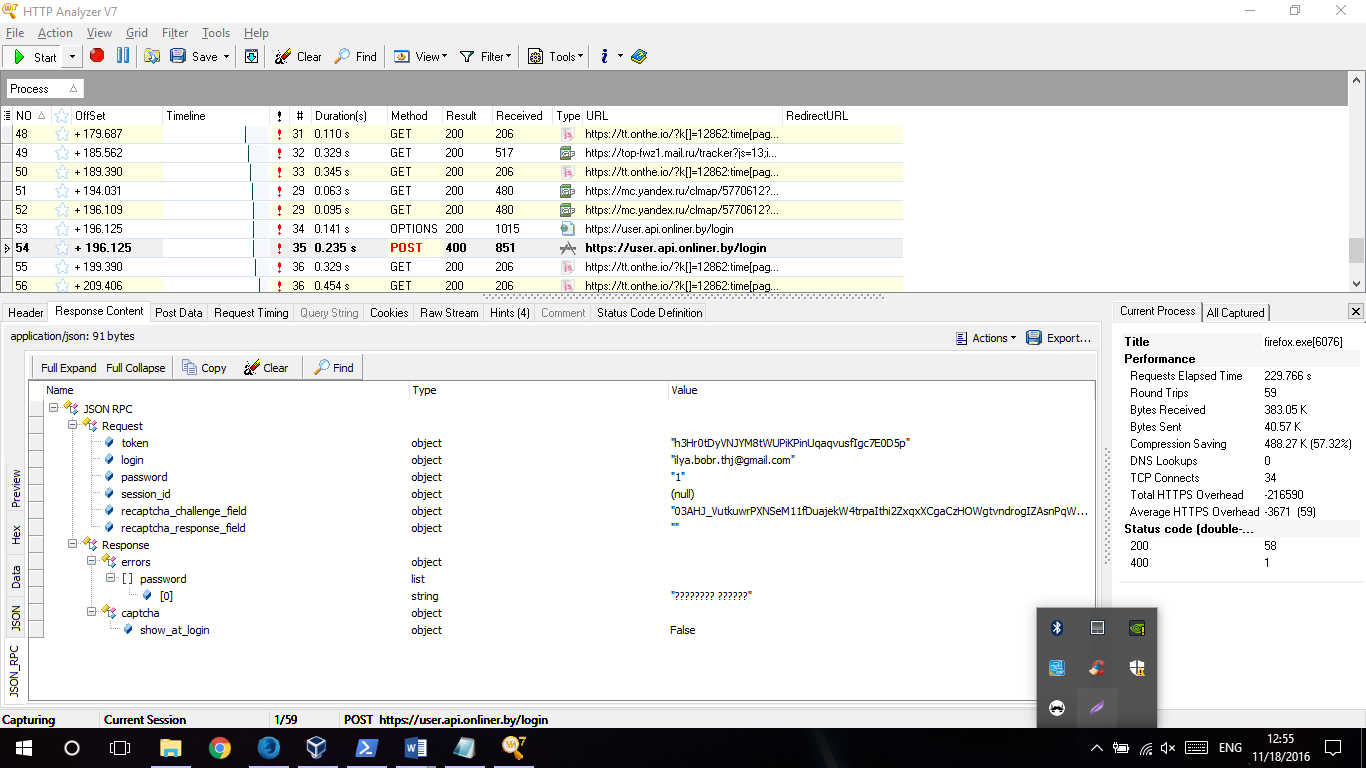
HTTP Analyzer позволяет посмотреть информацию, содержащую http и https заголовки, cookies, отправляемые и получаемые данные, редиректы, коды ответов сервера и др.

На примере сайта Onliner.by произведём анализ:



С помощью HTTP analyzer мы выяснили, что:

На данном сервере используется nginx, данные передаются по протоколу hhtp, то есть не шифруются, а передаются в открытом виде. Последняя модификация ресурса производилась 11 ноября 2016 в 8:38.



При входе данные передаются POST запросом без шифрования. Следовательно злоумышленник может перехватывать пакеты данных и получать из них информацию о пользователях.

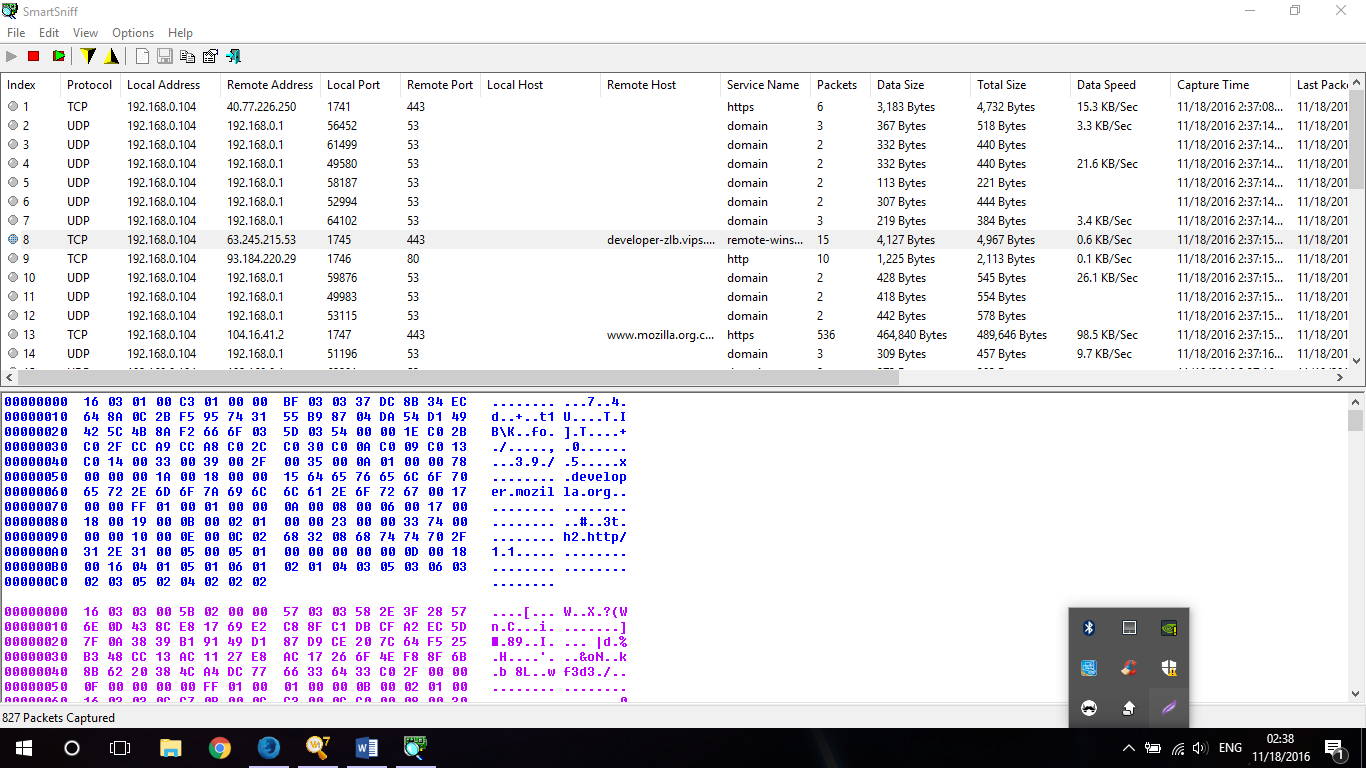


Рисунок 2 – Анализ https трафика при помощи SmartSniff

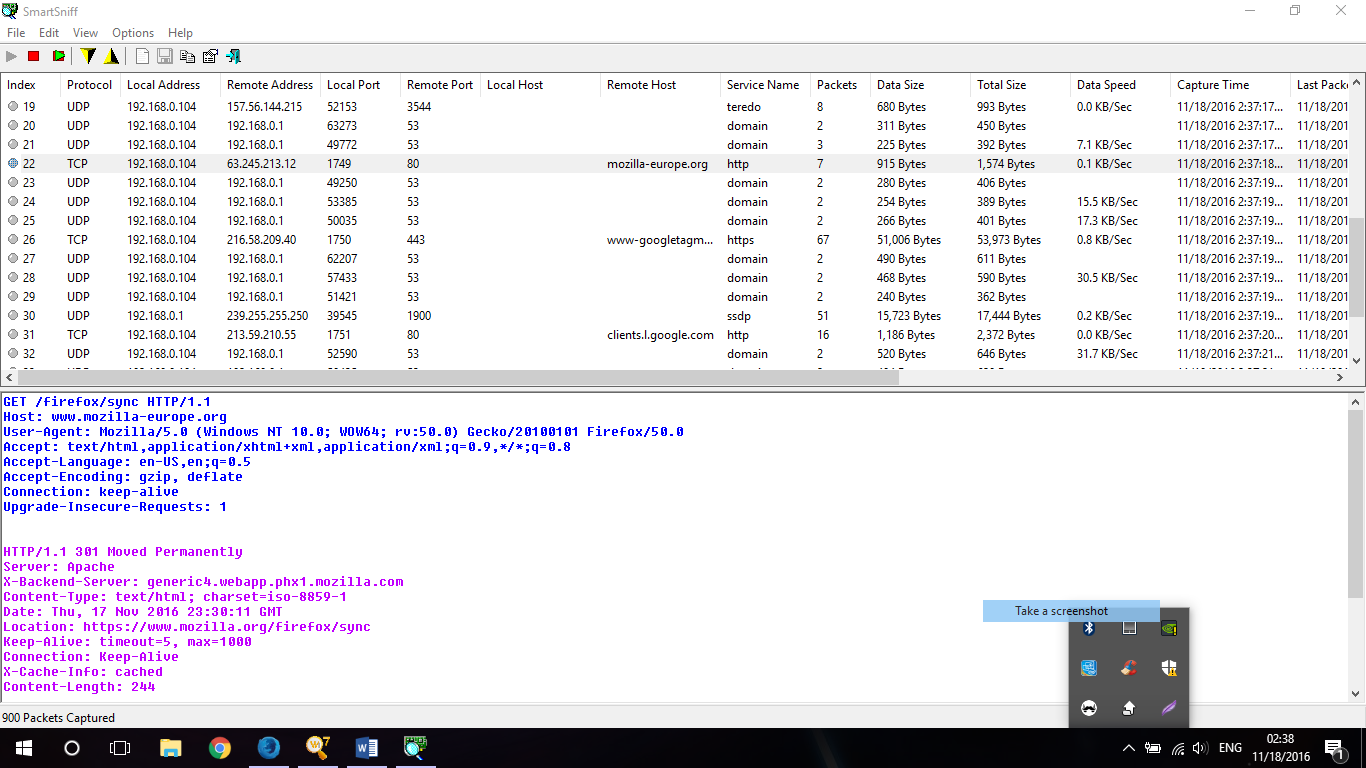


Рисунок 3 – Анализ http трафика при помощи SmartSniff

Важно отметить, что в случае, если трафик шифруется (идет HTTPS-запрос), его содержимое становится недоступным для просмотра. Если трафик шифруется, то невозможно просмотреть информацию о соединении (заголовки, cookies и т. д.)

Также проанализировать трафик можно при помощи средств веб-разработки, которые встроены в большинство современных браузеров по умолчанию. В своей работе мы использовали браузер FireFoxDeveloperEdition, в котором есть средства для разработки(FireBug). Данное дополнение позволяет отследить ответы, запросы и др. сайтов при соединении.

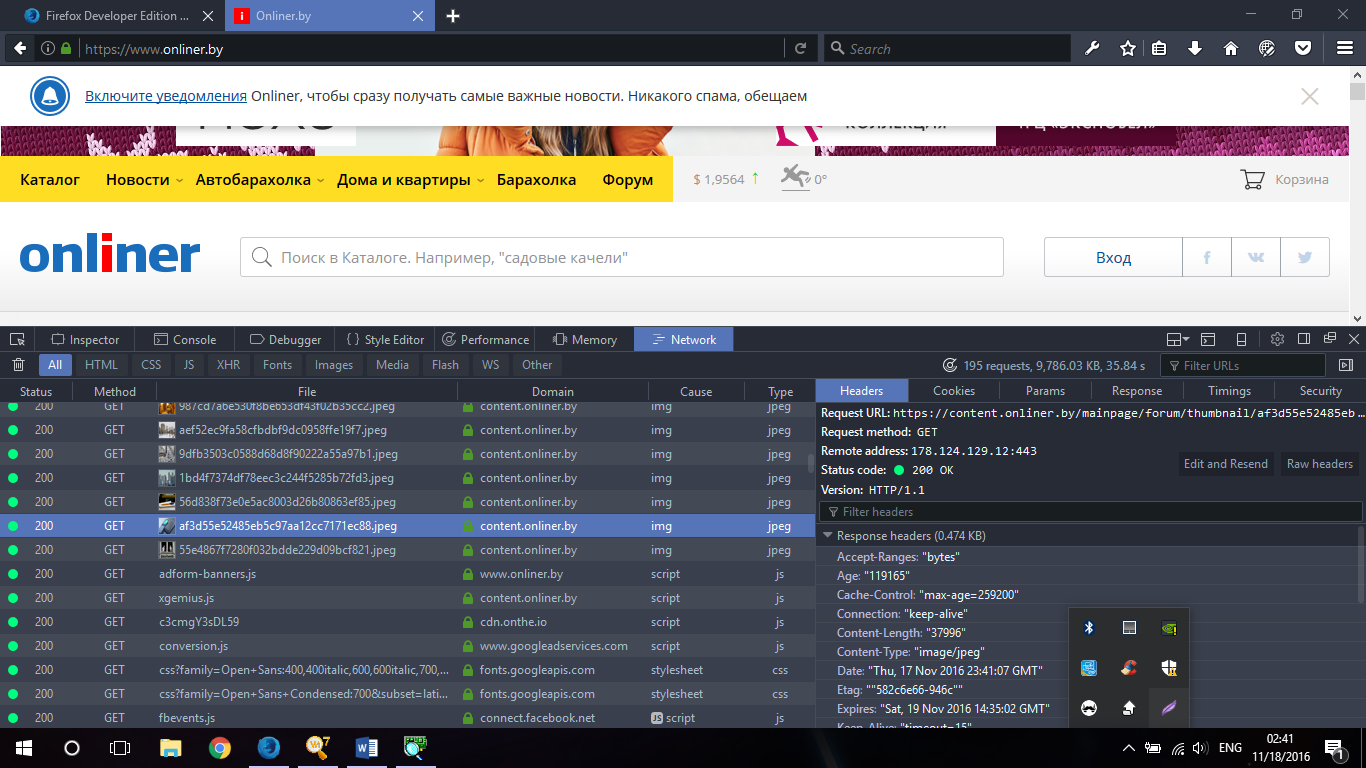


Рисунок 4 – Дополнение Firebug

1. Авторизация на сайте, на котором не настроен HTTPS

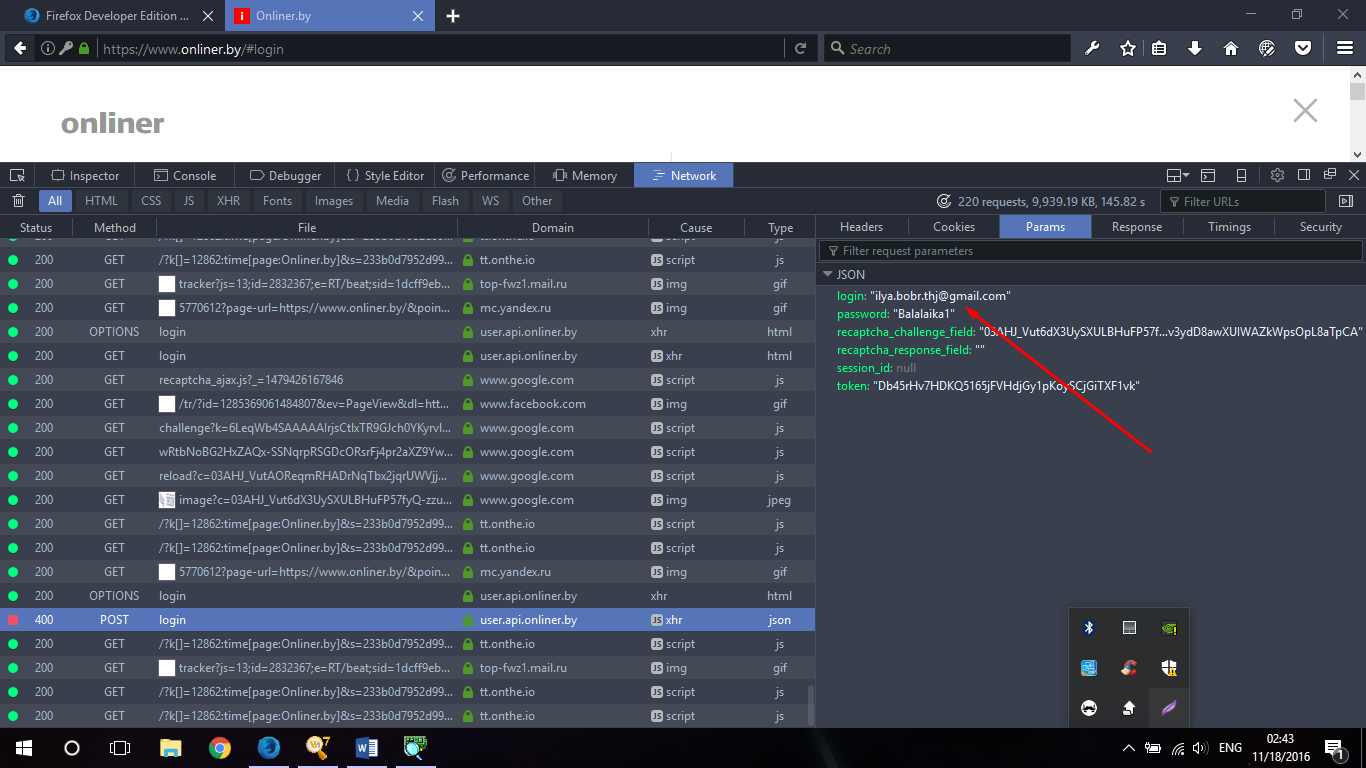


Рисунок 5 – Post запрос при авторизации на сайте, не использующем протокол https

Из приведенного выше скриншота видно, что если трафик не шифруется, то у злоумышленника есть возможность перехватить конфиденциальные данные (на скриншоте логин и пароль, которые передаются не зашифрованными).

**Вывод**

В данной лабораторной работе мы ознакомились со средствами мониторинга сетевой активности (в частности с такими инструментальными средствами, как Smart Sniff, HTTP Analyzer, FireFoxDeveloperEdition. Провели анализ сетевого траффика, выявили главный недостаток HTTP соединения при передаче конфиденциальных данных пользователя (передачу логина и пароля в открытом виде). Если на ресурсе используется протокол HTTP, злоумышленник может перехватить данные и использовать их в своих целях. Для передачи важных данных, лучше использовать протокол HTTPS. Это обычный HTTP, работающий через шифрованные транспортные механизмы [SSL](https://ru.wikipedia.org/wiki/SSL) и [TLS](https://ru.wikipedia.org/wiki/TLS).