Компьютерные системы и сети
Лабораторная работа №2
Часть 1
Знакомство с Wireshark
Протокол HTTP

ИУ9-31
Разборщикова Анастасия

Исследуемый сайт: http://students.bmstu.ru

Перехваченный HTTP-трафик:

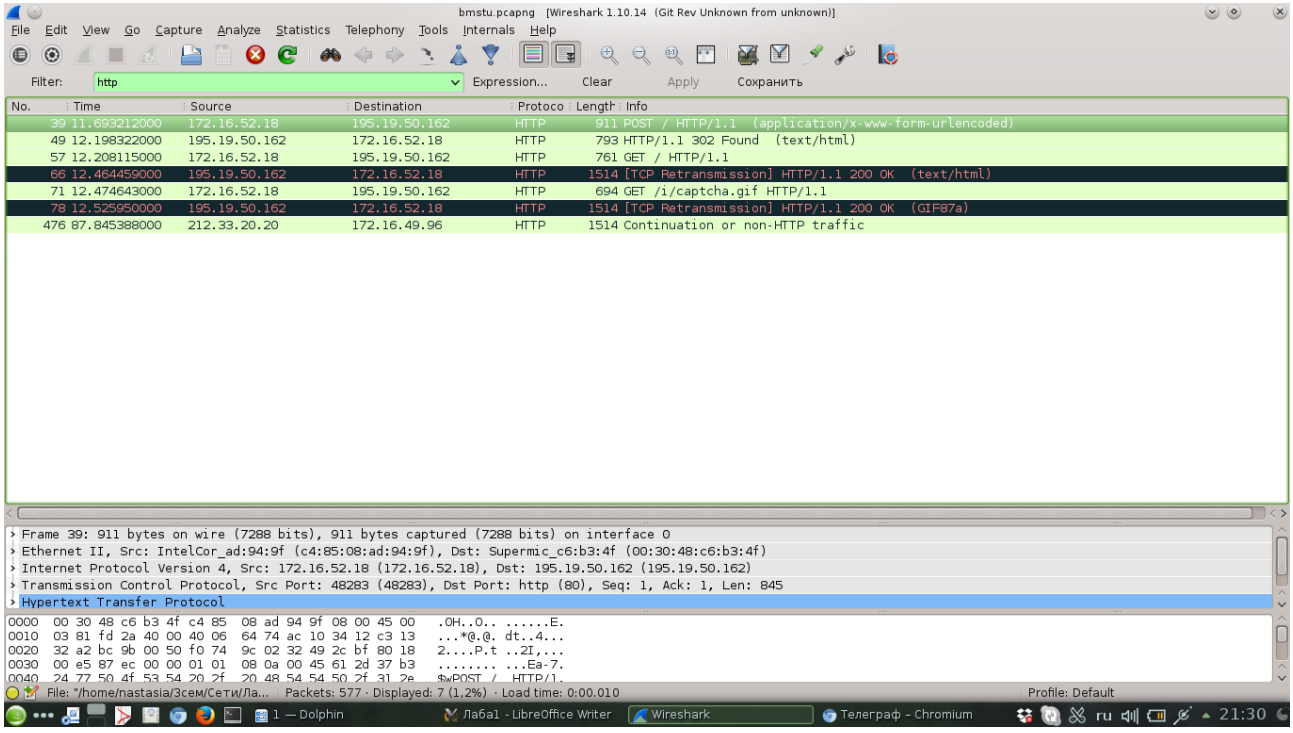

Рисунок 1: Перехваченный HTTP-трафик

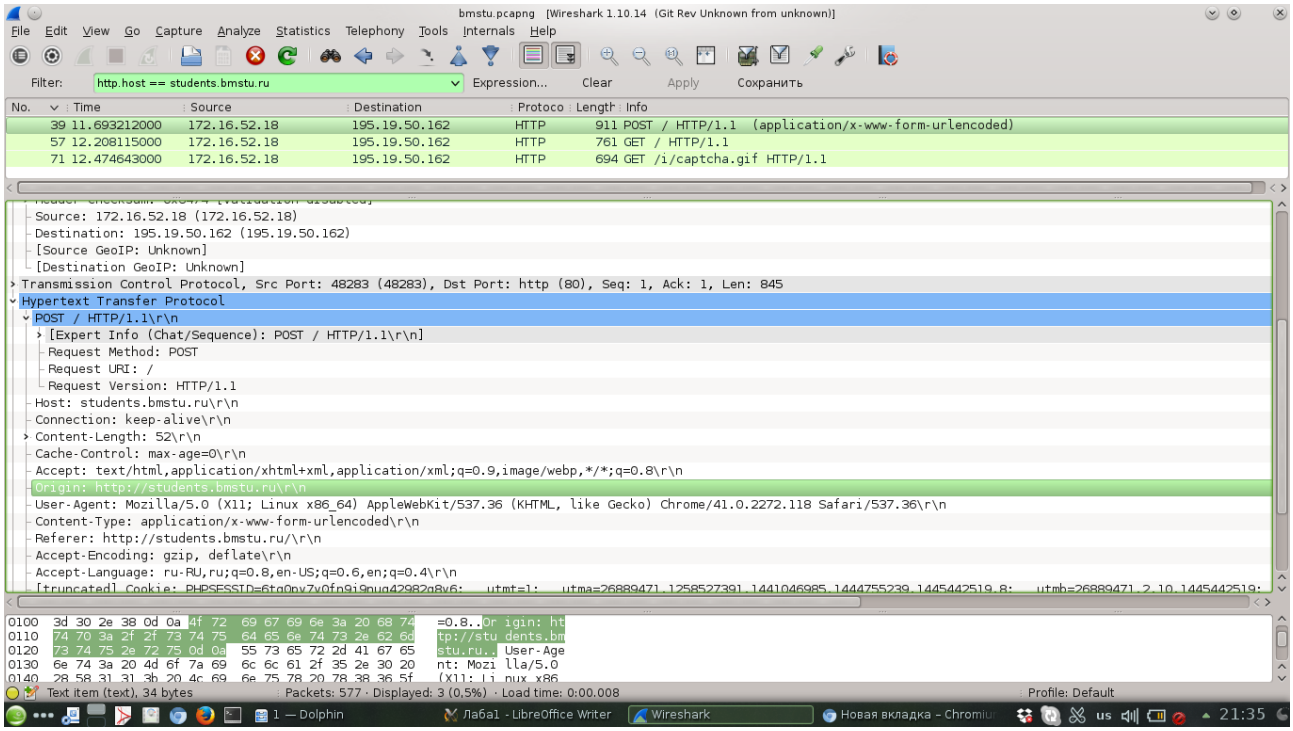

Рисунок 2: Трафик отфильтрован по параметру http.host

Как видно на Рисунке 1, данные, отправляемые компьютером на сервер (POST), имеют в поле Source IP-адрес 172.16.52.18, а в поле Destination — адрес 195.19.50.162.
Данные, получаемые с сервера (например, GIF-изображение) — наоборот.

IP-адрес сервера: 195.19.50.162

Рассмотрим подробнее содержание пакетов.

Пакет №49: text/html

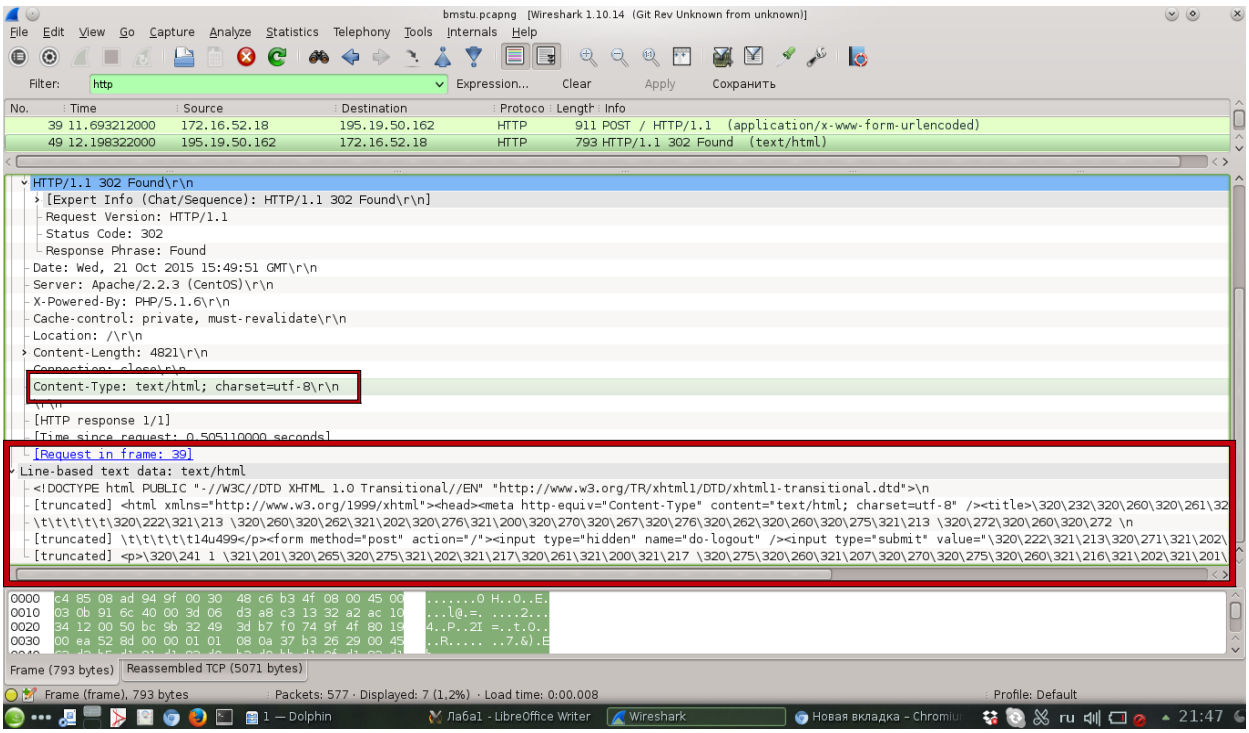

Рисунок 3: Содержание пакета 49: text/html

Content-Type: text/html; charset=utf-8\r\n
Тело пакета — содержимое вкладки Line-based text data (выделено красным).

Пакет №78: GIF

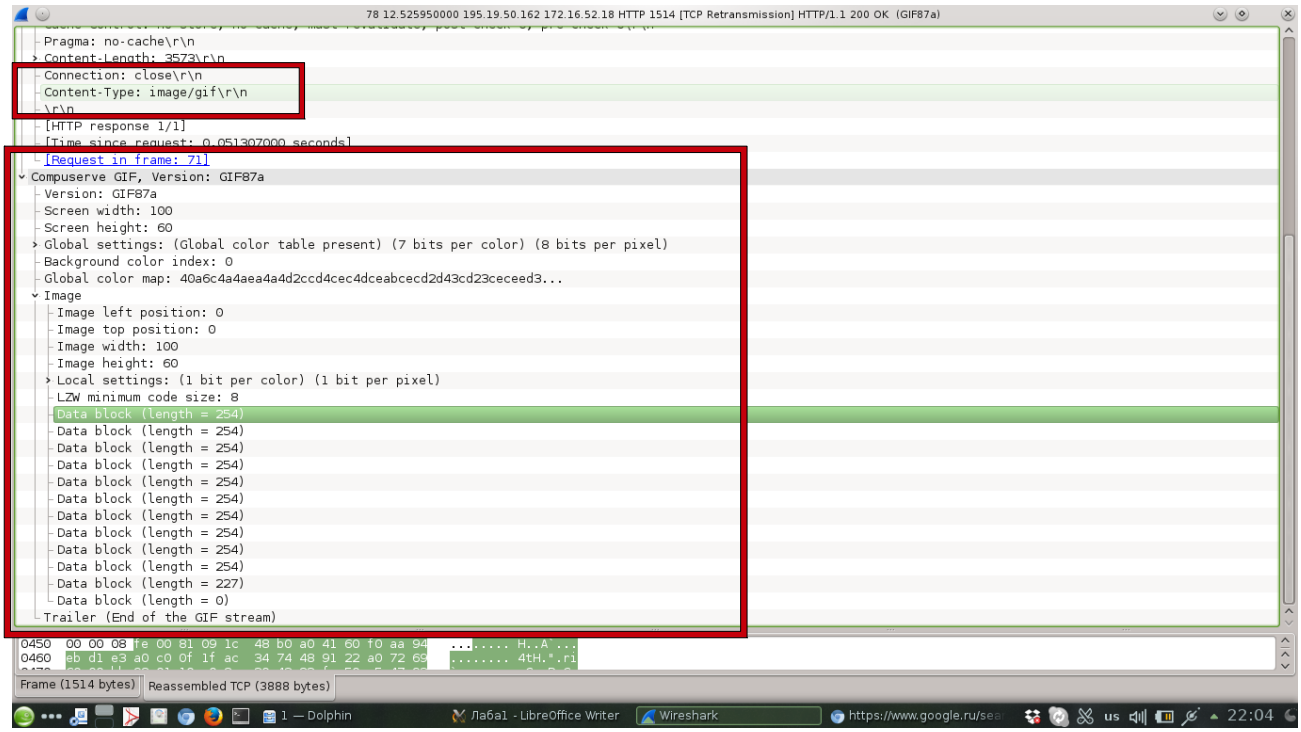

Рисунок 4: Содержание пакета №78: GIF

Content-Type: image/gif\r\n
В теле пакета находится информация об изображении и само изображение, представленное в виде блоков длины 254, 227 и 8.

Пакет №39: логин и пароль

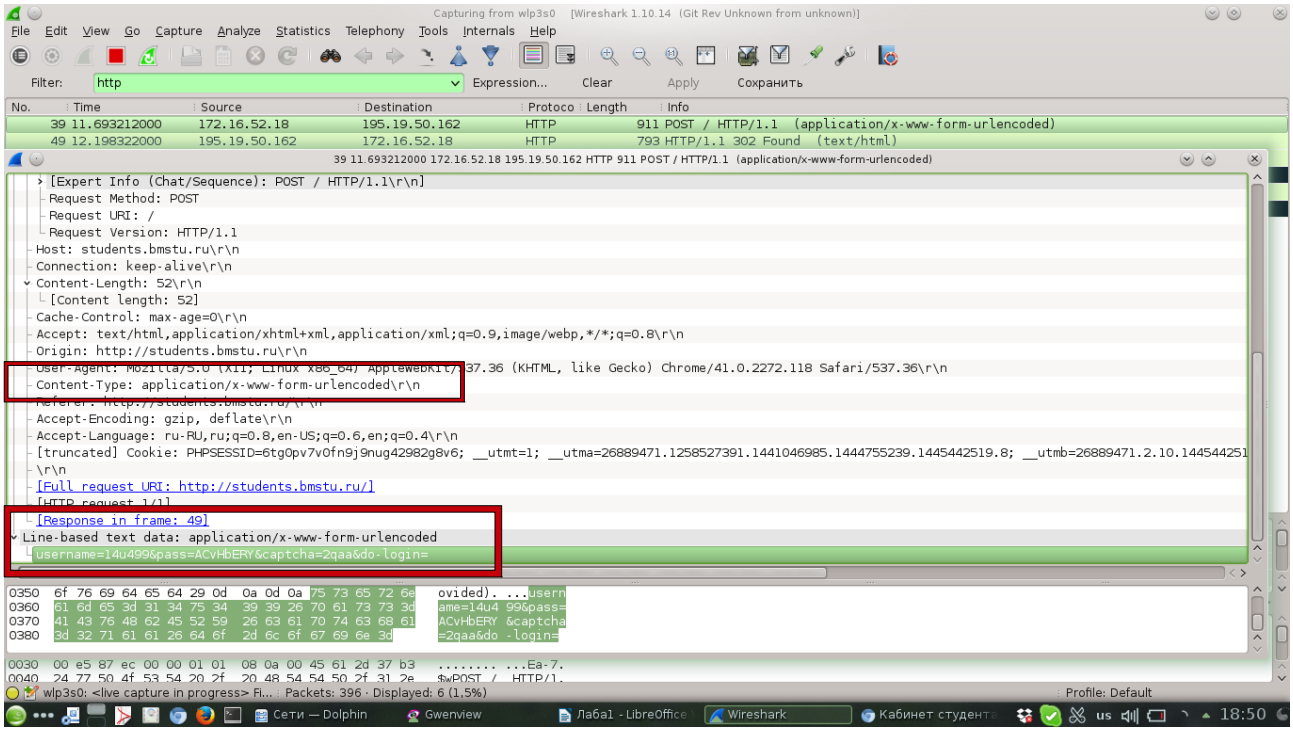

Рисунок 5: Содержание пакета №39: логин и пароль

Content-Type: application/x-www-form-urlencoded\r\n
Тело: Line-based text data
Можно видеть, какие данные были пересланы:
username=14u499
pass=ACvHbERY
captcha=2qaa

Более того, можно заметить, что были даны перекрестные ссылки на пакеты:
В пакете №39 с отправленными логином и паролем есть строка: «[Response in frame: 49]», в то время как в пакете №49 , который был рассмотрен самым первым, указано, что запрос был получен в пакете №39 (см. Рисунок 3, «[Request in frame: 39]»).