Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра программного обеспечения информационных технологий

Дисциплина: Сетевые технологии и администрирование операционных систем (СТиАОС)

**ОТЧЕТ**

По практической работе №1 (Вариант 12)

АНАЛИЗ СЕТЕВОГО ТРАФИКА И ПАКЕТОВ С ИСПОЛЬЗОВАНИЕМ СНИФФЕРА

Выполнил

студент: гр.851004 Краснова А.В

Проверил: Марцинкевич В.А.

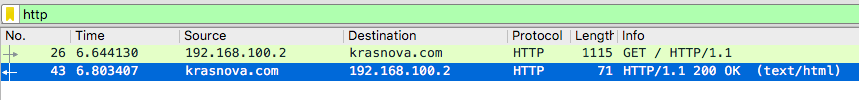
Минск 2021

**Задание 1. HTTP: Basic HTTP GET/response**

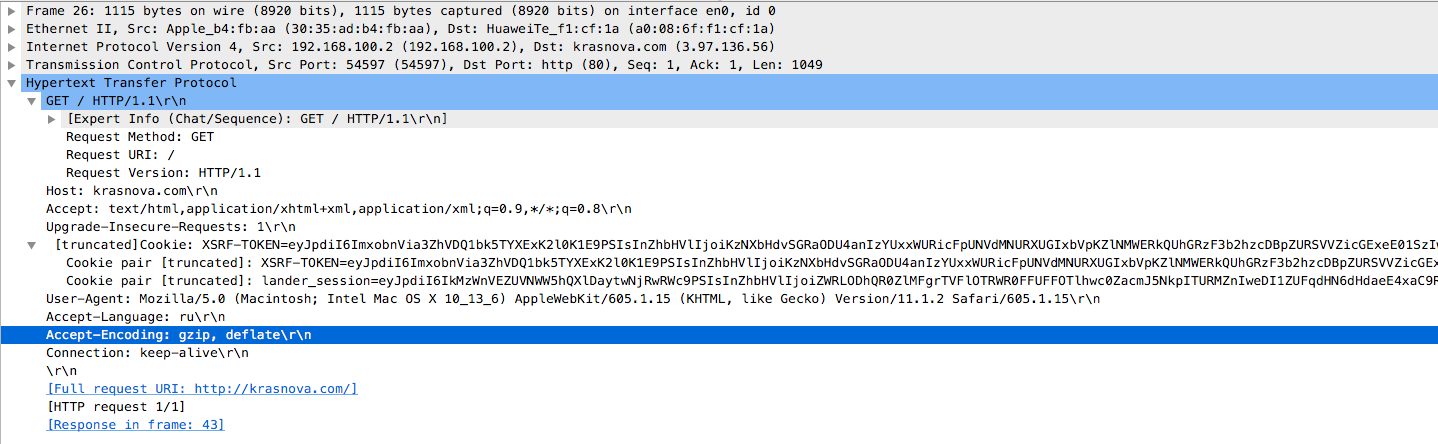
Исходный URL: <http://krasnova.com>

Браузер: Safari/605.1.15

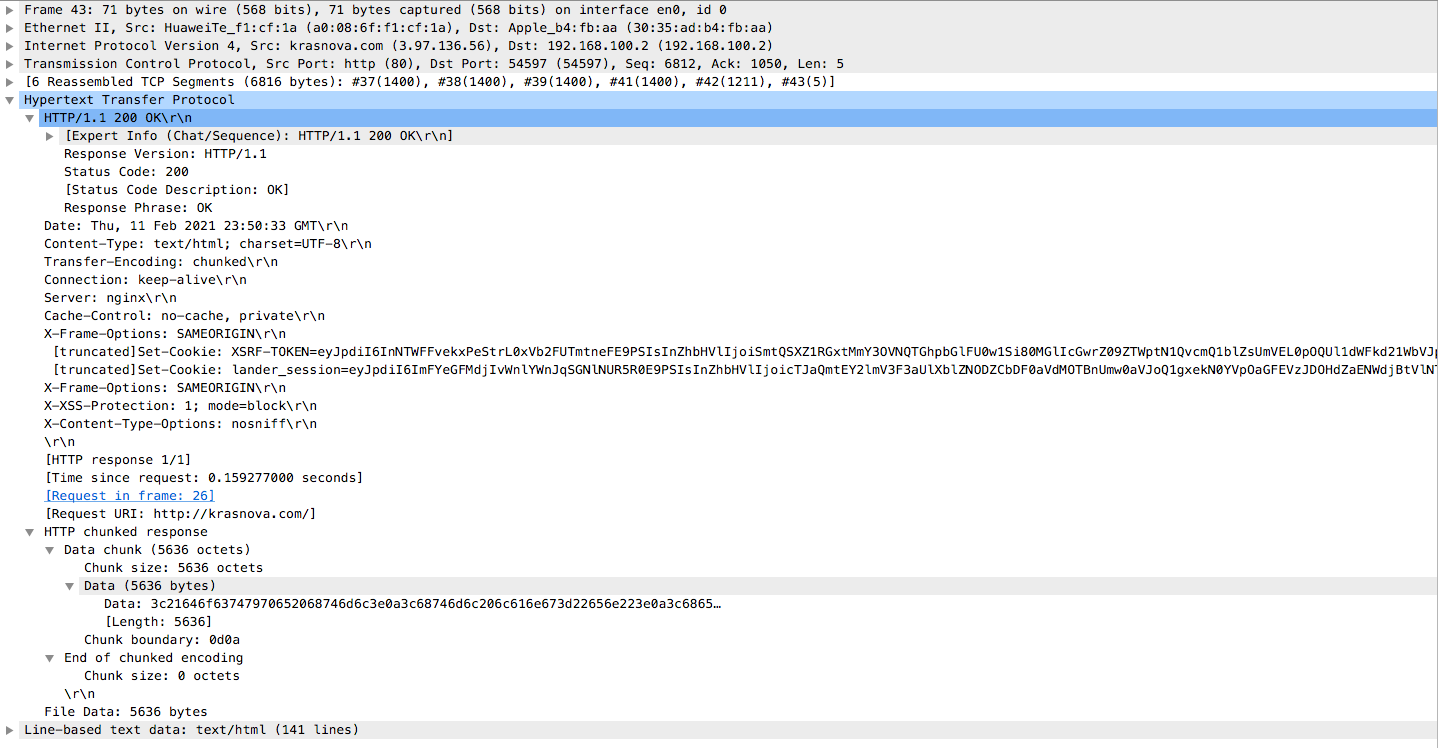
Результат перехвата пакетов (пара запрос-ответ):



Содержание GET пакета:



Содержание response пакета:



1. Версия HTTP/1.1 (Response version)

2.Принимаемые браузером языки: ru (Accept-Language)

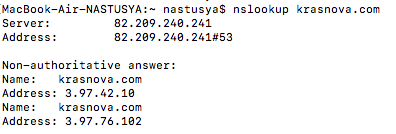
3.IP моего компьютера 192.168.100.2 (TCP: Src), сервера krasnova.com 3.97.136.56 (TCP: Dst)

4. Код состояния 200 (Status Code). Это часть заголовка при ответе сервера на запрос, показывающая результат выполнения запроса в цифровом виде.

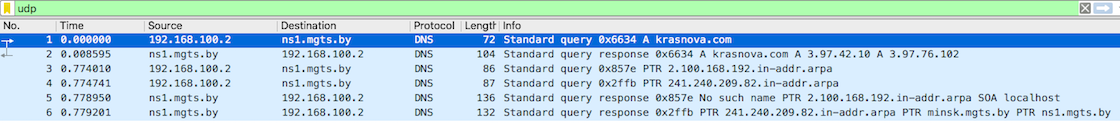
5. Длина тела сообщения 5636 octets (HTTP chunked response, Data chunk

**Задание 8. UDP**

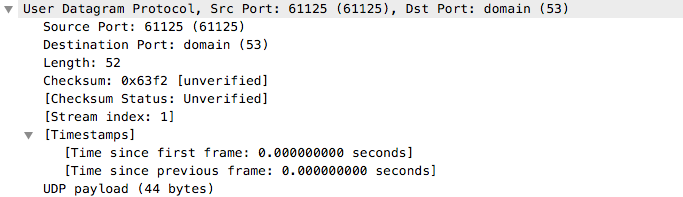
Исходный запрос:



Результат перехвата пакетов:



Содержание UDP пакета:



1. Порт отправителя(2 байта), порт получателя(2 байта), длина(2 байта), контрольная сумма(2 байта).

2. 4 поля по 2 байта, т.е. 8 байт на заголовок.

3. Length – длина всей дейтаграммы (заголовок+данные) в байтах. Теоретически, максимальный размер поля — 65535 байт для UDP-дейтаграммы (8 байт на заголовок и 65527 на данные). Фактический предел для длины данных при использовании IPv4 — 65507 (помимо 8 байт на UDP-заголовок требуется ещё 20 на IP-заголовок).

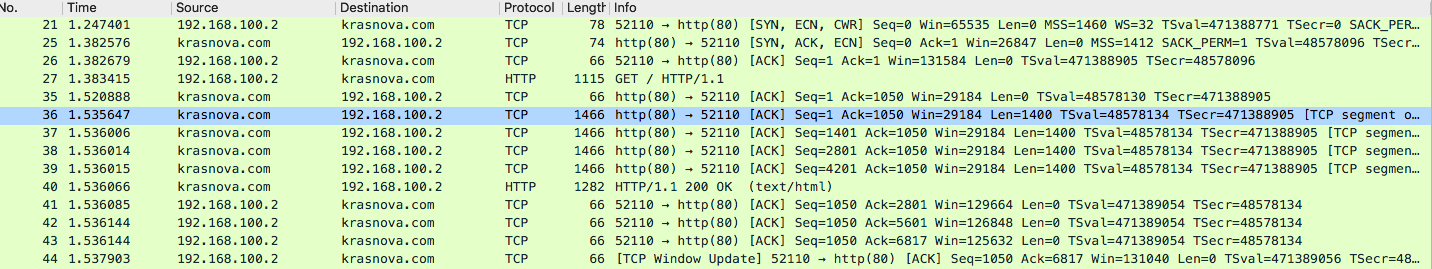
4. Длина поля порта источника 2 байта, значит максимально возможный номер порта 65535.

5. Номер протокола Protocol UDP: 17 (10-ричное) или 10 (16-ричное).

**Задание 9. TCP**

Исходный URL: <http://krasnova.com>

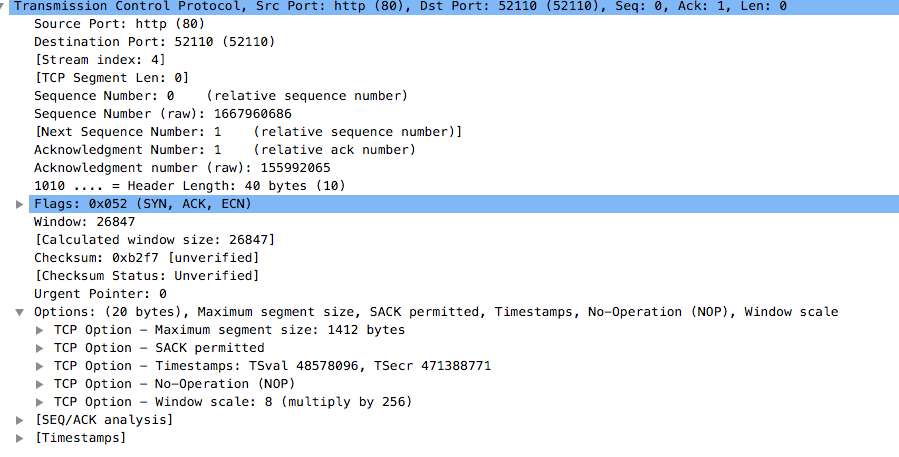
Результат перехвата пакетов (TCP+HTTP):

****

Тройное рукопожатие:



Содержание TCP-пакета:



1. Клиент, который намеревается установить соединение, посылает серверу сегмент с номером последовательности и флагом SYN.

* Сервер получает сегмент, запоминает номер последовательности (SEQ) и пытается создать сокет (буферы и управляющие структуры памяти) для обслуживания нового клиента.
* В случае успеха сервер посылает клиенту сегмент с номером последовательности +1 и флагами SYN и ACK, и переходит в состояние SYN-RECEIVED.
* В случае неудачи сервер посылает клиенту сегмент с флагом RST.

2. Если клиент получает сегмент с флагом SYN, то он запоминает номер последовательности и посылает сегмент с флагом ACK (SEQ+1).

* Если клиент одновременно получает и флаг ACK (что обычно и происходит), то он переходит в состояние ESTABLISHED.
* Если клиент получает сегмент с флагом RST, то он прекращает попытки соединиться.
* Если клиент не получает ответа в течение 10 секунд, то он повторяет процесс соединения заново.

3. Если сервер в состоянии SYN-RECEIVED получает сегмент с флагом ACK, то он переходит в состояние ESTABLISHED.

* В противном случае после тайм-аута он закрывает сокет и переходит в состояние CLOSED.

В данном примере:

192.168.100.2 krasnova.com

1. CLOSED LISTEN

2. SYN-SENT --> <SEQ=0><CTL=SYN> --> SYN-RECEIVED

3. ESTABLISHED <-- <SEQ=0><ACK=1><CTL=SYN,ACK> <-- SYN-RECEIVED

4. ESTABLISHED --> <SEQ=1><ACK=1><CTL=ACK> --> ESTABLISHED