**Электронный отчет**

по сайту conzu.de

По дисциплине “Основы информационной безопасности”

**Выполнил:**

Студент 1 курса группы БАСО-03-20

Гасанбеков Мансур Мажлумович

**Работа в командной строке**

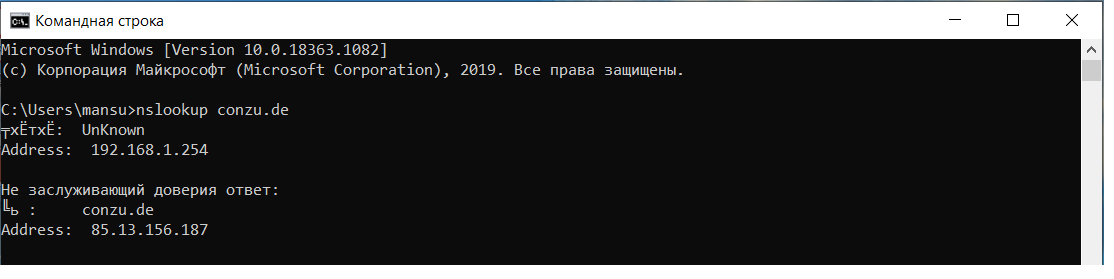
**1. Обнаружение сайта**

С помощью google dorks найдем нужный нам сайт используя следующий запрос: intitle:"letter" inurl:http after:2018 .

* Заголовок: Письмо
* Тип шифрования: http
* Дата создания: После 2018

**2 Определяем Ip адрес**

С помощь утилиты nslookup определяем Ip адрес сайта

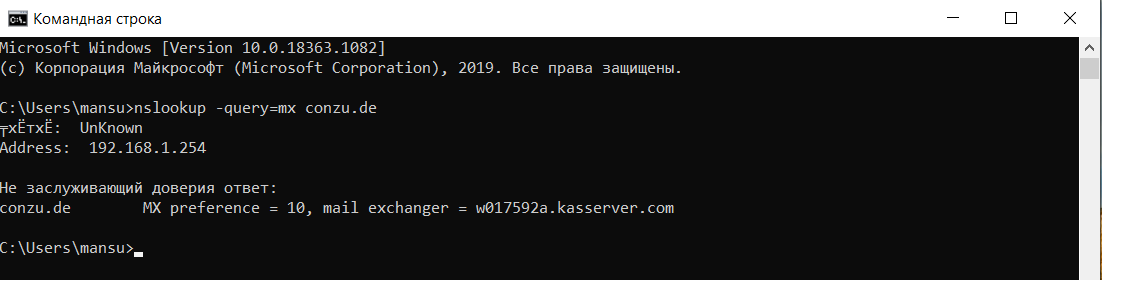


**Сайт:** conzu.de

**IP:** 85.13.156.187

**3 Определяем доменные имена, соответствующие почтовому серверу**

С помощь утилиты nslookup –query=mx узнаем соответствие доменных имен с почтовыми серверами домена

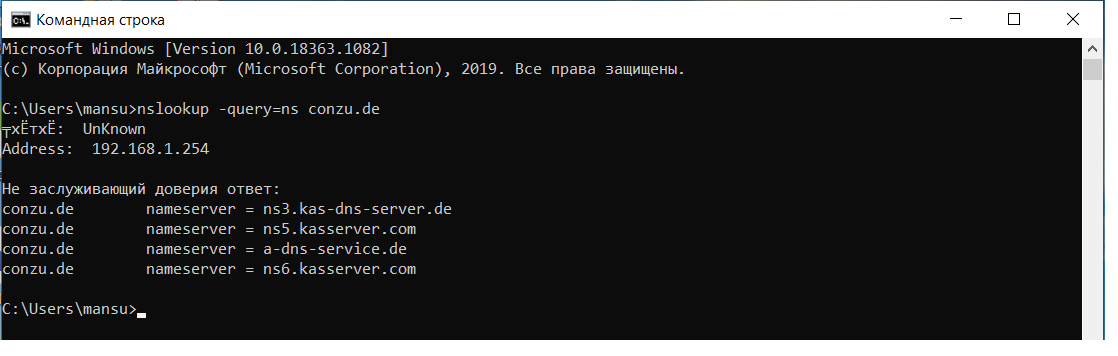


Данному домену соответствует один почтовый сервер

w017592a.kasserver.com , число 10 после MX preference показывает нам приоритет, причем, чем меньше число, тем больше его приоритет.

**4 Определяем доменные имена, соответствующие DNS-серверу**

С помощью утилиты nslookup –query=ns узнаем соответствие доменного имени DNS-серверу



Доменному имени conzu.de соответсвуют четыре DNS-сервера:

1) ns3.kas-dns-server.de

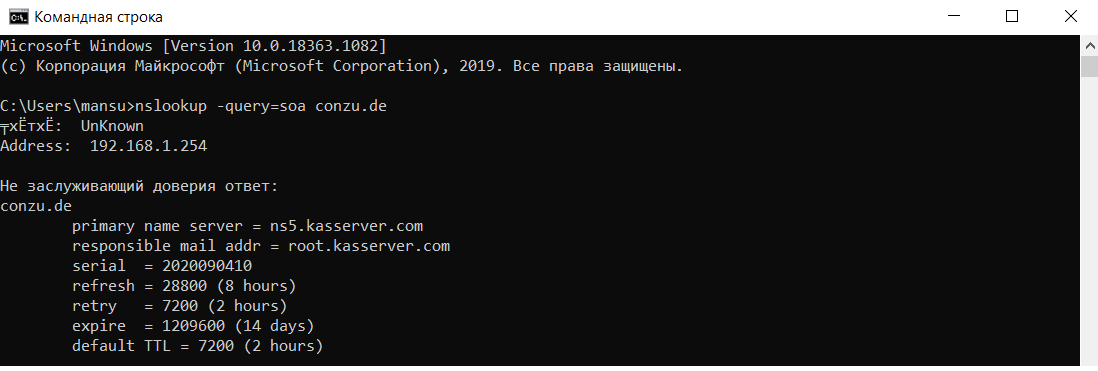
2) ns5.kasserver.com

3) a-dns-service.de

4) ns6.kasserver.com

**5 Определяем зону доменного имени, электронный адрес администратора и тд.**

С помощью утилиты nslookup -query=soa узнаем следующую информацию:



Имя первичного DNS-сервера: ns5.kasserver.com

Почтовый адрес администратора домена: root.kasserver.com

Серийный номер: 2020090410

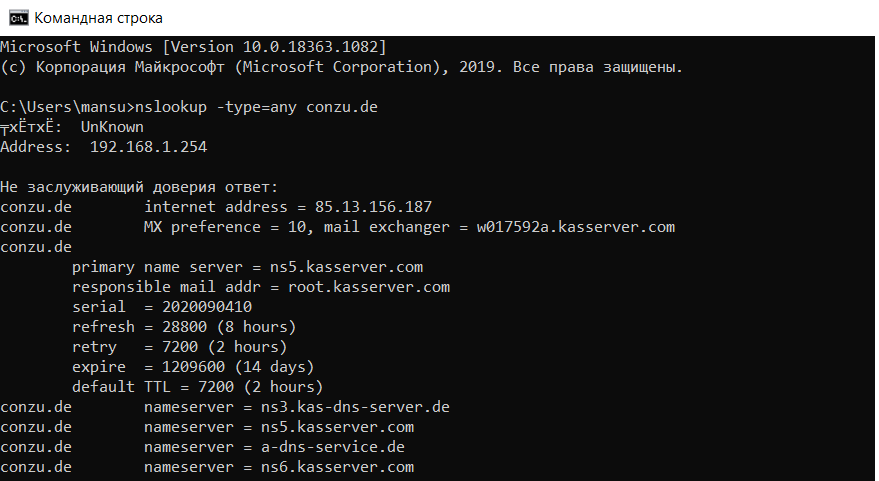
Период времени: 28800 секунд

Время до повторного соединения: 7200 секунд

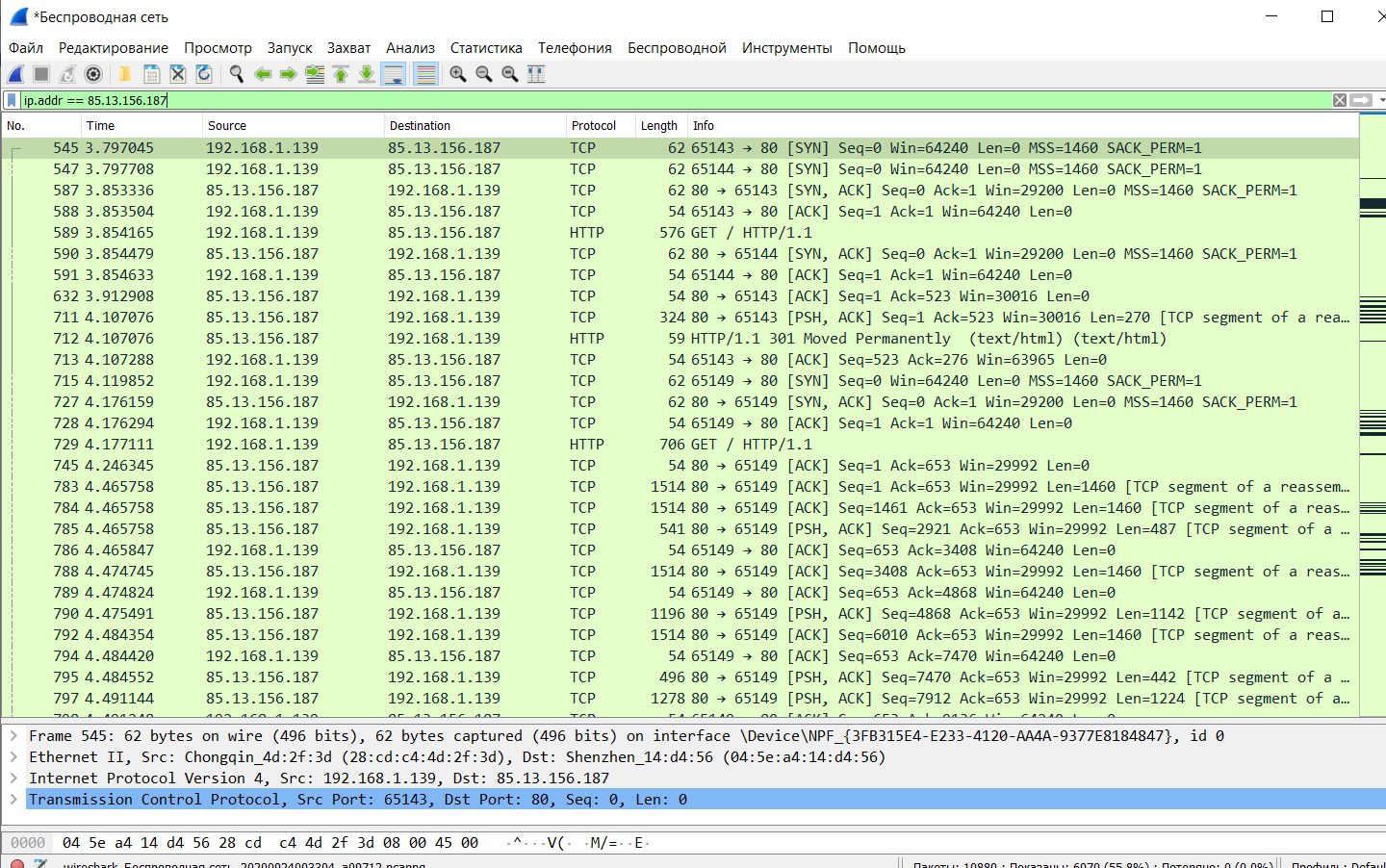
Время хранения кэша: 1209600 секунд

Время жизни пакета: 7200 секунд

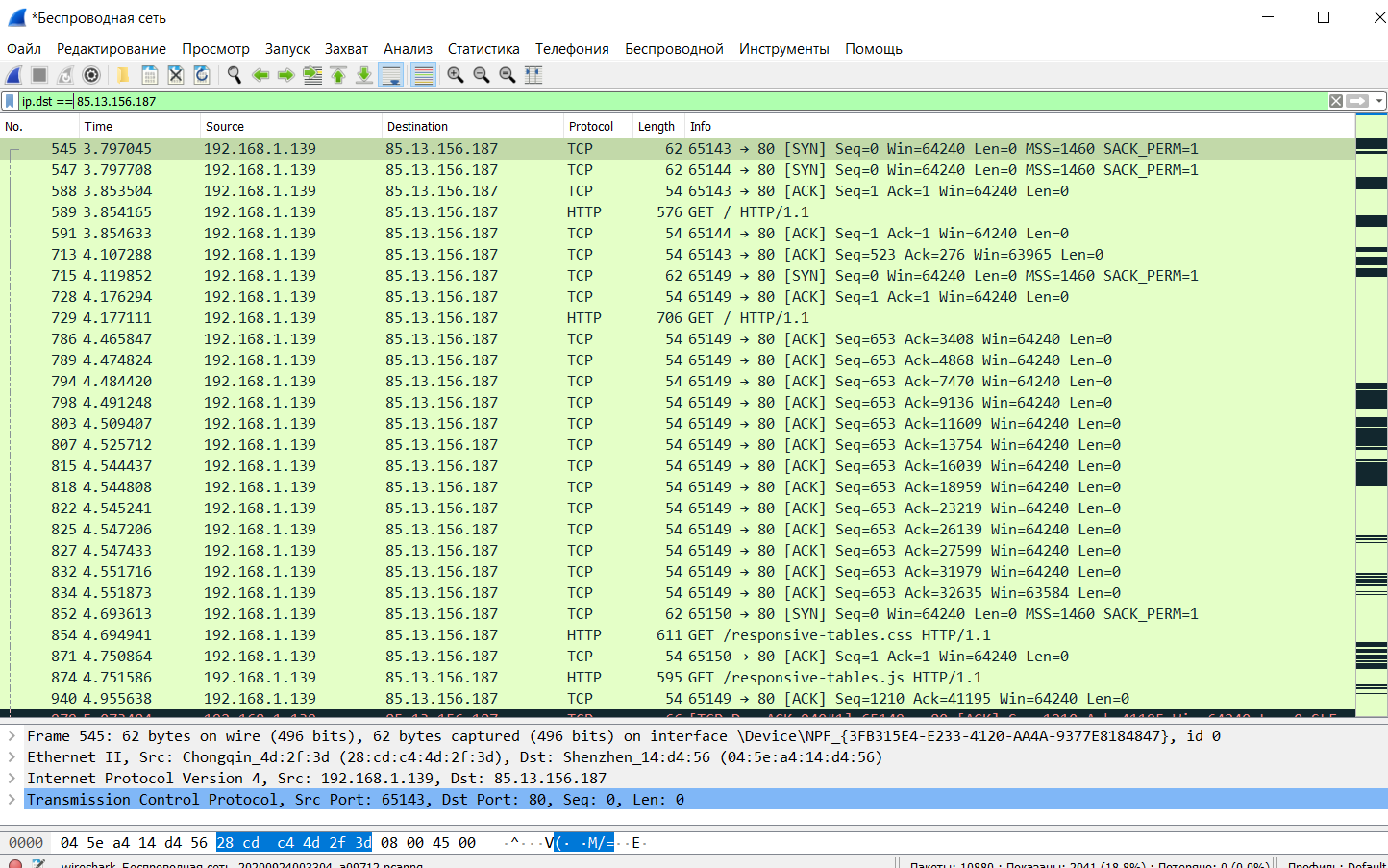
**6 Определяем все доступные записи DNS-сервера с помощью команды –type=any**



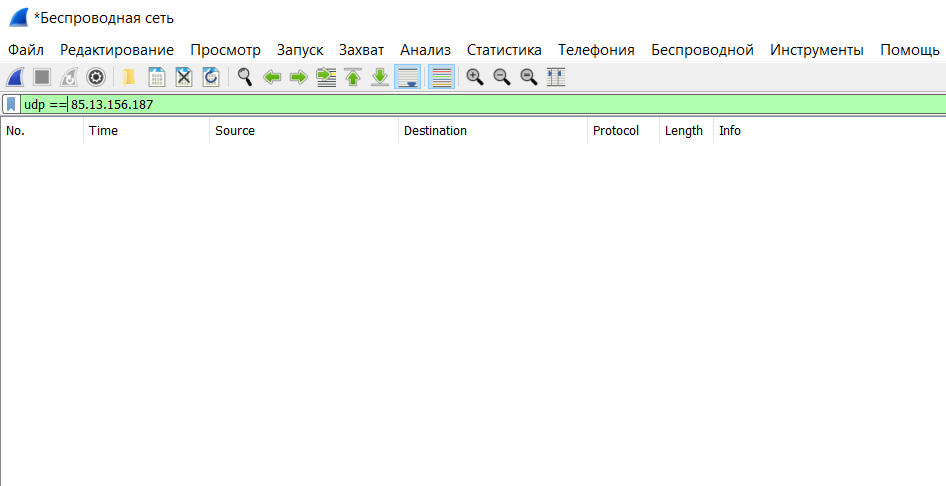
**7. Изучаем трафик сайта conzu.de**

Начнем захват пакетов сайта без применения фильтров совершив несколько переходов внутри сайта, после чего останавливаем захват пакетов и вводим фильтр ip.addr == 85.13.156.187

Применим фильтр: ip.dst == 85.13.156.187



Применив фильтр udp == 85.13.156.187 получаем пустой результат



Применив фильтры ip.src==85.13.156.187; ip.dst; ip.addr, udp.src, arp.src.hw\_mac, eth.dst, eth.src также получаем пустой результат.