Компьютерные сети (семинары). Домашнее задание №5.

Задание:

1. В приложенном файле “The Ultimate PCAP.pcap” (из раздаточного материала) найти e-mail. Что внутри письма и для кого оно?

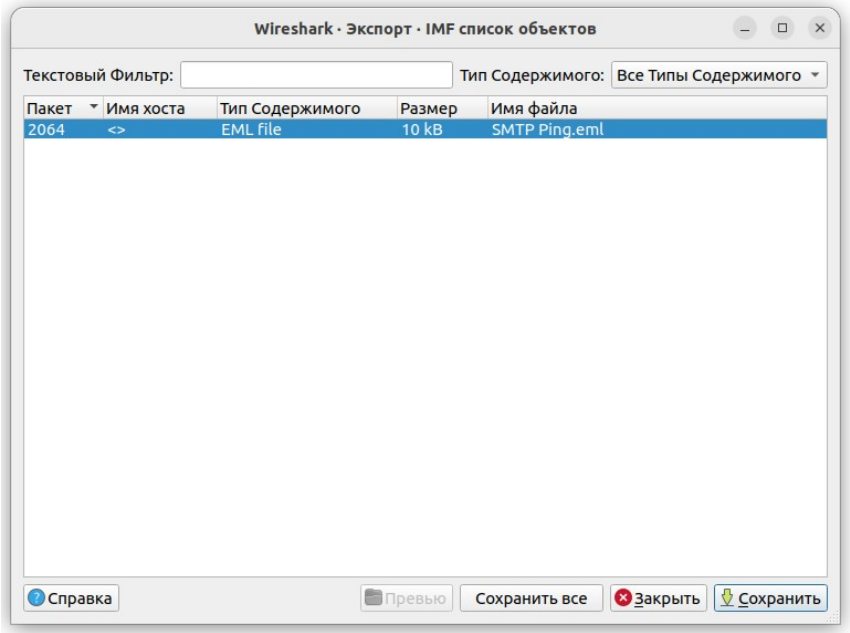
1. Закрепите навыки фильтрования. Запустите трейс до 8.8.8.8. И перехватите его в Wireshark. Проанализируйте.
2. Закрепите навыки фильтрования. Найдите еще один сайт без шифрования с возможностью ввода логина/пароля. (можно в гугл настроить соответствующую выдачу по запросу с ключом “-inurl:https” в конце). Перехватите их в Wiresharke, построив фильтр.

4*. На сайте https://launchpad.net/ubuntu/+archivemirrors представлены зеркала с образами Убунту по странам. Скачайте файл ls-lR.gz из Чили и с Яндекса. Снимите два дампа для каждого скачивания. Проанализируйте скорость скачивания и посмотрите tcptrace. Прикиньте средний RTT и поищите максимальный RWND для скачивающего.
Предоставить скриншоты графиков скорости и tcptrace. Есть ли разница? В чем она?

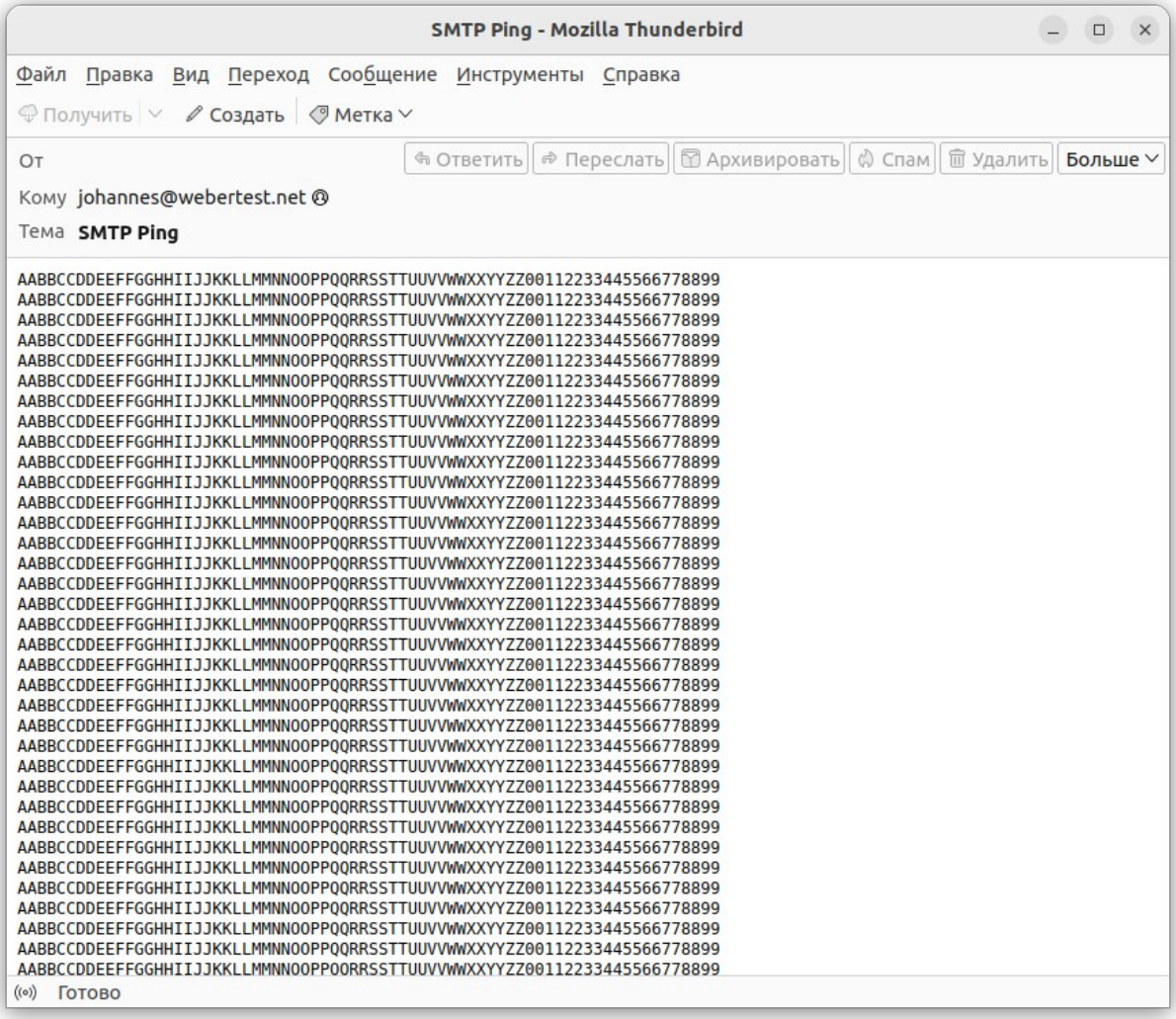
1. Посмотрите перед 2 семинаром к лекции по L4: https://disk.yandex.ru/i/6pAvRRMrK2e7jw файл из демонстрации: https://disk.yandex.ru/d/czW2ZAlsLFXYHw

Решение:

1. Найдем в дампе письмо:

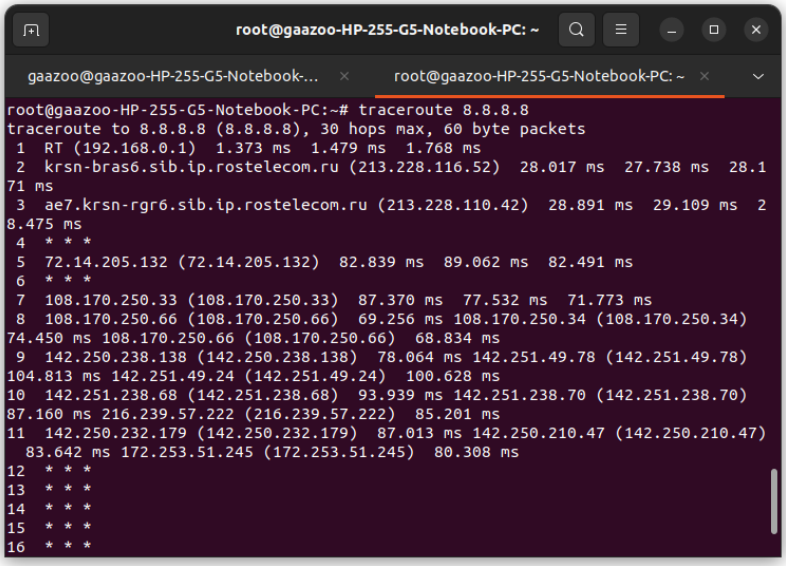


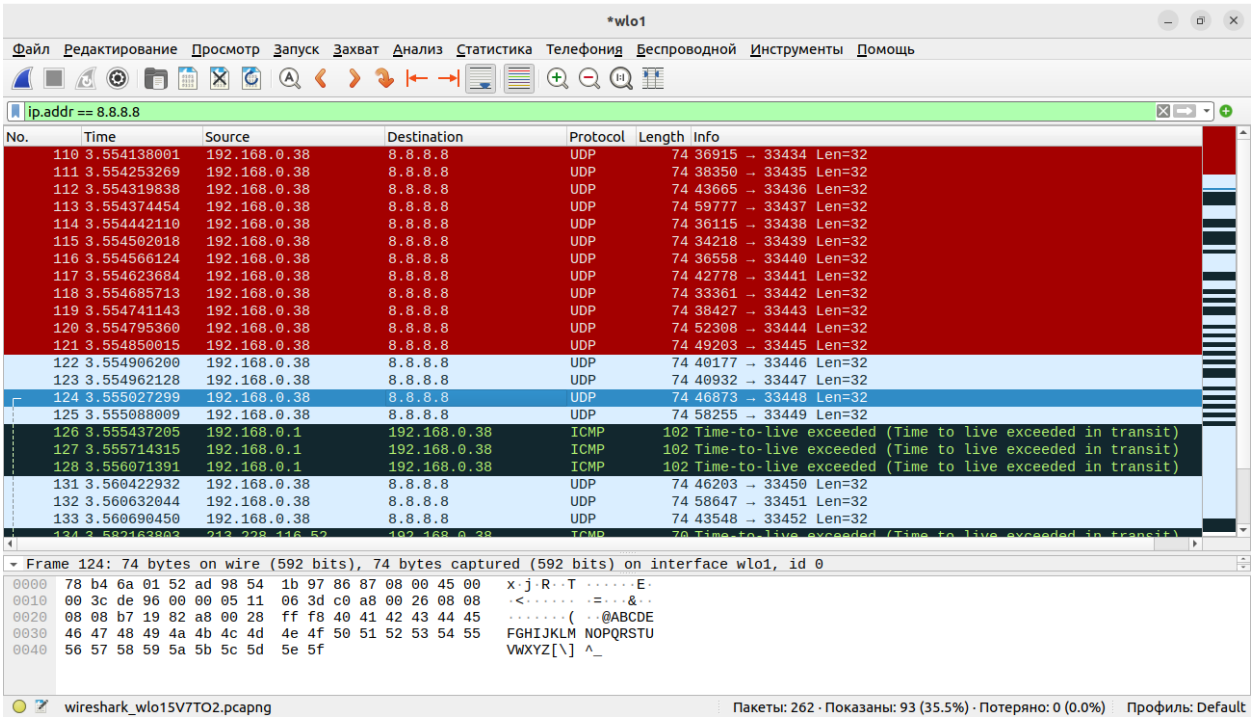
Посмотрим что внутри письма и кому оно адресовано:



Получатель письма: johannes@webertest.net

2. Запускаем трассировку маршрута до 8.8.8.8 командой traceroute (работаю на Ubuntu)

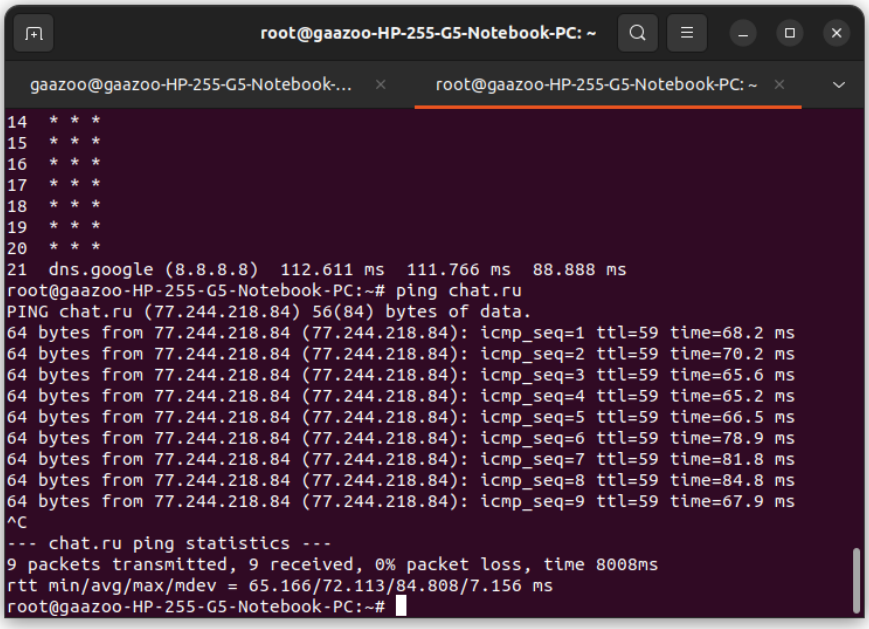




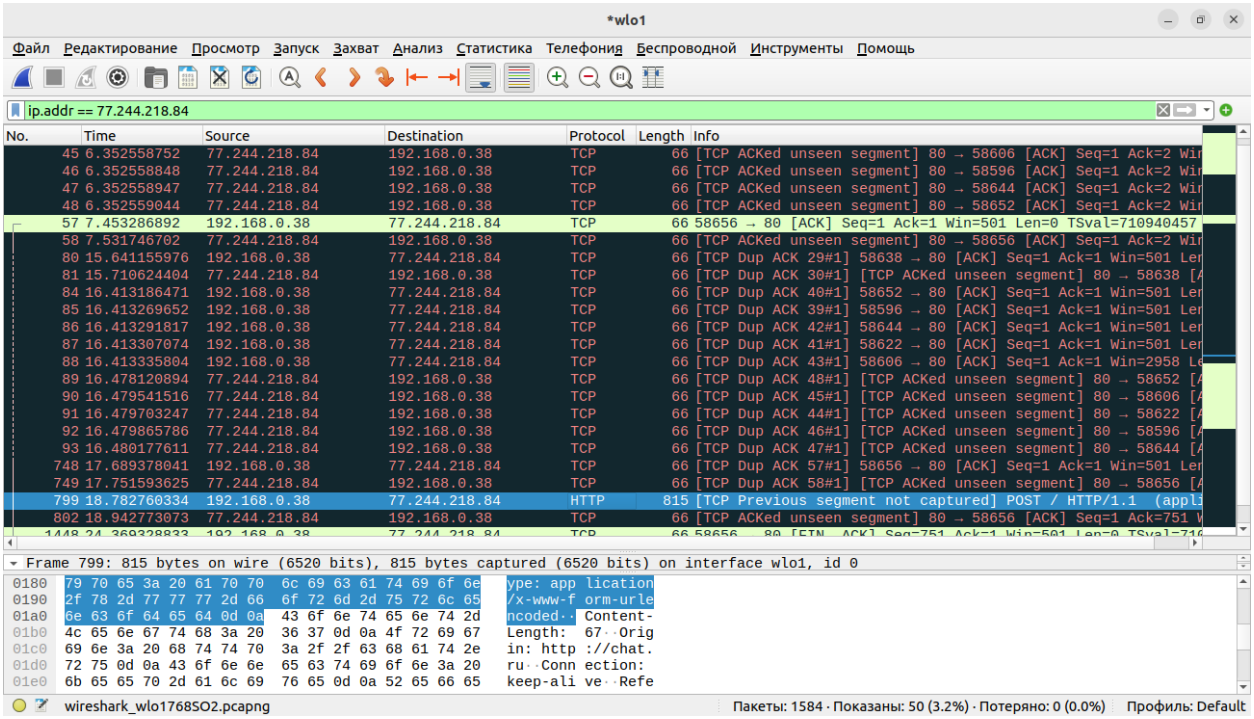
Трафик перехвачен

Wireshark отправляет пакеты по протоколу ICMP с постепенно увеличивающимся TTL от 1 до 30. Роутеры по пути следования пакета отвечают что TTL истек и уничтожают его (помечены черным цветом). Роутеры в конце пути перестают отправлять ответные пакеты, просто уничтожают запросы с истекшим TTL.

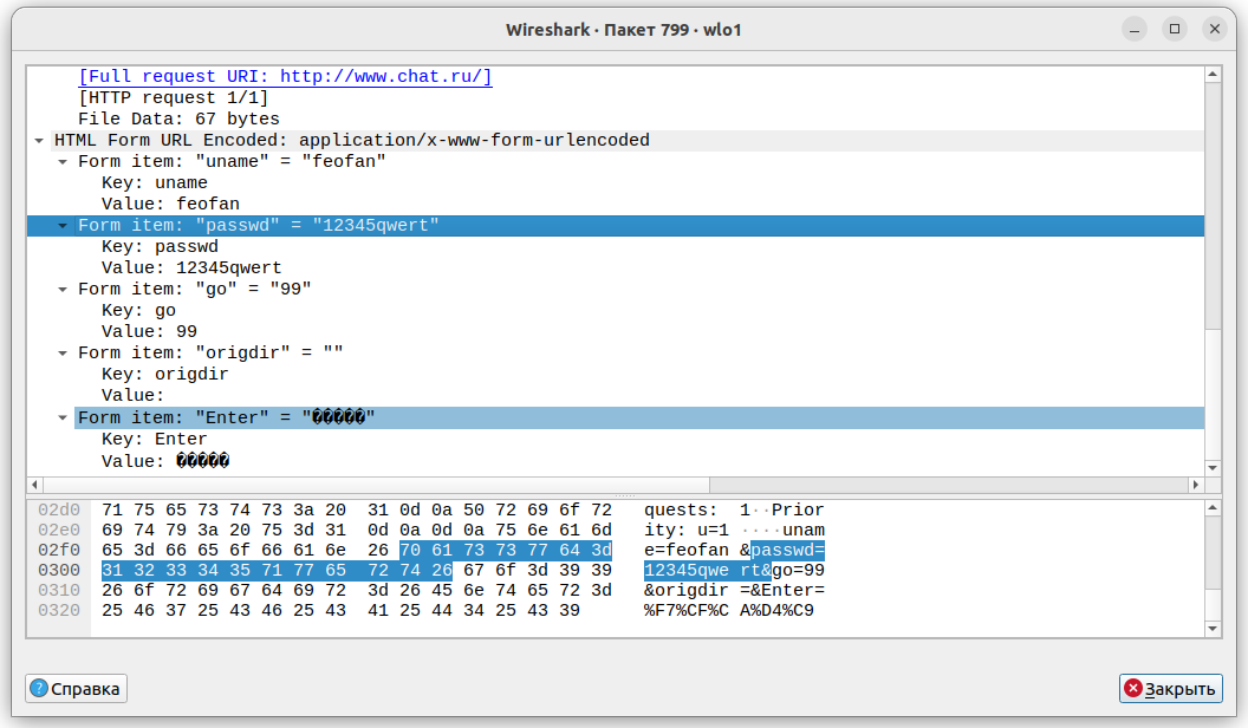
3. Для тестирования я выбрал старый добрый chat.ru



Определим IP-адрес сайта (77.244.218.84)



Перехватим трафик и отфильтруем по нужному IP-адресу



Найдем нужный пакет и посмотрим его содержимое:

Login: feofan
Password: 12345qwert