

## 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 фильтрации. Запустите трейс до 8.8.8.8. И перехватите его в Wireshark. Проанализируйте.
2. Закрепите навыки фильтрации. 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 Wireshark, построив фильтр.

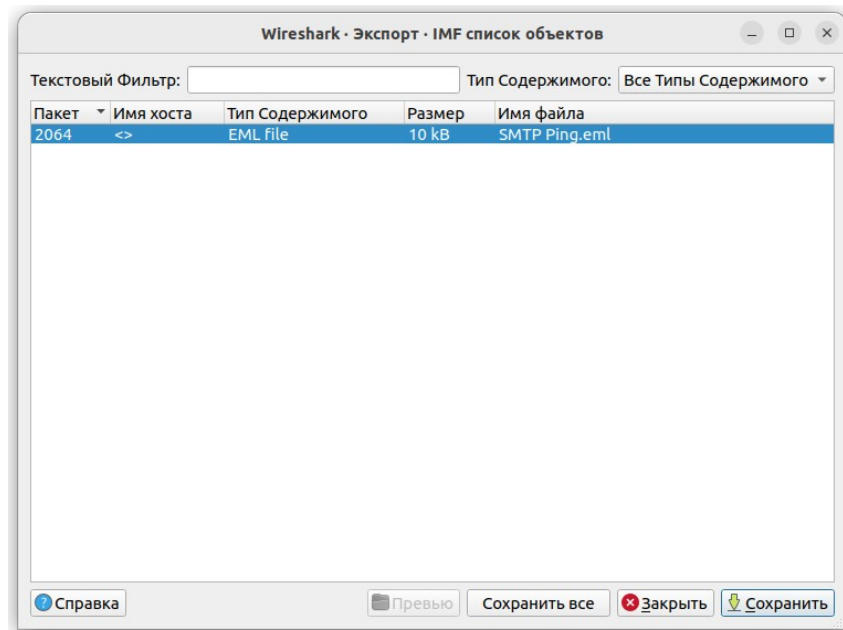
4\*. На сайте <https://launchpad.net/ubuntu/+archivemirrors> представлены зеркала с образами Убунту по странам. Скачайте файл ls-lR.gz из Чили и с Яндекса. Снимите два дампа для каждого скачивания. Проанализируйте скорость скачивания и посмотрите tcptrace. Прикиньте средний RTT и поищите максимальный RWND для скачивающего.

Предоставить скриншоты графиков скорости и tcptrace. Есть ли разница? В чем она?

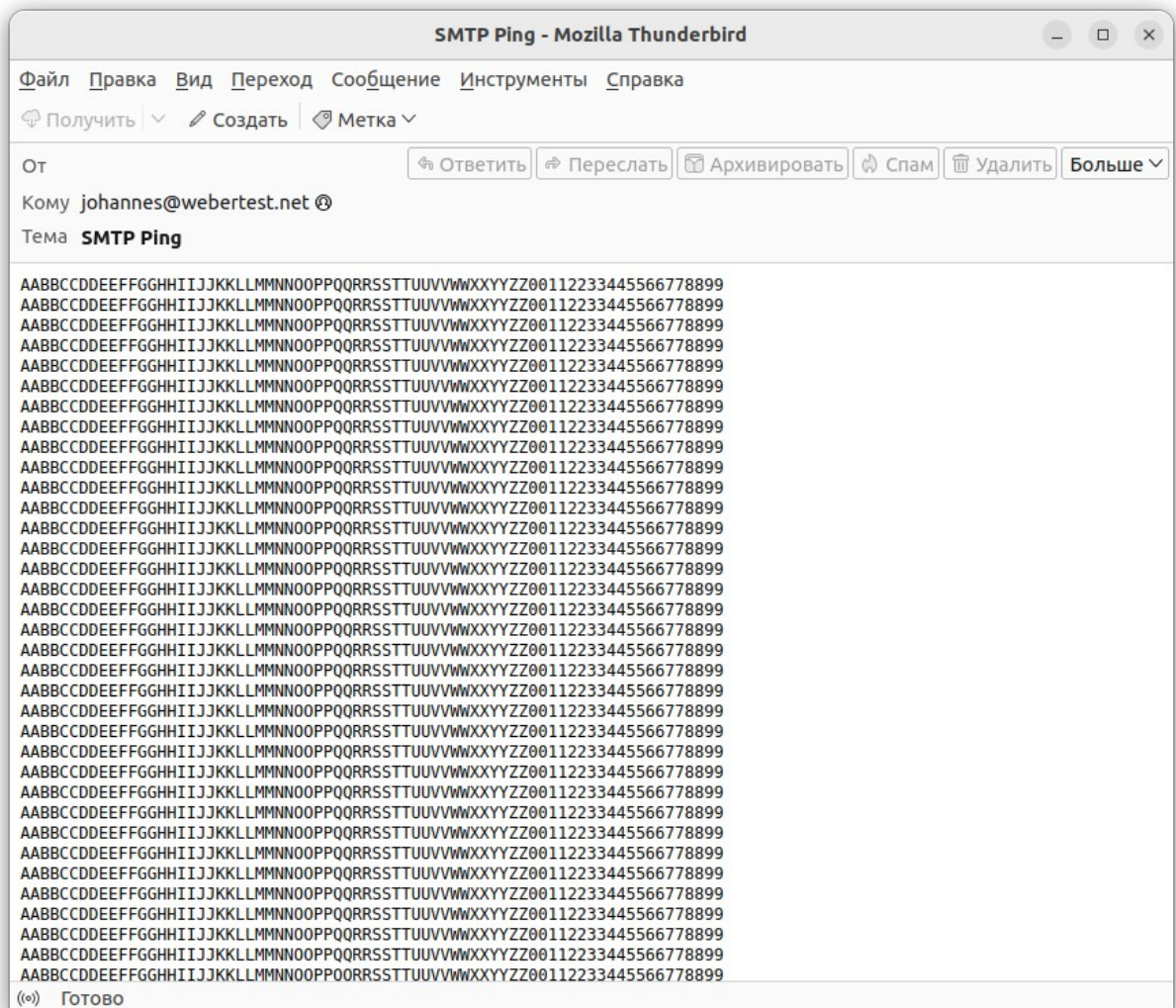
1. Посмотрите перед 2 семинаром к лекции по L4: <https://disk.yandex.ru/i/6pAvRRMrK2e7jw> файл из демонстрации: <https://disk.yandex.ru/d/czW2ZAIsLFXyHw>

### Решение:

1. Найдём в дампе письмо:



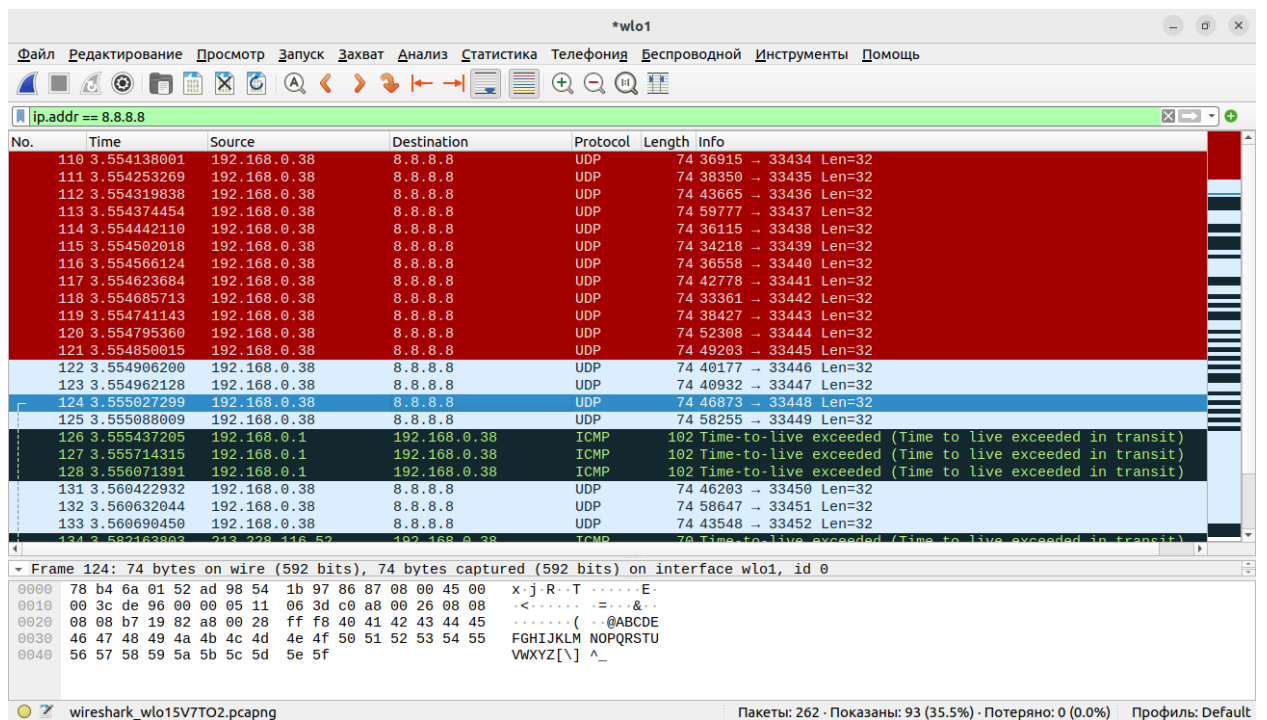
Посмотрим что внутри письма и кому оно адресовано:



Получатель письма: johannes@webertest.net

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

```
root@gaazoo-HP-255-G5-Notebook-PC: ~  
gaazoo@gaazoo-HP-255-G5-Notebook-PC: ~$ traceroute 8.8.8.8  
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets  
 1  RT (192.168.0.1)  1.373 ms  1.479 ms  1.768 ms  
 2  krsn-bras6.sib.ip.rostelecom.ru (213.228.116.52)  28.017 ms  27.738 ms  28.171 ms  
 3  ae7.krsn-rgr6.sib.ip.rostelecom.ru (213.228.110.42)  28.891 ms  29.109 ms  28.475 ms  
 4  * * *  
 5  72.14.205.132 (72.14.205.132)  82.839 ms  89.062 ms  82.491 ms  
 6  * * *  
 7  108.170.250.33 (108.170.250.33)  87.370 ms  77.532 ms  71.773 ms  
 8  108.170.250.66 (108.170.250.66)  69.256 ms  108.170.250.34 (108.170.250.34)  74.450 ms  108.170.250.66 (108.170.250.66)  68.834 ms  
 9  142.250.238.138 (142.250.238.138)  78.064 ms  142.251.49.78 (142.251.49.78)  104.813 ms  142.251.49.24 (142.251.49.24)  100.628 ms  
10  142.251.238.68 (142.251.238.68)  93.939 ms  142.251.238.70 (142.251.238.70)  87.160 ms  216.239.57.222 (216.239.57.222)  85.201 ms  
11  142.250.232.179 (142.250.232.179)  87.013 ms  142.250.210.47 (142.250.210.47)  83.642 ms  172.253.51.245 (172.253.51.245)  80.308 ms  
12  * * *  
13  * * *  
14  * * *  
15  * * *  
16  * * *
```



## 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.

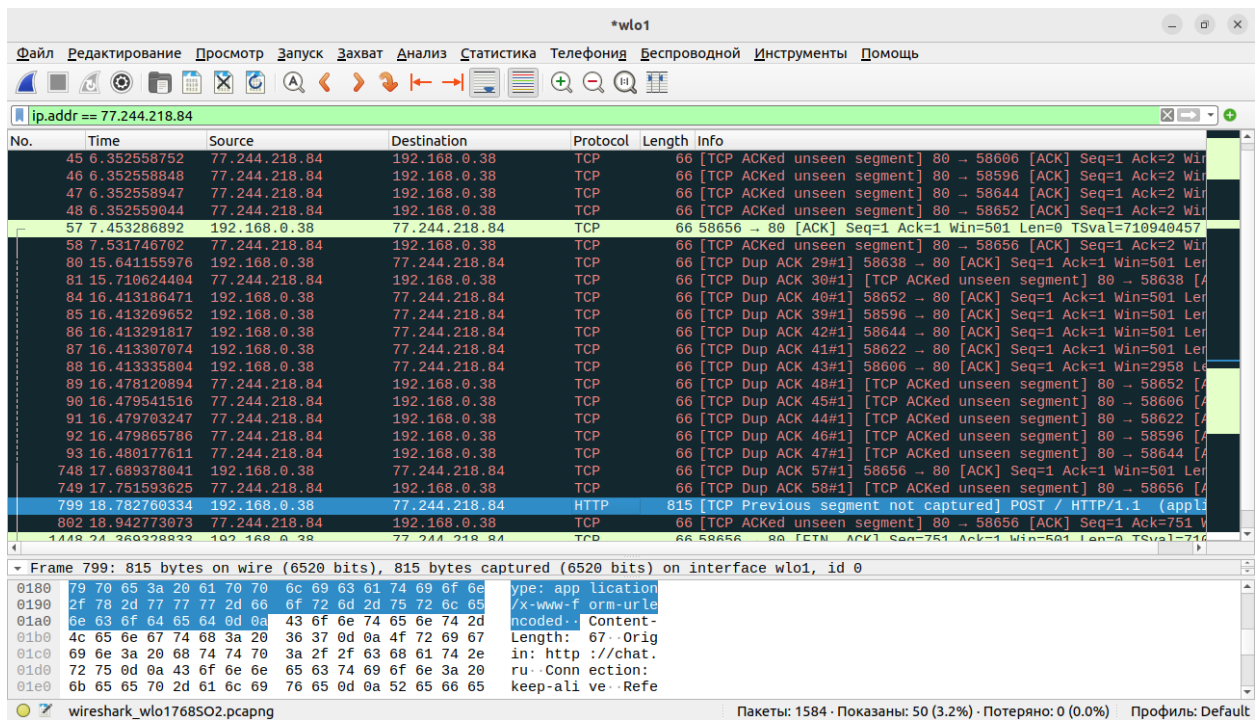
3. Для тестирования я выбрал старый добрый chat.ru

```

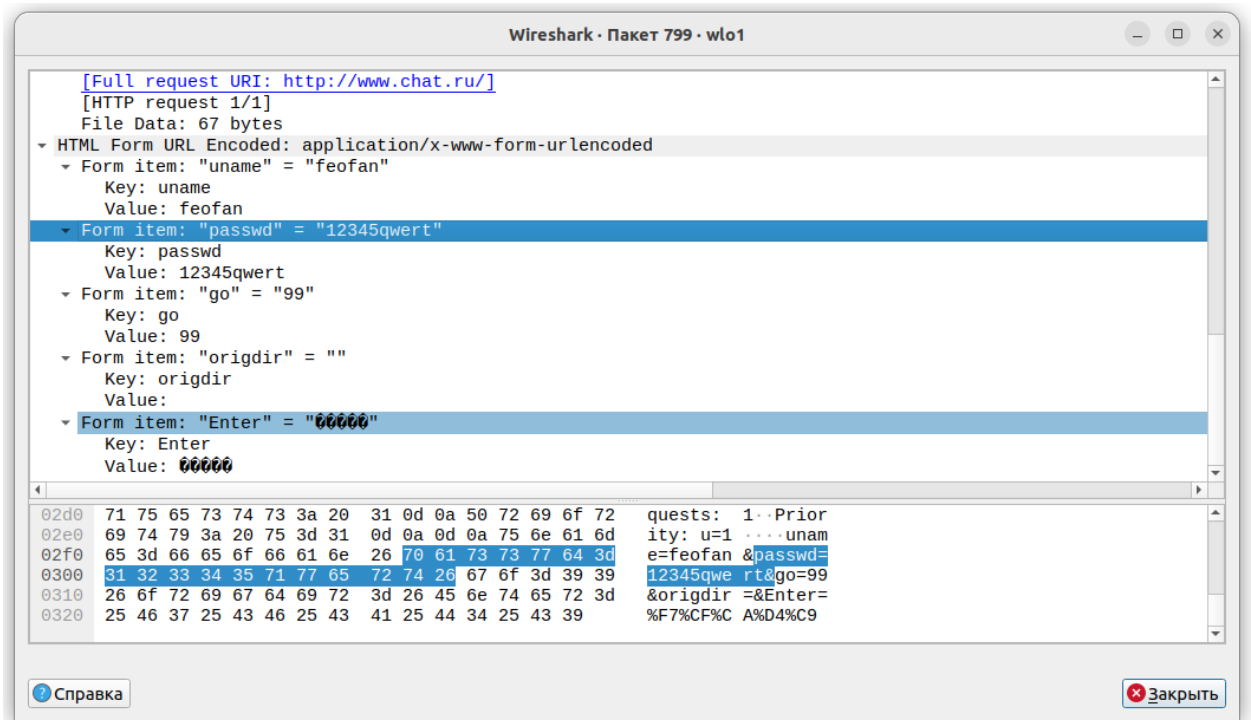
root@gaazoo-HP-255-G5-Notebook-PC: ~
gaazoo@gaazoo-HP-255-G5-Notebook-PC: ~$ ping chat.ru
PING chat.ru (77.244.218.84) 56(84) bytes of data:
64 bytes from 77.244.218.84 (77.244.218.84): icmp_seq=1 ttl=59 time=68.2 ms
64 bytes from 77.244.218.84 (77.244.218.84): icmp_seq=2 ttl=59 time=70.2 ms
64 bytes from 77.244.218.84 (77.244.218.84): icmp_seq=3 ttl=59 time=65.6 ms
64 bytes from 77.244.218.84 (77.244.218.84): icmp_seq=4 ttl=59 time=65.2 ms
64 bytes from 77.244.218.84 (77.244.218.84): icmp_seq=5 ttl=59 time=66.5 ms
64 bytes from 77.244.218.84 (77.244.218.84): icmp_seq=6 ttl=59 time=78.9 ms
64 bytes from 77.244.218.84 (77.244.218.84): icmp_seq=7 ttl=59 time=81.8 ms
64 bytes from 77.244.218.84 (77.244.218.84): icmp_seq=8 ttl=59 time=84.8 ms
64 bytes from 77.244.218.84 (77.244.218.84): icmp_seq=9 ttl=59 time=67.9 ms
^C
--- chat.ru ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 800ms
rtt min/avg/max/mdev = 65.166/72.113/84.808/7.156 ms
root@gaazoo-HP-255-G5-Notebook-PC: ~$

```

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