Московский государственный технический университет им. Н.Э. Баумана

Факультет «Информатика и системы управления»

Кафедра «Системы обработки информации и управления»



**Отчет**

**Лабораторная работа № 7**

**По курсу «Сети и телекоммуникации»**

**«Исследование протоколов сетевого и транспортного уровней IP-сетей с помощью анализатора протоколов NetInfo, Wireshark»**

**ИСПОЛНИТЕЛЬ:**

Группа ИУ5-55Б

\_Финк Д.Д.

"29"\_декабря\_\_2021 г.

**ПРЕПОДАВАТЕЛЬ:**

\_\_\_Канев А.И.\_\_\_\_

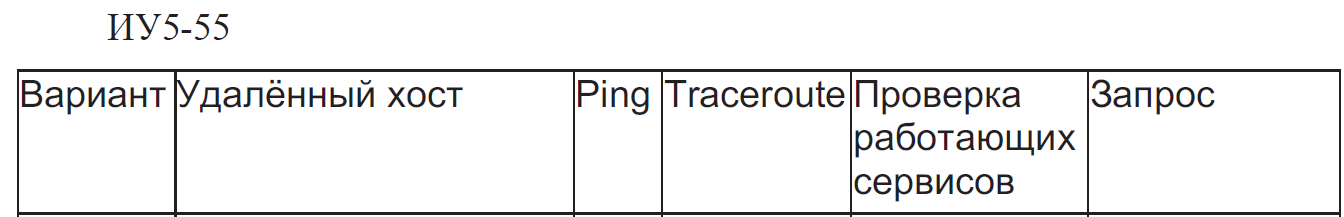
"\_\_"\_\_\_\_\_\_\_\_\_\_2021 г.

Москва 2021

1. Цель работы

Развитие практических навыков работы с протоколами TCP/IP и исследование возможностей протоколов ICMP, UDP, TCP.

1. Задание





В соответствии с вариантом либо послать СМР зхо-запрос на удалённый хост, либо определить количество «хопов» до удалённого хоста. При помощи пакетного анализатора проанализировать все пакеты, приходящие на сетевой интерфейс. Для нечётных вариантов просматривать [СМР трафик, а для чётных СМР и ЦОР трафик.

Результаты анализа представить в отчете.

Просканировать порты удалённого хоста, зафиксировать и описать службы на открытых портах.

Сделать запросы, соответствующие варианту. Объяснить реакцию хоста на каждый запрос.

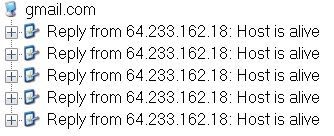
Отчет по лабораторной работе должен содержать сценарии выполнения вышеуказанных процедур. результаты анализа пакетов, описание служб на открытых портах удалённого хоста, описание реакции на запросы,

1. Ход работы.

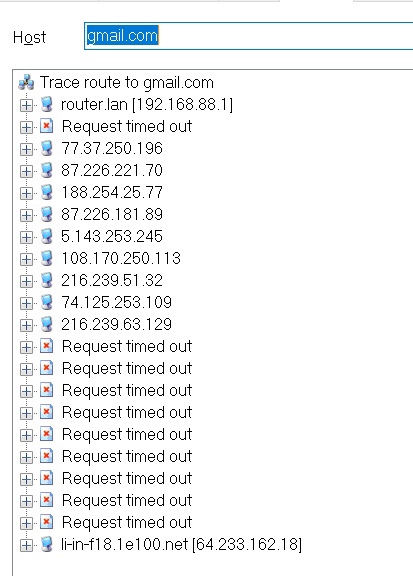
Узнаю ip-адрес ресурса с помощью утилиты Lookup



Очевидно, сервис работает. Проверю утилитой ping



Получу больше информации о маршруте помощью утилиты Traceroute

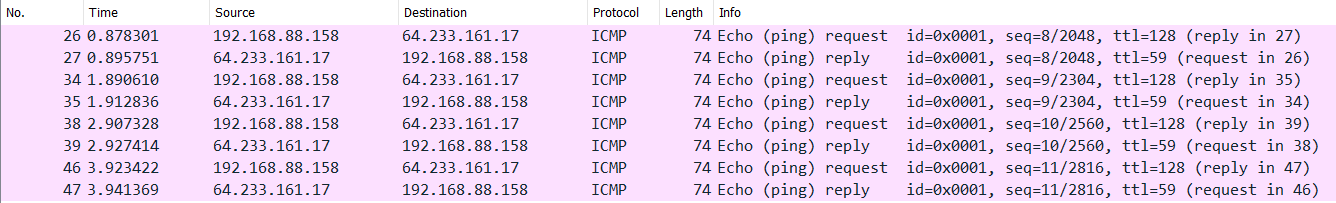


Чтобы просмотреть содержимое пакетов, воспользуюсь утилитой WebShark.

Мой компьютер соединен с интернетом по беспроводной сети WI-FI. Выберу ее.

Утилиты ping и traceroot работают по протоколу ICMP. Отправлю ping – запрос на gmail.com

Поле просмотра сразу заполнилось множеством ICMP-echo пакетов.



Для сканирования всех портов хоста использую утилиту N-Map (вкладка Services в NetInfo). Укажу хост ip 185.137.235.16.



Видно, что стандартные порты для http открыты: 443 для https, 80 для http, 8080.

Остальные же порты, в т.ч. finger, time, datetime, telnet и прочие закрыты. Такое поведение характерно для настроенного прокси-сервера, задача которого при обращении к нему по данному IP, отдавать html-страницы и статику веб-приложения. Остальные протоколы, может, и доступны, но по другим ip-адресам, не анонсируемым по DNS. Сделано это для изолированности ЛВС датацентра, на котором развернут ресурс от вешнего интернета.

Сделаю запросы:

Who-is:



Здесь получаем подробную информацию о юридической принадлежности домена.

Сделаю HTML запрос в браузере или в HTTP-утилите NetInfo

