МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»
ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
Кафедра компьютерной инженерии и моделирования

Анализ сетевого трафика с помощью программы wireshark

Отчет по лабораторной работе № 2
по дисциплине «Компьютерные сети»
студента 2 курса группы ИВТ-б-о-202(1)
Шор Константина Александровича

Направления подготовки 09.03.01«Информатика и вычислительная техника»

Симферополь, 2021

Цели:

Загрузка и установка wireshark.

Сбор и анализ данных протокола ICMP по удалённым узлам в программе Wireshark.

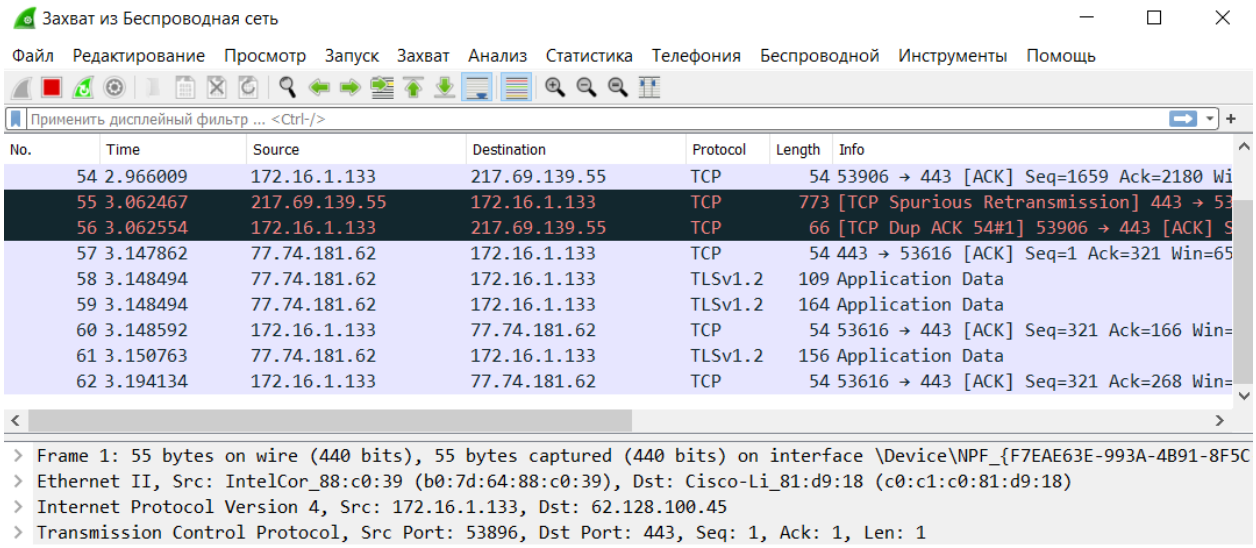
Изучить поле заголовков в кадре Ethernet

Захват и анализ кадров Ethernet с помощью программы Wireshark.

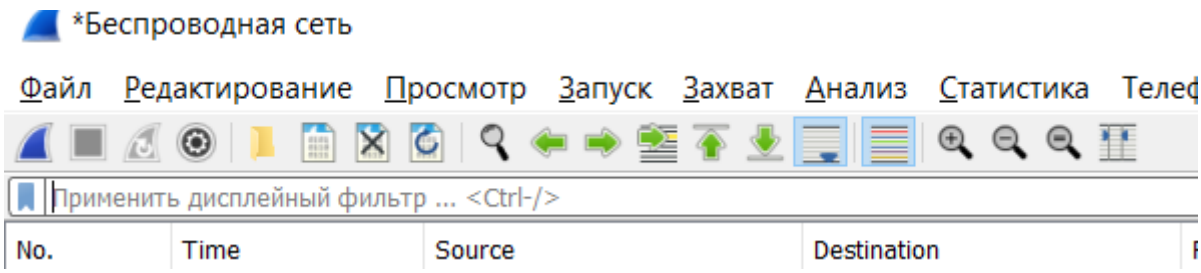
1.2 Анализ сетевого трафика с помощью программы « Wireshark»

Шаг 1 Запустить программу Wireshark

Шаг 2 Запустить процесс захвата трафика.



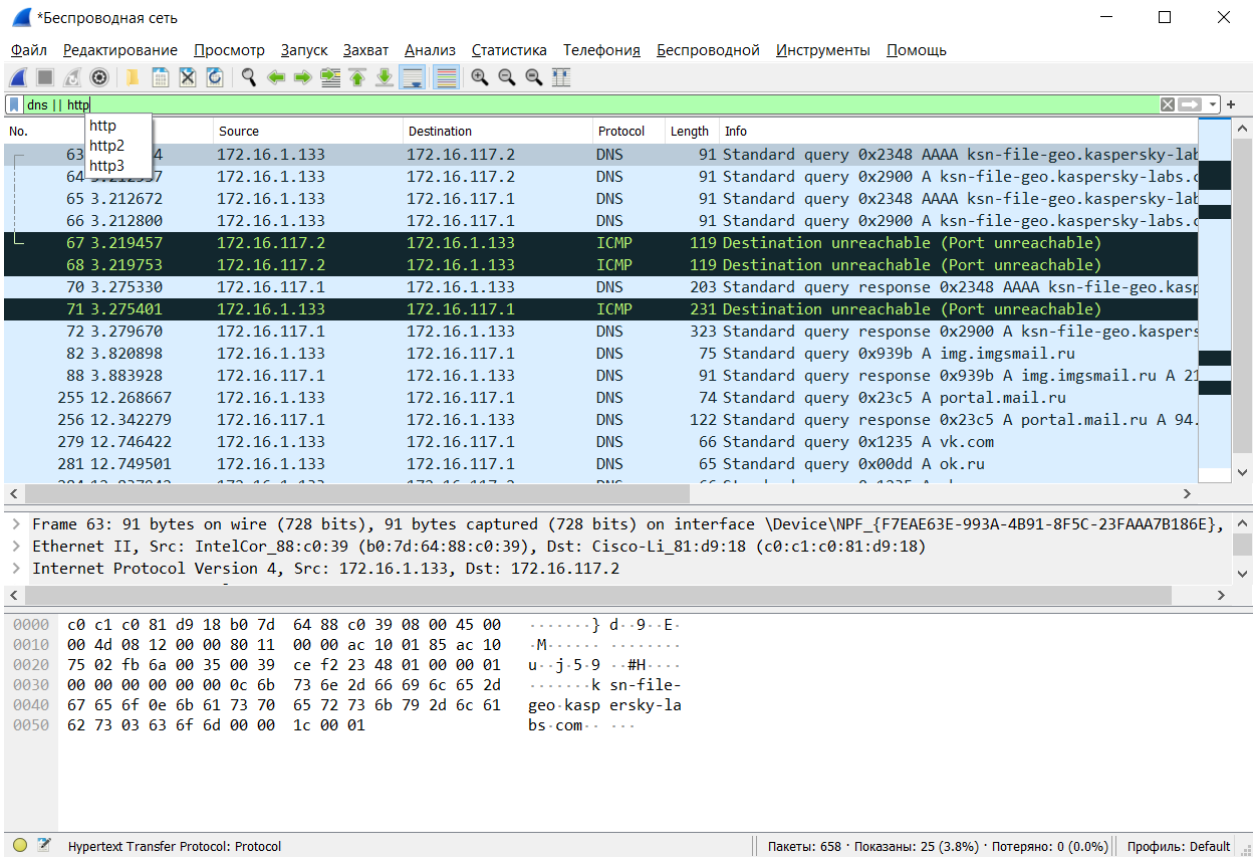
Шаг 3. Остановить процесс захвата



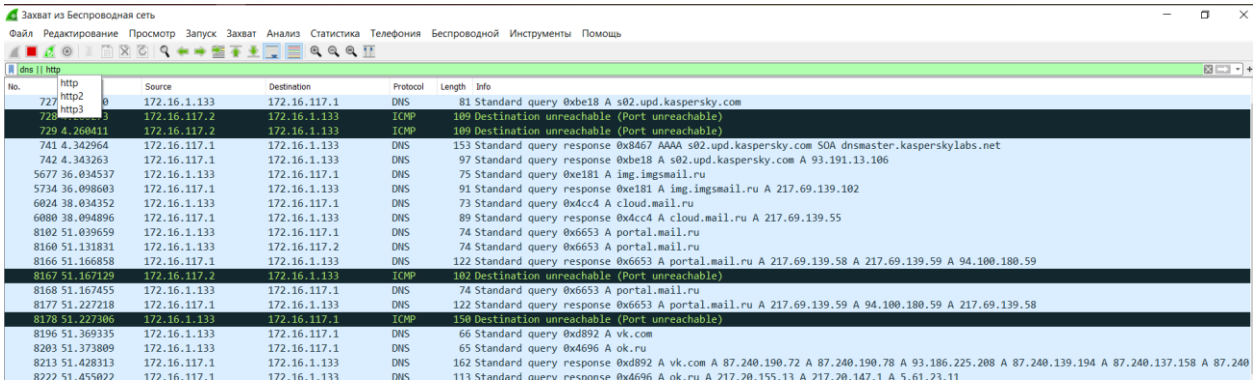
Шаг 4. Изучить интерфейс главного окна

Шаг 5. Запустить процесс захвата трафика заново.

Шаг 6. Настроить фильтрацию вывода по протоколам DNS и HTTP.



Шаг 7. Запустить обновление для установщика антивируса или проверку на наличие обновлений встроенного Защитника Windows.



Шаг 8. Остановить захват трафика

Шаг 9. Проанализировать трафик, захваченный программой.

9.1

```
DNS        81 Standard query 0x184a A s02.upd.kaspersky.com
DNS        97 Standard query response 0x184a A s02.upd.kaspersky.com A 93.191.13.106
```

9.2

DNS:

```
Standard query response 0x184a A s02.upd.kaspersky.com A 93.191.13.106
```

Адреса серверов обновления:

```
93.191.13.106
```

```
62.128.100.148
```

В процессе обновления dns отрабатывало несколько раз и в разных ответах было разное кол-во адресов у серверов.

9.3

```
HTTP       341 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?74dbf2e1ee135873 HTTP/1.1
```

9.4

Сетевой адрес компьютера: `172.16.1.133`

`User-Agent: Microsoft-CryptoAPI/10.0\r\n`

9.5

Сетевой адрес компьютера: `Src: 172.16.1.133`

MAC- адрес компьютера: `b0:7d:64:88:c0:39`

Сетевой адрес шлюза: `Dst: 62.140.236.163`

MAC- адрес шлюза: `c0:c1:c0:81:d9:18`

Сетевой адрес DNS- сервера: `ctldl.windowsupdate.com`

Протокол транспортного уровня, который использует DNS: `UDP (17)`

Порт, на который осуществляется DNS запрос: `Source Port: 54319`

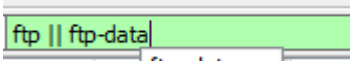
Протокол транспортного уровня, который использует HTTP: `TCP (6)`

Порт, на который осуществляется запрос обновления антивируса по протоколу HTTP: `Destination Port: 80`

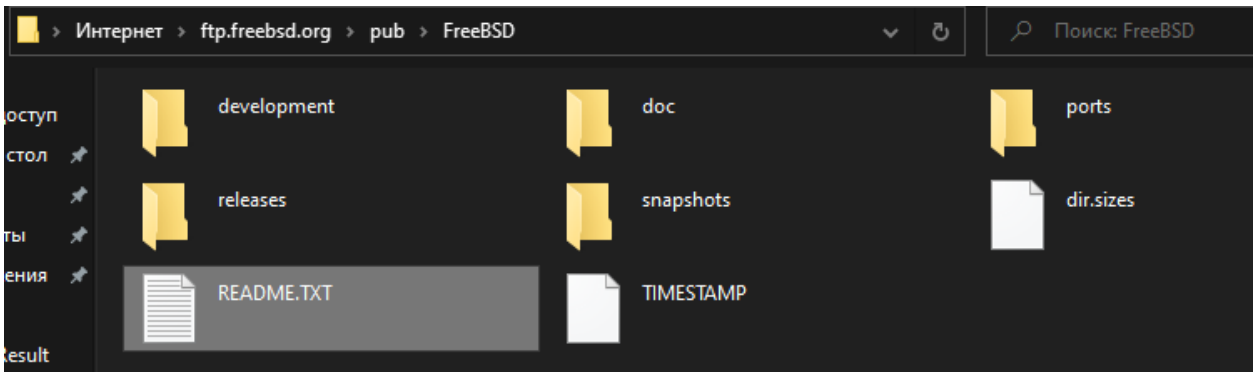
Шаг 10. Сохранить трафик

Шаг 11. Заново запустить захват трафика

Шаг 12. Настроить фильтрацию вывода по протоколу FTP.



Шаг 13. Скачать файл с FTP



Шаг 14. Проанализировать трафик, захваченный программой.

14.1

```
FTP-DATA      1514 FTP Data: 1460 bytes (PASV) (SIZE README.TXT)
FTP-DATA      1514 FTP Data: 1460 bytes (PASV) (SIZE README.TXT)
FTP-DATA      1393 FTP Data: 1339 bytes (PASV) (SIZE README.TXT)
```

14.2 Содержимое FTP data:

- 1460
- Сетевой адрес FTP: `139.178.72.202`
- MAC-адрес FTP: `50:ff:20:68:21:32)`
- Протокол транспортного уровня: `TCP (6)`
- Порт, который используется при передаче данных:

```
Source Port: 61125
Destination Port: 60529
```

Часть 1 сбор и анализ данных протокола ICMP по локальным узлам в программе Wireshark

Шаг 1. Узнать адрес своего ПК.

```
172.16.1.119(Основной)
```

Шаг 1. Запустить программу и узнать сбор данных.

35471	172.16.1.119	172.16.1.121	ICMP	74	Echo (ping) request	id=0x0001, seq=2/512, ttl=128 (reply in 4888)
4888 30.338426	172.16.1.121	172.16.1.119	ICMP	74	Echo (ping) reply	id=0x0001, seq=2/512, ttl=64 (request in 4887)
5041 31.199491	172.16.1.119	172.16.1.121	ICMP	74	Echo (ping) request	id=0x0001, seq=3/768, ttl=128 (reply in 5042)
5042 31.201531	172.16.1.121	172.16.1.119	ICMP	74	Echo (ping) reply	id=0x0001, seq=3/768, ttl=64 (request in 5041)
5198 32.214192	172.16.1.119	172.16.1.121	ICMP	74	Echo (ping) request	id=0x0001, seq=4/1024, ttl=128 (reply in 5205)
5205 32.248655	172.16.1.121	172.16.1.119	ICMP	74	Echo (ping) reply	id=0x0001, seq=4/1024, ttl=64 (request in 5198)
5360 33.228811	172.16.1.119	172.16.1.121	ICMP	74	Echo (ping) request	id=0x0001, seq=5/1280, ttl=128 (reply in 5361)
5361 33.231121	172.16.1.121	172.16.1.119	ICMP	74	Echo (ping) reply	id=0x0001, seq=5/1280, ttl=64 (request in 5360)

Шаг 3. Изучить полученные данные.

b)

MAC адрес источника совпадает

MAC адрес другого участника совпадает 74-E5-43-12-45-5A

Благодаря маршрутизатору, который знает MAC адреса

(Потому что Сетевой уровень находится выше чем канальный)

Часть 2. Сбор и анализ данных протокола ICMP по удаленным узлам в программе Wireshark.

Шаг 1. Захват данных интерфейса

1) 87.248.100.215
2) 2.18.196.94
3) 142.250.74.100

Шаг 2. Анализ полученных данных.

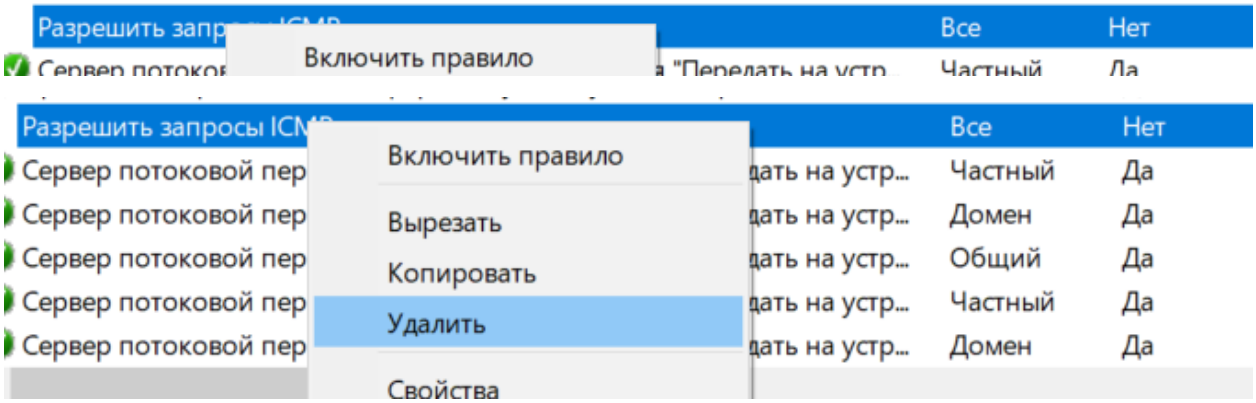
1) Yahoo 87.248.100.215 Cisco-Li_81:d9:18 (c0:c1:c0:81:d9:18)
2) Cisco 2.18.196.94 Cisco-Li_81:d9:18 (c0:c1:c0:81:d9:18)
3) Google 142.250.74.100 Cisco-Li_81:d9:18 (c0:c1:c0:81:d9:18)

Mac адрес у всех одинаковый (адрес маршрутизатора), в первой же лабе mac адрес был компьютера другого учащегося.

Приложение А. Пропуск трафика ICMP через межсетевой экран.

Часть 1. Создать новое правило, разрешающее прохождение ICMP- трафика через межсетевой экран.

Часть 2. Отключение и удаление нового правила ICMP



Лабораторная работа. Анализ кадров Ethernet с помощью программы Wireshark

Часть 1. Изучение полей заголовков в кадре Ethernet 2

Шаг 1. Посмотреть длины и описания полей заголовков

Шаг 2. Изучить конфигурацию сети ПК.

Шаг 3. Изучите кадры ethernet в данных, перехваченных Wireshark

IШаг 4. Изучите содержимое заголовков Ethernet в ARP-запросе

1) Адрес назначения может быть адресом широковещательной рассылкой или одноадресной рассылкой. Адрес источника всегда является адресом одноадресной рассылки.
2) Для построения соотношения MAC - Ip
3) (30:46:9a:99:c5:72)
4) (30:46:9a:
5) Первые 6 цифр

6) 99:c5:72

Часть 2. Перехват и анализ данных кадров Ethernet с помощью команды Wireshark

Шаг 1. Определить ip адрес шлюза по умолчанию на ПК

```
172.16.1.119
```

Шаг 2. Начните захват трафика своей сетевой платы

Шаг 3. С помощью фильтров программы Wireshark отобразите на экране только трафик ICMP.

Шаг 4. Из окна командной строки отправьте эхо-запрос на шлюз ПК по умолчанию

```
C:\Users\User>ping www.google.com

Обмен пакетами с www.google.com [142.250.74.4] с 32 байтами данных:
Ответ от 142.250.74.4: число байт=32 время=43мс TTL=52
Ответ от 142.250.74.4: число байт=32 время=48мс TTL=52
Ответ от 142.250.74.4: число байт=32 время=45мс TTL=52
Ответ от 142.250.74.4: число байт=32 время=45мс TTL=52
```

Шаг 5. Остановите захват трафика на сетевой плате.

Шаг 6. Изучите первый эхо-запрос в программе Wireshark.

C)

```
IntelCor_88:c0:39 (b0:7d:64:88:c0:39), Dst: Cisco-Li_81:d9:18 (c0:c1:c0:81:d9:18)
```

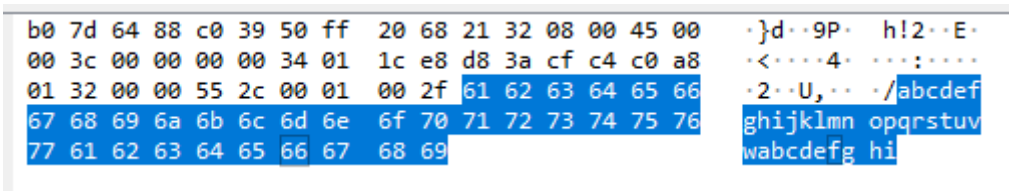
D)

```
Type: IPv4 (0x0800)
```

E)

```
Src: 172.16.1.119, Dst: 142.250.74.4
```

F)



Слово: hi

G)

```
Ethernet II, Src: Keenetic_68:21:32 (50:ff:20:68:21:32), Dst: IntelCor_88:c0:39 (b0:7d:64:88:c0:39)
```

MAC- адреса поменялись

Шаг 7. Захват пакетов для удалённого узла

D)

Mac:

Источник: `Src: IntelCor_88:c0:39 (b0:7d:64:88:c0:39)`

Назначение: `Dst: Keenetic_68:21:32 (50:ff:20:68:21:32)`

Ip:

Источник: `Src: 192.168.1.50,`

Назначение: `Dst: 2.23.130.48`

Физический адрес привязан к компьютеру. Ip поменялся потому, что мы захватывали пакеты разных DNS.