

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.

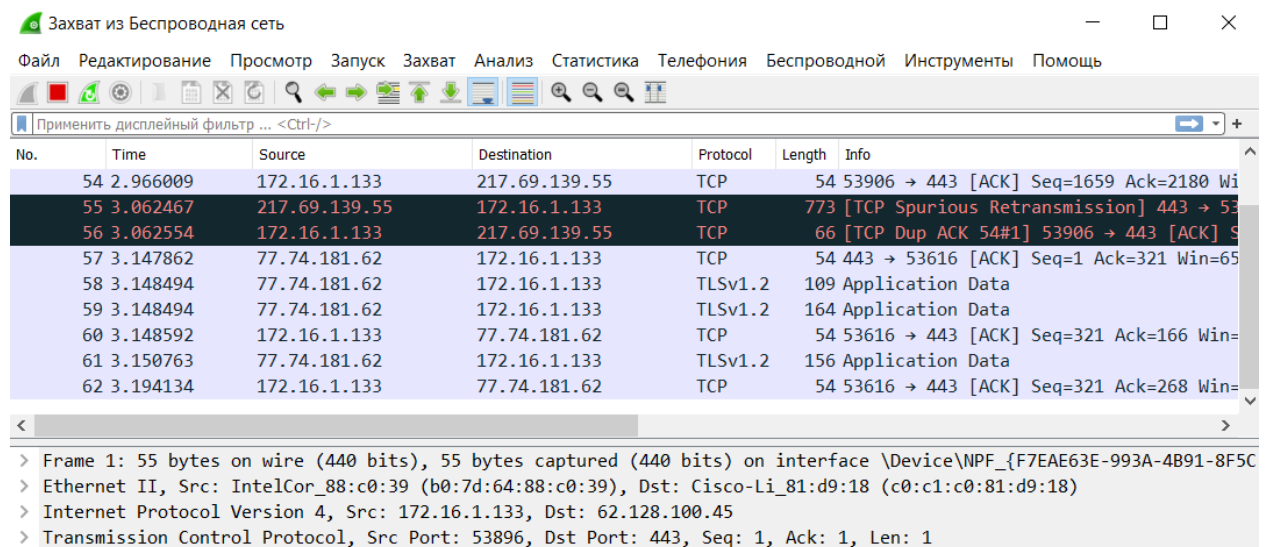
Изучить поле заголовков в кадре Ethernet

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

*Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония



Применить дисплейный фильтр ... <Ctrl-/>

No.	Time	Source	Destination
-----	------	--------	-------------

Шаг 4. Изучить интерфейс главного окна

Шаг 5. Запустить процесс захвата трафика заново.

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

*Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

dns | http

No.	Time	Source	Destination	Protocol	Length	Info
63	3.219457	172.16.1.133	172.16.117.2	DNS	91	Standard query 0x2348 AAAA ksn-file-geo.kaspersky-labs.com
64	3.219753	172.16.1.133	172.16.117.2	DNS	91	Standard query 0x2900 A ksn-file-geo.kaspersky-labs.com
65	3.212672	172.16.1.133	172.16.117.1	DNS	91	Standard query 0x2348 AAAA ksn-file-geo.kaspersky-labs.com
66	3.212800	172.16.1.133	172.16.117.1	DNS	91	Standard query 0x2900 A ksn-file-geo.kaspersky-labs.com
67	3.219457	172.16.117.2	172.16.1.133	ICMP	119	Destination unreachable (Port unreachable)
68	3.219753	172.16.117.2	172.16.1.133	ICMP	119	Destination unreachable (Port unreachable)
70	3.275330	172.16.117.1	172.16.1.133	DNS	203	Standard query response 0x2348 AAAA ksn-file-geo.kaspersky-labs.com
71	3.275401	172.16.1.133	172.16.117.1	ICMP	231	Destination unreachable (Port unreachable)
72	3.279670	172.16.117.1	172.16.1.133	DNS	323	Standard query response 0x2900 A ksn-file-geo.kaspersky-labs.com
82	3.820898	172.16.1.133	172.16.117.1	DNS	75	Standard query 0x939b A img.imgsmail.ru
88	3.883928	172.16.117.1	172.16.1.133	DNS	91	Standard query response 0x939b A img.imgsmail.ru A 213.180.200.10
255	12.268667	172.16.1.133	172.16.117.1	DNS	74	Standard query 0x23c5 A portal.mail.ru
256	12.342279	172.16.117.1	172.16.1.133	DNS	122	Standard query response 0x23c5 A portal.mail.ru A 94.130.130.130
279	12.746422	172.16.1.133	172.16.117.1	DNS	66	Standard query 0x1235 A vk.com
281	12.749501	172.16.1.133	172.16.117.1	DNS	65	Standard query 0x00dd A ok.ru

> Frame 63: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{F7EAE63E-993A-4B91-8F5C-23FAAA7B186E}, Ethernet II, Src: IntelCor_88:c0:39 (b0:7d:64:88:c0:39), Dst: Cisco-Li_81:d9:18 (c0:c1:c0:81:d9:18)

> Internet Protocol Version 4, Src: 172.16.1.133, Dst: 172.16.117.2

```
0000  c0 c1 c0 81 d9 18 b0 7d 64 88 c0 39 08 00 45 00  .....} d..9..E-
0010  00 4d 08 12 00 00 80 11 00 00 ac 10 01 85 ac 10  .M.....
0020  75 02 fb 6a 00 35 00 39 ce f2 23 48 01 00 00 01  u..j.5.9 ..#H....
0030  00 00 00 00 00 00 0c 6b 73 6e 2d 66 69 6c 65 2d  ....k sn-file-
0040  67 65 6f 0e 6b 61 73 70 65 72 73 6b 79 2d 6c 61  geo-kasp ersky-la
0050  62 73 03 63 6f 6d 00 00 1c 00 01                bs-com... ..
```

Hypertext Transfer Protocol: Protocol

Пакеты: 658 · Показаны: 25 (3.8%) · Потеряно: 0 (0.0%) · Профиль: Default

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

The screenshot shows a Wireshark packet capture of DNS traffic. The top pane displays a list of 17 packets. The bottom pane shows the details of the selected packet (No. 172, http2, 0), which is a DNS query from 172.16.1.133 to 172.16.117.1. The query is for the domain 's02.upd.kaspersky.com' and is a standard query type.

No.	Time	Source	Destination	Protocol	Length	Info
727	0.000000	172.16.1.133	172.16.117.1	DNS	81	Standard query 0xe18 A s02.upd.kaspersky.com
728	0.000000	172.16.117.2	172.16.1.133	ICMP	109	Destination unreachable (Port unreachable)
729	0.000000	172.16.117.2	172.16.1.133	ICMP	109	Destination unreachable (Port unreachable)
741	0.000000	172.16.117.1	172.16.1.133	DNS	153	Standard query response 0x8467 AAAA s02.upd.kaspersky.com SOA dnsmaster.kasperskylabs.net
742	0.000000	172.16.117.1	172.16.1.133	DNS	97	Standard query response 0xe18 A s02.upd.kaspersky.com A 93.191.13.106
5677	36.034537	172.16.1.133	172.16.117.1	DNS	75	Standard query 0xe181 A img.ingsmail.ru
5734	36.098603	172.16.117.1	172.16.1.133	DNS	91	Standard query response 0xe181 A img.ingsmail.ru A 217.69.139.102
6024	39.04352	172.16.1.133	172.16.117.1	DNS	73	Standard query 0xc4c A cloud.mail.ru
6080	38.094806	172.16.117.1	172.16.1.133	DNS	89	Standard query response 0xc4c A cloud.mail.ru A 217.69.139.55
8102	51.039659	172.16.1.133	172.16.117.1	DNS	74	Standard query 0x6653 A portal.mail.ru
8168	51.13181	172.16.1.133	172.16.117.2	DNS	74	Standard query 0x6653 A portal.mail.ru
8166	51.166858	172.16.117.1	172.16.1.133	DNS	122	Standard query response 0x6653 A portal.mail.ru A 217.69.139.58 A 217.69.139.59 A 94.100.180.59
8167	51.167129	172.16.117.2	172.16.1.133	ICMP	102	Destination unreachable (Port unreachable)
8168	51.167455	172.16.1.133	172.16.117.1	DNS	74	Standard query 0x6653 A portal.mail.ru
8177	51.227218	172.16.117.1	172.16.1.133	DNS	122	Standard query response 0x6653 A portal.mail.ru A 217.69.139.59 A 94.100.180.59 A 217.69.139.58
8178	51.227306	172.16.1.133	172.16.117.1	ICMP	150	Destination unreachable (Port unreachable)
8196	51.369335	172.16.1.133	172.16.117.1	DNS	66	Standard query 0xd892 A vk.com
8203	51.373809	172.16.1.133	172.16.117.1	DNS	65	Standard query 0x4696 A ok.ru
8213	51.428313	172.16.117.1	172.16.1.133	DNS	162	Standard query response 0xd892 A vk.com A 87.240.190.72 A 87.240.190.78 A 93.186.225.208 A 87.240.139.194 A 87.240.137.158 A 87.240.137.159

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

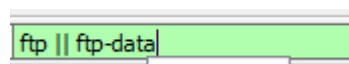
Протокол транспортного уровня, который использует HTTP: TCP (6)

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

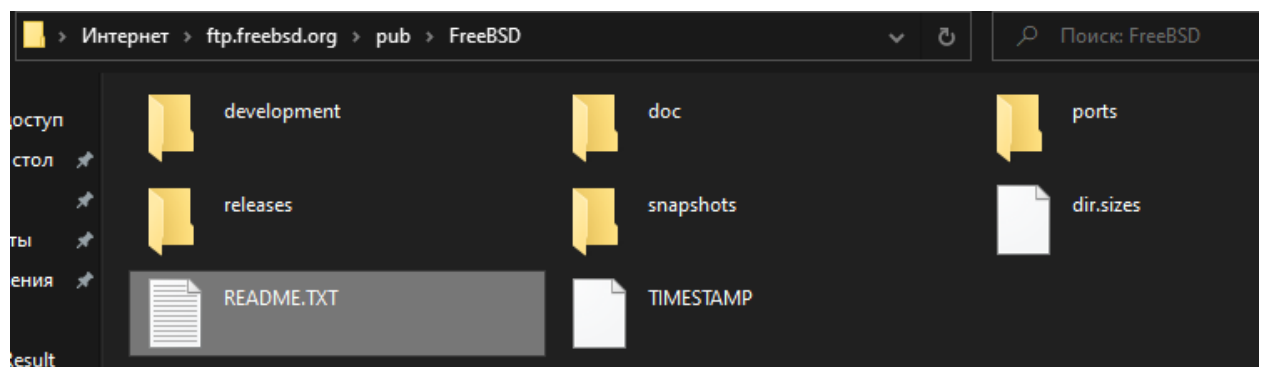
Шаг 10. Сохранить трафик

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.

icmpv6	5471	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.

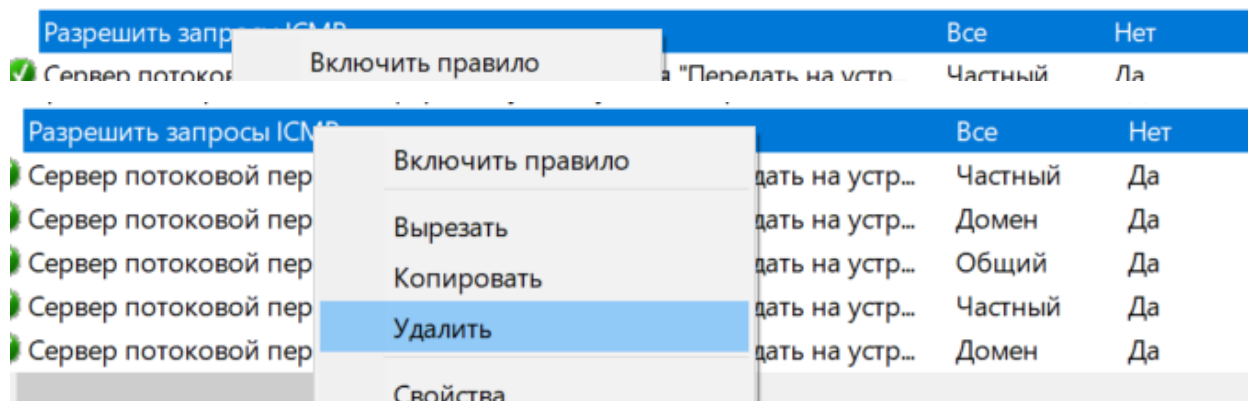
Часть 1. Создать новое правило, разрешающее прохождение ICMP- трафика через межсетевой экран.

Разрешить запросы ICMP

Все

Нет

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

Шаг 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:99:c5:72)
- 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)

b0	7d	64	88	c0	39	50	ff	20	68	21	32	08	00	45	00	·}	d·	·9P·	h!	2·	·E·
00	3c	00	00	00	00	34	01	1c	e8	d8	3a	cf	c4	c0	a8	·<	·	·	·	·	·
01	32	00	00	55	2c	00	01	00	2f	61	62	63	64	65	66	·2	·	·U,	·	·/abcdef	
67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	g	h	i	j	k	
77	61	62	63	64	65	66	67	68	69							l	m	n	o	p	

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.