

Санкт-Петербургский Политехнический Университет Петра
Великого
Институт компьютерных наук и технологий
Кафедра компьютерных систем и программных технологий

Отчёт по лабораторной работе №1

Дисциплина: Защита информации

Тема: Исследование сетевого трафика

Выполнил студент группы 43501/3

_____ Круминьш Д.В.
(подпись)

Преподаватель

_____ Новопашенный А.Г.
(подпись)

Санкт-Петербург
2017 г.

Содержание

1	Цель работы	2
2	Программа работы	2
3	Конфигурация сети	2
4	Ход работы	3
4.1	Утилита ping	3
4.1.1	Ping без фрагментации	3
4.1.2	Ping с фрагментацией	4
4.2	Утилита tracert	7
4.3	Протокол ARP	8
4.4	Протокол ICMP	10
4.5	Протокол UDP	11
4.6	Протокол TCP	12
4.6.1	Установка соединения	12
4.6.2	Разрыв соединения	13
4.6.3	Попытка соединения на отсутствующий порт	14
5	Вывод	14

1 Цель работы

Получение навыков по исследованию сетевого трафика.

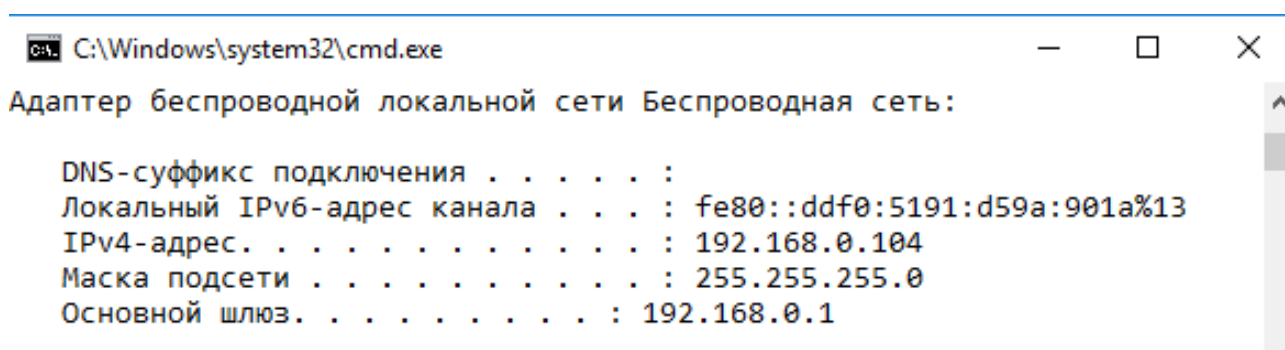
2 Программа работы

При помощи анализатора сетевого трафика Wireshark продемонстрировать в сети работу, следующих протоколов и утилит:

1. Утилиты ping:
 - без фрагментации,
 - с фрагментацией.
2. Утилиты tracer;
3. Протокола ARP:
 - запрос,
 - ответ.
4. Протокола ICMP:
 - пронаблюдать ошибку типа 3.
5. Протокола UDP:
 - попытка отправить udp пакет на несуществующий порт.
6. Протокола TCP:
 - установка соединения,
 - разрыв соединения,
 - попытка соединения на отсутствующий порт.

3 Конфигурация сети

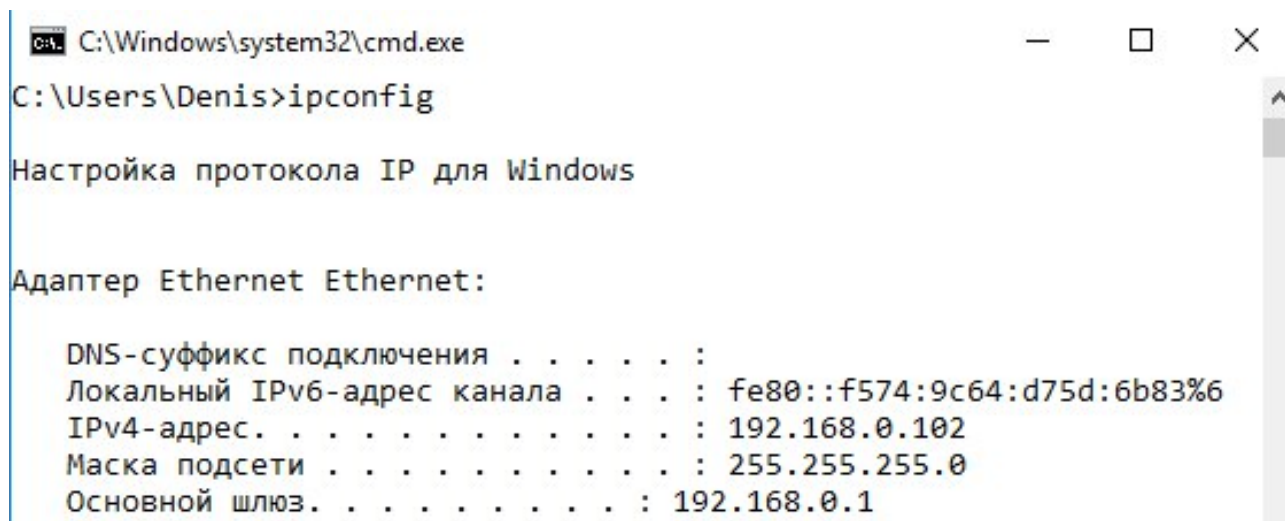
Опыты проводились используя два ПК, конфигурации которых представлены ниже. ПК находились в одной сети.



```
C:\Windows\system32\cmd.exe
Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . :
Локальный IPv6-адрес канала . . . . : fe80::ddf0:5191:d59a:901a%13
IPv4-адрес. . . . . : 192.168.0.104
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . : 192.168.0.1
```

Рис. 1: Конфигурация ПК 1



```
C:\Windows\system32\cmd.exe
C:\Users\Denis>ipconfig

Настройка протокола IP для Windows

Адаптер Ethernet Ethernet:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::f574:9c64:d75d:6b83%6
    IPv4-адрес. . . . . : 192.168.0.102
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 192.168.0.1
```

Рис. 2: Конфигурация ПК 2

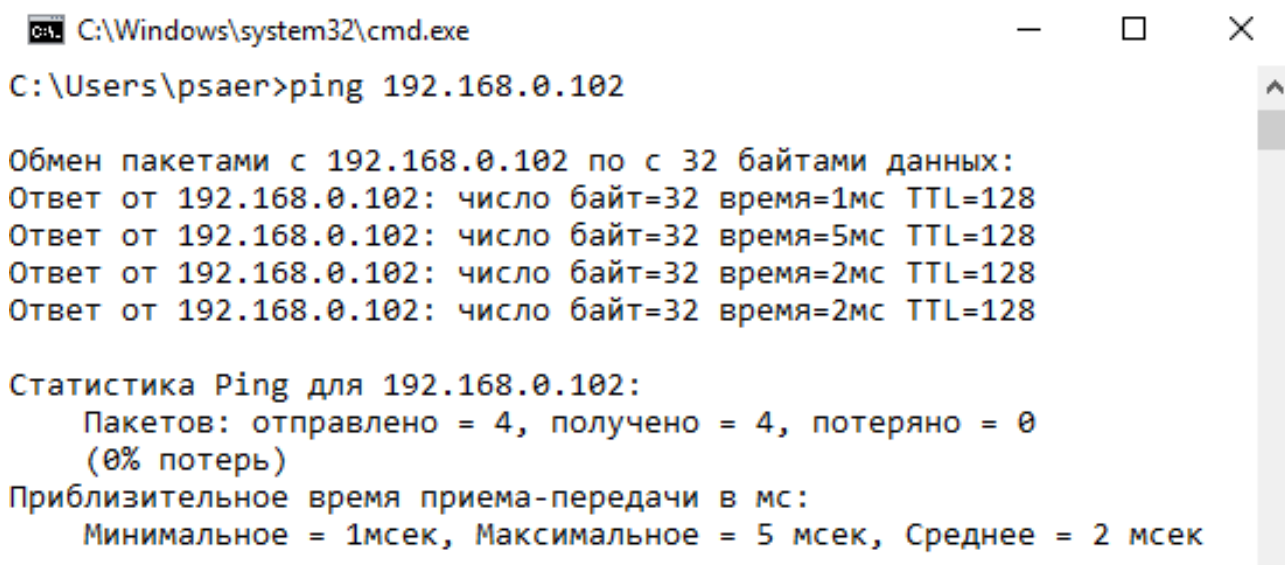
4 Ход работы

4.1 Утилита ping

Утилита Ping отправляет эхо-запрос ICMP, после чего, в случае успеха должен прийти симметричный эхо-ответ ICMP. Если пакет не пришел за некоторое TTL, то удаленный сервер считается недостижимым. По умолчанию производится четыре попытки.

4.1.1 Ping без фрагментации

Трафик утилиты Ping со стандартными параметрами (**bytes** = 32, **TTL** = 128):



```
C:\Windows\system32\cmd.exe
C:\Users\psaer>ping 192.168.0.102

Обмен пакетами с 192.168.0.102 по с 32 байтами данных:
Ответ от 192.168.0.102: число байт=32 время=1мс TTL=128
Ответ от 192.168.0.102: число байт=32 время=5мс TTL=128
Ответ от 192.168.0.102: число байт=32 время=2мс TTL=128
Ответ от 192.168.0.102: число байт=32 время=2мс TTL=128

Статистика Ping для 192.168.0.102:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 5 мсек, Среднее = 2 мсек
```

Рис. 3: Вызов утилиты в командной строке

No.	Time	Source	Destination	Protocol	Length	Info
→ 1	0.000000	192.168.0.104	192.168.0.102	ICMP	74	Echo (ping) request
← 2	0.001806	192.168.0.102	192.168.0.104	ICMP	74	Echo (ping) reply
3	1.009068	192.168.0.104	192.168.0.102	ICMP	74	Echo (ping) request
> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0 > Ethernet II, Src: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd), Dst: Giga-Byt_24:4a:24 (> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.102 > Internet Control Message Protocol Type: 8 (Echo (ping) request) Code: 0						
0000	94 de 80 24 4a 24 14 2d	27 49 6d bd 08 00 45 00	...\$J\$. - 'Im...E.			
0010	00 3c 31 f9 00 00 80 01	86 a9 c0 a8 00 68 c0 a8	.<1.....h..			
0020	00 66 08 00 4d 5a 00 01	00 01 61 62 63 64 65 66	.f.MZ.. ..abcdef			
0030	67 68 69 6a 6b 6c 6d 6e	6f 70 71 72 73 74 75 76	ghijklmn opqrstuv			
0040	77 61 62 63 64 65 66 67	68 69	wabcdefg hi			

Рис. 4: ICMP эхо-запрос

No.	Time	Source	Destination	Protocol	Length	Info
→ 1	0.000000	192.168.0.104	192.168.0.102	ICMP	74	Echo (ping) request
← 2	0.001806	192.168.0.102	192.168.0.104	ICMP	74	Echo (ping) reply
3	1.009068	192.168.0.104	192.168.0.102	ICMP	74	Echo (ping) request
> Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0 > Ethernet II, Src: Giga-Byt_24:4a:24 (94:de:80:24:4a:24), Dst: HonHaiPr_49:6d:bd (> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.104 > Internet Control Message Protocol Type: 0 (Echo (ping) reply) Code: 0						
0000	14 2d 27 49 6d bd 94 de	80 24 4a 24 08 00 45 00	.-'Im... . \$J\$..E.			
0010	00 3c 31 7e 00 00 80 01	87 24 c0 a8 00 66 c0 a8	.<1~.... . \$...f..			
0020	00 68 00 00 55 5a 00 01	00 01 61 62 63 64 65 66	.h.UZ.. ..abcdef			
0030	67 68 69 6a 6b 6c 6d 6e	6f 70 71 72 73 74 75 76	ghijklmn opqrstuv			
0040	77 61 62 63 64 65 66 67	68 69	wabcdefg hi			

Рис. 5: ICMP эхо-ответ

Пакеты были распознаны как ICMP с пометкой "Echo (ping) reply/request" что означает эхо запрос/ответ.

Тип сообщения равный 8 означает эхо-запрос, а тип 0 означает эхо-ответ.

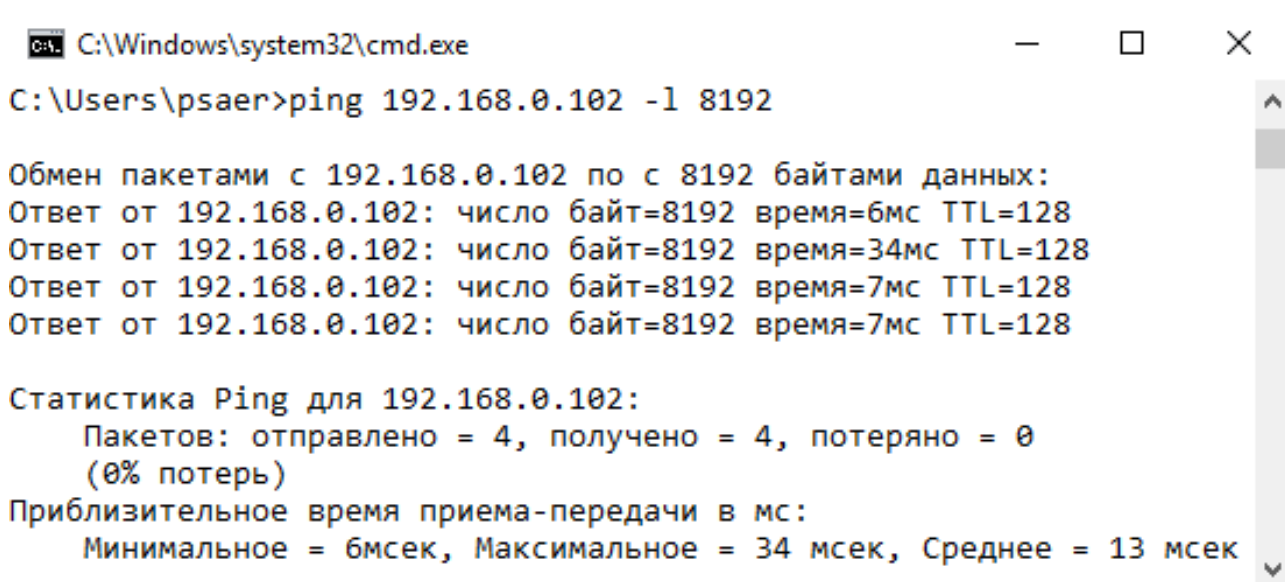
Графа Destination показывает IP адрес удаленного сервера, который мы пингуем, Source показывает IP адрес текущего компьютера.

В качестве передаваемой информации передаются коды символов A-W.

4.1.2 Ping с фрагментацией

Для фрагментации пакета необходимо указать его размер, превышающий MTU (maximum transmission unit) - максимальный размер полезного блока данных одного пакета, который может быть передан протоколом без фрагментации. Максимальный размер одного блока данных, который может быть передан без фрагментации составляет 1480 байт.

С помощью утилиты ping изменяем размер буфера отправки на 8192 байт.



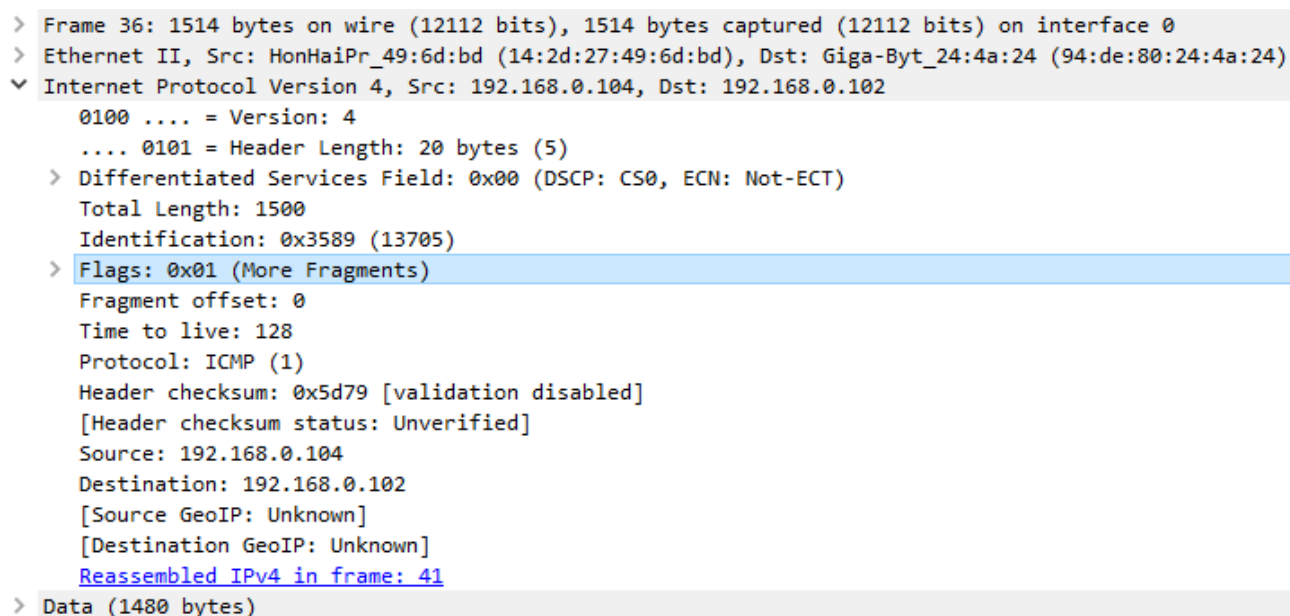
```
C:\Windows\system32\cmd.exe

C:\Users\psaer>ping 192.168.0.102 -l 8192

Обмен пакетами с 192.168.0.102 по с 8192 байтами данных:
Ответ от 192.168.0.102: число байт=8192 время=6мс TTL=128
Ответ от 192.168.0.102: число байт=8192 время=34мс TTL=128
Ответ от 192.168.0.102: число байт=8192 время=7мс TTL=128
Ответ от 192.168.0.102: число байт=8192 время=7мс TTL=128

Статистика Ping для 192.168.0.102:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 6мсек, Максимальное = 34 мсек, Среднее = 13 мсек
```

Рис. 6: Вызов утилиты в командной строке



```
> Frame 36: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd), Dst: Giga-Byt_24:4a:24 (94:de:80:24:4a:24)
▼ Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 1500
        Identification: 0x3589 (13705)
    > Flags: 0x01 (More Fragments)
        Fragment offset: 0
        Time to live: 128
        Protocol: ICMP (1)
        Header checksum: 0x5d79 [validation disabled]
        [Header checksum status: Unverified]
        Source: 192.168.0.104
        Destination: 192.168.0.102
        [Source GeoIP: Unknown]
        [Destination GeoIP: Unknown]
        Reassembled IPv4 in frame: 41
    > Data (1480 bytes)
```

Рис. 7: Первый фрагмент пакета ping-запроса

О фрагментированности пакета свидетельствуют флаги пакета IP (0x01 – имеются еще фрагменты). О том, что это первый пакет из фрагментированных, свидетельствует нулевое смещение фрагмента.

```

> Frame 37: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd), Dst: Giga-Byt_24:4a:24 (94:de:80:24:4a:24)
▼ Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x3589 (13705)
> Flags: 0x01 (More Fragments)
    Fragment offset: 1480
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x5cc0 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.104
    Destination: 192.168.0.102
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 41
> Data (1480 bytes)

```

Рис. 8: Второй фрагмент пакета ping-запроса

Второй пакет все так же имеет флаг в заголовке IP-пакета (0x01), свидетельствующий о наличии пакетов кроме данного. От первого пакета его отличает ненулевое смещение фрагмента.

```

> Frame 41: 834 bytes on wire (6672 bits), 834 bytes captured (6672 bits) on interface 0
> Ethernet II, Src: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd), Dst: Giga-Byt_24:4a:24 (94:de:80:24:4a:24)
▼ Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 820
    Identification: 0x3589 (13705)
> Flags: 0x00
    Fragment offset: 7400
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x7c84 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.104
    Destination: 192.168.0.102
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
> [6 IPv4 Fragments (8200 bytes): #36(1480), #37(1480), #38(1480), #39(1480), #40(1480), #41(800)]
▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4526 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 36 (0x0024)
    Sequence number (LE): 9216 (0x2400)
    [Response frame: 47]
> Data (8192 bytes)

```

Рис. 9: Последний фрагмент пакета ping-запроса

Пакет, содержащий последний фрагмент ping-запроса, уже не имеет флагов в заголовке

IP-пакета. При этом параметр «смещение фрагмента» ненулевой, а идентификатор совпадает с идентификаторами пакетов, отправленных ранее.

4.2 Утилита tracert

Пронаблюдаем трассировку маршрута пакетов до узла **kspt.icc.spbstu.ru** при помощи протокола ICMP и утилиты **tracert**.

```
C:\Windows\system32\cmd.exe
C:\Users\psaer>tracert kspt.icc.spbstu.ru

Трассировка маршрута к kspt.icc.spbstu.ru [91.151.191.13]
с максимальным числом прыжков 30:

 1      2 ms      1 ms      4 ms  lan-82-001.users.mns.ru [178.162.82.1]
 2      4 ms      2 ms      4 ms  df-1-142.users.mns.ru [80.70.224.142]
 3      5 ms      5 ms      5 ms  gw.mns.ru [80.70.239.254]
 4      4 ms      5 ms      5 ms  as5433.ix.dataix.ru [178.18.224.121]
 5      4 ms      4 ms      5 ms  gw-politech.nw.ru [91.151.178.42]
 6      4 ms      8 ms      4 ms  white.ftk.spbstu.ru [91.151.191.13]

Трассировка завершена.
```

Рис. 10: Результат трассировки маршрута в консоли

Первый пакет трассировки маршрута отправляется с TTL равным 1. Это значит, что на первом же маршрутизаторе пакет будет уничтожен и нам придет сообщение об ошибке.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.004983	178.162.82.1	192.168.0.104	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5	0.005552	192.168.0.104	91.151.191.13	ICMP	106	Echo (ping) request id=0x0001, seq=78/19968, ttl=1 (no response found!)
6	0.007434	178.162.82.1	192.168.0.104	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
7	1.025660	192.168.0.104	91.151.191.13	ICMP	106	Echo (ping) request id=0x0001, seq=79/20224, ttl=2 (no response found!)
8	1.028936	80.70.224.142	192.168.0.104	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

> Frame 6: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6), Dst: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd)
v Internet Protocol Version 4, Src: 178.162.82.1, Dst: 192.168.0.104
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
Total Length: 56
Identification: 0x271f (10015)
> Flags: 0x00
Fragment offset: 0
Time to live: 254
Protocol: ICMP (1)
Header checksum: 0xcf31 [validation disabled]
[Header checksum status: Unverified]
Source: 178.162.82.1
Destination: 192.168.0.104
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
v Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xf4ff [correct]
[Checksum Status: Good]
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 91.151.191.13
> Internet Control Message Protocol

Рис. 11: Ответ на первый пакет трассировки

В сообщении об ошибке указан тип ICMP-пакета – 11.0, что означает, что время жизни пакета истекло. Сообщение пришло от маршрутизатора сети, который имеет адрес 178.162.82.1.

6	0.007434	178.162.82.1	192.168.0.104	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
7	1.025660	192.168.0.104	91.151.191.13	ICMP	106	Echo (ping) request id=0x0001, seq=79/20224, ttl=2 (no response found!)
8	1.028936	80.70.224.142	192.168.0.104	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

>	Frame 7: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
>	Ethernet II, Src: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd), Dst: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6)
>	Internet Protocol Version 4, Src: 192.168.0.104, Dst: 91.151.191.13
>	0100 = Version: 4
> 0101 = Header Length: 20 bytes (5)
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
>	Total Length: 92
>	Identification: 0x5e05 (24069)
>	Flags: 0x00
>	Fragment offset: 0
>	Time to live: 2
>	Protocol: ICMP (1)
>	Header checksum: 0x7ee7 [validation disabled]
>	[Header checksum status: Unverified]
>	Source: 192.168.0.104
>	Destination: 91.151.191.13
>	[Source GeoIP: Unknown]
>	[Destination GeoIP: Unknown]
>	Internet Control Message Protocol
>	Type: 8 (Echo (ping) request)
>	Code: 0

Рис. 12: Второй пакет трассировки маршрута

Следующий пакет будет отправлен на тот же адрес, что и ранее, но параметр TTL будет установлен в 2, чтобы пройти маршрутизатор по адресу 178.162.82.1 и попасть в следующий пункт передачи.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.004983	178.162.82.1	192.168.0.104	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5	0.005552	192.168.0.104	91.151.191.13	ICMP	106	Echo (ping) request id=0x0001, seq=78/19968, ttl=1 (no response found!)
6	0.007434	178.162.82.1	192.168.0.104	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
7	1.025660	192.168.0.104	91.151.191.13	ICMP	106	Echo (ping) request id=0x0001, seq=79/20224, ttl=2 (no response found!)
8	1.028936	80.70.224.142	192.168.0.104	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

>	Frame 8: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
>	Ethernet II, Src: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6), Dst: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd)
>	Internet Protocol Version 4, Src: 80.70.224.142, Dst: 192.168.0.104
>	0100 = Version: 4
> 0101 = Header Length: 20 bytes (5)
>	Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
>	Total Length: 56
>	Identification: 0x9746 (38726)
>	Flags: 0x00
>	Fragment offset: 0
>	Time to live: 254
>	Protocol: ICMP (1)
>	Header checksum: 0x32d9 [validation disabled]
>	[Header checksum status: Unverified]
>	Source: 80.70.224.142
>	Destination: 192.168.0.104
>	[Source GeoIP: Unknown]
>	[Destination GeoIP: Unknown]
>	Internet Control Message Protocol
>	Type: 11 (Time-to-live exceeded)

Рис. 13: Ответ на второй пакет трассировки

В ответе на второй пакет трассировки маршрута в качестве отправителя сообщения об ошибке истечения жизни пакета указан адрес 80.70.224.142. Значит, это и есть следующий пункт передачи.

Аналогично продолжается трассировка маршрута дальше с постепенным инкрементом параметра TTL. Таким образом составляется примерный маршрут прохождения IP-пакета до узла с адресом **kspt.icc.spbstu.ru**.

4.3 Протокол ARP

Рассмотрим пару APR пакетов, которая демонстрирует работу протокола

No.	Time	Source	Destination	Protocol	Length	Info
39	23.5943...	D-Link_3e:a6:d6	HonHaiPr_49:6d:bd	ARP	42	Who has 192.168.0.104? Tell 192.168.0.1
40	23.5944...	HonHaiPr_49:6d:bd	D-Link_3e:a6:d6	ARP	42	192.168.0.104 is at 14:2d:27:49:6d:bd
41	24.2564...	fe80::ffff:ffff::...	ff02::2	ICMPv6	103	Router Solicitation

> Frame 39: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6), Dst: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd)
▼ Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6)
Sender IP address: 192.168.0.1
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.0.104

Рис. 14: ARP запрос

В пакете ARP-запроса указывается его тип (поле Opcode) – 0x1 для запроса и 0x2 для ответа. Указан целевой IP-адрес для которого запрашивается MAC-адрес, MAC-адрес цели при этом обнулен.

No.	Time	Source	Destination	Protocol	Length	Info
39	23.5943...	D-Link_3e:a6:d6	HonHaiPr_49:6d:bd	ARP	42	Who has 192.168.0.104? Tell 192.168.0.1
40	23.5944...	HonHaiPr_49:6d:bd	D-Link_3e:a6:d6	ARP	42	192.168.0.104 is at 14:2d:27:49:6d:bd
41	24.2564...	fe80::ffff:ffff::...	ff02::2	ICMPv6	103	Router Solicitation

> Frame 40: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd), Dst: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6)
▼ Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd)
Sender IP address: 192.168.0.104
Target MAC address: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6)
Target IP address: 192.168.0.1

Рис. 15: ARP ответ

В ответе возвращается результирующий MAC-адрес.

При попытке отправить ICMP эхо запрос на несуществующий адрес, ARP - запрос был широковещательным.

12	0.994381	D-Link_3e:a6:d6	Broadcast	ARP	42	Who has 192.168.0.156? Tell 192.168.0.1
13	1.916082	D-Link_3e:a6:d6	Broadcast	ARP	42	Who has 192.168.0.156? Tell 192.168.0.1
14	2.940127	D-Link_3e:a6:d6	Broadcast	ARP	42	Who has 192.168.0.156? Tell 192.168.0.1

> Frame 12: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
 > Ethernet II, Src: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 > Address Resolution Protocol (request)

Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: request (1)
 Sender MAC address: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6)
 Sender IP address: 192.168.0.1
 Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
 Target IP address: 192.168.0.156

Рис. 16: Широковещательный ARP-запрос

4.4 Протокол ICMP

Для того чтобы пронаблюдать ошибку типа 3.1 (целевой узел недостижим), отправим ping-запрос на адрес(192.168.0.156), которого не существует.

```

C:\Windows\system32\cmd.exe
C:\Users\psaer>ping 192.168.0.156

Обмен пакетами с 192.168.0.156 по с 32 байтами данных:
Ответ от 192.168.0.1: Заданный узел недоступен.
Ответ от 192.168.0.1: Заданный узел недоступен.
Ответ от 192.168.0.1: Заданный узел недоступен.
Ответ от 192.168.0.1: Заданный узел недоступен.

Статистика Ping для 192.168.0.156:
    Пакетов: отправлено = 4, получено = 0, потеряно = 4
    (0% потерь)
  
```

Рис. 17: Вызов утилиты в командной строке

В пакете можно наблюдать типичный ping-запрос (ICMP-пакет типа 8.0).

11	0.912540	192.168.0.104	192.168.0.156	ICMP	74	Echo (ping) request id=0x0001, seq=1
12	0.994381	D-Link_3e:a6:d6	Broadcast	ARP	42	Who has 192.168.0.156? Tell 192.168.0.1

> Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 > Ethernet II, Src: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd), Dst: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6)
 > Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.156
 > Internet Control Message Protocol

Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0x4cf4 [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence number (BE): 103 (0x0067)
 Sequence number (LE): 26368 (0x6700)

 > [No response seen]
 > Data (32 bytes)

Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
 [Length: 32]

Рис. 18: ICMP - эхо запрос

Ответом на указанный выше запрос будет ICMP-пакет типа 3.1, свидетельствующий об ошибке «целевой узел недостижим».

15	4.470359	192.168.0.1	192.168.0.104	ICMP	102 Destination unreachable (Host unreachable)
> Frame 15: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0 > Ethernet II, Src: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6), Dst: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd) > Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.104 > Internet Control Message Protocol					
Type: 3 (Destination unreachable) Code: 1 (Host unreachable) Checksum: 0xfcfe [correct] [Checksum Status: Good] Unused: 00000000					
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.156 > Internet Control Message Protocol					

Рис. 19: ICMP-ответ

17	4.477851	192.168.0.1	192.168.0.104	ICMP	102 Redirect (Redirect for host)
> Frame 17: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0 > Ethernet II, Src: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6), Dst: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd) > Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.104 > Internet Control Message Protocol					
Type: 5 (Redirect) Code: 1 (Redirect for host) Checksum: 0x39ba [correct] [Checksum Status: Good] Gateway address: 192.168.0.156					
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.156					

Рис. 20: Пакет перенаправления

4.5 Протокол UDP

Для отправки udp-пакета на несуществующий адрес, была написана соответствующая программа.

No.	Time	Source	Destination	Protocol	Length	Info
16	0.650855	64.233.164.188	192.168.0.104	TCP	66	5228 → 58968 [ACK] Seq=
17	1.563911	192.168.0.104	192.168.56.2	UDP	50	52913 → 8005 Len=8
18	2.062237	192.168.0.104	74.125.205.200	SSL	55	Continuation Data
> Frame 17: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface 0 > Ethernet II, Src: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd), Dst: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6) > Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.56.2 > User Datagram Protocol, Src Port: 52913, Dst Port: 8005						
Source Port: 52913 Destination Port: 8005 Length: 16 Checksum: 0xb77f [unverified] [Checksum Status: Unverified] [Stream index: 2]						
> Data (8 bytes) Data: 7465737444617461 [Length: 8]						
0000	f0 7d 68 3e a6 d6 14 2d 27 49 6d bd 08 00 45 00	.}h>...- 'Im...E.				
0010	00 24 37 eb 00 00 80 11 49 23 c0 a8 00 68 c0 a8	.\$7..... I#...h..				
0020	38 02 ce b1 1f 45 00 10 b7 7f 74 65 73 74 44 61	8....E.. ..testDa				
0030	74 61	ta				

Рис. 21: UDP - пакет

Чего и требовалось ожидать, UDP - пакет был отправлен на несуществующий адрес **192.168.56.2**, с портом **8005**, в качестве пересылаемых данных выступали 8 байт текста - **testData**.

4.6 Протокол TCP

Все последующие опыты будут выполнены при использовании двух ПК, находящихся в одной сети. Их сетевые параметры представлены в пункте **Конфигурация сети**. Были написаны программы tcp сервера и клиента. На одном из ПК будет запущен TCP - сервер, а на другой TCP - клиент.

4.6.1 Установка соединения

При установке соединения между клиентом и сервером, происходит передача трех пакетов. Клиент, посылает серверу сегмент с номером последовательности и флагом SYN.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.104	192.168.0.102	TCP	66	61064 → 8005 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
2	0.001815	192.168.0.102	192.168.0.104	TCP	66	8005 → 61064 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
3	0.001910	192.168.0.104	192.168.0.102	TCP	54	61064 → 8005 [ACK] Seq=1 Ack=1 Win=16384 Len=0

>	Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
>	Ethernet II, Src: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd), Dst: Giga-Byt_24:4a:24 (94:de:80:24:4a:24)
>	Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.102
>	Transmission Control Protocol, Src Port: 61064, Dst Port: 8005, Seq: 0, Len: 0
	Source Port: 61064
	Destination Port: 8005
	[Stream index: 0]
	[TCP Segment Len: 0]
	Sequence number: 0 (relative sequence number)
	Acknowledgment number: 0
	Header Length: 32 bytes
>	Flags: 0x002 (SYN)
	Window size value: 8192
	[Calculated window size: 8192]
	Checksum: 0x59d7 [unverified]
	[Checksum Status: Unverified]
	Urgent pointer: 0

Рис. 22: Первый пакет при установке TCP-соединения

В случае успеха сервер посылает клиенту сегмент с номером последовательности и флагами SYN и ACK, и переходит в состояние SYN-RECEIVED. В случае неудачи сервер посылает клиенту сегмент с флагом RST.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.104	192.168.0.102	TCP	66	61064 → 8005 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
2	0.001815	192.168.0.102	192.168.0.104	TCP	66	8005 → 61064 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
3	0.001910	192.168.0.104	192.168.0.102	TCP	54	61064 → 8005 [ACK] Seq=1 Ack=1 Win=16384 Len=0

>	Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
>	Ethernet II, Src: Giga-Byt_24:4a:24 (94:de:80:24:4a:24), Dst: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd)
>	Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.104
>	Transmission Control Protocol, Src Port: 8005, Dst Port: 61064, Seq: 0, Ack: 1, Len: 0
	Source Port: 8005
	Destination Port: 61064
	[Stream index: 0]
	[TCP Segment Len: 0]
	Sequence number: 0 (relative sequence number)
	Acknowledgment number: 1 (relative ack number)
	Header Length: 32 bytes
>	Flags: 0x012 (SYN, ACK)
	Window size value: 8192
	[Calculated window size: 8192]
	Checksum: 0x1bf5 [unverified]
	[Checksum Status: Unverified]
	Urgent pointer: 0
>	Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP)
>	[SEQ/ACK analysis]

Рис. 23: Второй пакет при установке TCP-соединения

Последний этап это отправка на сервер пакета с установленным флагом ACK, после чего соединение переходит в состояние ESTABLISHED.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.104	192.168.0.102	TCP	66	61064 → 8005 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
2	0.001815	192.168.0.102	192.168.0.104	TCP	66	8005 → 61064 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
3	0.001910	192.168.0.104	192.168.0.102	TCP	54	61064 → 8005 [ACK] Seq=1 Ack=1 Win=16384 Len=0

```

> Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd), Dst: Giga-Byt_24:4a:24 (94:de:80:24:4a:24)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.102
✓ Transmission Control Protocol, Src Port: 61064, Dst Port: 8005, Seq: 1, Ack: 1, Len: 0
  Source Port: 61064
  Destination Port: 8005
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number)
  Acknowledgment number: 1 (relative ack number)
  Header Length: 20 bytes
  > Flags: 0x010 (ACK)
  Window size value: 64
  [Calculated window size: 16384]
  [Window size scaling factor: 256]
  Checksum: 0x7c88 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  > [SEQ/ACK analysis]

```

Рис. 24: Третий пакет при установке TCP-соединения

4.6.2 Разрыв соединения

При разрыве соединения сервер отправляет клиенту пакет с установленным флагом RST.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.102	192.168.0.104	TCP	60	8005 → 61064 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2	2.247258	192.168.0.104	173.194.222.189	QUIC	65	Payload (Encrypted), PKN: 240, CID: 165440551945

```

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Giga-Byt_24:4a:24 (94:de:80:24:4a:24), Dst: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.104
✓ Transmission Control Protocol, Src Port: 8005, Dst Port: 61064, Seq: 1, Ack: 1, Len: 0
  Source Port: 8005
  Destination Port: 61064
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number)
  Acknowledgment number: 1 (relative ack number)
  Header Length: 20 bytes
  ✓ Flags: 0x014 (RST, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    ... 0... = Congestion Window Reduced (CWR): Not set
    .... 0... = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 = Acknowledgment: Set
    .... .... 0... = Push: Not set
  ✓ .... .... 1.. = Reset: Set
    > [Expert Info (Warning/Sequence): Connection reset (RST)]
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: .....A·R··]

```

Рис. 25: Пример пакета с флагом RST

Если соединение уже было установлено, то завершение соединения производится следующим образом:

- Посылка серверу от клиента флага FIN на завершение соединения.
- Сервер посылает клиенту флаги ответа ACK, FIN, что соединение закрыто.
- После получения этих флагов клиент закрывает соединение и в подтверждение отправляет серверу ACK, что соединение закрыто.

4.6.3 Попытка соединения на отсутствующий порт

При попытке подключения к отсутствующему порту, от адреса, к которому происходит подключение, приходят пакеты с флагами ACK и RST. После трех попыток соединения, написанная программа сообщает об ошибке.

No.	Time	Source	Destination	Protocol	Length	Info
3	1.181013	192.168.0.104	192.168.0.102	TCP	66	61095 → 8006 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
4	1.191041	192.168.0.102	192.168.0.104	TCP	60	8006 → 61095 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	1.702971	192.168.0.104	192.168.0.102	TCP	66	[TCP Spurious Retransmission] 61095 → 8006 [SYN]
6	1.704589	192.168.0.102	192.168.0.104	TCP	60	8006 → 61095 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	2.218602	192.168.0.104	192.168.0.102	TCP	62	[TCP Spurious Retransmission] 61095 → 8006 [SYN]
8	2.221428	192.168.0.102	192.168.0.104	TCP	60	8006 → 61095 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

> Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 > Ethernet II, Src: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd), Dst: Giga-Byt_24:4a:24 (94:de:80:24:4a:24)
 > Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.102
 ▼ Transmission Control Protocol, Src Port: 61095, Dst Port: 8006, Seq: 0, Len: 0

Source Port: 61095
 Destination Port: 8006
 [Stream index: 0]
 [TCP Segment Len: 0]
 Sequence number: 0 (relative sequence number)
 Acknowledgment number: 0
 Header Length: 32 bytes
 ▼ Flags: 0x002 (SYN)

000. = Reserved: Not set
 ...0 = Nonce: Not set
 0... = Congestion Window Reduced (CWR): Not set
0.. = ECN-Echo: Not set
0. = Urgent: Not set
0 = Acknowledgment: Not set
 0... = Push: Not set
0.. = Reset: Not set
 ▼1. = Syn: Set

Рис. 26: Попытка tcp - соединения на 192.168.0.104:8006

```

C:\Windows\system32\cmd.exe
C:\study\s08\Защита информации\lab\task_2\tex\Listings>a.exe
Socket created
Connect failed. Error

C:\study\s08\Защита информации\lab\task_2\tex\Listings>_

```

Рис. 27: Окно консоли при попытке соединения

5 Вывод

В ходе работы был исследован сетевой трафик утилит ping и tracert а также протоколов ICMP, ARP, TCP и UDP.

При выполнении работы были рассмотрены различные ситуации, возникающие во время функционирования сети, такие как:

- Работа ICMP-протокола при:
 - отправке фрагментированного ping'a,
 - возникновение ошибки 3.1 (Destination host unreachable),
 - трассировка маршрута.
- работа протокола TCP при:
 - установке соединения,
 - разрыве соединения,
 - попытке соединения на отсутствующий порт.

Для вышеизложенных ситуаций, использование какой-либо программы по анализу сетевого трафика, позволяет более подробно рассмотреть происходящие при этом события.