

НИУ ИТМО
Факультет программной инженерии и компьютерных технологий

Отчет по лабораторной работе №4
по дисциплине Компьютерные сети

Студент группы № Р33151
Преподаватель

Шипулин Павел Андреевич
Тропченко Андрей Александрович

Санкт-Петербург
2024

ЭТАПЫ И ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Этап 1. Анализ трафика утилиты ping

Необходимо отследить и проанализировать трафик, создаваемый утилитой ping, запустив её следующим образом из командной строки:

- «ping -l размер_пакета адрес_сайта_по_варианту».
- Например, «ping -l 2000 wireshark.org» (без кавычек).

В качестве «размера_пакета» необходимо поочерёдно использовать различные значения от 100 до 10000, самостоятельно выбрав шаг изменения. По результатам анализа собранной трассы, необходимо ответить на следующие вопросы и выполнить указанные задания.

```
C:\Users\User>ping -l 1472 shipulinpa.temp.swtest.ru

Обмен пакетами с shipulinpa.temp.swtest.ru [77.222.40.238] с 1472 байтами данных:
Ответ от 77.222.40.238: число байт=1472 время=4мс TTL=59
Ответ от 77.222.40.238: число байт=1472 время=4мс TTL=59
Ответ от 77.222.40.238: число байт=1472 время=3мс TTL=59
Ответ от 77.222.40.238: число байт=1472 время=241мс TTL=59

Статистика Ping для 77.222.40.238:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 3мсек, Максимальное = 241 мсек, Среднее = 63 мсек

C:\Users\User>ping -l 1473 shipulinpa.temp.swtest.ru

Обмен пакетами с shipulinpa.temp.swtest.ru [77.222.40.238] с 1473 байтами данных:
Ответ от 77.222.40.238: число байт=1473 время=3мс TTL=59
Ответ от 77.222.40.238: число байт=1473 время=3мс TTL=59
Ответ от 77.222.40.238: число байт=1473 время=5мс TTL=59
Ответ от 77.222.40.238: число байт=1473 время=5мс TTL=59

Статистика Ping для 77.222.40.238:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 3мсек, Максимальное = 5 мсек, Среднее = 4 мсек

C:\Users\User>
```

Файл

Редактирование

Просмотр

Запуск

Захват

Анализ

Статистика

Телефония

Беспроводной

Инструменты

Помощь

ip.dst == 77.222.40.238

1. Имеет ли место фрагментация исходного пакета, какое поле на это указывает?

Да. Поле More Fragments = 1.

2. Какая информация указывает, является ли фрагмент пакета последним или промежуточным?

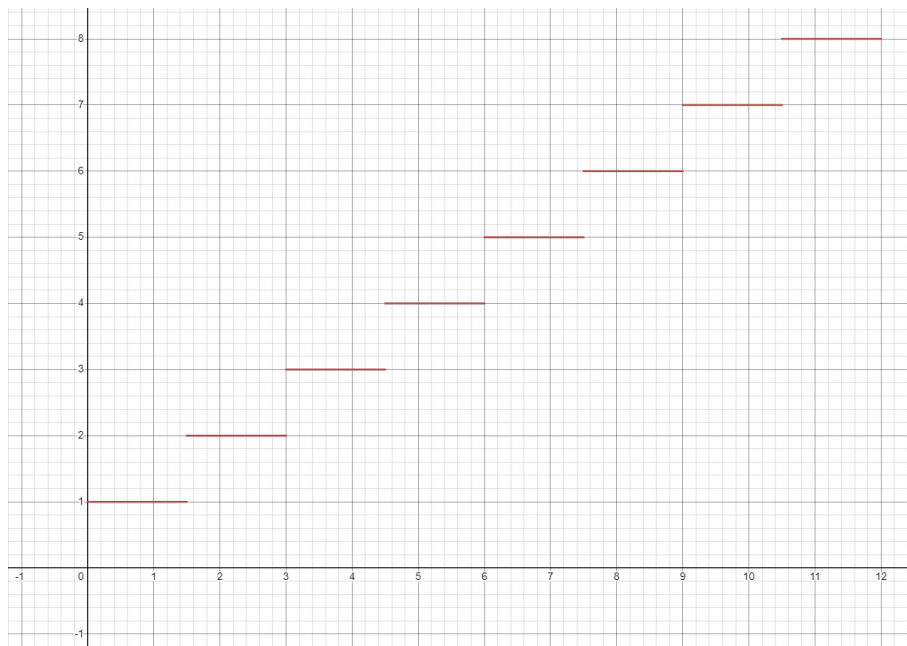
Если поле More Fragments = 0, то пакет является последним.

3. Чему равно количество фрагментов при передаче ping-пакетов?

Зависит от количества передаваемой информации, которая будет разбита на пакеты, у которых есть максимальный размер поля данных, равный 1472 байт (получено путём опыта).

$$\text{Количество пакетов} = \frac{\text{Весь объем данных}}{\text{максимальный объем данных пакета}}$$

4. Построить график, в котором на оси абсцисс находится размер пакета (килобайт), а по оси ординат – количество фрагментов, на которое был разделён каждый ping-пакет.



5. Как изменить поле TTL с помощью утилиты ping?

`ping -i <число>`

```
Приблизительное время приема-передачи в мс:
  Минимальное = 3мсек, Максимальное = 241 мсек, Среднее = 63 мсек

C:\Users\User>ping -l 1473 shipulinpa.temp.swtest.ru

Обмен пакетами с shipulinpa.temp.swtest.ru [77.222.40.238] с 1473 байтами данных:
Ответ от 77.222.40.238: число байт=1473 время=3мс TTL=59
Ответ от 77.222.40.238: число байт=1473 время=3мс TTL=59
Ответ от 77.222.40.238: число байт=1473 время=5мс TTL=59
Ответ от 77.222.40.238: число байт=1473 время=5мс TTL=59

Статистика Ping для 77.222.40.238:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потерь)
Приблизительное время приема-передачи в мс:
  Минимальное = 3мсек, Максимальное = 5 мсек, Среднее = 4 мсек

C:\Users\User>ping -l 100 -i 1 shipulinpa.temp.swtest.ru

Обмен пакетами с shipulinpa.temp.swtest.ru [77.222.40.238] с 100 байтами данных:
Ответ от 172.28.16.1: Превышен срок жизни (TTL) при передаче пакета.
Ответ от 172.28.16.1: Превышен срок жизни (TTL) при передаче пакета.
Ответ от 172.28.16.1: Превышен срок жизни (TTL) при передаче пакета.
Ответ от 172.28.16.1: Превышен срок жизни (TTL) при передаче пакета.

Статистика Ping для 77.222.40.238:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потерь)

C:\Users\User>
```

6. Что содержится в поле данных ping-пакета?

Байты передаваемой информации. При использовании ping – это будут последовательные символы английского алфавита и прочие символы кодировки.

Этап 2. Анализ трафика утилиты *tracert* (*tracert*)

Необходимо отследить и проанализировать трафик, создаваемый утилитой *tracert* (или *tracert* в Linux), запустив её следующим образом из командной строки:

- «*tracert -d адрес_сайта_по_варианту*»
- Например, *tracert wireshark.org*.

По результатам анализа собранной трассы, ответьте на следующие вопросы.

```
C:\Users\User>tracert -d shipulinpa.temp.swtest.ru

Трассировка маршрута к shipulinpa.temp.swtest.ru [77.222.40.238]
с максимальным числом прыжков 30:

  1    1 ms    1 ms    1 ms  172.28.16.1
  2    1 ms    2 ms    2 ms  77.234.199.66
  3    3 ms    3 ms    3 ms  87.248.228.102
  4    4 ms    3 ms    5 ms  185.1.152.93
  5    *      *      *      Превышен интервал ожидания для запроса.
  6    2 ms    2 ms    2 ms  77.222.40.238

Трассировка завершена.

C:\Users\User>tracert -d shipulinpa.temp.swtest.ru

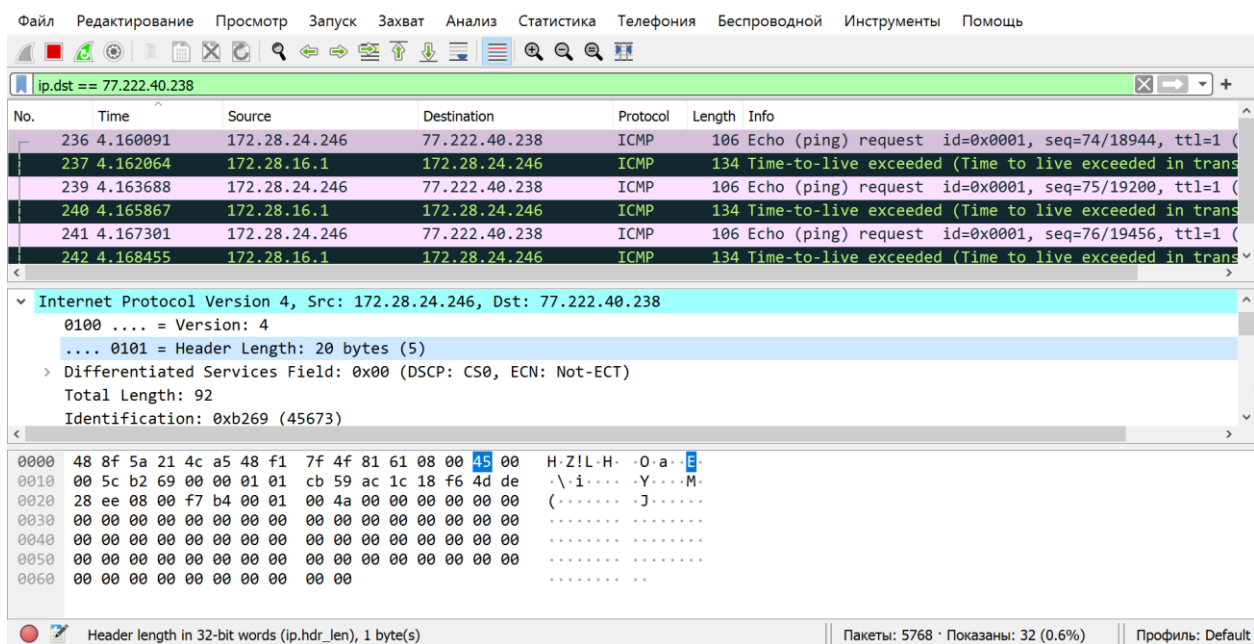
Трассировка маршрута к shipulinpa.temp.swtest.ru [77.222.40.238]
с максимальным числом прыжков 30:

  1    2 ms    2 ms    1 ms  172.28.16.1
  2    2 ms    3 ms    2 ms  77.234.199.66
  3    3 ms    2 ms    2 ms  87.248.228.102
  4    8 ms    4 ms    6 ms  185.1.152.93
  5    *      4 ms    *      31.177.85.165
  6    3 ms    2 ms    4 ms  77.222.40.238

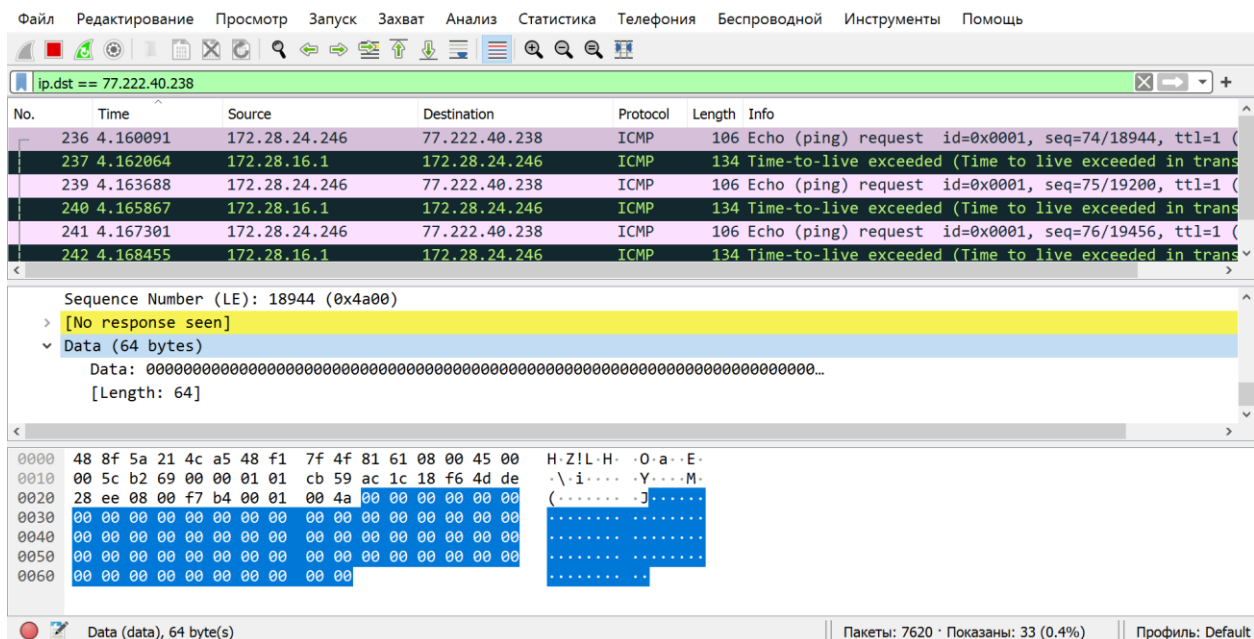
Трассировка завершена.

C:\Users\User>
```

1. Сколько байт содержится в заголовке IP? Сколько байт содержится в поле данных?



20 байт для заголовка.



64 байт для поля данных.

2. Как и почему изменяется поле TTL в следующих друг за другом ICMP пакетах tracer? Для ответа на этот вопрос нужно проследить изменение TTL при передаче по маршруту, состоящему из более чем двух хопов.

Команда увеличивает TTL на 1 пока не будет получен ответ от следующего узла в маршруте.

3. Чем отличаются ICMP-пакеты, генерируемые утилитой tracer, от ICMP пакетов, генерируемых утилитой ping (см. предыдущее задание).

Поле данных пакетов ICMP заполнено нулевыми байтами.

4. Чем отличаются полученные пакеты «ICMP reply» от «ICMP error» и зачем нужны оба этих типа ответов?

Reply – ответ от узла. Error – произошла ошибка, например истекло время TTL.

5. Что изменится в работе tracert, если убрать ключ «-d»? Какой дополнительный трафик при этом будет генерироваться?

```
C:\Users\User>tracert -d shipulinpa.temp.swtest.ru

Трассировка маршрута к shipulinpa.temp.swtest.ru [77.222.40.238]
с максимальным числом прыжков 30:

  1    2 ms    2 ms    1 ms  172.28.16.1
  2    2 ms    3 ms    2 ms  77.234.199.66
  3    3 ms    2 ms    2 ms  87.248.228.102
  4    8 ms    4 ms    6 ms  185.1.152.93
  5    *      4 ms    *    31.177.85.165
  6    3 ms    2 ms    4 ms  77.222.40.238

Трассировка завершена.

C:\Users\User>tracert shipulinpa.temp.swtest.ru

Трассировка маршрута к shipulinpa.temp.swtest.ru [77.222.40.238]
с максимальным числом прыжков 30:

  1    4 ms    2 ms    3 ms  172.28.16.1
  2    4 ms    4 ms    3 ms  77.234.199.66
  3    5 ms    4 ms    5 ms  87.248.228.102.pool.sknt.ru [87.248.228.102]
  4    6 ms    8 ms   11 ms  spaceweb.rucenter.spb.piter-ix.net [185.1.152.93]
  5   10 ms    *      *    spb-sdn-gw1.net.p8.ru [31.177.85.165]
  6    6 ms    7 ms    8 ms  fvh1.sweb.ru [77.222.40.238]

Трассировка завершена.

C:\Users\User>
```

Будут отображаться домены.

Этап 3. Анализ HTTP-трафика

Необходимо отследить и проанализировать HTTP-трафик, создаваемый браузером при посещении Интернет-сайта, заданного по варианту. В списке захваченных пакетов необходимо проанализировать следующую пару HTTP сообщений (запрос-ответ):

- GET-сообщение от клиента (браузера);
- ответ сервера.

Для этого в поле с детальной информацией о пакете нужно развернуть строку «HTTP». Затем необходимо обновить страницу в браузере так, чтобы вместо «HTTP GET» был сгенерирован «HTTP CONDITIONAL GET» (так называемый «условный GET»). Условные запросы GET содержат поля

IfModified-Since, If-Match, If-Range и подобные, которые позволяют при повторном запросе не передавать редко изменяемые данные. В ответ на условный GET тело запрашиваемого ресурса передается только в том случае, если этот ресурс изменялся после даты «If-Modified-Since». Если ресурс не изменялся, сервер вернет код статуса «304 Not Modified».

По результатам анализа собранной трассы покажите, каким образом протокол HTTP передавал содержимое страницы при первичном посещении страницы и при вторичном запросе-обновлении от браузера (т. е. при различных видах GET-запросов).

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.dst == 77.222.40.238

No.	Time	Source	Destination	Protocol	Length	Info
16793	210.850409	172.28.24.246	77.222.40.238	TCP	66	50943 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
16795	210.853130	172.28.24.246	77.222.40.238	TCP	54	50943 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
16796	210.853317	172.28.24.246	77.222.40.238	HTTP	494	GET / HTTP/1.1
16804	210.911950	172.28.24.246	77.222.40.238	TCP	54	50943 → 80 [ACK] Seq=441 Ack=408 Win=130816 Len=0
17292	220.884317	172.28.24.246	77.222.40.238	TCP	54	50943 → 80 [ACK] Seq=441 Ack=409 Win=130816 Len=0
19956	265.888293	172.28.24.246	77.222.40.238	TCP	55	[TCP Keep-Alive] 50943 → 80 [ACK] Seq=440 Ack=409 Win=

Frame 16796: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits) on interface \Device\NPF_{B758C04E-45AA-4E68-80D0-3EDF}

Interface id: 0 (\Device\NPF_{B758C04E-45AA-4E68-80D0-3EDF99F7EFF})

Encapsulation type: Ethernet (1)

Arrival Time: May 24, 2024 13:06:51.464753000 RTZ 2 (зима)

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1716545211.464753000 seconds

0020 28 ee c6 ff 00 50 37 1c c1 d6 fb 58 c2 87 50 18 (...P7...X..P..

0030 02 01 d0 46 00 00 47 45 54 20 2f 20 48 54 54 50 ...F...GE T / HTTP

0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 73 68 69 70 /1.1..Host: ship

0050 75 6c 69 6e 70 61 2e 74 65 6d 70 2e 73 77 74 65 ulinpa.t emp.swte

0060 73 74 2e 72 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f st.ru..C onnectio

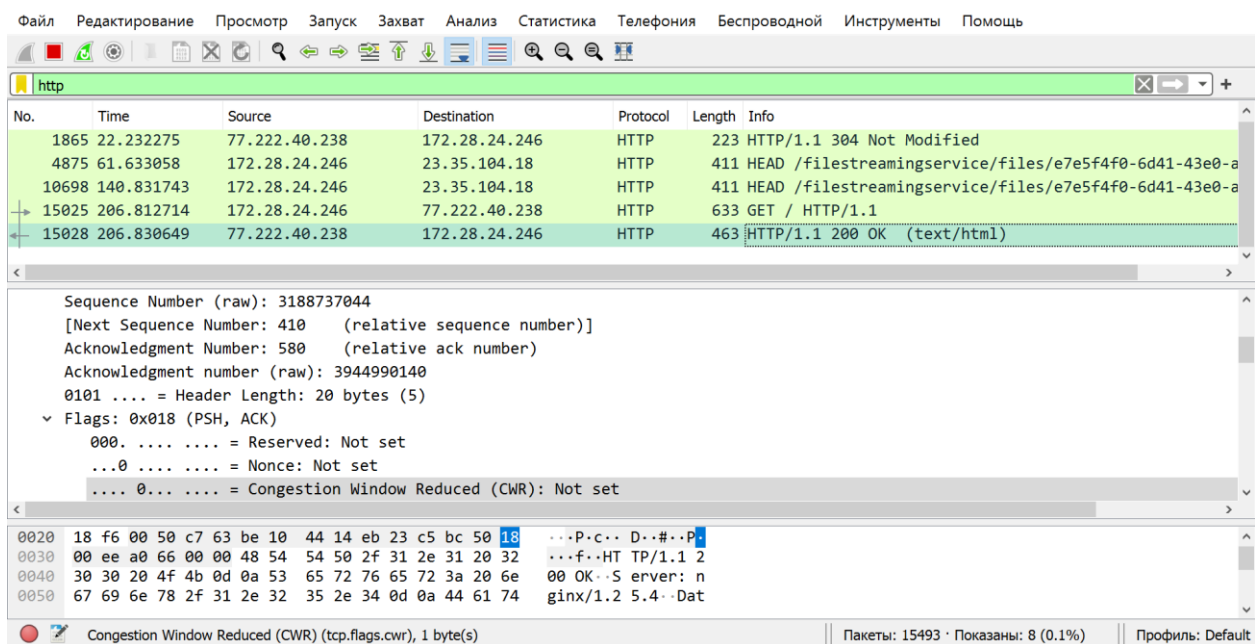
0070 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n: keep-alive..J

0080 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d pgrade-I nsecure-

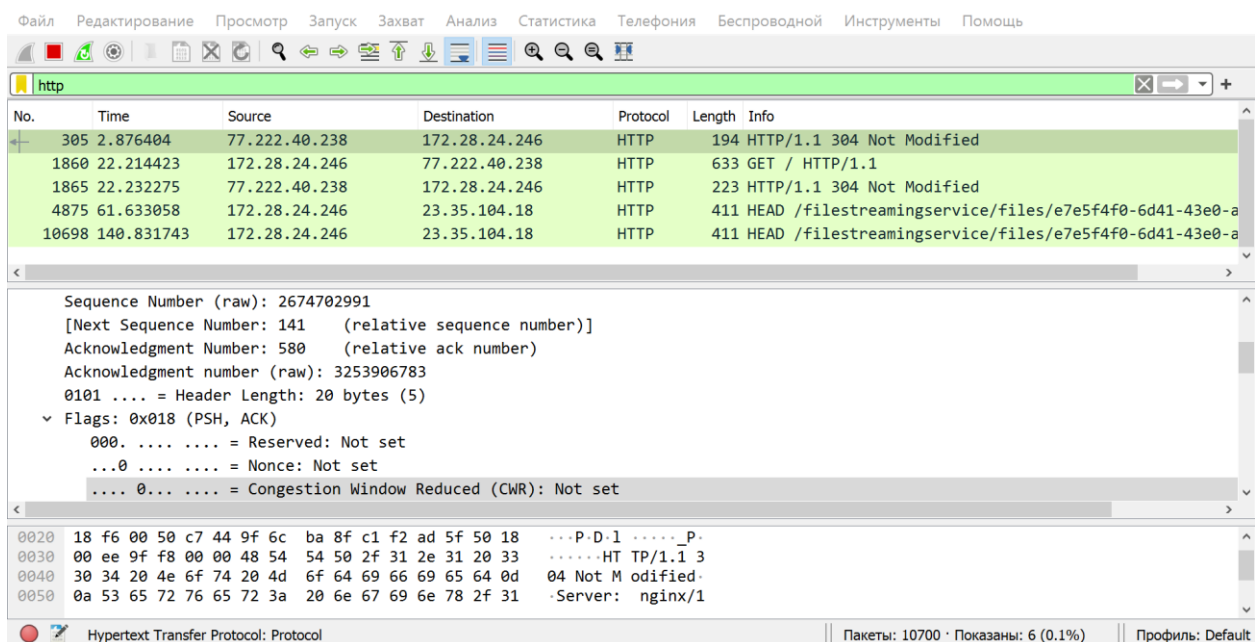
0090 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 Requests : 1..Use

This frame has some of the TCP analysis shown (tcp.analysis) | Пакеты: 28851 · Показаны: 7 (0.0%) | 24 мая 2024 г. пятница default

Сначала устанавливается TCP соединение, затем появляется ответ на GET запрос.



При обновлении содержимого страницы и её запросе – снова получаем HTTP OK с данными HTML.



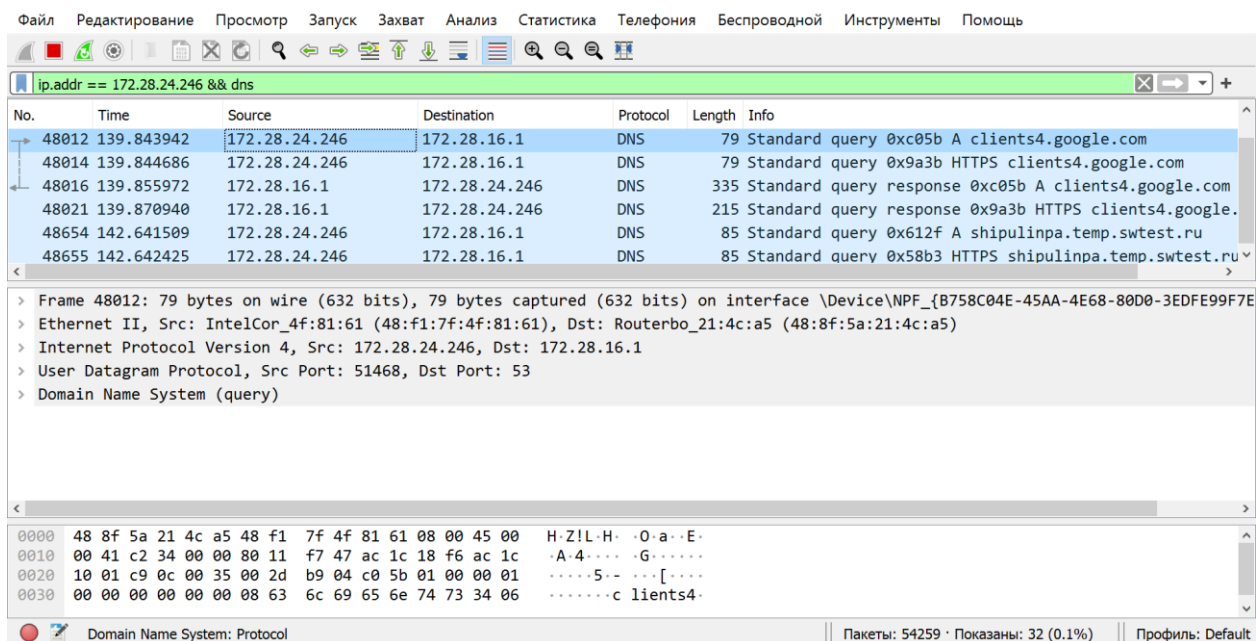
При повторном запросе страницы которая не обновлялась – компьютер получает “Not Modified”.

Этап 4. Анализ DNS-трафика

Необходимо отследить и проанализировать трафик протокола DNS, сгенерированный в результате выполнения следующих действий:

- настроить Wireshark-фильтр: «ip.addr == ваш_IP_адрес»;

- очистить кэш DNS с помощью команды `ipconfig /flushdns`
- очистить кэш браузера;
- зайти на Интернет-сайт, заданный по варианту.



По результатам анализа собранной трассы, ответьте на следующие вопросы.

1. Почему адрес, на который отправлен DNS-запрос, не совпадает с адресом посещаемого сайта?

Потому что компьютер не имеет достаточно информации про необходимый ресурс, и чтобы узнать о нём – обращается к маршрутизатору.

2. Какие бывают типы DNS-запросов?

- Прямой – получить адрес по имени
- Обратный – получить имя по адресу
- Итеративный – ??
- Рекурсивный – выполняется DNS сервером, чтобы найти домен.

3. В какой ситуации нужно выполнять независимые DNS-запросы для получения содержащихся на сайте изображений?

Если эти изображения хранятся на другом ресурсе.

Этап 5. Анализ ARP-трафика

Необходимо отследить и проанализировать трафик протокола ARP, сгенерированный в результате выполнения следующих действий:

- очистить ARP-таблицу командой «netsh interface ip delete arpccache» (проверить очистилась ли таблица можно с помощью команды команды «arp -a», выводящей таблицу на экран);
- очистить кэш браузера;
- зайти на Интернет-сайт, заданный по варианту.

По результатам анализа собранной трассы, ответьте на следующие вопросы.

```
адрес в Интернете    Физический адрес    Тип
172.28.16.1          48-8f-5a-21-4c-a5    динамический
224.0.0.2            01-00-5e-00-00-02    статический
224.0.0.22           01-00-5e-00-00-16    статический
224.0.0.250          01-00-5e-00-00-fa    статический
255.255.255.255      ff-ff-ff-ff-ff-ff    статический

C:\Users\User>arp -a

Интерфейс: 172.28.24.246 --- 0xd
адрес в Интернете    Физический адрес    Тип
172.28.16.1          48-8f-5a-21-4c-a5    динамический
224.0.0.2            01-00-5e-00-00-02    статический
224.0.0.22           01-00-5e-00-00-16    статический
224.0.0.250          01-00-5e-00-00-fa    статический
255.255.255.255      ff-ff-ff-ff-ff-ff    статический

C:\Users\User>netsh interface ip delete arpccache
OK.

C:\Users\User>arp -a

Интерфейс: 172.28.24.246 --- 0xd
адрес в Интернете    Физический адрес    Тип
172.28.16.1          48-8f-5a-21-4c-a5    динамический
224.0.0.22           01-00-5e-00-00-16    статический
255.255.255.255      ff-ff-ff-ff-ff-ff    статический

C:\Users\User>
```

Файл

Редактирование

Просмотр

Запуск

Захват

Анализ

Статистика

Телефония

Беспроводной

Инструменты

Помощь

arp

No.	Time	Source	Destination	Protocol	Length	Info
46907	149.285923	IntelCor_6d:a9:b6	IntelCor_4f:81:61	ARP	56	Who has 172.28.30.53? Tell 172.28.30.155
46908	149.286746	Routerbo_21:4c:a5	IntelCor_4f:81:61	ARP	56	Who has 172.28.19.201? Tell 172.28.16.1
46912	149.291584	Apple_51:7b:e7	IntelCor_4f:81:61	ARP	56	Who has 172.28.22.53? (ARP Probe)
46928	149.316558	Apple_8a:a1:9d	IntelCor_4f:81:61	ARP	56	Who has 172.28.30.216? Tell 172.28.19.92
46940	149.338835	Apple_7b:03:91	IntelCor_4f:81:61	ARP	56	Who has 172.28.30.216? Tell 172.28.31.156
46951	149.356498	Routerbo_21:4c:a5	IntelCor_4f:81:61	ARP	56	Who has 172.28.20.177? Tell 172.28.16.1
46957	149.362408	IntelCor_f1:86:c8	IntelCor_4f:81:61	ARP	56	Who has 172.28.19.201? Tell 172.28.20.213
46962	149.364967	IntelCor_38:ff:c2	IntelCor_4f:81:61	ARP	56	Who has 172.28.22.55? (ARP Probe)
46965	149.366645	Routerbo_21:4c:a5	IntelCor_4f:81:61	ARP	56	Who has 172.28.19.87? Tell 172.28.16.1
46970	149.370244	IntelCor_fc:14:58	IntelCor_4f:81:61	ARP	56	Who has 192.168.0.1? Tell 172.28.26.203
46980	149.386100	Routerbo_21:4c:a5	IntelCor_4f:81:61	ARP	56	Who has 172.28.20.145? Tell 172.28.16.1
46981	149.388899	Routerbo_21:4c:a5	IntelCor_4f:81:61	ARP	56	Who has 172.28.23.132? Tell 172.28.16.1

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

0000

48 f1 7f 4f 81 61 48 8f 5a 21 4c a5 08 06 00 01

H...aH. Z!L....

0010

08 00 06 04 00 01 48 8f 5a 21 4c a5 ac 1c 10 01

.....H. Z!L....

0020

00 00 00 00 00 00 ac 1c 14 b6 00 00 00 00 00 00

.....4.

0030

00 00 00 00 00 00 00 00

.....

Target IP address (arp.dst.proto_ipv4), 4 byte(s)

Пакеты: 47318 · Показаны: 7010 (14.8%)

Профиль: Default

1. Какие MAC-адреса присутствуют в захваченных пакетах ARP протокола? Что означают эти адреса? Какие устройства они идентифицируют?

Адрес отправителя (source) – маршрутизатор.

Адрес получателя – компьютер, который делал запрос.

2. Какие MAC-адреса присутствуют в захваченных HTTP-пакетах и что означают эти адреса? Что означают эти адреса? Какие устройства они идентифицируют?

Получатель ответа на GET запрос – мой компьютер.

Отправитель – маршрутизатор.

3. Для чего ARP-запрос содержит IP-адрес источника?

Чтобы те компьютеры, которые получают запрос могли сделать запись в ARP таблицу и не опрашивать снова.

Этап 6. Анализ трафика утилиты nslookup

Это задание является необязательным, его необходимо выполнить только для желающих получить оценку «хорошо» или «отлично». Необходимо отследить и проанализировать трафик протокола DNS, сгенерированный в результате выполнения следующих действий:

1. Настроить Wireshark-фильтр: «ip.addr == ваш_IP_адрес».

2. Запустить в командной строке команду «nslookup адрес_сайта_по_варианту».
3. Дождаться отправки трёх DNS-запросов и трёх DNS-ответов (в работе нужно использовать только последние из них, т.к. первые два набора запросов/ответов специфичны для nslookup и не генерируются другими сетевыми приложениями).
4. Повторить предыдущие два шага, используя команду: «nslookup -type=NS имя_сайта_по_варианту».

По результатам анализа собранной трассы, ответьте на следующие вопросы.

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.addr == 172.28.24.246 && dns

No.	Time	Source	Destination	Protocol	Length	Info
1246	3.286998	172.28.24.246	172.28.16.1	DNS	84	Standard query 0x0001 PTR 1.16.28.172.in-addr.arpa
1317	3.460834	172.28.16.1	172.28.24.246	DNS	84	Standard query response 0x0001 No such name PTR 1.16.28.172.in-addr.arpa
1318	3.466469	172.28.24.246	172.28.16.1	DNS	85	Standard query 0x0002 A shipulinpa.temp.swtest.ru
1528	3.940383	172.28.16.1	172.28.24.246	DNS	273	Standard query response 0x0002 A shipulinpa.temp.swtest.ru
1531	3.950431	172.28.24.246	172.28.16.1	DNS	85	Standard query 0x0003 AAAA shipulinpa.temp.swtest.ru
1734	4.340573	172.28.16.1	172.28.24.246	DNS	257	Standard query response 0x0003 AAAA shipulinpa.temp.swtest.ru
12660	34.819378	172.28.24.246	172.28.16.1	DNS	83	Standard query 0xddf9 A ctldl.windowsupdate.com
12675	34.861644	172.28.16.1	172.28.24.246	DNS	760	Standard query response 0xddf9 A ctldl.windowsupdate.com

> Frame 1246: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{B758C04E-45AA-4E68-80D0-3EDFE99F7...}

> Ethernet II, Src: IntelCor_4f:81:61 (48:f1:7f:4f:81:61), Dst: Routerbo_21:4c:a5 (48:8f:5a:21:4c:a5)

```

0000  48 8f 5a 21 4c a5 48 f1 7f 4f 81 61 08 00 45 00  H.Z!L.H. .O.a..E.
0010  00 46 c2 ba 00 00 00 11 f6 bc ac 1c 18 f6 ac 1c  .F.....
0020  10 01 d9 1a 00 35 00 32 ea bc 00 01 01 00 00 01  ...;5.2...
0030  00 00 00 00 00 00 01 31 02 31 36 02 32 38 03 31  ....1.16.28.1

```

Беспроводная сеть: <live capture in progress> | Пакеты: 18949 · Показаны: 8 (0.0%) | Профиль: Default

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.addr == 172.28.24.246 && dns

No.	Time	Source	Destination	Protocol	Length	Info
12660	34.819378	172.28.24.246	172.28.16.1	DNS	83	Standard query 0xddf9 A ctldl.windowsupdate.com
12675	34.861644	172.28.16.1	172.28.24.246	DNS	760	Standard query response 0xddf9 A ctldl.windowsupdate.com
29709	86.878866	172.28.24.246	172.28.16.1	DNS	84	Standard query 0x0001 PTR 1.16.28.172.in-addr.arpa
29721	86.904930	172.28.16.1	172.28.24.246	DNS	84	Standard query response 0x0001 No such name PTR 1.16.28.172.in-addr.arpa
29725	86.909548	172.28.24.246	172.28.16.1	DNS	85	Standard query 0x0002 NS shipulinpa.temp.swtest.ru
29777	87.016266	172.28.16.1	172.28.24.246	DNS	257	Standard query response 0x0002 NS shipulinpa.temp.swtest.ru
47900	138.053062	172.28.24.246	172.28.16.1	DNS	96	Standard query 0x1599 A functional.events.data.microsoft.com
47901	138.053661	172.28.24.246	172.28.16.1	DNS	96	Standard query 0x91a6 HTTPS functional.events.data.microsoft.com
47933	138.146136	172.28.16.1	172.28.24.246	DNS	294	Standard query response 0x91a6 HTTPS functional.events.data.microsoft.com
47936	138.147681	172.28.16.1	172.28.24.246	DNS	418	Standard query response 0x1599 A functional.events.data.microsoft.com
49168	142.355041	172.28.24.246	172.28.16.1	DNS	92	Standard query 0xab24 A mobile.events.data.microsoft.com
49173	142.367276	172.28.16.1	172.28.24.246	DNS	408	Standard query response 0xab24 A mobile.events.data.microsoft.com

> Frame 29709: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{B758C04E-45AA-4E68-80D0-3EDFE99F7...}

> Ethernet II, Src: IntelCor_4f:81:61 (48:f1:7f:4f:81:61), Dst: Routerbo_21:4c:a5 (48:8f:5a:21:4c:a5)

```

0000  48 8f 5a 21 4c a5 48 f1 7f 4f 81 61 08 00 45 00  H.Z!L.H. .O.a..E.
0010  00 46 c2 be 00 00 00 11 f6 b8 ac 1c 18 f6 ac 1c  .F.....
0020  10 01 de 3b 00 35 00 32 e5 9b 00 01 01 00 00 01  ...;5.2...
0030  00 00 00 00 00 00 01 31 02 31 36 02 32 38 03 31  ....1.16.28.1

```

Беспроводная сеть: <live capture in progress> | Пакеты: 59405 · Показаны: 18 (0.0%) | Профиль: Default

```

Не заслуживающий доверия ответ:
   : shipulinpa.temp.swtest.ru
Address: 77.222.40.238

C:\Users\User>nslookup shipulinpa.temp.swtest.ru
Полученный ответ:
Address: 172.28.16.1

Не заслуживающий доверия ответ:
   : shipulinpa.temp.swtest.ru
Address: 77.222.40.238

C:\Users\User>nslookup -type=NS shipulinpa.temp.swtest.ru
Полученный ответ:
Address: 172.28.16.1

ru      nameserver = d.dns.ripn.net
ru      nameserver = b.dns.ripn.net
ru      nameserver = e.dns.ripn.net
ru      nameserver = f.dns.ripn.net
ru      nameserver = a.dns.ripn.net
d.dns.ripn.net internet address = 194.190.124.17
b.dns.ripn.net internet address = 194.85.252.62
e.dns.ripn.net internet address = 193.232.142.17
f.dns.ripn.net internet address = 193.232.156.17
a.dns.ripn.net internet address = 193.232.128.6

C:\Users\User>

```

1. Чем различается трасса трафика в п.2 и п.4, указанных выше?

Name Server – поле Answers будет пустым, но поле Authoritative nameservers будет содержать список серверов.

2. Что содержится в поле «Answers» DNS-ответа?

▼ Answers

```

▼ shipulinpa.temp.swtest.ru: type A, class IN, addr 77.222.40.238
   Name: shipulinpa.temp.swtest.ru
   Type: A (Host Address) (1)
   Class: IN (0x0001)
   Time to live: 548 (9 minutes, 8 seconds)
   Data length: 4
   Address: 77.222.40.238

```

Для типа “A”: IPv4 адрес

Для типа “AAAA”: IPv6 адрес

Для типа “NS”: не содержит ничего в поле Answers

3. Каковы имена серверов, возвращающих авторитативный (authoritative) отклик?

ip.addr == 172.28.24.246 && dns

Transaction ID: 0x0002

- > Flags: 0x8180 Standard query response, No error
- Questions: 1
- Answer RRs: 0
- Authority RRs: 5
- Additional RRs: 5
- > Queries
- > Authoritative nameservers
 - > ru: type NS, class IN, ns d.dns.ripn.net
 - > ru: type NS, class IN, ns b.dns.ripn.net
 - > ru: type NS, class IN, ns e.dns.ripn.net
 - > ru: type NS, class IN, ns f.dns.ripn.net
 - > ru: type NS, class IN, ns a.dns.ripn.net
- > Additional records
- [Request In: 29725]
- [Time: 0.106718000 seconds]

```

0050 00 00 02 00 01 c0 23 00 02 00 01 00 01 20 2a 00 .....#.....*
0060 10 01 64 03 64 6e 73 04 72 69 70 6e 03 6e 65 74 ..d.dns.ripn.net
0070 00 c0 23 00 02 00 01 00 01 20 2a 00 04 01 62 c0 ..#.....*...b
0080 39 c0 23 00 02 00 01 00 01 20 2a 00 04 01 65 c0 9.#.....*...e
    
```

Text item (text), 92 byte(s) | Пакеты: 314470 · Показаны: 60 (0.0%) | Профиль: Default