Сайт: sgi.com

Ping:

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

Да, фрагментация имеет место, если размер файла больше MTU (1500 байт). На фрагментацию указывает третий бит в поле Flags, а так же Offset.

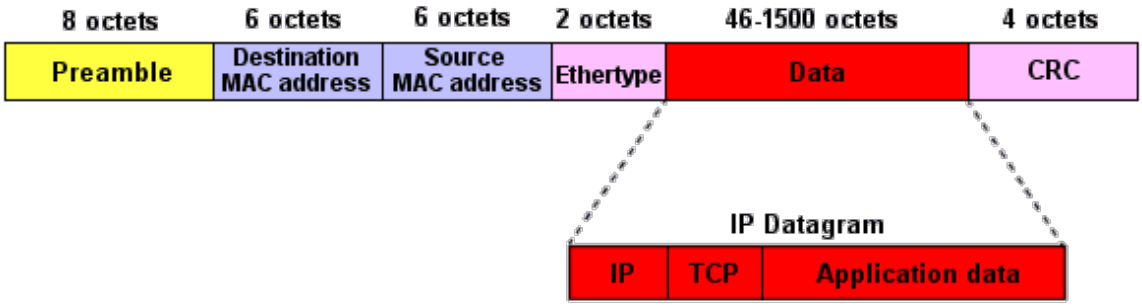
```
Flags: 0x01 (More Fragments)
   0... .... = Reserved bit: Not set
   .0.. .... = Don't fragment: Not set
   ..1. .... = More fragments: Set
```

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

У промежуточного пакета третий бит флага установлен в 1 (см. ответ 1), у последнего в 0.

```
▼ Flags: 0x00
     0... .... = Reserved bit: Not set
     .0.. .... = Don't fragment: Not set
     ..0. .... = More fragments: Not set
  Fragment offset: 1480
  Time to live: 64
```

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



Количество фрагментов можно рассчитать по формуле: (Data + 8) / 1480;

5. Как изменить поле TTL с помощью утилиты ping?

ping -m TTL_VALUE

6. Что содержится в поле данных ping-пакета?

```
▼ Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.48.178.134
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x125d (4701)
  ▼ Flags: 0x01 (More Fragments)
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x0efe [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.103
    Destination: 192.48.178.134
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 41
▼ Data (1480 bytes)
    Data: 08009568ee7b000058e6909b000a527708090a0b0c0d0e0f...
    [Length: 1480]
```

traceroute:

1. Сколько байт содержится в заголовке IP? Сколько байт содержится в поле данных?
Header - 40
UDP - 8
Data - 32

2. Как и почему именно так изменяется поле TTL в следующих друг за другом ICMP-пакетах tracert (проследить изменение TTL в как минимум пяти подряд идущих пакетах)?
Для определения промежуточных маршрутизаторов traceroute отправляет целевому узлу серию ICMP-пакетов (по умолчанию 3 пакета), с каждым шагом увеличивая значение поля TTL на 1. Первая серия пакетов отправляется с TTL, равным 1, и поэтому первый же маршрутизатор возвращает обратно ICMP-сообщение «time exceeded in transit», указывающее на невозможность доставки данных. Traceroute фиксирует адрес маршрутизатора, а также время между отправкой пакета и получением ответа (эти сведения выводятся на монитор компьютера). Затем traceroute повторяет отправку серии пакетов, но уже с TTL, равным 2, что заставляет первый маршрутизатор уменьшить TTL пакетов на единицу и направить их ко второму маршрутизатору. Второй маршрутизатор, получив пакеты с TTL=1, так же возвращает «time exceeded in transit».

Процесс повторяется до тех пор, пока пакет не достигнет целевого узла. При получении ответа от этого узла процесс трассировки считается завершённым.

3. Чем отличаются ICMP-пакеты, генерируемые утилитой tracert, от ICMP-пакетов, генерируемых утилитой ping (см. предыдущее задание).
Traceroute импользует UDP вместо ICMP.

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

хз !!!

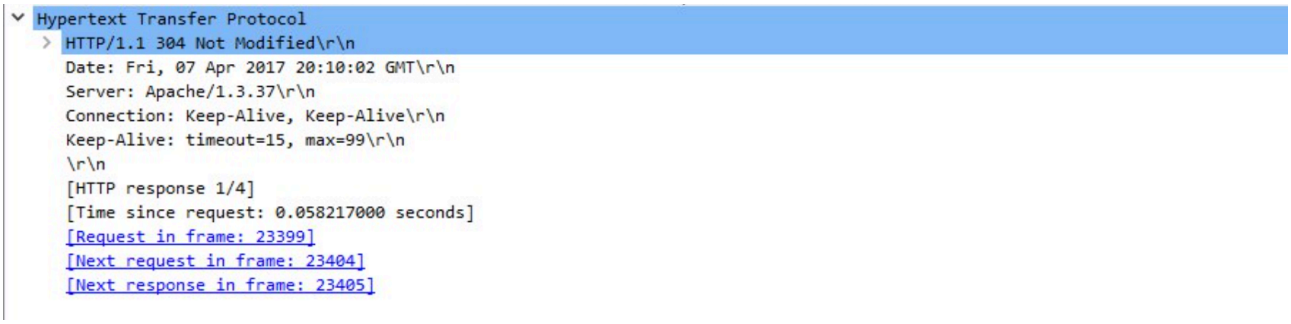
5. Что изменится в работе tracert, если убрать ключ “-d”? Какой дополнительный трафик при этом будет генерироваться?
Утилита начнет преобразовавывать IP адреса узлов сети в их строковые адреса, для этого потребуются дополнительные DNS запросы.

HTTP:
Для данного задания использовался сайт с поддержкой "условных" запросов.
Первичный GET запрос:

Ответ на первичный GET запрос:

Повторный GET запрос:

Ответ на повторный запрос:



DNS:

```
▼ Domain Name System (response)
    [Request In: 753]
    [Time: 0.542656000 seconds]
    Transaction ID: 0x60ad
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 2
    Additional RRs: 0
  ▶ Queries
  ▶ Answers
  ▶ Authoritative nameservers
```

```
▼ Domain Name System (query)
    [Response In: 757]
    Transaction ID: 0x60ad
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▶ Queries
```

1. Почему адрес, на который отправлен DNS-запрос, не совпадает с адресом посещаемого сайта?
Т. к. DNS - это хранилище, используемое для получения ip адреса сайта по его строковому адресу. Адрес DNS != адрес сайта **(переписать нормально)**

2. Какие бывают типы DNS-запросов?
Прямой (forward) запрос — запрос на преобразование имени (символьного адреса) хоста в его IP-адрес.
Обратный (reverse) запрос — запрос на преобразование IP-адреса хоста в его имя.
Рекурсивный запрос предполагает получение окончательного ответа от сервера, к которому он направлен. Рекурсию выполняет сервер.
Итеративный запрос предполагает (допускает) выполнение рекурсии клиентом.

3. В какой ситуации нужно выполнять независимые DNS-запросы для получения содержащихся на сайте изображений?
Если на сайте лежит не само изображение, а его адрес.

ARP:

```
Address Resolution Protocol (request)
   Hardware type: Ethernet (1)
   Protocol type: IPv4 (0x0800)
   Hardware size: 6
   Protocol size: 4
   Opcode: request (1)
   Sender MAC address: Apple_cc:02:dc (3c:15:c2:cc:02:dc)
   Sender IP address: 192.168.0.103
   Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
   Target IP address: 192.168.0.105
```

```
Address Resolution Protocol (reply)
   Hardware type: Ethernet (1)
   Protocol type: IPv4 (0x0800)
   Hardware size: 6
   Protocol size: 4
   Opcode: reply (2)
   Sender MAC address: Apple_2c:a8:a1 (b8:78:2e:2c:a8:a1)
   Sender IP address: 192.168.0.105
   Target MAC address: Apple_cc:02:dc (3c:15:c2:cc:02:dc)
   Target IP address: 192.168.0.103
```

1. Какие MAC-адреса присутствуют в захваченных пакетах ARP-протокола? Что означают эти адреса? Какие устройства они идентифицируют?
В запросе: MAC адрес устройства (3c...)
В ответе: MAC адрес роутера (b8...)
Эти адреса позволяют определить физический узел сети на канальном уровне.

2. Какие MAC-адреса присутствуют в захваченных HTTP-пакетах и что означают эти адреса? Какие устройства они идентифицируют?
Адреса компьютера и роутера, позволяют определить физический узел сети на канальном уровне.

```
▶ Ethernet II, Src: Apple_cc:02:dc (3c:15:c2:cc:02:dc), Dst: Tp-LinkT_bf:c3:a8 (30:b5:c2:bf:c3:a8)
```

3. Для чего ARP-запрос содержит IP-адрес источника?
Т.к. запрос широковещательный, то другие устройства сети, получив этот запрос, могут добавить в ARP таблицу информацию об отправителе.

nslookup:

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

```
MacBook-Pro-Sitora:~ sitora$ nslookup sgi.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   sgi.com
Address: 192.48.178.134

MacBook-Pro-Sitora:~ sitora$ nslookup -type=NS sgi.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
sgi.com nameserver = d.ns.sgi.com.
sgi.com nameserver = a.ns.sgi.com.
sgi.com nameserver = b.ns.sgi.com.
sgi.com nameserver = c.ns.sgi.com.

Authoritative answers can be found from:
a.ns.sgi.com    internet address = 192.48.157.14
b.ns.sgi.com    internet address = 192.48.176.23
c.ns.sgi.com    internet address = 192.48.176.11
d.ns.sgi.com    internet address = 192.48.160.6
```

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

```
▼ Answers
  ▼ sgi.com: type A, class IN, addr 192.48.178.134
      Name: sgi.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 27997
      Data length: 4
      Address: 192.48.178.134
```

В первом случае - имя хоста, класс и тип записи, время жизни записи, размер данных и запрашиваемый адрес хоста.

```
  ▼ Answers
    ▼ sgi.com: type NS, class IN, ns d.ns.sgi.com
        Name: sgi.com
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 27991
        Data length: 7
        Name Server: d.ns.sgi.com
    ▼ sgi.com: type NS, class IN, ns a.ns.sgi.com
        Name: sgi.com
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 27991
        Data length: 4
        Name Server: a.ns.sgi.com
```

Во втором - 2 ответа, содержащие имя хоста, класс и тип записи, время жизни записи, размер данных и имена авторитативный серверов.

3. Каковы имена серверов, возвращающих авторитативный (authoritative) отклик?
a.ns.sgi.com, b.ns.sgi.com, c.ns.sgi.com, d.ns.sgi.com
ПРОВЕРИТЬ!!!!

FTP:
Найти ftp сервер с нужными инициалами не удалось, поэтому использовался этот: ftp.cert.fr

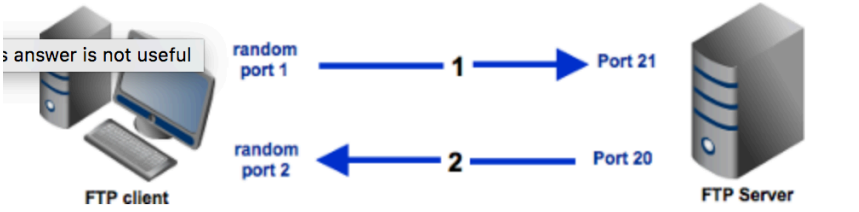
```
FTP-DATA        421 FTP Data: 355 bytes
```

1. Сколько байт данных содержится в пакете FTP-DATA?
В пакете FTP-DATA максимум может содержаться 1448байт данных. Это связано с тем, что MTU=1500, куда входит заголовок IP(20 байт) и заголовок TCP(32 байта)

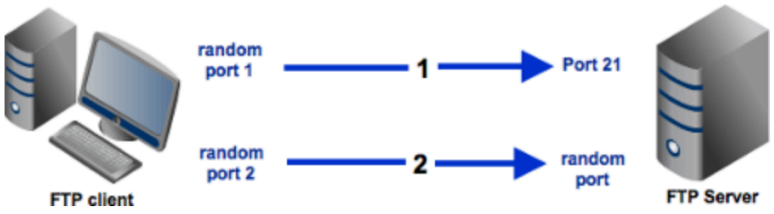
2. Как выбирается порт транспортного уровня, который используется для передачи FTP-пакетов?

В активном режиме клиент сообщает серверу номер порта (из динамического диапазона 1024-65535) для того, чтобы сервер мог подключиться к клиенту для установки соединения для передачи данных. FTP-сервер подключается к заданному номеру порта клиента используя со своей стороны номер TCP-порта 20 для передачи данных.

В пассивном режиме сервер сообщает клиенту номер TCP-порта (из динамического диапазона 1024-65535), к которому можно подключиться для установки соединения передачи данных.



Passive mode:



3. Чем отличаются пакеты FTP от FTP-DATA?
FTP - передача команд.
FTP-DATA - передача данных.

Skype:

DHCP:

1. Чем различаются пакеты «DHCP Discover» и «DHCP Request»?
DHCP Discover посылается в качестве запроса на получение конфигураций от одного или более DHCP серверов, после их ответа выбирается одна из них и посылается DHCP Request, в котором указывается запрашиваемый IP адрес и идентификатор DHCP сервера.

4. Что произойдёт, если очистить использованный фильтр “bootp”?
Отобразятся все пакеты, захаваченные за время выполнения задания