1. 21:25
   При помощи анализатора протоколова WireShark исследовать и описать работу команды ping
   например: ping 8.8.8.8;
2. При помощи анализатора протоколова WireShark исследовать и описать работу команды tracert
   например: tracert -d -w 1 (если без -d (разрешение имен) очень долго)
3. Исследовать ключ -r команды ping.
   например: ping -r 9 yandex.ru;
4. _***Построить полный маршрут до какого-либо узла в интернете.
5. почитать RFC – xxx 23:32

---

1. При помощи анализатора протоколова WireShark исследовать и описать работу команды ping
   например: **ping 8.8.8.8**;

```
C:\Users\rls>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=133ms TTL=107
Reply from 8.8.8.8: bytes=32 time=133ms TTL=107
Reply from 8.8.8.8: bytes=32 time=132ms TTL=107
Reply from 8.8.8.8: bytes=32 time=133ms TTL=107

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 132ms, Maximum = 133ms, Average = 132ms
```

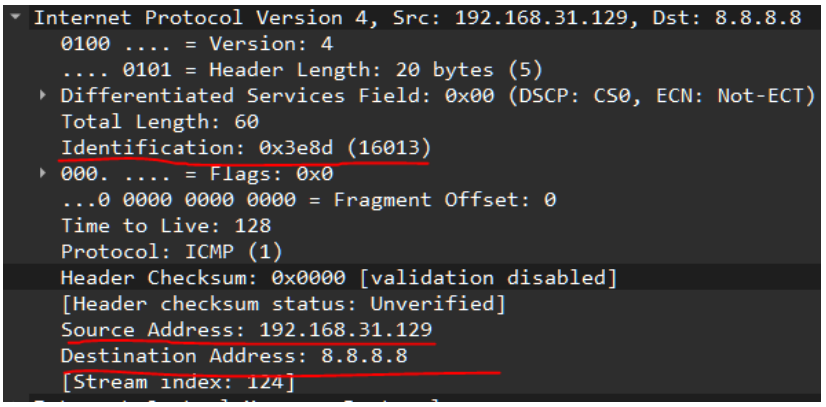
Команда **ping** на определенный узел для его проверки доступа отправляет 4 запроса сообщения **Echo request** по протоколу ICMP с типом 8 кодом 0. При этом выводится информация сколько пакетов отправлено, получено и потеряно. А также min, max и average время прохождения пакетов туда и обратно.

89543	719.252371	192.168.31.129	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=470/54785, ttl=128 (reply in 89611)
89611	719.385382	8.8.8.8	192.168.31.129	ICMP	74	Echo (ping) reply id=0x0001, seq=470/54785, ttl=107 (request in 89543)
89867	720.864012	192.168.31.129	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=471/55041, ttl=128 (reply in 89881)
89881	720.996833	8.8.8.8	192.168.31.129	ICMP	74	Echo (ping) reply id=0x0001, seq=471/55041, ttl=107 (request in 89867)
90036	722.041961	192.168.31.129	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=472/55297, ttl=128 (reply in 90049)
90049	722.174548	8.8.8.8	192.168.31.129	ICMP	74	Echo (ping) reply id=0x0001, seq=472/55297, ttl=107 (request in 90036)
90147	723.058168	192.168.31.129	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=473/55553, ttl=128 (reply in 90200)
90200	723.191030	8.8.8.8	192.168.31.129	ICMP	74	Echo (ping) reply id=0x0001, seq=473/55553, ttl=107 (request in 90147)

При этом на единицу увеличивается поле Sequence Number (BE) и Sequence Number (LE) последний в Little Endian формате.

```
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4b85 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 470 (0x01d6)
    Sequence Number (LE): 54785 (0xd601)
    [Response frame: 89611]
  ▸ Data (32 bytes)
```

По IP протоколу запросы отличаются полем Identification увеличивающимся также на единицу. В поле Source Address этого протокола указывается IP-адрес отправителя , в поле Destination Address IP-адрес получателя.

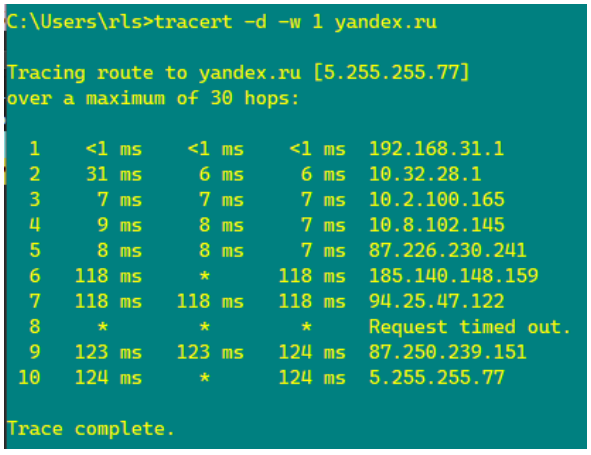


В сообщении ответа (**Echo reply**) от запрашиваемого узла поле Type устанавливается в 0 код 0. Sequence Number при этом не изменяется. Т.е. оно увеличивается только при следующем запросе.

В IP-протоколе соответственно меняются местами IP-адреса. Поле Identification устанавливается в 0. Поле TTL равно 107, что означает до запрашиваемого узла примерно 21 маршрутизатор и операционная система, отправляющая ответ, Windows.

2. При помощи анализатора протоколова WireShark исследовать и описать работу команды **tracert** например: tracert -d -w 1

Команда tracert отправляет на каждый промежуточный узел по 3 ping запроса с увеличивающимся TTL на единицу до запрашиваемого IP-адреса.

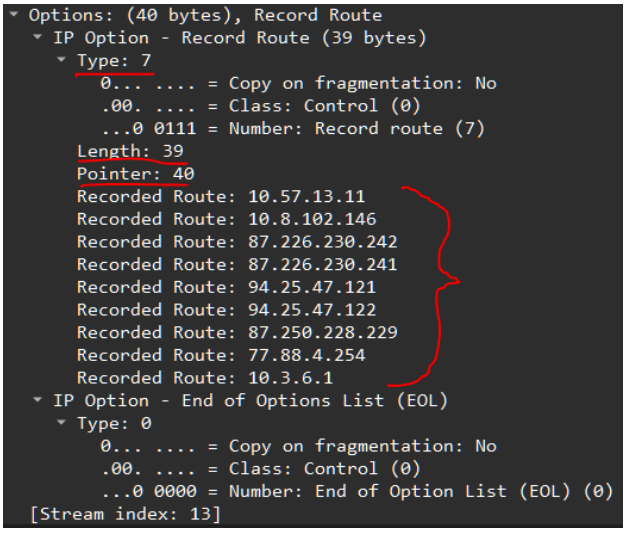


Параметры -d выключает разрешение символьных имен, что увеличивает скорость прохождения пакета, -w 1 устанавливает время ожидания ответа от маршрутизатора в 1 ms, если время выходит выводит знак * . Когда очередной маршрутизатор получает пакет с TTL равным 1 он уменьшает его до 0 и

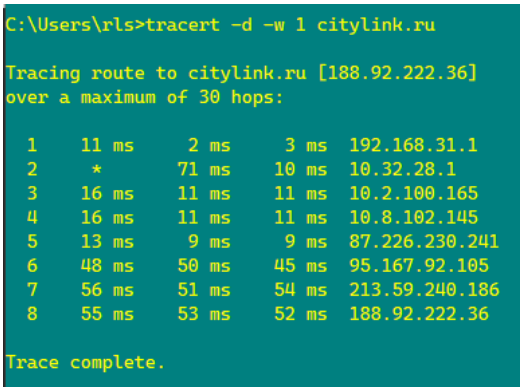
уничтожает его, при этом направляет отправителю пакета сообщение Time Exceeded Type: 11 Code: 0, а также информацию о своем IP-адресе как отправителя в поле Source IP протокола.

3. Исследовать ключ -r команды ping.
   например: ping -r 9 yandex.ru;

   Команда ping с ключом -r 9 отправляет запрос до указанного узла при этом включает опцию RR (Record Route) пакета протокола IP с полями: Type 7, Length - длина в байтах, максимально 39, Pointer - смещение относительно следующего адреса в байтах и Recorded Route. В последних в ответе в этих полях записываются адреса маршрутизаторов, через которые проходит пакет, максимум 9 x 4 байта = 36 + 3 служебных байта, при условии, что на этих маршрутизаторах включена эта опция.



4. ***Построить полный маршрут до какого-либо узла в интернете.



0) хост отправителя

1) 192.168.31.1

частная сеть, где находится наш хост маска подсети 255.255.255.0 или 192.168.31.0/24
Локальная сеть

2) 10.32.28.1
узел vlan271.0-agr3-16.agr3.vl.podryad.tv интернет провайдера podryad.tv
Локальная сеть

3) 10.2.100.165
Локальная сеть

4) 10.8.102.145 частные(крупные) сети провайдера ip диапазон каждой 10.0.0.0 - 10.255.255.255 или 10.0.0.0/8

5) 87.226.230.241 выход в интернет (белый IP)
провайдер Rostelecomnet
IP диапазон 87.266.230.0-87.226.230.255
CIDR 87.226.230.0/24
Москва

6) 95.167.92.105
провайдер Rostelecomnet
IP-диапазон 95.167.88.0-95.167.95.255
CIDR 95.167.88.0/21
Москва

7) 213.59.240.186
провайдер RU-RTK-20000224
IP диапазон 213.59.192.0-213.59.255.255
CIDR 213.59.192.0/18
Москва

8) 188.92.222.36
провайдер RU-ARBUZ-WEBHOSTING-NET
IP диапазон 188.92.222.0-188.92.222.255
CIDR 188.92.222.0/24
Магадан