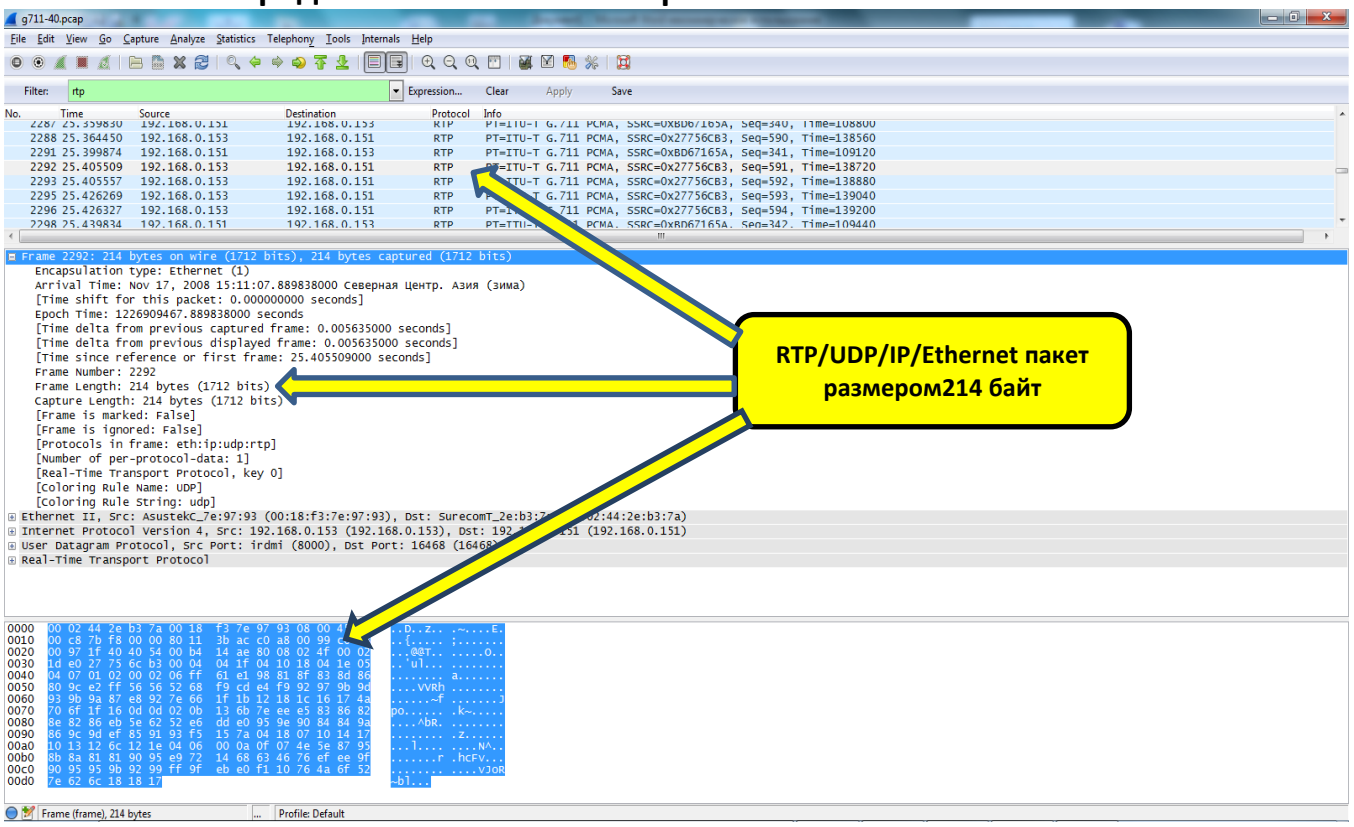
## <u>Задание</u>: Расшифровать речевой IP-пакет (см. свой вариант !!!)

**Пояснить содержимое каждой части заголовка стека протоколов RTP/UDP/IP/Ethernet**

**<u>Пример</u> речевого IP-пакета**

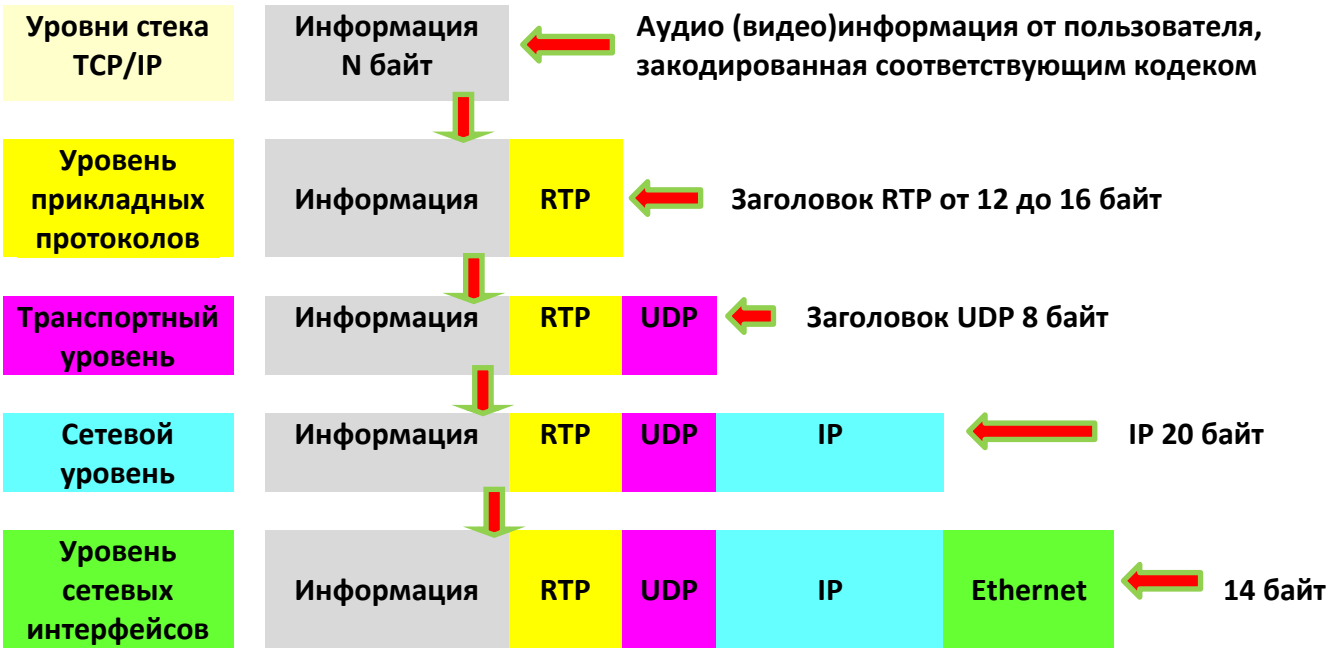
| Номера байт | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00 | 00 | 02 | 44 | 2e | b3 | 7a | 00 | 18 | f3 | 7e | 97 | 93 | 08 | 00 | 45 | 00 |
| 10 | 00 | c8 | 7b | f8 | 00 | 00 | 80 | 11 | 3b | ac | c0 | a8 | 00 | 99 | c0 | a8 |
| 20 | 00 | 97 | 1f | 40 | 40 | 54 | 00 | b4 | 14 | ae | 80 | 08 | 02 | 4f | 00 | 02 |
| 30 | 1d | e0 | 27 | 75 | 6c | b3 | 00 | 04 | 04 | 1f | 04 | 10 | 18 | 04 | 1e | 05 |
| 40 | 04 | 07 | 01 | 02 | 00 | 02 | 06 | ff | 61 | e1 | 98 | 81 | 8f | 83 | 8d | 86 |
| 50 | 80 | 9c | e2 | ff | 56 | 56 | 52 | 68 | f9 | cd | e4 | f9 | 92 | 97 | 9b | 9d |
| 60 | 93 | 9b | 9a | 87 | e8 | 92 | 7e | 66 | 1f | 1b | 12 | 18 | 1c | 16 | 17 | 4a |
| 70 | 70 | 6f | 1f | 16 | 0d | 0d | 02 | 0b | 13 | 6b | 7e | ee | e5 | 83 | 86 | 82 |
| 80 | 8e | 82 | 86 | eb | 5e | 62 | 52 | e6 | dd | e0 | 95 | 9e | 90 | 84 | 84 | 9a |
| 90 | 86 | 9c | 9d | ef | 85 | 91 | 93 | f5 | 15 | 7a | 04 | 18 | 07 | 10 | 14 | 17 |
| a0 | 10 | 13 | 12 | 6c | 12 | 1e | 04 | 06 | 00 | 0a | 0f | 07 | 4e | 5e | 87 | 95 |
| b0 | 8b | 8a | 81 | 81 | 90 | 95 | e9 | 72 | 14 | 68 | 63 | 46 | 76 | efee | 9f | |
| c0 | 90 | 95 | 95 | 9b | 92 | 99 | ff | 9f | eb | e0 | f1 | 10 | 76 | 4a | 6f | 52 |
| d0 | 7e | 62 | 6c | 18 | 18 | 17 | | | | | | | | | | |

## Тот же пакет в представлении анализатора Wireshark:

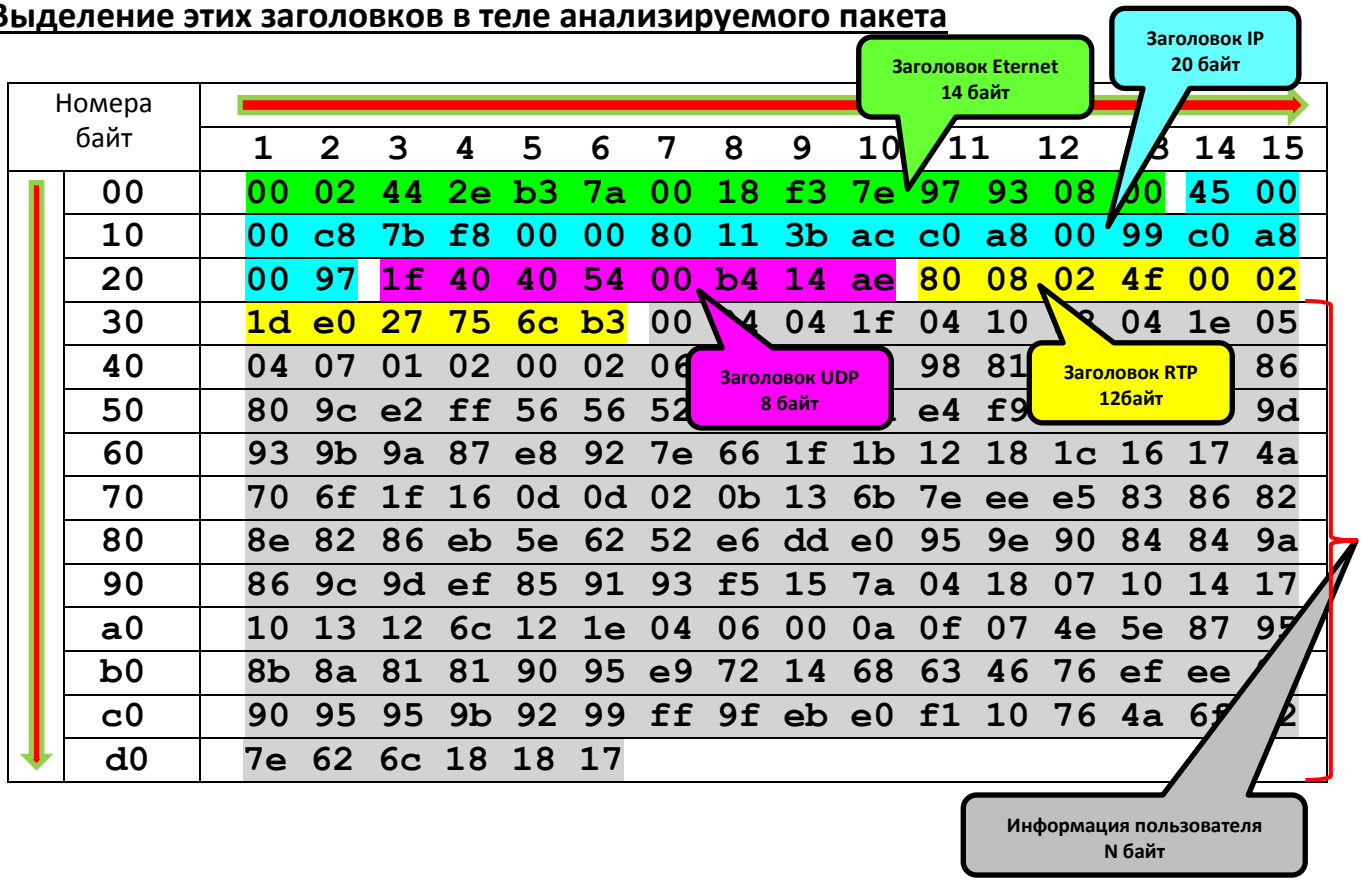


## Пример расшифровки:

### 1. Заголовки RTP/UDP/IP/Ethernet




### 3. Выделение этих заголовков в теле анализируемого пакета




| Номера байт | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00 | 00 | 02 | 44 | 2e | b3 | 7a | 00 | 18 | f3 | 7e | 97 | 93 | 08 | 00 | 45 | 00 |
| 10 | 00 | c8 | 7b | f8 | 00 | 00 | 80 | 11 | 3b | ac | c0 | a8 | 00 | 99 | c0 | a8 |
| 20 | 00 | 97 | 1f | 40 | 40 | 54 | 00 | b4 | 14 | ae | 80 | 08 | 02 | 4f | 00 | 02 |
| 30 | 1d | e0 | 27 | 75 | 6c | b3 | 00 | 4 | 04 | 1f | 04 | 10 | 8 | 04 | 1e | 05 |
| 40 | 04 | 07 | 01 | 02 | 00 | 02 | 06 | | | | 98 | 81 | | | | 86 |
| 50 | 80 | 9c | e2 | ff | 56 | 56 | 52 | | | | e4 | f9 | | | | 9d |
| 60 | 93 | 9b | 9a | 87 | e8 | 92 | 7e | 66 | 1f | 1b | 12 | 18 | 1c | 16 | 17 | 4a |
| 70 | 70 | 6f | 1f | 16 | 0d | 0d | 02 | 0b | 13 | 6b | 7e | ee | e5 | 83 | 86 | 82 |
| 80 | 8e | 82 | 86 | eb | 5e | 62 | 52 | e6 | dd | e0 | 95 | 9e | 90 | 84 | 84 | 9a |
| 90 | 86 | 9c | 9d | ef | 85 | 91 | 93 | f5 | 15 | 7a | 04 | 18 | 07 | 10 | 14 | 17 |
| a0 | 10 | 13 | 12 | 6c | 12 | 1e | 04 | 06 | 00 | 0a | 0f | 07 | 4e | 5e | 87 | 9 |
| b0 | 8b | 8a | 81 | 81 | 90 | 95 | e9 | 72 | 14 | 68 | 63 | 46 | 76 | ef | ee | |
| c0 | 90 | 95 | 95 | 9b | 92 | 99 | ff | 9f | eb | e0 | f1 | 10 | 76 | 4a | 6 | 2 |
| d0 | 7e | 62 | 6c | 18 | 18 | 17 | | | | | | | | | | |

## 3. Расшифровка полей каждого заголовка

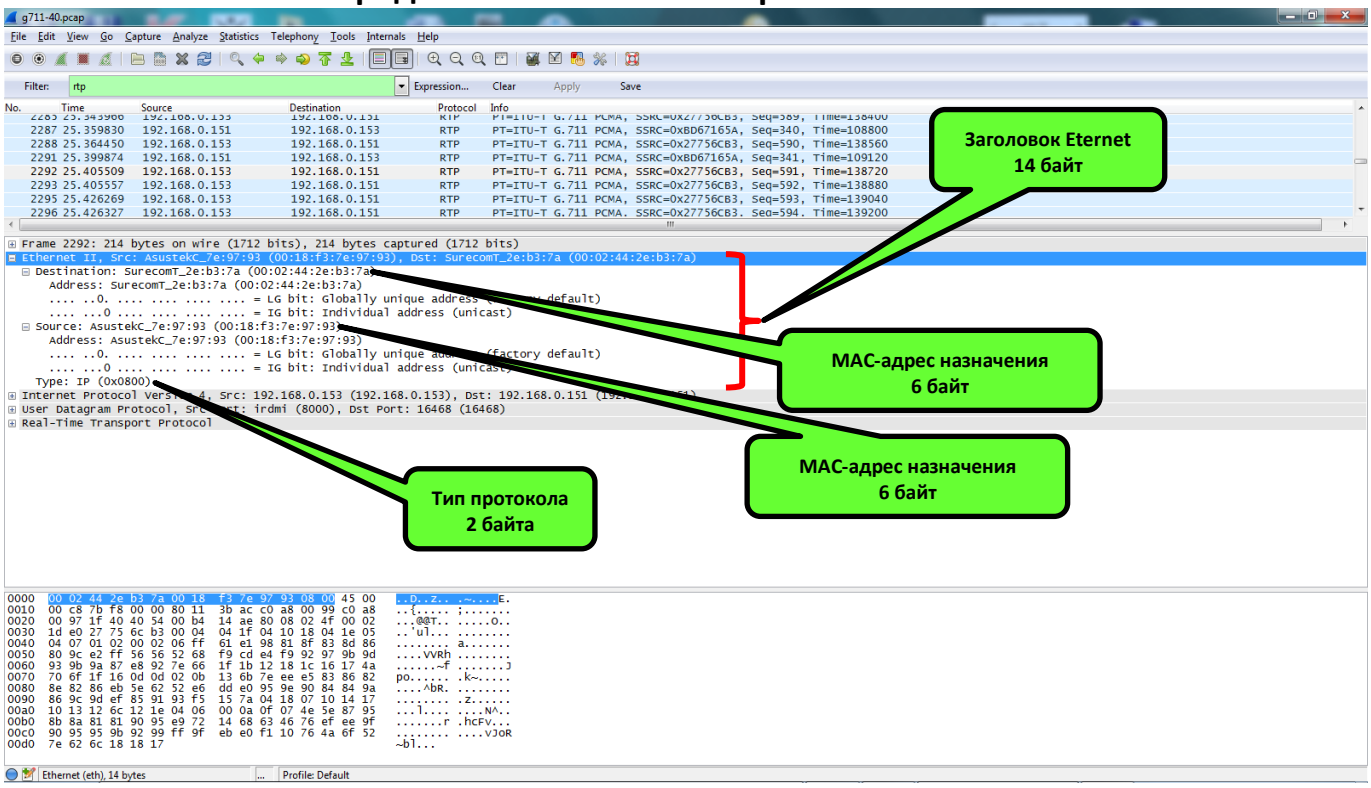
### 3.1 Поля заголовка протокола Ethernet (14 байт):

| MAC-адрес сетевой платы назначения | | | | | | MAC-адрес сетевой платы источника | | | | | | Тип протокола, информация которого помещена в поле Data | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00 | 02 | 44 | 2e | b3 | 7a | 00 | 18 | f3 | 7e | 97 | 93 | 08 | 00 |
| OUI вендора (SURECOM Technology) | | | | | | OUI вендора (ASUSTek) | | | | | | | |

Первые 3 байта MAC-адреса – это Уникальный Идентификатор Организации (OUI – Organizationally UniqueIdentifier ) , т.е. номер, который присваивается организацией IEEE производителю оборудования (вендору).
OUI производителя (вендора) можно определить, например, по ссылке http://www.ep.ph.bham.ac.uk/poynters/mirror/eth-vendor.html

Или в режиме онлайн по ссылке: http://aruljohn.com/mac.pl

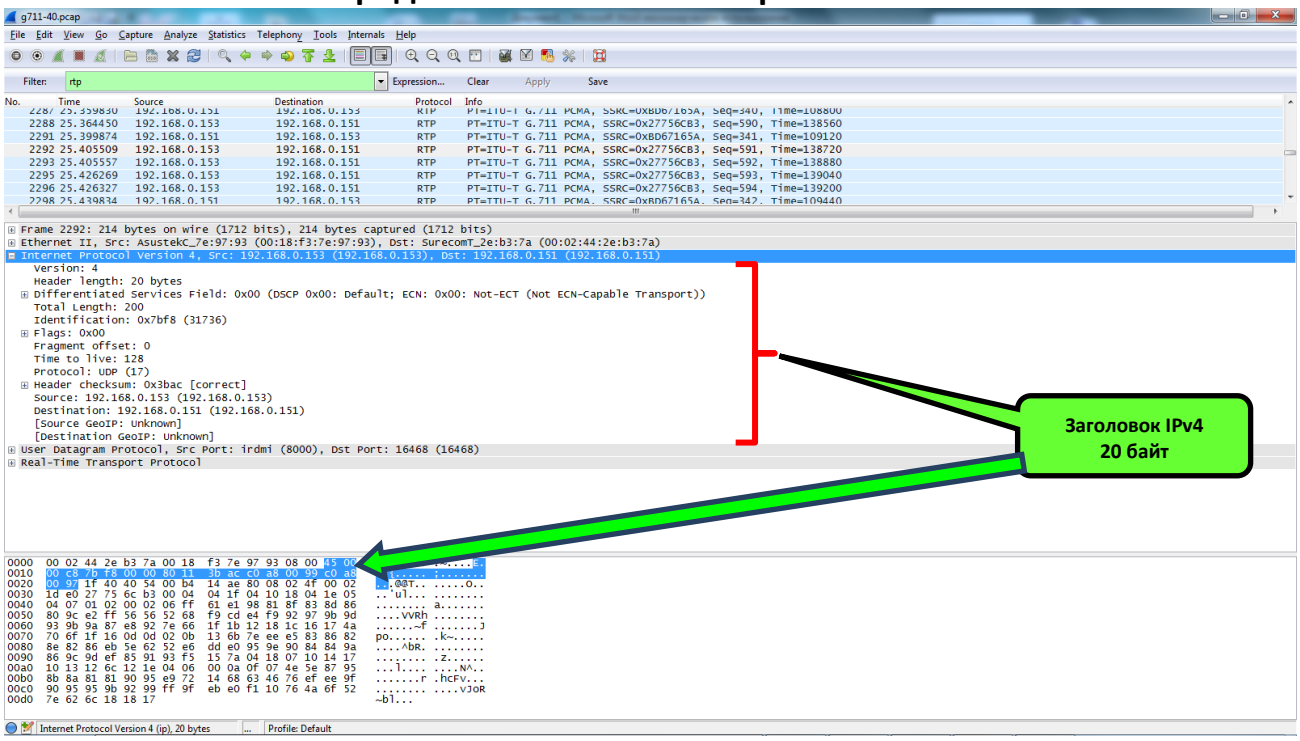
### Те же поля пакета в представлении анализатора Wireshark:



## 3.2 Поля заголовка протокола IP (20 байт):

| V/ IHL | ToS | Длина IP-пакета | | Поля для сборки/разборки фрагментов | | | | TTL | Protocol | Контр. сумма | | IP-Source | | | | IP-Dest | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 45 | 00 | 00 | c8 | 7b | f8 | 00 | 00 | 80 | 11 | 3b | ac | c0 | a8 | 00 | 99 | c0 | a8 | 00 | 97 |
| | | | | | | | | | | | | | | | | | | | |

## Те же поля пакета в представлении анализатора Wireshark:




## 3.2.1.Расшифровка полей заголовка протокола IP

**Назначение полей заголовка протокола IPv4 в типовом представлении по 32 бита (5 слов по 32 бита):**

| 0 1 2 3 | 4 5 6 7 | 8 9 10 11 12 13 14 15 | 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 |
|---|---|---|---|
| **Версия** | Длина IP-заголовка (HLength) | **Тип сервиса** ToS<br>0 1 2 3 4 5 6 7<br>Приоритет D T R C Не использ. | **Длина IP-пакета** (дейтаграммы), включая заголовки IP и UDP |
| Идентификатор фрагмента | | | Флаги: Указатель фрагмента |
| **Время жизни** (TTL) | | **Протокол**, которому предоставлена услуга | **Контрольная сумма заголовка** |
| **IP-адрес отправителя – Source (откуда)** | | | |
| **IP-адрес получателя – Destination (куда)** | | | |

Приведем пример расшифровки заголовка IP из трассировки нашего сообщения:

| 45 | 00 | 00 | c8 | 7b | f8 | 00 | 00 | 80 | 11 | 3b | ac | c0 | a8 | 00 | 99 | c0 | a8 | 00 | 97 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Ниже в таблице приведена расшифровка заголовка IP-датаграммы:

| 0 1 2 3 | 4 5 6 7 | 8 9 10 11 12 13 14 15 | 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 |
|---|---|---|---|
| **Версия** | Длина IP-заголовка (HLength) | **Тип сервиса** ToS<br>0 1 2 3 4 5 6 7<br>Приоритет \| D \| T \| R \| C \| Не использ. | **Длина IP-пакета** (дейтаграммы), включая заголовки IP и UDP |
| 4 | 5 | 00 | 00 c8 'hex = 200'Dec байт |
| | | Prio D T R C x | |
| | | 0 0 0 0 0 0 0 0 | |

| 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 | 16 17 18 | 19 20 21 22 23 24 25 26 27 28 29 30 31 |
|---|---|---|
| Идентификатор фрагмента | Флаги | Указатель фрагмента |
| 7b f8 | | 00 00 |
| | 0 0 0 | |

| **Время жизни** (TTL) | **Протокол**, которому предоставлена услуга | **Контрольная сумма заголовка** |
|---|---|---|
| 80'hex<br>(128'Dec) | 11'hex<br>(17'Dec - UDP) | 3b ac |

| **IP-адрес отправителя – Source (откуда)** | | | |
|---|---|---|---|
| C0'hex<br>192'Dec | A8'hex<br>168'Dec | 00'hex<br>00'Dec | 99'hex<br>153'Dec |
| **IP-адрес получателя – Destination (куда)** | | | |
| C0'hex<br>192'Dec | A8'hex<br>168'Dec | 00'hex<br>00'Dec | 97'hex<br>151'Dec |

Из расшифровки видно, что IP-пакет длиной 200 байт, перевозящий данный UDP-пакет, направляется от устройства с адресом IP – 192.168.00.153 к устройству с адресом IP – 192.168.00.151, при этом время жизни IP-пакета в сети ограничено значением TTL=128, что допускает 128 транзитных пункта.

Также видно, что приоритет данного пакета самый низкий (0), и для обслуживания голосового пакета используется протокол UDP (код – 11'hex или 17'dec).

Поле **контрольная сумма** заголовка вычисляется с использованием операций сложения 16-разрядных слов **заголовка** по модулю 1.

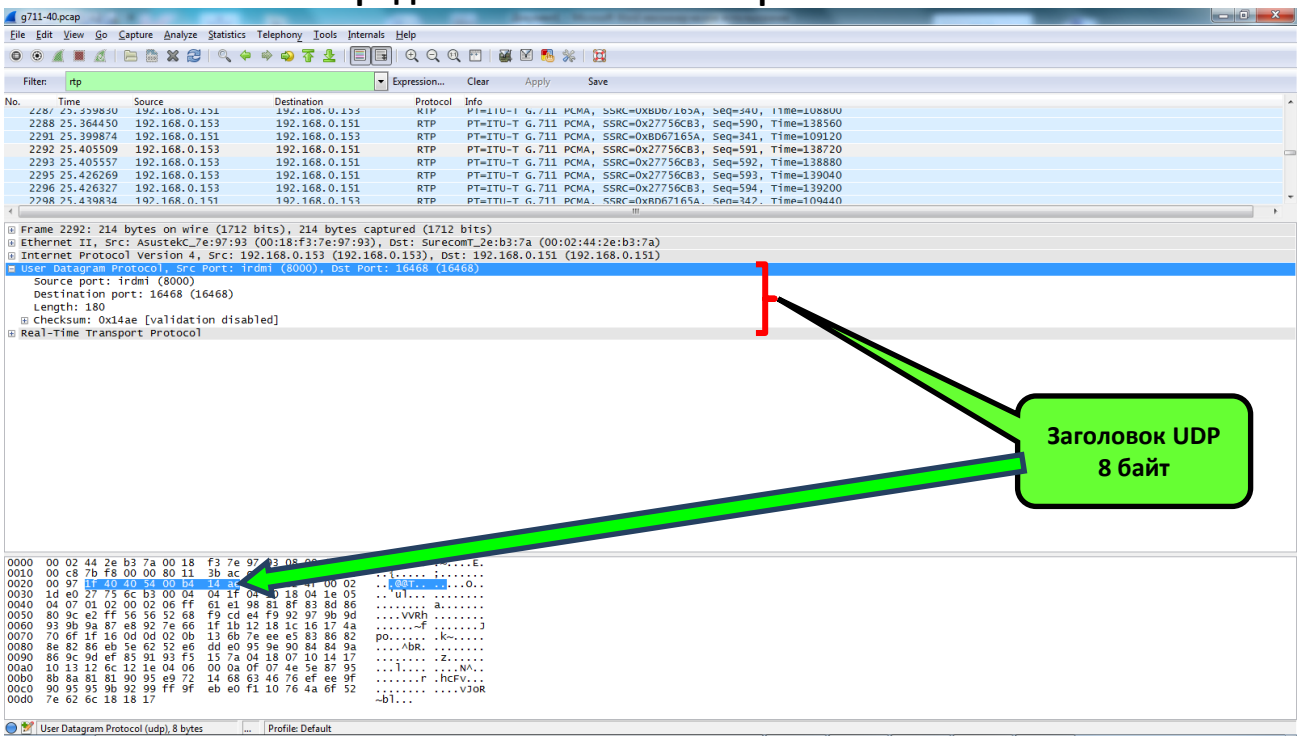
Обратите внимание, здесь осуществляется контрольное суммирование слов **заголовка, а не всей дейтаграммы**.

### 3.3 Поля заголовка протокола UDP (8 байт):

| Порт отправителя | | Порт получателя | | Длина дейтаграммы | | Контрольная сумма | |
|---|---|---|---|---|---|---|---|
| 1f | 40 | 40 | 54 | 00 | b4 | 14 | ae |
| 8000 | | 16468 | | 180 байт | | | |

- Порт отправителя/Порт получателя - в этих полях указываются номер порта отправителя / получателя. Для протокола RTP – это динамически назначаемые порты во время инициализации сеанса (например, посредством протокола SIP)
- Длина дейтаграммы - поле, задающее длину всей дейтаграммы (заголовка и данных) в байтах. Минимальная длина равна длине заголовка - 8 байт.
- Контрольная сумма - поле контрольной суммы используется для проверки заголовка и данных на ошибки. Если сумма не сгенерирована передатчиком, то поле заполняется нулями.

### Те же поля пакета в представлении анализатора Wireshark:




### 3.3.1. Расшифровка полей протокола UDP (заголовка UDP-датаграммы)

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1-ое 32-х разрядное слово UDP-заголовка | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Порт отправителя (от кого) | | | | | | | | | | | | | | | | Порт назначения (кому) | | | | | | | | | | | | | | | |
| 1f 40 (8000'Dec – RTP) | | | | | | | | | | | | | | | | 40 54 (16468'Dec – RTP) | | | | | | | | | | | | | | | |
| 2-ое 32-х разрядное слово UDP-заголовка | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Длина UDP-пакета | | | | | | | | | | | | | | | | Контрольная сумма заголовка | | | | | | | | | | | | | | | |
| 00 b4 (180'Dec байт) | | | | | | | | | | | | | | | | 14 ae | | | | | | | | | | | | | | | |

Полный перечень номеров UDP-портов приведен в RFC-1700.
Номера портов от 0 до 1023 стандартизованы и закреплены за наиболее известными сервисными протоколами. Использовать эти «очень известные порты» в прикладных задачах не рекомендуется, поэтому прежде чем использовать какой-то порт в своей программе, следует заглянуть в RFC-1700.

Номера портов с 8000 по 65536, назначаются динамически по согласованию сторон, участвующих в обмене информацией.

Для RTP-сеанса такое согласование производится во время установления сеанса с помощью протокола SIP.

Длина сообщения (**UDP-пакета**) равна числу байт в UDP-датаграмме, включая заголовок UDP.

Поле «контрольная сумма» содержит код, полученный в результате контрольного суммирования **UDP-заголовка и поля «данные»**.

Из данной расшифровки видно, что UDP-дейтаграмма, имеет общую длину 180 байт и предназначена для приложения с портом 16468.

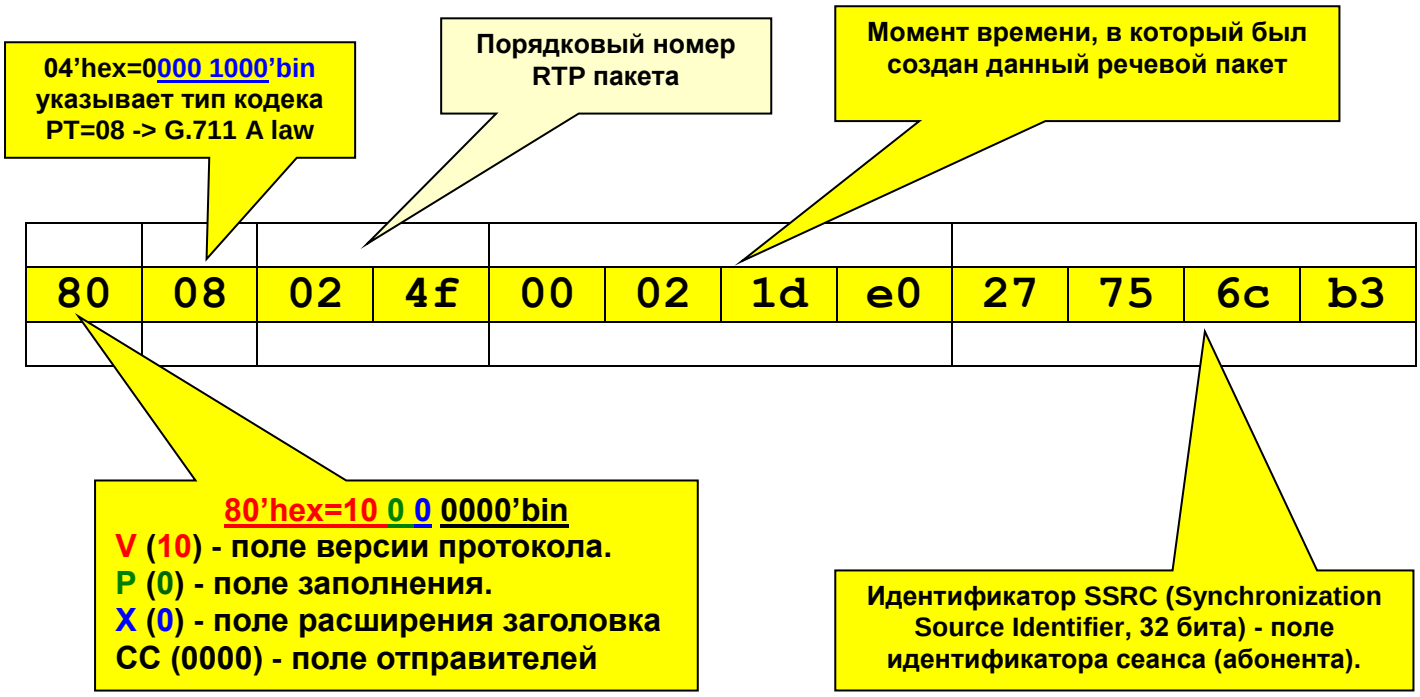
Со стороны источника используется динамически назначенный порт с номером 8000.

### 3.4 Пример полей заголовка протокола RTP (12 байт):

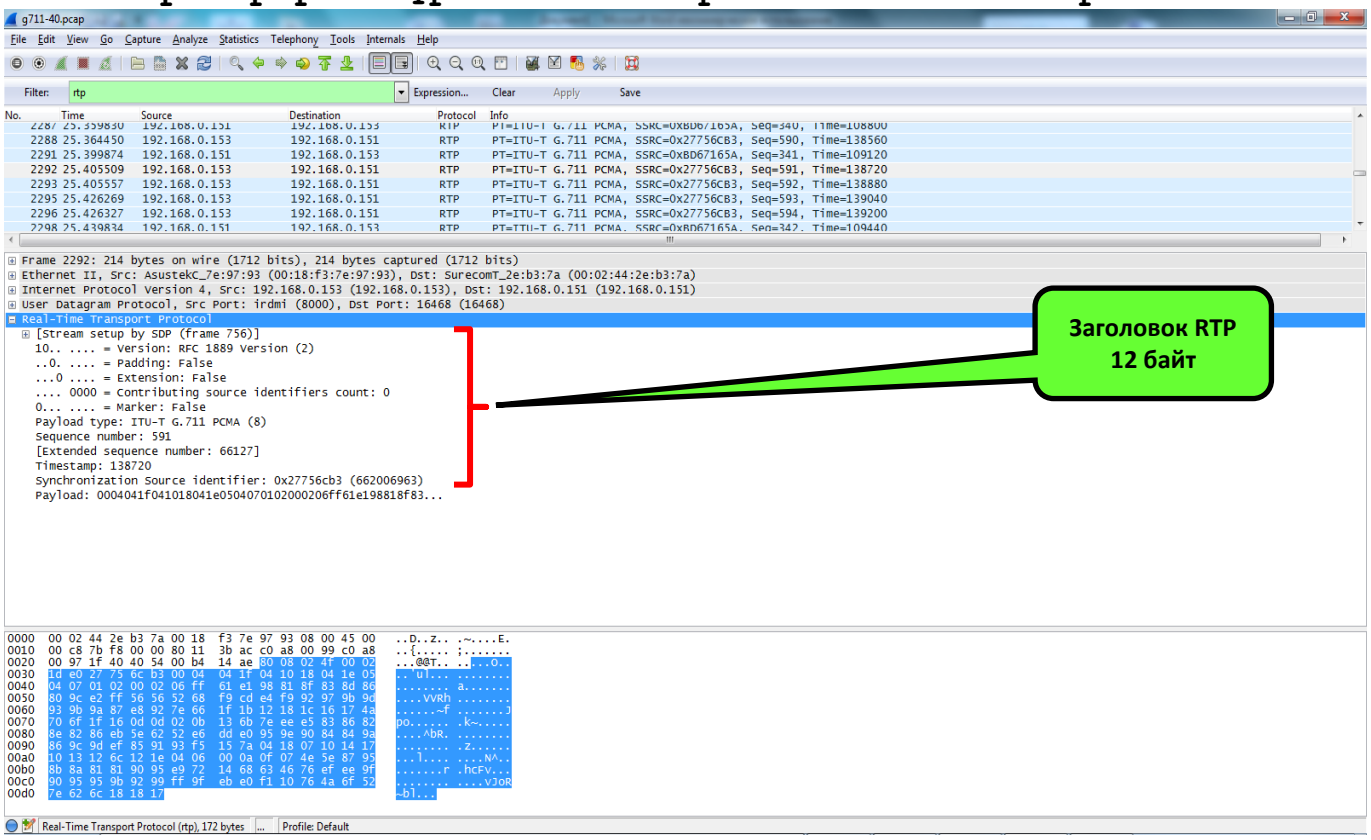
| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 80 | 08 | 02 | 4f | 00 | 02 | 1d | e0 | 27 | 75 | 6c | b3 |

### 3.4.1 Назначение полей заголовка протокола RTP (16 байт):

## 3.4.2 Расшифровка полей RTP-заголовка




## 3.4.3 Пример расшифровки в отображении анализатора Wireshark



## 4. Голосовые данные

**В поле данных RTP-пакета помещаются аудио (или видео) данные после их обработки соответствующим аудио/видео кодеком.**

**В данном примере голосовые данные обработаны аудиокодеком G.711 A-law, что следует согласно значению поля PT=08 заголовка RTP (см. RFC-1889, RFC-1890, RFC-3500, RFC-3551).**
**https://www.ietf.org/rfc/rfc3551.txt**

```
0000   00 02 44 2e b3 7a 00 18 f3 7e 97 93 08 00 45 00
0010   00 c8 7b f8 00 00 80 11 3b ac c0 a8 00 99 c0 a8
0020   00 97 1f 40 40 54 00 b4 14 ae 80 08 02 4f 00 02
0030   1d e0 27 75 6c b3 00 04 04 1f 04 10 18 04 1e 05
0040   04 07 01 02 00 02 06 ff 61 e1 98 81 8f 83 8d 86
0050   80 9c e2 ff 56 56 52 68 f9 cd e4 f9 92 97 9b 9d
0060   93 9b 9a 87 e8 92 7e 66 1f 1b 12 18 1c 16 17 4a
0070   70 6f 1f 16 0d 0d 02 [illegible] 13 6b 7e ee e5 83 86 82
0080   8e 82 86 eb 5e 62 52 [illegible] e0 95 9e 90 84 84 9a
0090   86 9c 9d ef 85 91 93 f5 [illegible] 04 18 07 10 14 17
00a0   10 13 12 6c 12 1e 04 06 [illegible] 07 4e 5e 87 95
00b0   8b 8a 81 81 90 95 e9 [illegible]
00c0   90 95 95 9b 92 99 ff [illegible]
00d0   7e 62 6c 18 18 17
```

**Voice Data, обработанные кодеком G.111 A-law**

### 4.1 Пример голосовых данных в отображении анализатора Wireshark