

Задание: Расшифровать речевой IP-пакет (см. свой вариант !!!)

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

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

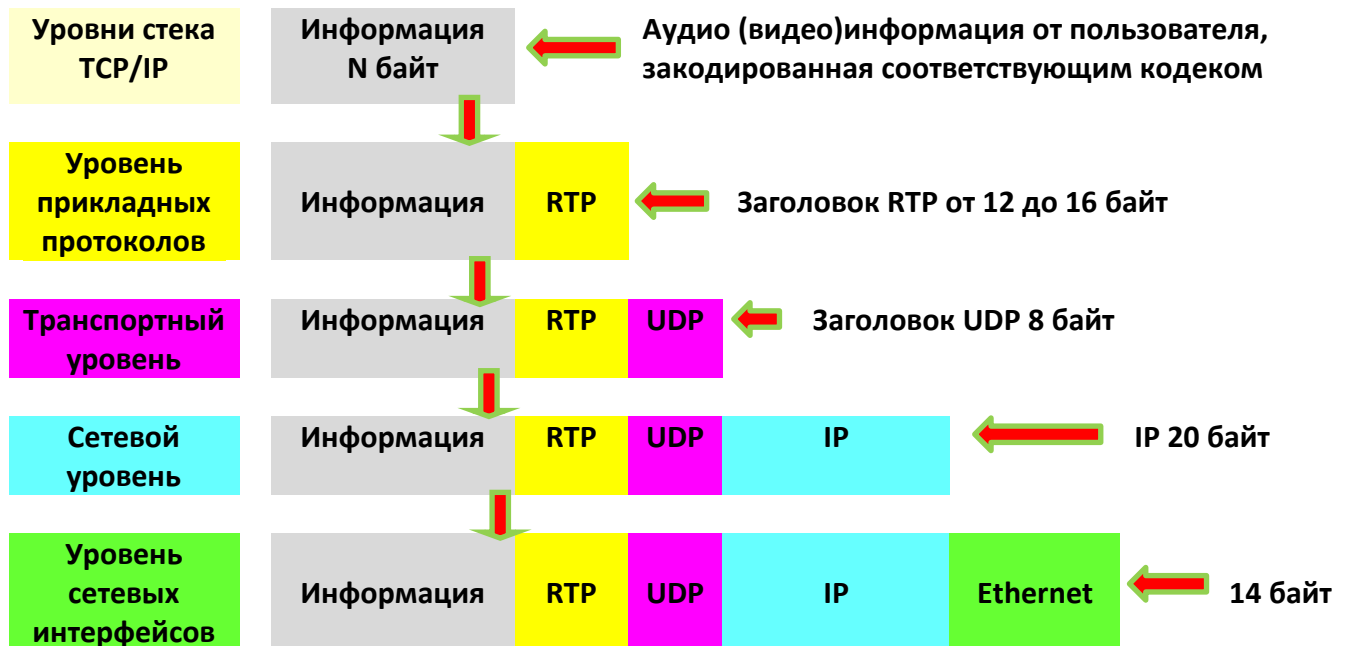
Тот же пакет в представлении анализатора Wireshark:

The screenshot shows the Wireshark interface with a packet capture of an RTP/UDP/IP/Ethernet packet. The packet list shows a packet of 214 bytes. The packet details pane shows the packet structure: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Real-Time Transport Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

RTP/UDP/IP/Ethernet пакет размером 214 байт

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

Annotations from the diagram:

- Заголовок Ethernet 14 байт:** Points to the first 14 bytes of the packet (offset 00 to 0e).
- Заголовок IP 20 байт:** Points to the IP header (offset 0f to 1f).
- Заголовок UDP 8 байт:** Points to the UDP header (offset 12 to 19).
- Заголовок RTP 12 байт:** Points to the RTP header (offset 1a to 23).
- Информация пользователя N байт:** Points to the audio data starting at offset 24.

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 Unique Identifier), 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:

The screenshot shows the Wireshark interface with a packet list and packet details pane. The packet list shows a packet of type Ethernet II. The packet details pane shows the structure of the Ethernet II frame. Callouts highlight the following fields:

- Заголовок Ethernet 14 байт**: Points to the Ethernet II header in the packet details pane.
- MAC-адрес назначения 6 байт**: Points to the Destination MAC address field in the packet details pane.
- MAC-адрес источника 6 байт**: Points to the Source MAC address field in the packet details pane.
- Тип протокола 2 байта**: Points to the EtherType field in the packet details pane.

The packet details pane shows the following structure:

- Ethernet II, Src: Asustek_7e:97:93 (00:18:f3:7e:97:93), Dst: Surecom_2e:b3:7a (00:02:44:2e:b3:7a)
- Destination: Surecom_2e:b3:7a (00:02:44:2e:b3:7a)
- Source: Asustek_7e:97:93 (00:18:f3:7e:97:93)
- Type: IP (0x0800)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000  00 02 44 2e b3 7a 00 18 f3 7e 97 93 08 00 45 00  ..D..Z...E.
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  ..BT.....
0030  1d e0 27 75 6c b3 00 04 04 1f 04 10 18 04 1e 05  ..ul.....
0040  04 07 01 02 00 02 06 ff 61 e1 98 81 8f 83 8d 86  ....a.....
0050  80 9c e2 ff 56 56 52 68 f9 cd e4 f9 92 97 9b 9d  ....VVRH...
0060  93 9b 9a 87 e8 92 7e 66 1f 1b 12 1c 16 17 4a  ....f.....
0070  70 6f 1f 16 0d 0d 02 0b 13 6b 7e ee e5 83 86 82  ....po.....k...
0080  8e 82 86 eb 5e 62 52 e6 dd e0 95 9e 90 84 84 9a  ....AbR.....
0090  86 9c 9d ef 85 91 93 f5 15 7a 04 18 07 10 14 17  ....Z.....
00a0  10 13 12 6c 12 1e 04 06 00 0a 0f 07 4e 5e 87 95  ....l.....NA..
00b0  8b 8a 81 81 90 95 e9 72 14 68 63 46 7e ef ee 9f  ....r.hcFV...
00c0  90 95 95 9b 92 99 ff 9f eb e0 f1 10 76 4a ef 52  ....VJOR....
00d0  7e 62 6c 18 18 17  ....bl...
```

3.2 Поля заголовка протокола IP (20 байт):

[illegible]

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								Длина IP-пакета (дейтаграммы), включая заголовки IP и UDP															
								<table><tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr><tr><td>Приоритет</td><td>D</td><td>T</td><td>R</td><td>C</td><td colspan="3">Не использ.</td></tr></table>																							
0	1	2	3	4	5	6	7																								
Приоритет	D	T	R	C	Не использ.																										
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 01234567 ПриоритетDTRCНе 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																
Идентификатор фрагмента																Флаги		Указатель фрагмента													
7b f8																		00 00													
																0	0	0													
Время жизни (TTL)				Протокол, которому предоставлена услуга								Контрольная сумма заголовка																			
80`hex (128`Dec)				11`hex (17`Dec - UDP)								3b ac																			
IP-адрес отправителя – Source (откуда)																															
C0`hex 192`Dec				A8`hex 168`Dec								00`hex 00`Dec								99`hex 153`Dec											
IP-адрес получателя – Destination (куда)																															
C0`hex 192`Dec				A8`hex 168`Dec								00`hex 00`Dec								97`hex 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 (заголовок 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:

The screenshot shows the Wireshark interface with a packet capture of RTP data. The packet details pane is expanded to show the User Datagram Protocol (UDP) section. A red bracket highlights the UDP header fields: Source port: 8000, Destination port: 16468, Length: 180, and Checksum: 0x14ae. A green callout box with an arrow points to this bracket and contains the text "Заголовок UDP 8 байт".

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

Заголовок RTP
12 байт

```

0000  00 02 44 2e b3 7a 00 18 f3 7e 97 93 08 00 45 00  ..D..Z...E.
0010  00 c8 7b f8 00 00 80 11 3b ac c0 a8 00 99 c0 a8  ..{....f.....
0020  00 97 1f 40 40 54 00 b4 1a ae 80 08 02 4f 00 02  ..8BT...f...0.
0030  1d e0 27 75 6c b3 00 04 04 1f 04 10 18 04 1e 03  ..ul....a.....
0040  04 07 01 02 00 02 06 ff 61 e1 98 81 8f 83 8d 86  ..vWR.....k...
0050  80 9c e2 ff 56 36 32 68 f9 cd e4 f9 92 97 9b 9e  ..f.....N...
0060  93 9b 9a 87 e8 92 7e 66 1f 1b 12 18 1c 16 17 4a  .....f.....
0070  70 6f 1f 16 0d 0d 02 0b 13 6b 7e ee e5 83 86 82  ..po.....k...
0080  8e 82 86 eb 5e 62 32 e6 dd e0 95 9e 90 84 84 9a  .....AbR.....
0090  86 9c 9d ef 85 91 93 f5 15 7a 04 18 07 10 14 17  .....Z.....
00a0  10 13 12 6c 12 1e 04 06 00 0a 0f 07 4e 5e 87 95  .....f.....N...
00b0  8b 8a 81 81 90 95 e9 72 14 68 63 46 7e ef ee 9f  .....f...hCFV...
00c0  90 95 95 9b 92 99 ff 9f eb e0 f1 10 76 4a 6f 52  .....f...VJor...
00d0  7e 62 6c 18 18 17  ..b...
  
```

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 0b 13 6b 7e ee e5 83 86 82
0080	8e 82 86 eb 5e 62 52 e0 dd e0 95 9e 90 84 84 9a
0090	86 9c 9d ef 85 91 93 f5 04 18 07 10 14 17
00a0	10 13 12 6c 12 1e 04 06 00 07 4e 5e 87 95
00b0	8b 8a 81 81 90 95 e9
00c0	90 95 95 9b 92 99 ff
00d0	7e 62 6c 18 18 17

Voice Data, обработанные
кодеком G.111 A-law

4.1 Пример голосовых данных в отображении анализатора Wireshark

The screenshot shows the Wireshark interface with the following details:

- Filter:** rtp
- Packet List:** Shows several RTP packets. Packet 2292 is selected.
- Packet Details:**
 - Frame 2292: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
 - Ethernet II, Src: AsustekC_7e:97:93 (00:18:f3:7e:97:93), Dst: SurecomT_2e:b3:7a (00:02:44:2e:b3:7a)
 - Internet Protocol Version 4, Src: 192.168.0.153 (192.168.0.153), Dst: 192.168.0.151 (192.168.0.151)
 - User Datagram Protocol, Src Port: 16468, Dst Port: 16468
 - Real-time Transport Protocol
 - [Stream setup by SDP (frame 756)]
 - 10... = Version: RFC 1889 version (2)
 - ...0... = Padding: False
 - ...0... = Extension: False
 - ...0000 = Contributing source identifiers count: 0
 - 0... = Marker: False
 - Payload type: ITU-T G.711 PCMA (8)
 - Sequence number: 591
 - [Extended sequence number: 66127]
 - Timestamp: 138720
 - Synchronization source identifier: 0x27756cb3 (662006963)
 - Payload: 0004041f041018041e0504070102000206ff61e19881ef83...
- Packet Bytes:** Shows the raw data of the selected packet, with a red box highlighting the payload data.

Голосовые данные, обработанные
кодеком G.711 A-law