Использование принципов реверс-инжиниринга при автоматизации восстановления видеоданных с поврежденной логической структурой.

Абрамец А.С.

Стационарный видеорегистратор

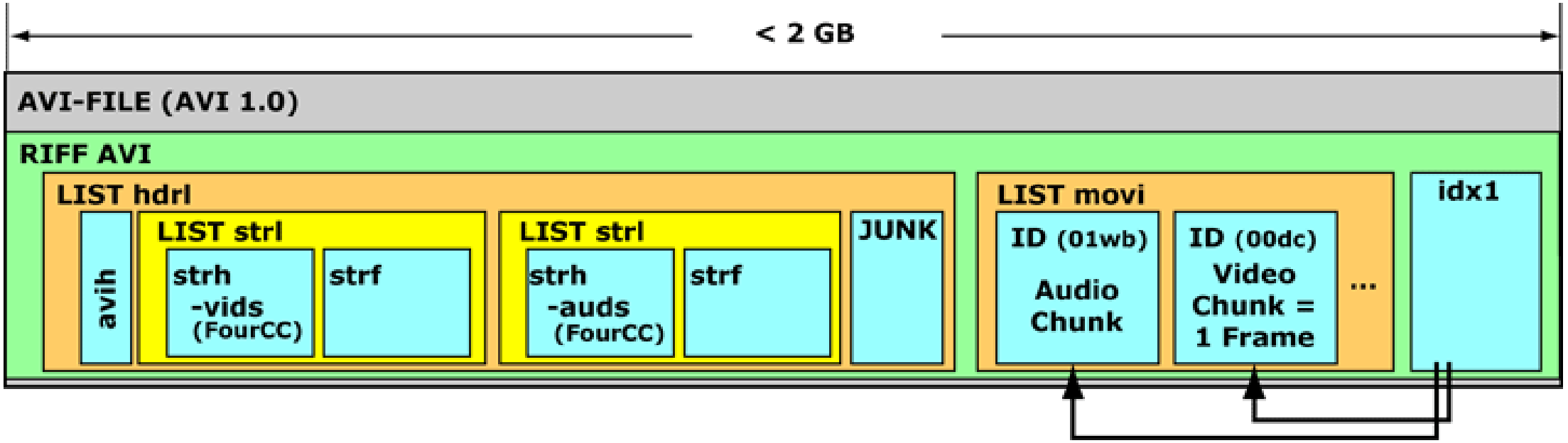
Мобильные устройства с функцией видеозаписи

Типы памяти устройств видеозаписи

SD, microSD

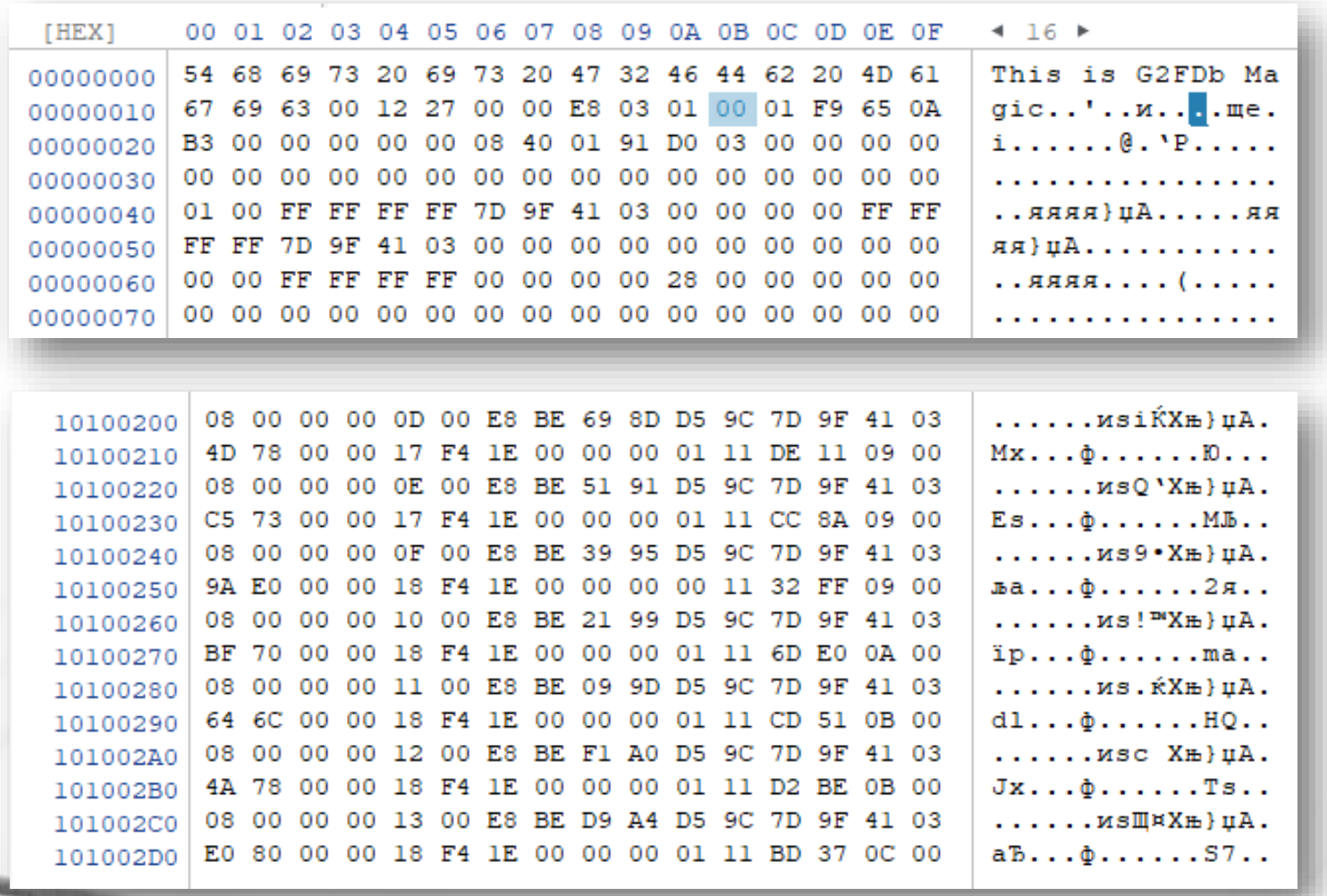
HDD

Структура файла формата AVI



LIST hdrl – header list
Avih – main AVI header
LIST strl – video stream list
strh – video stream header
strf – video stream format
JUNK – BITMAPINFOHEADER
idx1 – блок данных
LIST movi – codec video

Типовая структура размещения данных на накопителях видеорегистраторов



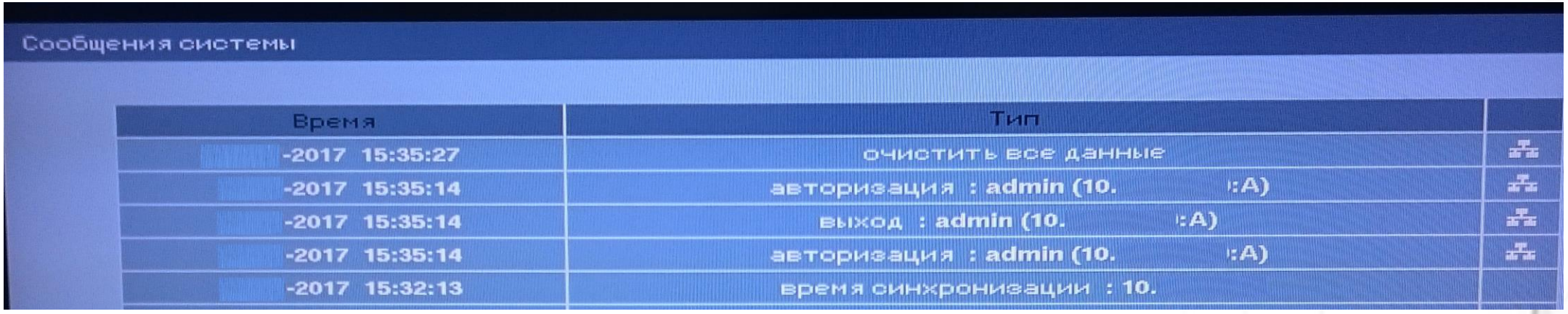
[HEX]	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	◂ 16 ▸
00000000	54 68 69 73 20 69 73 20 47 32 46 44 62 20 4D 61	This is G2FDb Ma
00000010	67 69 63 00 12 27 00 00 E8 03 01 00 01 F9 65 0A	gic..'..и..ù.ще.
00000020	B3 00 00 00 00 00 08 40 01 91 D0 03 00 00 00 00	i......@.‘Р.....
00000030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
00000040	01 00 FF FF FF FF 7D 9F 41 03 00 00 00 00 FF FF	..яяяя}ЏA.....яя
00000050	FF FF 7D 9F 41 03 00 00 00 00 00 00 00 00 00 00	яя}ЏA.....
00000060	00 00 FF FF FF FF 00 00 00 00 28 00 00 00 00 00	..яяяя....(.....
00000070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

Метка видеорегистратора, либо тип файловой системы

10100200	08 00 00 00 0D 00 E8 BE 69 8D D5 9C 7D 9F 41 03	......иsiЌХњ}ЏA.
10100210	4D 78 00 00 17 F4 1E 00 00 00 01 11 DE 11 09 00	Mx...ф......Ю...
10100220	08 00 00 00 0E 00 E8 BE 51 91 D5 9C 7D 9F 41 03	......иsQ‘Хњ}ЏA.
10100230	C5 73 00 00 17 F4 1E 00 00 00 01 11 CC 8A 09 00	Es...ф......МЉ..
10100240	08 00 00 00 0F 00 E8 BE 39 95 D5 9C 7D 9F 41 03	......иs9•Хњ}ЏA.
10100250	9A E0 00 00 18 F4 1E 00 00 00 00 11 32 FF 09 00	ља...ф......2я..
10100260	08 00 00 00 10 00 E8 BE 21 99 D5 9C 7D 9F 41 03	......иs!™Хњ}ЏA.
10100270	BF 70 00 00 18 F4 1E 00 00 00 01 11 6D E0 0A 00	їр...ф......mа..
10100280	08 00 00 00 11 00 E8 BE 09 9D D5 9C 7D 9F 41 03	......иs.ќХњ}ЏA.
10100290	64 6C 00 00 18 F4 1E 00 00 00 01 11 CD 51 0B 00	dl...ф......HQ..
101002A0	08 00 00 00 12 00 E8 BE F1 A0 D5 9C 7D 9F 41 03	......иsc Хњ}ЏA.
101002B0	4A 78 00 00 18 F4 1E 00 00 00 01 11 D2 BE 0B 00	Jx...ф......Ts..
101002C0	08 00 00 00 13 00 E8 BE D9 A4 D5 9C 7D 9F 41 03	......иsЩ¤Хњ}ЏA.
101002D0	E0 80 00 00 18 F4 1E 00 00 00 01 11 BD 37 0C 00	аЂ...ф......S7..

Таблица размещения видеозаписей, т.н. “календарь”

Пример попытки уничтожения данных штатными средствами видеорегистратора



Типовая структура размещения данных на накопителях видеорегистраторов

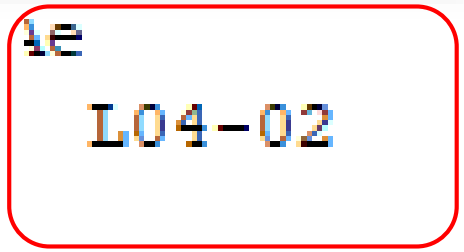
Начало блока видеоданных

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00273678320	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00273678336	F0	F0	00	00	01	00	00	00	00	00	00	00	E2	01	A4	15	ðð â ¤
00273678352	5D	42	00	00	C2	EA	0E	00	06	00	01	11	00	00	00	00	]B Âê
00273678368	D0	02	20	01	06	00	4C	30	34	2D	30	32	00	00	00	00	Ð L04-02
00273678384	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00273678400	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00273678416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00273678432	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00273678448	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00273678464	00	15	1D	FF	FF	0E	00	00	02	91	D0	03	00	2A	00	08	ÿÿ ‘Ð *
00273678480	04	00	64	00	01	00	00	00	00	54	E2	F6	39	55	04	00	d Tâö9U
00273678496	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00273678512	00	00	00	00	00	00	00	00	00	00	00	00	01	61	E0	62	aàb
00273678528	2B	FF	F4	83	7F	C9	37	E6	69	16	8E	5D	B9	4E	4E	F5	+ÿôƒ É7æi Ž]¹NNõ
00273678544	C6	A8	68	22	04	A9	A0	96	DD	2E	66	4A	8F	6D	DB	4F	Æ¨h" © –Ý.fJ mÛO
00273678560	C3	66	A8	19	2C	7C	DD	EC	9E	A3	48	D3	B0	66	AC	D0	Ãf¨ ,|Ýìž£HÓ°f¬Ð
00273678576	27	F5	F1	BD	B2	6F	5B	E7	61	B5	0A	0D	A1	B9	50	21	'õñ½²o[çaµ ¡¹P!
00273678592	13	B3	53	13	97	B5	98	26	3A	4C	D3	57	81	96	03	93	³S –µ&ç:LÓW – “
00273678608	2A	E6	B7	0A	C7	72	FF	76	39	95	51	20	28	22	B9	51	*æ· Çrÿv9•Q ("¹Q
00273678624	FC	13	A4	C3	B5	17	B6	82	A4	EA	E4	A7	B5	21	1B	73	ü ¤Ãµ ¶,¤êä§µ! s
00273678640	34	52	8C	DA	27	04	85	9E	FC	F7	2A	15	64	53	45	B9	4RŒÚ' …žü÷* dSE¹
00273678656	04	21	83	D9	74	04	4D	4C	DB	1B	0D	3E	F9	C9	DC	B6	!ƒÙt MLÛ >ùÉÜ¶
00273678672	5A	2B	DA	9A	AC	89	44	D4	35	AA	35	91	F8	60	91	4D	Z+ÚšŒ‰DÔ5ª5‘ø`‘M
00273678688	8D	54	37	38	9B	3D	EC	69	7E	BD	FF	BA	B4	80	BB	DE	T78›=ìi~½ÿº´€»Þ
00273678704	89	1C	D3	D8	85	A6	0F	A7	41	A4	FC	22	85	F7	77	B1	‰ ÓØ…¦ §A¤ü"…÷w±

Типовая структура размещения данных на накопителях видеорегистраторов

Название видеокамеры

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00273678320	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00273678336	F0	F0	00	00	01	00	00	00	00	00	00	00	E2	01	A4	15	ðð â ¤
00273678352	5D	42	00	00	C2	EA	0E	00	06	00	01	11	00	00	00	00	]B ÂÊ
00273678368	D0	02	20	01	06	00	4C	30	34	2D	30	32	00	00	00	00	Đ L04-02
00273678384	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00273678400	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00273678416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00273678432	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00273678448	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00273678464	00	15	1D	FF	FF	0E	00	00	02	91	D0	03	00	2A	00	08	ÿÿ ‘Đ *
00273678480	04	00	64	00	01	00	00	00	00	54	E2	F6	39	55	04	00	d Tâö9U



Служебные характеристики видеоданных

```
MagicBlockSize = 268435456          # Размер блока видеозаписей
IndexOffsetMagicBlock  = 1024*1024  # Смещение блока индексов в блоке видеоданных
VideoOffsetMagicBlock  = 5120*1024  # Смещение блока видео в блоке видеоданных
CurrentVideoBlock = 1

Count_Video_Block = 3686            # параметр "66 0E" в первом блоке по смещению 5242880
                                    # находятся индексы длиной 64 байта
```

Функция поиска названия камер в «потоке»

```
def CamNameSearch (FileName):
      CurrentVideoBlock = 0
      f = open(FileName, "rb")                          # Открывает файл на поиск названий камер
      print("Файл для поиска названий камер открыт")    #

      #Проверка блоков размером по 256 МБ
      cam_name = []                                     # Список с именами камер
      StopSearch = False
      while CurrentVideoBlock <Count_Video_Block and (not StopSearch):
              CurrentVideoBlock = CurrentVideoBlock + 1
              f.seek (CurrentVideoBlock*MagicBlockSize+VideoOffsetMagicBlock)
              point = f.tell()
              while (point < (CurrentVideoBlock+1)*MagicBlockSize) and (not StopSearch): # пока не кончился блок
                  #поиск видеопотоков
                  Frame_search =True
                  while Frame_search:
                          point = f.tell()
                          buf = f.read (10000)
                          MagicFrame = b'\x00\x00\x01\x67\x64\x00\x1E\xAD'
```

Вывод списка с названиями обнаруженных камер

```
if poz >=0 :
    #print ("найден видео блок по смещению :"+ str(point+poz-148))
    f.seek (point+poz-148)
    idx= f.read(6)
    if idx not in cam_name:
       cam_name.append (idx)
       print ("Добавлена в список  камера :"+ str( idx) + ",  Всего найдено камер - " + str(len (cam_name)))
f.seek (point+9990)
if point > (CurrentVideoBlock+1)*MagicBlockSize :
    Frame_search = False
if len(cam_name)>=16 :   #  !!!! ОГРАНИЧЕНИЕ количества камер для ускорения поиска
    Frame_search = False # искать больше не надо
    StopSearch = True
```

Благодарю за внимание!