

Экспертиза видео и аудио Готовим доказательства для суда

Спикеры



Юрий Баркалов

- **Руководитель** направления экспертиз технического департамента
- **Полковник** МВД РФ в отставке
- **Экспертная** работа с 1993 года



Фёдор Музалевский

- **Директор** технического департамента **RTM Group**
- **Кандидат** физико-математических наук
- **Профессиональный опыт** с 2006 года



О компании RTM Group

RTM Group — ведущая консалтинговая компания в области информационной безопасности, судебной экспертизы и ИТ-права.

Информационная безопасность:

Аудиты, пентест, КИИ, защита
ПДн, оценка защищённости и др.

Компьютерно-технические экспертизы:

44-ФЗ, расследования
инцидентов, ИТ-контракты и др.

ИТ-право:

Судебное и досудебное
урегулирование, сопровождение
и др.

СОДЕРЖАНИЕ

- 01** **Когда нужна** экспертиза аудио и видео
- 02** **Дословное содержание** аудио и видеозаписи
- 03** **Поиск монтажа** и проверка подлинности
- 04** **Очистка шумов** звука и покадровый просмотр видео
- 05** **Идентификация** устройства записи
- 06** **Что может и не может** быть объектом исследования
- 07** **Восстановление** удалённых данных
- 08** **Восстановление** данных с повреждённых устройств
- 09** На какие вопросы эксперты ответить **не могут**

1. Когда нужна экспертиза аудио и видео

- **Уголовные** дела
- **Арбитражные** дела
- **Гражданские** дела
- **Досудебное** урегулирование споров
- **Споры** с контрагентом
- **Трудовые** разногласия
- **Семейные** споры



2. Дословное содержание аудио и видеозаписи

M1: «Добрый вечер!»

M2: «Здравствуйте, я хотел поговорить по поводу взятки»

M1: «Хорошо, давайте поговорим»

M2: «[неразборчиво] как в прошлый раз, два миллиона»

Идентификация дикторов:

1. По полу
2. По обращениям в разговоре
3. Со слов заявителя экспертизы

Вопросы эксперту:

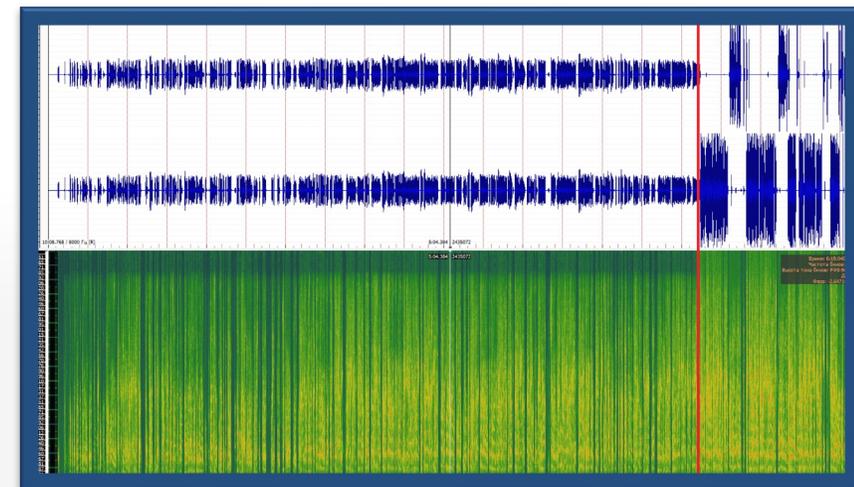
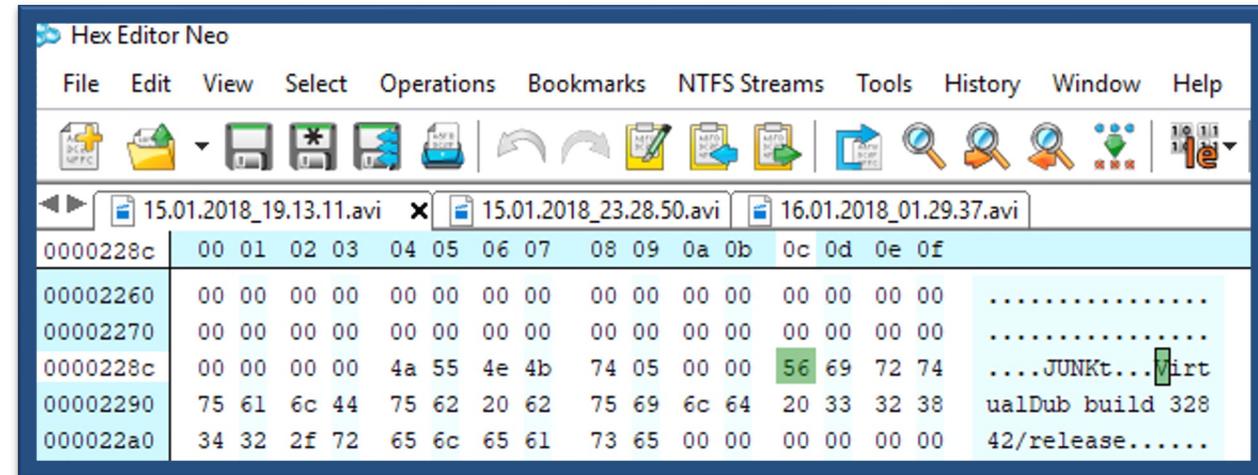
1. Каково дословное содержание разговора?
2. Сколько дикторов участвует в разговоре?



3. Поиск монтажа и проверка подлинности

Вопросы эксперту:

- «Имеются ли признаки монтажа в представленной аудио/видео записи?»
- «Является ли запись подлинной?» – *неверный вопрос!*



4. Очистка шумов звука и покадровый просмотр видео

Задачи:

- Предоставление в суд
- Самостоятельный анализ
- Предоставление экспертам других специальностей

Вопросы эксперту:

- «Как повысить разборчивость речи аудиозаписи?»
- «Какие кадры видеоизображения находятся на мм.сс.мс видео?»
- «Какие кадры видеоизображения находятся между мм.сс1 и мм.сс2 видео?»

Важно

В некоторых случаях повысить разборчивость речи невозможно.



5. Идентификация устройства записи

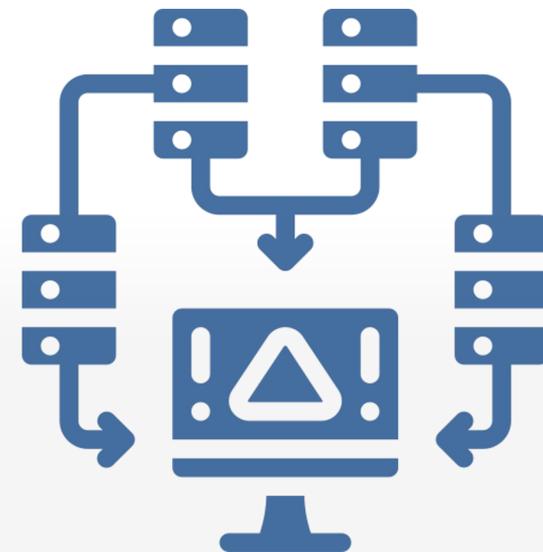
- **По бинарным** данным заголовка файла
- **По особенностям** микрофона записывающего устройства
- **По служебным** гармоникам (для отдельных моделей диктофонов)

Вопросы эксперту

- «На каком классе устройств (модели устройств) создана аудио/видео запись?»
- «Какими особенностями обладает устройство, при помощи которого создана аудио/видео запись?»

Важно

В некоторых случаях идентифицировать устройство невозможно.



6. Что может, а что не может быть объектом исследования

Может:

- Аудио или видеозапись (на любом носителе/ресурсе)
- Смартфон/диктофон/камера

Не может:

- Магнитная пленка
- Виниловая пластинка



7. Восстановление удаленных данных

- **Обычно** необходимо восстановить данные с flash-накопителя, это, как правило, формат FAT32.

The screenshot displays a hex editor window with a file system entry for 'AF387-1 XLS'. The entry is shown in hexadecimal and ASCII. Several fields are highlighted in red, including the file name 'AF387-1 XLS', the file size '60L', and the file type 'XLS'. The hex editor shows the following data:

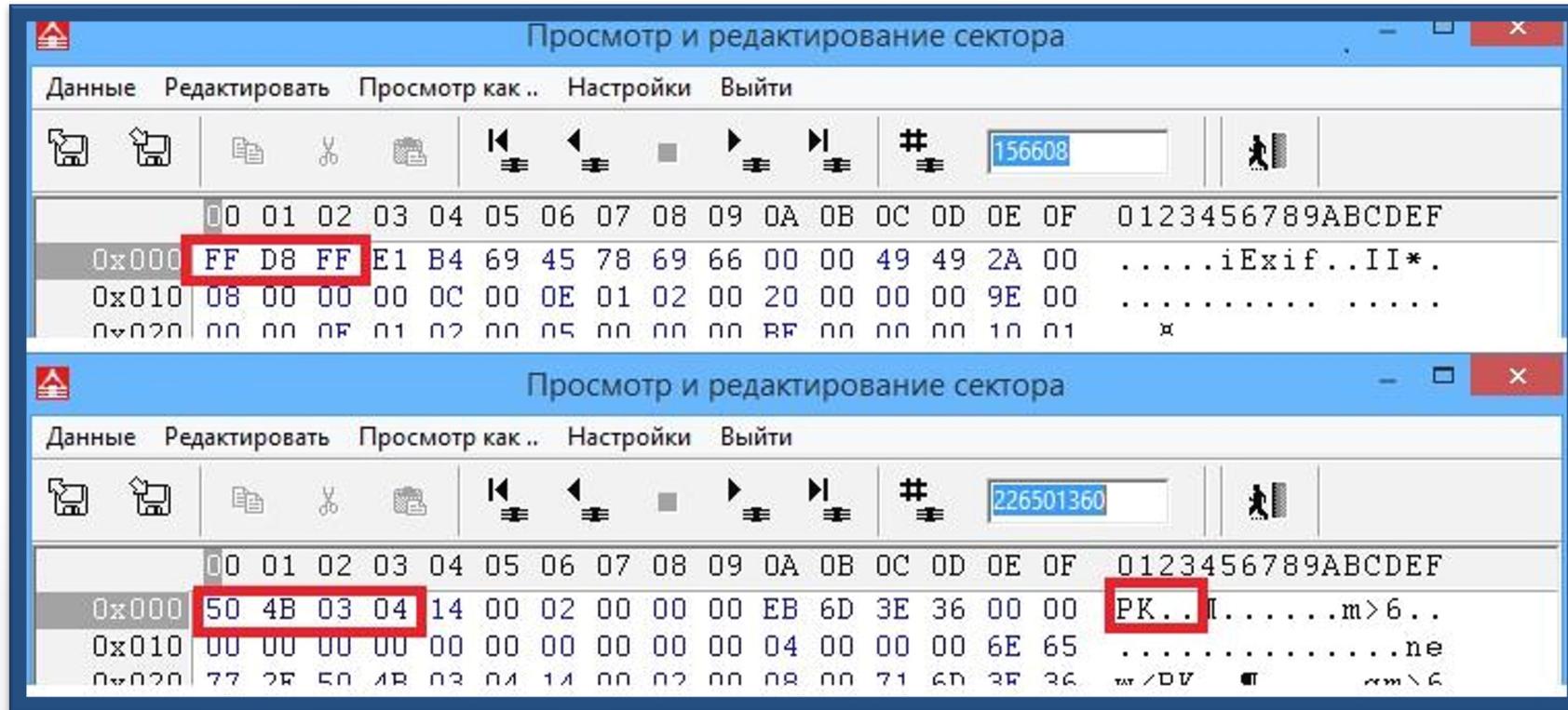
Address	Hex	ASCII
0003E070	DD 52 DD 52 00 00 20 4A DD 52 02 00 00 00 00 00	IRIK ,DIR
0003E080	E5 31 00 2E 00 78 00 6C 00 73 00 0F 00 41 78 00	ã1 . x 1 s Ax
0003E090	00 00 FF FF FF FF FF FF FF FF 00 00 FF FF FF FF	YYYYYYYY YY
0003E0A0	E5 46 33 38 37 7E 31 20 58 4C 53 20 00 36 30 4C	AF387-1 XLS 60L
0003E0B0	DD 52 DD 52 00 00 E0 5D C9 52 05 00 F7 17 00 00	YRIR aJER +
0003E0C0	E5 7E 00 24 00 31 00 2E 00 78 00 0F 00 36 6C 00	ã~ \$ 1 . x 61
0003E0D0	73 00 78 00 00 00 FF FF FF FF 00 00 FF FF FF FF	s x YYY YYY
0003E0E0	E5 24 31 7E 31 20 20 20 58 4C 53 22 00 1A 32 4C	ã\$1-1 XLS" 2L
0003E0F0	DD 52 DD 52 00 00 39 4C DD 52 06 00 A5 00 00 00	YR YR 9LYR Y
0003E100	E5 46 44 31 30 30 30 30 20 20 20 20 00 36 30 4C	ãFD10000 60L
0003E110	DD 52 DD 52 00 00 39 4C DD 52 07 00 6B 20 00 00	YR YR 9LYR k
0003E120	E5 41 41 31 42 42 38 31 54 4D 50 20 10 36 30 4C	ãAA1BB81TMP 60L
0003E130	DD 52 DD 52 00 00 E0 5D C9 52 05 00 F7 17 00 00	YR YR aJER +
0003E140	E5 31 00 2E 00 78 00 6C 00 73 00 0F 00 41 78 00	ã1 . x 1 s Ax

On the right side of the hex editor, there is a status bar with the following information:

- Режим: hex
- Смещения: hex
- Байт в странице: 51x16=816
- Окно №: 1
- Кол-во окон: 2
- Буфер обмена: доступно
- Каталог TEMP: 178 GB свободно
- Users\Expert\AppData\Local\Temp

7. Восстановление удаленных данных

- Видеоизображение с видеорегистратора можно восстановить как набор JPG файлов.

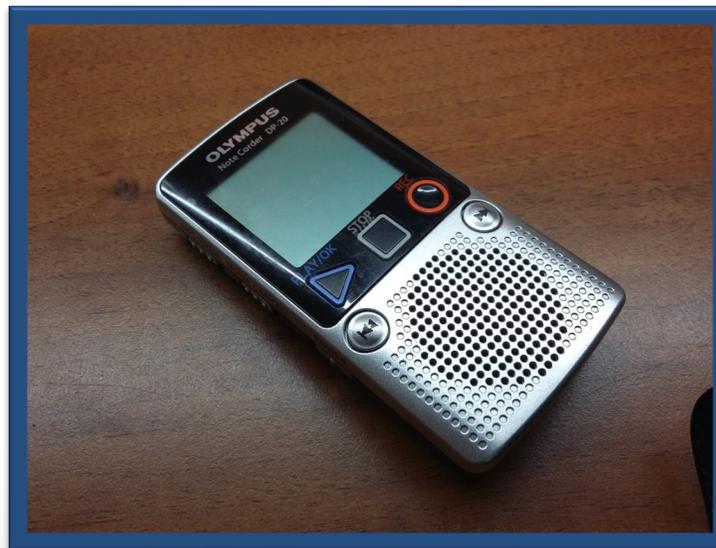


8. Восстановление данных с поврежденных устройств

- **Даже в случае сильного повреждения** устройства всегда есть шанс восстановить сохранённые на нём данные.



Повреждённая карта памяти



Повреждённый диктофон



Память повреждённого диктофона

9. На какие вопросы эксперты ответить не могут?

- **Дата и место создания файла** (данные опираются на данные записывающего устройства) предоставление устройства.
- **Поведенческие особенности дикторов** (выходит за рамки технической экспертизы) проверка на аутентичность для передачи экспертам других специальностей.



ГОТОВЫ ОТВЕТИТЬ НА ВАШИ ВОПРОСЫ!

Юрий Баркалов

Руководитель направления судебных экспертиз **RTM Group**

Фёдор Музалевский

Директор технического департамента **RTM Group**



+7 (495) 197-64-95



info@rtmtech.ru



<https://rtmtech.ru>



[rtm.group](https://vk.com/rtm.group)



t.me/kurilka_ib