Бояров А.Г.
старший эксперт ЛСЭВиЗ ФБУ РФЦСЭ при Минюсте России

СПОСОБЫ ВЫЯВЛЕНИЯ ПРИЗНАКОВ ИЗМЕНЕНИЙ ВИДЕО- И ЗВУКОЗАПИСЕЙ, ПРОИЗВЕДЁННЫХ ПОСЛЕ ПРОЦЕССА ЗАПИСИ, НА ЦИФРОВЫХ НАКОПИТЕЛЯХ С ФАЙЛОВЫМИ СИСТЕМАМИ FAT16 И FAT32

(МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ЭКСПЕРТОВ)

В работе приведены методы и средства анализа цифровых накопителей информации с файловыми системами FAT16 или FAT32 с целью выявления признаков изменения видео- и звукозаписей, произведённых после завершения процесса записи. Рассмотрены следующие виды изменений: нарушения закономерностей размещения данных на цифровых накопителях, нарушения закономерностей формирования временных атрибутов файлов и их последовательностей, нарушения особенностей заполнения имён файлов, наличие удалённых файлов, свидетельствующих об использовании программ редакторов.

Ключевые слова: криминалистическая экспертиза видео- и звукозаписей, исследование цифровых устройств видео- и звукозаписей, файловые структуры FAT16 и FAT32.

A. Boyarov
Senior forensic examiner, Laboratory of Video and Audio Forensics
Russian Federal Center of Forensic Science of the Russian Ministry of Justice

DETECTING POST-PRODUCTION TAMPERING ARTIFACTS IN VIDEO AND AUDIO RECORDINGS ON FAT16 AND FAT32 FORMATTED STORAGE DEVICES

(METHODOLOGY RECOMMENDATIONS FOR FORENSIC PRACTITIONERS)

Abstract. This article represents tools and methods for authenticity analysis of video and audio recordings stored on FAT16 or FAT32 digital media storages. Different types of editing are taken into consideration: breaches of media data allocation order, media files and their sequences creation and modification date and time attributes disorder, naming features mismatch, search for deleted data proving sound/video editors usage.

Keywords: forensic video examination, forensic audio examination, forensic digital data analysis, data forensics, FAT16 and FAT32 features.

Автор выражает благодарность Липатову Алексею Анатольевичу и Байрамовой Фирузе Оруджевне за помощь в проведении исследований и написании данной работы.

Введение

В настоящее время всё большее количество фонограмм и видеофонограмм, содержащих значимую для расследования правонарушений информацию, поступает на экспертное исследование в файлах на цифровых носителях – накопителях информации, встроенных в устройства записи, или в виде сменных карт памяти различных форматов.

Как показывает практика, для проведения всестороннего исследования необходимо проводить анализ не только аудио- и видеосигналов, но и структуры файлов, их содержащих, а также файловой системы цифровых накопителей устройств видео- и звукозаписи, на которых эти файлы представлены (об этом см. [1]). Настоящая работа посвящена поиску признаков изменения записи, которые могут быть обнаружены при исследовании цифровых накопителей устройств записи, содержащих разделы с файловой системой FAT16 или FAT32.

Структура файловых систем FAT16 и FAT32

Исследование предваряет краткая теоретическая часть, состоящая из основных терминов и описания основ размещения данных в файловых структурах FAT16 и FAT32. При составлении данной части работы использовался материал, изложенный в [2] и адаптированный для данного исследования.

1.1. Основные термины

Накопитель цифровой информации – запоминающее устройство, предназначенное для долговременного хранения цифровой информации, основанное, как правило, на использовании энергонезависимой твердотельной памяти или жёсткого магнитного диска.

FAT (File Allocation Table) – таблица размещения файлов. Также термином FAT с добавлением разрядности адресации (например, FAT12, FAT16, FAT32) называются файловые системы, построенные на базе данной таблицы.

Файл (англ. file) – именованная область на накопителе информации, предназначенная для хранения информации.

Файловая система (англ. file system) – порядок, определяющий способ организации, хранения и именования данных на накопителях информации. Файловая система:

- определяет способ хранения файлов на накопителе;
- определяетспособхраниядополнительнойслужебнойинформации,например, файловых атрибутов или сведений о поврежденных элементах памяти, не пригодных для хранения данных исследуемого накопителя;
- можетпредоставлятьдополнительныевозможности,например,разграничение доступа к информации или её шифрование.

Сектор – минимальный адресуемый на физическом уровне блок информации накопителя.

Кластер – минимальный адресуемый блок информации накопителя в файловых системах семейства FAT. Кластер обычно состоит из 2^N секторов, где может принимать значения N=0,1,2,... .

Раздел – логически выделенная и состоящая из смежных секторов область данных накопителя. Разделы бывают основными и дополнительными.

1.2. Главный загрузочный сектор

В нулевом секторе большинства встречающихся в экспертной практике накопителей цифровой информации (далее – накопителей) присутствует главная загрузочная запись, далее в тексте обозначенная как MBR (от англ. Master Boot Record). MBR содержит три основные части: загрузочный код, таблица разделов и сигнатура (Таблица 1).

Загрузочный код получает управление при использовании накопителя в качестве загрузочного устройства. В общем случае, если код и данные не помещаются в одном секторе, то код главного загрузочного сектора обеспечивает загрузку данных в память остальных секторов MBR. В этом случае MBR представляет собой совокупность всех секторов, которые должны быть загружены.

Таблица 1. Структура данных первого сектора MBR

Смещение от начала сектора	Описание	
0-445 байты	Загрузочный код	
446-461 байты	Таблица разделов	Запись таблицы разделов № 1
462-477 байты		Запись таблицы разделов № 2
478-493 байты		Запись таблицы разделов № 3
494-509 байты		Запись таблицы разделов № 4
510-511 байты	Сигнатура 0xAA55 (43605 в десятичной системе счисления)	

В случае когда накопитель не предназначен для осуществления запуска с него каких-либо устройств, то заполнение области загрузочного кода не является обязательным и наличие какой-либо информации в указанной области может являться одним из индивидуализирующих признаков устройства и программного обеспечения, производившего формирование логической структуры исследуемого накопителя.

Таблица разделов содержит сведения о четырёх основных разделах накопителя. В каждой записи таблицы разделов зафиксирована информация, которая приводится в таблице 2.

Таблица 2. Структура данных записи таблицы разделов

Смещение от начала записи в таблице разделов	Описание
0-0	Флаг загрузочного раздела
1-3	Начальный адрес CHS[1]
4-4	Тип раздела
5-7	Конечный адрес CHS
8-11	Начальный адрес LBA
12-15	Размер в секторах

Сигнатура главного загрузочного сектора используется для проверки корректности данных. В случае если сигнатура имеет неправильное значение, все сведения игнорируются и разделы не определяются.

1.3. Структура раздела с файловой системой FAT16 и FAT32

Любой раздел, имеющий файловую систему FAT, делится на три физические области (рис. 1).

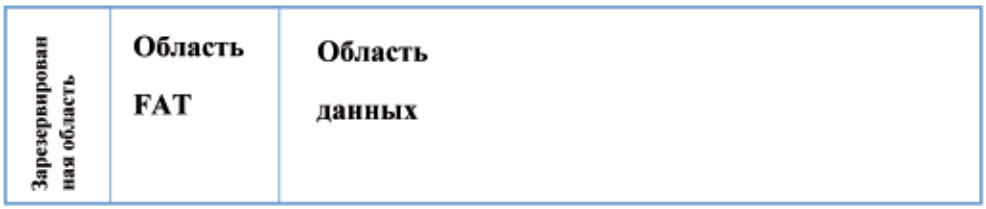

Рис. 1. Три основные области раздела с файловой системой семейства FAT.

Первая область называется «Зарезервированная область». В ней хранятся данные загрузочной записи раздела и её копии. Для файловой системы FAT32 в зарезервированной области может храниться блок данных FSInfo, который содержит сведения о свободном дисковом пространстве: первый свободный кластер и количество свободных кластеров. Значения полей зарегистрированной области данных приведены в Таблица 3.

Таблица 3. Данные загрузочной записи раздела с файловой системой FAT16 и FAT32

FAT16	FAT32	Описание
0-2	0-2	Команда ассемблера перехода к загрузочному коду
3-10	3-10	Имя OEM в кодировке ASCII
11-12	11-12	Количество байтов в секторе. Допустимые значения 512, 1024, 2048, 4096
13	13	Количество секторов в кластере
14-15	14-15	Размер зарезервированной области в секторах
16	16	Количество копий FAT
17-18	17-18	Максимальное количество файлов в корневой директории для FAT16. В FAT32 поле=0, а в FAT16=512
19-20	19-20	16-разрядное количество секторов в файловой системе. 0 – если нельзя представить 2 байтами (количество в байтах 32-35)
21	21	Тип накопителя 0xf8 – стационарный диск, 0xf0 – съёмный диск
22-23	22-23	16-разрядный размер (в секторах) каждой копии FAT в FAT16. Для FAT32 равно 0.
24-25	24-25	Количество секторов в дорожке
26-27	26-27	Количество головок
28-31	28-31	Количество секторов перед началом раздела
32-35	32-35	32-разрядное количество секторов в файловой системе. 0 – если можно представить 2 байтами (количество в байтах 19-20)
Отсутствуют	36-39	32-разрядный размер одной копии FAT
	40-41	Режим обновления нескольких сигнатур FAT. Если бит 7 равен 1, активна одна копия FAT, индекс которой определён разрядами 0-3. В противном случае все структуры FAT являются зеркальными копиями друг друга
	42-43	Основной и дополнительный номер версии
	44-47	Кластер, в котором находится первая запись корневой директории
	48-49	Сектор, в котором находится структура FSINFO
	50-51	Сектор, в котором находится резервная копия загрузочного сектора (обычно 6)
	52-63	Зарезервировано
36	64	Идентификатор подключения диска BIOS
38	66	Расширенная сигнатура, которая показывает, действительны ли следующие три значения (должна быть 0x29)
39-42	67-70	Серийный номер тома
43-53	71-81	Метка тома в кодировке ASCII
54-61	82-89	Метка типа файловой системы в кодировке ASCII (FAT32)
510-511	510-511	Сигнатура 0xAA55

Вторая область называется **«Область FAT».** Она содержит основные и резервные структуры FAT. Она начинается в секторе, следующем за зарезервированной областью, а её размер определяется количеством и размером структур FAT.

Таблица FAT занимает центральное место в одноимённой файловой системе. Она предназначена для определения, занят ли кластер или свободен, и для поиска следующего выделенного кластера файла или директории. Обычно в файловой системе FAT хранятся две копии FAT, но их точное количество указывается в MBR. Размер каждой копии FAT также хранится в загрузочной записи. Первая копия FAT начинается после зарезервированной области. Вторая копия FAT (если она существует) начинается в следующем секторе за первой копией.

Таблица FAT состоит из записей одинакового размера и не содержит ни служебных заголовков, ни маркеров завершения. Размер записи отдельной записи таблицы зависит от версии файловой системы. В FAT16 – 16-разрядные записи, в FAT32 – 32-разрядные.

Адресация записей начинается с 0. Каждая запись соответствует кластеру с тем же адресом, за исключением кластеров 0 и 1. Если кластер свободен, его запись равна 0.

Записи выделенных кластеров отличны от нуля и содержат адрес следующего кластера в файле или директории. Если кластер завершает цепочку файла или директории, в его записи содержится маркер конца файла: в FAT16 – 0xfff8, в FAT32 – 0x0fff. Если запись содержит значение 0xfff7 в FAT16 или 0x0fff fff7 в FAT32, кластер помечен как повреждённый и не должен выделяться системой.

Адресация кластеров файловой системы начинается с 2. Это означает, что записи 0 и 1 в структуре FAT не используются. Обычно в записи 0 хранится копия типа накопителя, а в записи 1 – статус обновления файловой системы. Статус обновления может использоваться для идентификации ошибок демонтирования файловых систем (некорректное отключение) или аппаратных ошибок накопителя.

Третья область – **«Область данных».** Она содержит кластеры, выделяемые для хранения файлов и записей директорий.

Одной из отличительных особенностей файловой системы FAT32 является то, что записи корневой директории могут располагаться в любом кластере области данных, при этом положение первого кластера записей корневой директории указано в загрузочной записи раздела, а область данных начинается сразу же за последней таблицей FAT.

В файловой системе FAT16 записи корневой директории размещаются сразу же за областью FAT. Размер области определяется по максимальному числу файлов в корневой директории, указанному в загрузочной записи раздела. За областью данных, содержащих описание корневой директории, следуют данные кластера с номером 2. Таким образом, записи корневой директории находятся не в области данных, как у FAT32, а размещаются отдельно.

Записи директории для одного файла или поддиректории представляют собой набор параметров, занимающих 32 байта. При этом имя файла или поддиректории соответствует структуре коротких имён по схеме «8+3» (8 символов имени, 3 символа расширения). Современные операционные системы оперируют более длинными именами, для хранения которых в дополнение к обычной записи директории (далее обозначенной как SFN – от англ. Small File Name) создаются одна или несколько записей LFN (от англ. Long File Name). Данные, хранящиеся в SFN-записи директории, приведены в Таблица 4.

Таблица 4. Структура SFN-записи директории FAT

Диапазон	Описание	Необходимость
0-0	Первый символ имени файла в кодировке ASCII и состояние выделения 0xe5 или 0x00, если запись не выделена	Да
1-10	Символы 2-11 имени файла в кодировке ASCII	Да
11-11	Атрибуты файла (см. Таблица 5)	Да
12-12	Зарезервировано	Нет
13-13	Время создания (сотые доли секунды)	Нет
14-15	Время создания (часы, минуты, секунды)	Нет
16-17	День создания	Нет
18-19	День последнего обращения	Нет
20-21	Старшие 2 байта адреса первого кластера 0 для FAT16	Да
22-23	Время последней записи (часы, минуты, секунды)	Нет
24-25	День последней записи	Нет
26-27	Младшие 2 байта адреса первого кластера	Да
28-31	Размер файла. Для директории должно быть 0	Да

Первый байт структуры данных используется как признак выделения. Если он равен 0xe5 или 0x00, то запись директории свободна. В противном случае байт содержит первый символ имени файла. Как правило, имена файлов задаются в кодировке ASCII, но они также могут содержать символы национальных алфавитов, для чего используются кодовые страницы Microsoft. Если в этом байте имени файла содержится символ 0xe5, вместо него используется код 0x05. Если имя файла короче 8 символов, неиспользуемые байты обычно заполняются ASCII-кодом пробела 0x20. Поле размера файла занимает 4 байта, следовательно, максимальный размер файла – 4 ГБ. У директории поле размера равно 0. Для определения количества выделенных под записи директории кластеров следует использовать таблицу FAT. Поле атрибутов содержит один или несколько флагов, перечисленных в таблице 5.

Таблица 5. Файловые атрибуты, хранящиеся в SFN-записи директории FAT

Флаг	Описание	Необходимость
0000 0001 (0x01)	Доступ только для чтения	Нет
0000 0010 (0x02)	Скрытый файл	Нет
0000 0100 (0x04)	Системный файл	Нет
0000 1000 (0x08)	Метка тома	Да
0000 1111 (0x0f)	Длинное имя файла	Да
0001 0000 (0x10)	Директория	Да
0010 0000 (0x20)	Архивный файл	Нет

Следует иметь в виду, что атрибут длинного имени представляет собой поразрядную комбинацию первых четырёх атрибутов.

Компонент даты во временных штампах представляет собой 16-разрядное значение, состоящее из трёх частей (см. [2]). Младшие 5 бит определяют день месяца (диапазон допустимых значений 1-31). Биты 5-8 определяют месяц (допустимые значения 1-12). Биты 9-15 определяют год (их значение прибавляется к 1980). Диапазон допустимых значений 0-127 позволяет представлять годы с 1980 по 2107.

Рис. 2. Схема представления даты во временных штампах файловой системы FAT

Время также задаётся 16-разрядной величиной, состоящей из трёх компонентов. Пять младших битов определяют секунды (измеряемые в 2-секундных интервалах). Диапазон допустимых значений 0-29 позволяет представить значение секунд в диапазоне 0-58 с двухсекундными интервалами. Следующие 6 бит определяют минуты (допустимые значения 0-59). Последние 5 бит определяют часы (допустимые значения 0-23). Структура поля времени продемонстрирована на рис. 3.

В файловой системе FAT для более точной регистрации времени создания файла отведён еще один байт, содержащий сотые доли секунд (см. Таблица 4).

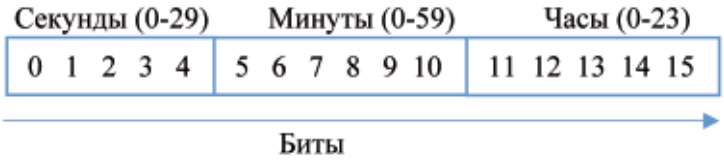

Рис. 3. Схема представления времени во временных штампах файловой системы FAT

Учитывая особенности представления времени, можно определить точность представления временных атрибутов в файловой системе FAT:

1) время создания файла может быть представлено с точностью до сотых долей секунды;

2) время последнего изменения файла – с точностью до двух секунд;

3) дата последнего обращения к файлу – с точностью до одного дня.

Если имя файла/директории имеет большую длину или содержит специальные символы, для него требуются особые записи директории – записи LFN. Помимо записей LFN для файла также создаётся обычная запись, причем записи LFN должны предшествовать обычной записи. Поля LFN-версии записи директории перечислены в таблице 6.

Таблица 6. Файловые атрибуты, хранящиеся в LFN-записи директории FAT

Диапазон	Описание	Необходимость
0-0	Порядковый номер и признак выделения (0xe5, если запись свободна)	Да
1-10	Имя файла, символы 1-5 (Unicode)	Да
11-11	Атрибуты файла (0x0f)	Да
12-12	Зарезервировано	Нет
13-13	Контрольная сумма	Да
14-25	Имя файла, символы 6-11 (Unicode)	Да
26-27	Зарезервировано	Нет
28-31	Имя файла, символы 12-13 (Unicode)	Да

Поле порядкового номера LFN-записи файла содержит счётчик записей, необходимых для хранения имени файла. Первой записи соответствует порядковый номер 1. Порядковый номер увеличивается на единицу для каждой последующей записи LFN вплоть до последней, в которой он объединяется со значением 0x40 поразрядной операцией OR. При выполнении этой операции результат содержит «1» во всех разрядах, в которых хотя бы один из двух операндов содержит «1».

Записи LFN располагаются в обратном порядке перед записью короткого имени файла. Следовательно, первая запись, находящаяся в директории, является последней записью LFN для файла и имеет наибольший порядковый номер.

Неиспользуемые символы дополняются кодами 0xff, а имя завершается символом 0x00 (NULL) при наличии свободного места. В поле атрибутов записи LFN должно быть указано 0x0F.

Контрольная сумма (см. таблицу 6) вычисляется с использованием короткого имени файла и должна быть одинаковой для всех записей LFN. Если контрольная сумма записи LFN не совпадает с контрольной суммой соответствующего короткого имени, то возможной причиной этого является повреждение каталога при использовании ОС, не поддерживающих длинные имена. Алгоритм вычисления контрольной суммы перебирает символы имени, на каждом шаге сдвигает текущую контрольную сумму на один бит вправо и прибавляет ASCII-код следующей буквы [2].

1.4. Размещение данных в файловых системах FAT16 и FAT32

В файловых системах FAT16 и FAT32 данные файла считываются из накопителя путём выполнения определённой последовательности действий. Например, для файла с именем x:\Dir_level1\Dir_level2\File.dat данная последовательность будет состоять из следующих действий (рис. 4):

1. По главной записи раздела накопителя с логическим именем X определяется адрес блока записей корневой директории.

2. В корневой директории производится поиск записи о директории с информацией о Dir_level1. Из записи о директории Dir_level1 извлекается номер первого кластера N1 – блока данных, в котором хранятся записи о поддиректории и файлах директории.

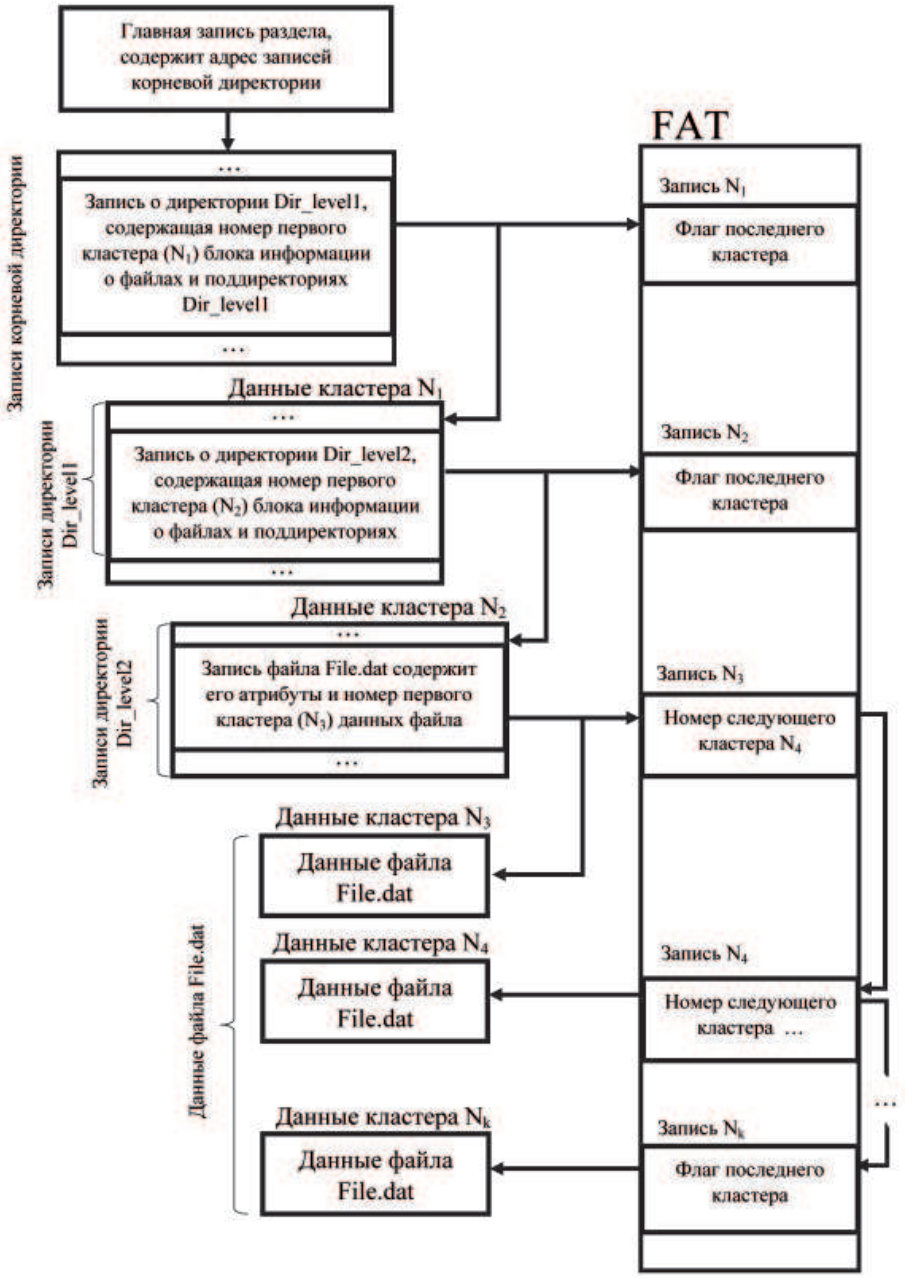

Рис.4. Схема получения данных файла x:\Dir_level1\Dir_level2\File.dat в файловых системах FAT16 или FAT32

3. В записях директории Dir_level1 производится поиск записи о директории Dir_level2 (в примере для упрощения записи директории Dir_level1 занимают один кластер, в реальности записи директории могут занимать несколько кластеров). Из записи о директории Dir_level2 извлекается номер первого кластера N2 – блока данных, в котором хранятся записи о поддиректории и файлах директории.

4. В записях директории Dir_level2 ищется запись о файле File.dat. В данной записи хранятся атрибуты файла, даты его создания, изменения, просмотра, размер и номер первого кластера файла N3 (см. таблицы 4, 5, 6).

5. Считываются данные из первого кластера файла N3. Далее в таблице FAT проверяется значение в ячейке N3. Если в ячейке хранится «флаг» последнего кластера, то считывание данных завершается, иначе ячейка содержит номер следующего кластера файла. Так, в нашем примере ячейка содержит номер кластера N4. Считывание блоков данных файла продолжается по цепочке кластеров, указанных в таблице FAT, до того момента, пока не встретится ячейка с «флагом» последнего кластера.

2. Исследование накопителей устройств видео- и звукозаписи с файловыми системами FAT16 и FAT32

При проведении исследований был выявлен ряд особенностей типовых элементов и структур данных файловых систем семейства FAT, которые формировались различными устройствами видео- и звукозаписи.

Эти особенности можно объединить в следующие группы:

1) особенности размещения данных в цепочке кластеров, которые можно выявить при анализе таблицы FAT;

2) особенности заполнения временных атрибутов файлов и директорий;

3) особенности заполнения имён файлов.

Криминалистически значимой является информация, содержащаяся в файлах, хранящихся на носителе вместе с подлежащими исследованию видео- и звукозаписями, а также информация о ранее удалённых файлах.

2.1. Особенности размещения файлов в цепочке кластеров, которые можно выявить при анализе таблицы FAT

В большинстве случаев файл располагается в кластерах накопителя, последовательно следующих друг за другом. Такая непрерывная цепочка кластеров на схемах, представленных ниже, будет изображена в виде отдельного блока (рис. 5).

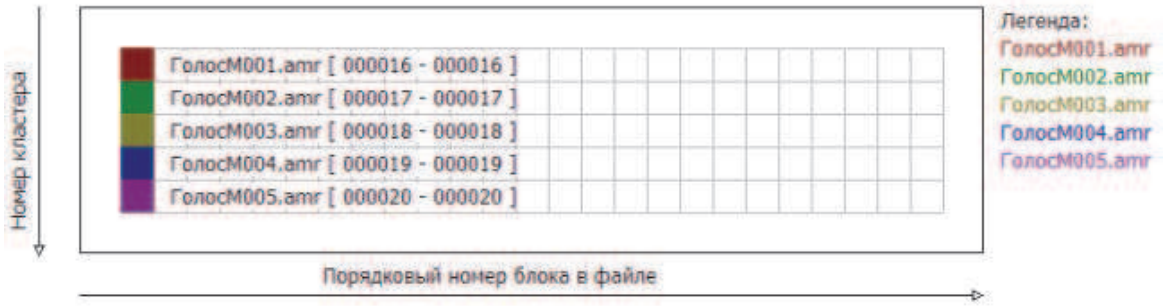

Рис. 5. Размещение шести нефрагментированных файлов, следующих друг за другом, каждый из которых занимает один блок кластеров

Когда при записи на накопителе нет непрерывного диапазона свободных кластеров для размещения файла, то производится фрагментация файла: он располагается последовательно в нескольких блоках кластеров, между которыми могут находиться другие данные (рис. 6).

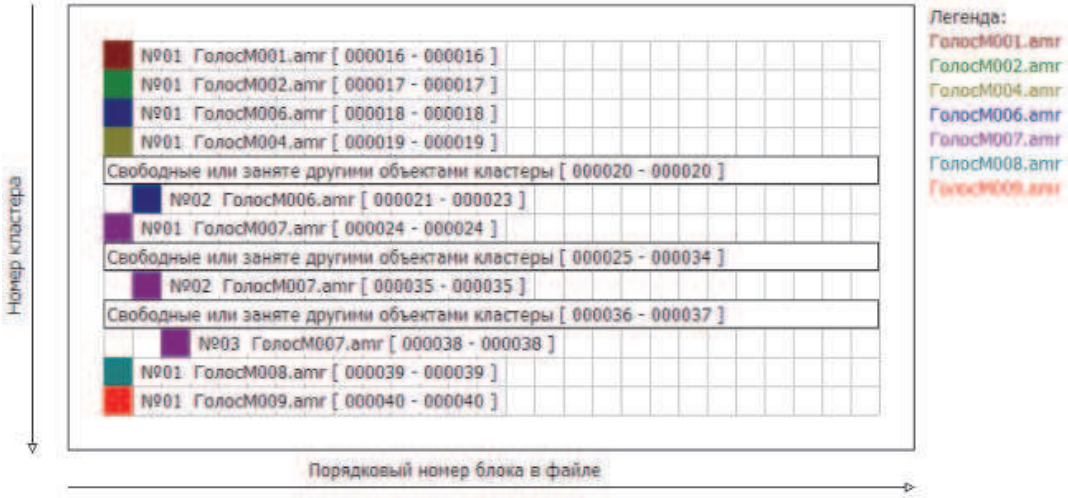

Рис. 6. Размещение семи файлов, два из которых фрагментированы

При проведении исследований цифровых накопителей устройств видео- и звукозаписи было обнаружено, что у некоторых устройств последовательность размещения данных в файле не соответствует последовательности размещения данных в кластерах. То есть данные, которые в файле имеют большее смещение относительно его начала, могут размещаться в кластерах, имеющих меньшие номера, чем у кластеров с данными, имеющих меньшее смещение. Зачастую подобное размещение данных можно обнаружить у устройств с циклической записью аудио- и видеоинформации. В таких устройствах по исчерпании свободного места на накопителе удаляются наиболее ранние записи, и продолжение записи осуществляется в освободившиеся участки области данных, располагающихся в кластерах с меньшим номером. На рис. 7 приведена схема размещения файла, созданного видеорегистратором CarCam. Первая часть файла хранится в кластерах с номерами с 239982 по 244960, а вторая – с 5 по 6097.

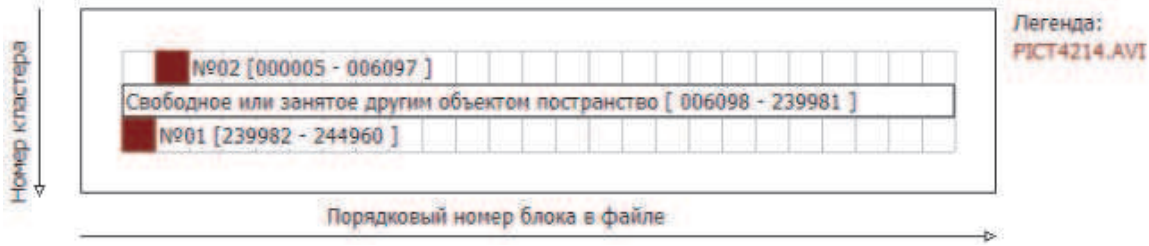

Рис. 7. Схема размещения файла с «обратным» порядком блоков

На практике встречается и более «сложный» порядок размещения записей в области данных файловой системы. В качестве примера рассмотрим порядок размещения видеозаписей, созданных видеорегистраторами texet DVR-101 HD и AdvoCam 1080P FullHD на сменных картах памяти.

Схема размещения трёх файлов, записанных устройством AdvoCam 1080P FullHD, приведена на рис. 8, последовательность блоков – в таблице 7.

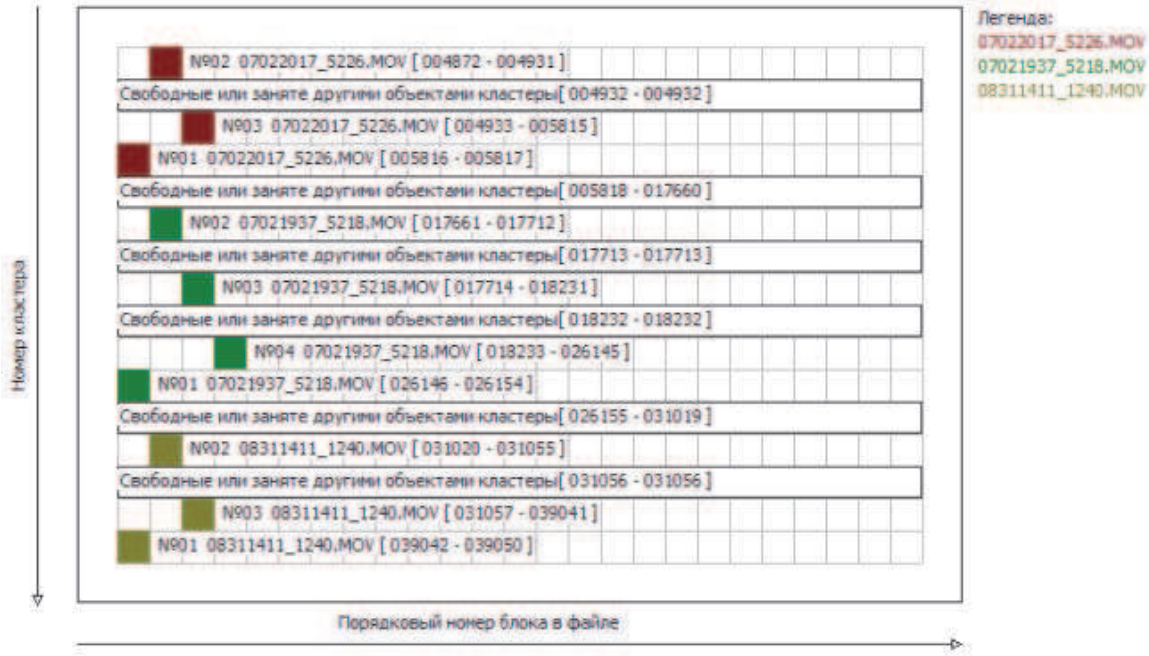

Рис. 8. Схема размещения трёх файлов с карты памяти видеорегистратора AdvoCam 1080P FullHD

Таблица 7. Размещение блоков для файлов 07022017_5226.MOV, 07021937_5218.MOV и 08311411_1240.MOV (отсортировано по порядку следования кластеров)

Имя файла	Номер блока	Диапазон кластеров.	Число кластеров
07022017_5226.MOV	000002	004872 - 004931	000060
07022017_5226.MOV	000003	004933 - 005815	000883
07022017_5226.MOV	000001	005816 - 005817	000002
07021937_5218.MOV	000002	017661 - 017712	000052
07021937_5218.MOV	000003	017714 - 018231	000518
07021937_5218.MOV	000004	018233 - 026145	007913
07021937_5218.MOV	000001	026146 - 026154	000009
08311411_1240.MOV	000002	031020 - 031055	000036
08311411_1240.MOV	000003	031057 - 039041	007985
08311411_1240.MOV	000001	039042 - 039050	000009

В данном случае особенностью размещения видеофайлов является то, что первый блок файла располагается в последних кластерах. Наиболее вероятной причиной подобного явления может быть то, что заголовок файла полностью формируется в момент завершения видеозаписи и записывается последним, а затем редактируется таблица FAT.

Схема размещения двух файлов, записанных на устройстве texet DVR-101 HD, приведена на рис. 9, последовательность блоков – в таблице 8.

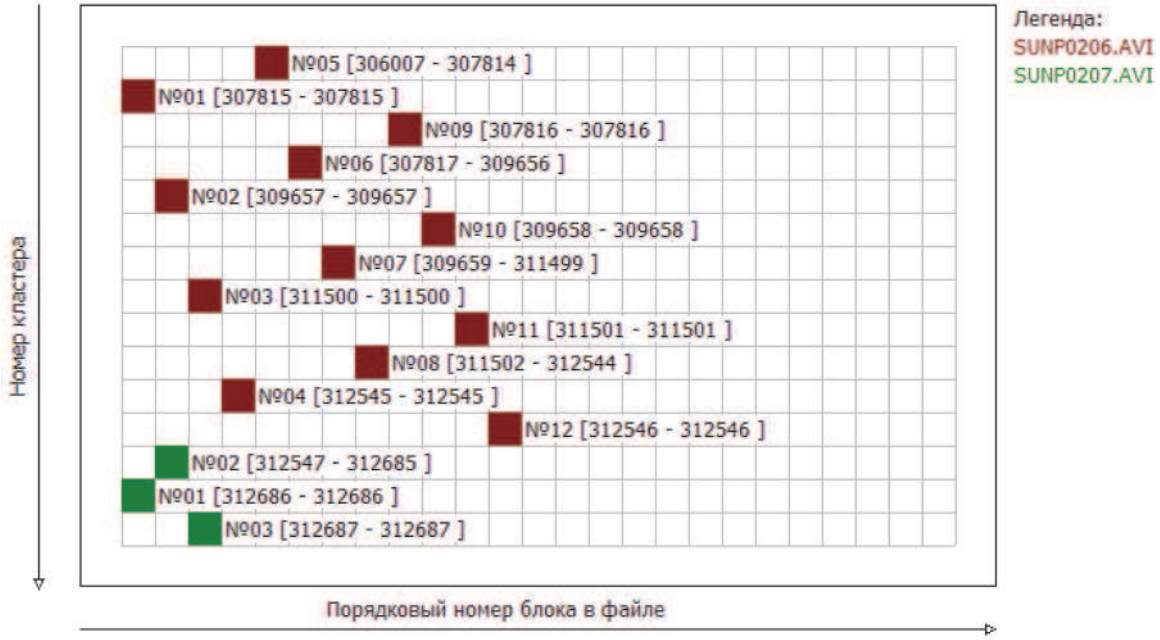

Рис. 9. Схема размещения двух файлов с карты памяти видеорегистратора texet DVR-101 HD

Таблица 8. Размещение блоков для файлов SUNP0206.avi и SUNP0207.avi (отсортировано по порядку следования кластеров)

Имя файла	Номер блока	Диапазон кластеров	Число кластеров
SUNP0206.AVI	000005	306007 – 307814	001808
SUNP0206.AVI	000001	307815 – 307815	000001
SUNP0206.AVI	000009	307816 – 307816	000001
SUNP0206.AVI	000006	307817 – 309656	001840
SUNP0206.AVI	000002	309657 – 309657	000001
SUNP0206.AVI	000010	309658 – 309658	000001
SUNP0206.AVI	000007	309659 – 311499	001841
SUNP0206.AVI	000003	311500 – 311500	000001

Имя файла	Номер блока	Диапазон кластеров	Число кластеров
SUNP0206.AVI	000011	311501 – 311501	000001
SUNP0206.AVI	000008	311502 – 312544	001043
SUNP0206.AVI	000004	312545 – 312545	000001
SUNP0206.AVI	000012	312546 – 312546	000001
SUNP0207.AVI	000002	312547 – 312685	000139
SUNP0207.AVI	000001	312686 – 312686	000001
SUNP0207.AVI	000003	312687 – 312687	000001

При исследовании размещения блоков файлов, созданных устройством texet, было установлено, что блоки сгруппированы в группы по трое. Каждая группа обладает следующими свойствами:

1) первый блок в тройке занимает достаточно большую цепочку кластеров, второй и третий блоки занимают только по одному кластеру;

2) в каждой тройке блоков порядок их следования в области данных накопителя не соответствует порядку их следования в файле, второй блок всегда раньше первого в файле, а третий блок всегда позже;

3) данные, хранящиеся во втором и третьем блоке каждой группы, идентичны.

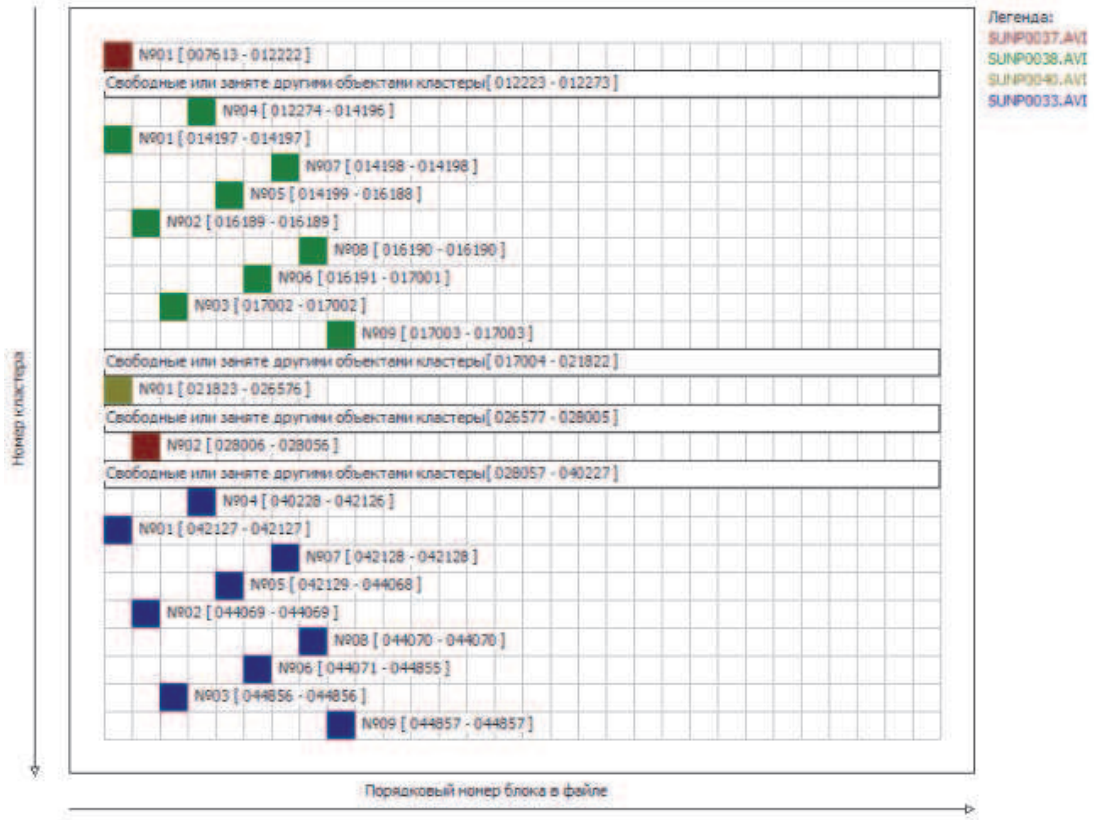

Рис. 10. Схема размещения файлов с карты памяти видеорегистратора texet DVR-101 HD

На рис. 10 приведена схема размещения блоков файлов на карте памяти после переноса файлов SUNP0037.AVI и SUNP0040.AVI на жёсткий диск ПК и обратно на карту памяти. На рисунке видно, что файл SUNP0040.AVI размещен единым блоком, что противоречит ранее установленному порядку размещения блоков файла на носителе видеорегистратором texet DVR-101 HD. Файл SUNP0037.AVI размещён в двух блоках, однако закономерность размещения блоков на накопителе не выполняется. Таким образом, можно утверждать, что файлы SUNP0037.AVI и SUNP0040 были записаны на накопитель не устройством записи texet DVR-101 HD, а другими средствами.

Наличие такой особенности в расположении файлов в области данных файловой системы является индивидуализирующим признаком устройства записи данной модели (производителя), при использовании которого данный файл был создан.

2.2. Особенности заполнения временных атрибутов файлов и директорий

При проведении технического исследования фонограмм и видеофонограмм в качестве дополнительной информации эксперт может учитывать значения временных атрибутов файлов, содержащих фонограммы и видеофонограммы. При этом можно обнаружить следующие особенности их заполнения:

1) специфичное заполнение «Байта сотых секунды» – байта, содержащего сотые доли секунды времени создания файла;

2) наличие закономерностей заполнения временных атрибутов в файле;

3) наличие закономерностей заполнения временного атрибута у последовательности файлов.

Заполнение байта, содержащего информацию о сотых долях секунды времени создания файла

Устройства записи по результатам анализа заполнения «Байта сотых секунды», содержащего сотые доли секунды времени создания файла, можно разделить на три основные группы.

К первой группе относятся устройства, которые при создании файла «Байту сотых секунды» всегда присваивают значение «0». У файлов, созданных такими устройствами, время создания всегда содержит чётное число секунд. В качестве примера в таблице 9 приведены временные атрибуты файлов, записанных при помощи видеорегистратора texet DVR-101 HD.

Таблица 9. Временные атрибуты файлов с карты памяти видеорегистратора texet DVR-101 HD

Имя	«Байт сотых секунды»	Время создания	Время изменения	Дата открытия
SUNP0200.AVI	000	17:15:26.000 24/03/2011	17:15:26 24/03/2011	02/04/2014
SUNP0201.AVI	000	17:25:26.000 24/03/2011	17:25:26 24/03/2011	02/04/2014
SUNP0202.AVI	000	17:35:26.000 24/03/2011	17:35:26 24/03/2011	02/04/2014
SUNP0203.AVI	000	17:43:00.000 24/03/2011	17:43:00 24/03/2011	02/04/2014
SUNP0204.AVI	000	18:01:32.000 24/03/2011	18:01:32 24/03/2011	02/04/2014
SUNP0205.AVI	000	18:11:32.000 24/03/2011	18:11:32 24/03/2011	02/04/2014
SUNP0206.AVI	000	18:14:30.000 24/03/2011	18:14:30 24/03/2011	2/04/2014
SUNP0207.AVI	000	12:00:08.000 01/01/2011	12:00:08 01/01/2011	02/04/2014
SUNP0209.AVI	000	12:41:18.000 01/01/2011	12:41:18 01/01/2011	02/04/2014
SUNP0210.AVI	000	12:47:08.000 01/01/2011	12:47:08 01/01/2011	02/04/2014
SUNP0212.AVI	000	16:03:00.000 01/01/2011	16:03:00 01/01/2011	02/04/2014
SUNP0213.AVI	000	16:13:02.000 01/01/2011	16:13:02 01/01/2011	02/04/2014
SUNP0214.AVI	000	16:23:02.000 01/01/2011	16:23:02 01/01/2011	02/04/2014
SUNP0215.AVI	000	16:33:02.000 01/01/2011	16:33:02 01/01/2011	02/04/2014

Ко второй группе относятся устройства, которые при создании файлов задают время создания с точностью до целой секунды. У таких устройств «Байт сотых секунды» может принимать одно из двух значений – 0 или 100. В качестве примера в таблице 10 приведены временные атрибуты файлов, записанных при помощи мобильного телефона Samsung.

Таблица 10. Временные атрибуты файлов с карты памяти телефона Samsung

Имя	«Байт сотых секунды»	Время создания	Время изменения	Длительность записи	Дата открытия
ГолосМ001.amr	100	17:21:43.000 31/03/2014	17:21:54 31/03/2014	0:08.98	31/03/2014
ГолосМ002.amr	100	17:22:01.000 31/03/2014	17:22:08 31/03/2014	0:06.94	31/03/2014
ГолосМ003.amr	000	17:22:12.000 31/03/2014	17:22:20 31/03/2014	0:06.76	31/03/2014
ГолосМ004.amr	100	17:22:23.000 31/03/2014	17:22:24 31/03/2014	0:01.24	31/03/2014
ГолосМ005.amr	000	17:22:26.000 31/03/2014	17:22:30 31/03/2014	0:03.76	31/03/2014

К третьей группе относятся устройства, которые заполняют «Байт сотых секунды» при создании файла различными значениями. Файлы, созданные такими устройствами, имеют время создания, представленное с точностью до 0.01 секунды.

При копировании файлов на накопители устройств, отнесённых к первой или ко второй группе, средствами ПК, работающего под управлением ОС семейства Windows, «Байты сотых секунды» могут быть заполнены отличными от вышеуказанных значениями, что позволяет достаточно легко обнаружить подобные файлы.

Наличие особенностей заполнения «Байта сотых секунды» является признаком устройства записи, при использовании которого данный файл был создан. По данному признаку устройство, производившее запись, можно отнести к одной из трёх групп.

Заполнение временных атрибутов файлов

Устройства записи по результатам анализа заполнения файловых временных атрибутов можно разделить на три группы по следующим критериям:

1) время/дата создания и модификации файлов «почти» совпадают, отличаясь менее чем на 2 с (точность представления времени и даты модификации файла 2 с);

2) время/дата создания и модификации файлов не совпадают, а отличаются на величину, сопоставимую с продолжительностью аудио- или видеозаписей, содержащихся в файлах;

3) один из временных атрибутов не заполняется, например, время создания остается нулевым, что соответствует дате «1 января 1980 года» и времени «0 ч 0 мин 0 с».

Если время и дата создания файла имеет более позднее значение, чем время и дата последней модификации (изменения) файла, или разница этих временных штампов существенно отличается от продолжительности записи, то вероятнее всего над этим файлом производилась процедура копирования или редактирования.

Заполнение временных атрибутов последовательности файлов

При анализе файлов для определения последовательности их создания можно использовать следующие параметры, хранящиеся в файловой системе:

1) Нумерованное имя файла. Большинство устройств записи именуют файлы с добавлением порядкового номера. Несоответствие последовательностей номеров и временных атрибутов файлов может являться свидетельством того, что либо файлы были скопированы на носитель при помощи другого устройства, либо показания таймера устройства записи были изменены (умышленно или неумышленно, например, при отключении питания УЗ).

2) Последовательность размещения записей директории для файлов в области данных, описывающих директорию. Если из директории не производилось удаление файлов, то записи директории добавляются последовательно и, соответственно, корневые записи более поздних файлов имеют большее смещение. Эту последовательность можно также сравнить с последовательностью временных атрибутов. Если же перед записью производилось удаление файлов, то для вновь записанных файлов запись директории может быть

размещена на место записи директории для удалённого файла, и тогда последовательность размещения записей директории будет нарушена.

3) Последовательность размещения файлов в области данных (можно использовать номер первого кластера, хранящийся в записи директории). Как правило, файлы в области данных размещены последовательно. Нарушение последовательности размещения файлов может быть вызвано размещением файлов в освобождённом после удаления других файлов месте. В этом случае более поздние файлы могут занять кластеры с меньшим адресом, ранее занимаемые удалённым файлом.

4) Последовательность записей директории, ссылающихся на один и тот же первый кластер. При удалении файла или директории в таблице FAT их кластеры обозначаются как свободные, а в записи директории первому байту короткого имени присваивается значение 229 (или в шестнадцатеричной системе отчёта E5h), при этом сведения о первом кластере и временные атрибуты сохраняются в записи директории. Проводя сравнительный анализ временных атрибутов существующего файла и временных атрибутов объекта, ранее занимавшего этот кластер, можно оценить корректность временных атрибутов данного файла. Если временные атрибуты удалённого файла имеют более позднее значение, то либо показания таймера устройства записи были изменены (умышленно или неумышленно, например, при отключении питания УЗ) между моментом удаления файла и созданием на его месте другого файла, либо существующий файл был создан и скопирован другим устройством, а его временные атрибуты изменены. Такие пары записей директорий (файлов), ссылающихся на один и тот же первый кластер, можно получить при переименовании файла на накопителе. Основным признаком такой пары записей является полное совпадение всех файловых атрибутов (в том числе размера, временных атрибутов и т.д.).

2.3. Особенности заполнения имён файлов

Структура файловых систем FAT16 и FAT32 позволяет хранить две записи об имени файла/директории: LFN-запись (несколько блоков), хранящую длинное имя, и SFN-запись, в которой хранится короткое имя. Современное программное обеспечение корректно работает с файловыми системами FAT и, как правило, отображает пользователю длинное имя файла, хранящееся в кодировке Unicode. При проведении исследования было установлено, что не все устройства используют кириллические кодовые страницы для представления короткого имени файла, и эта особенность тоже является устойчивым признаком устройства записи. В связи с этим при анализе файлов следует обращать внимание на то, в какой кодировке хранится короткое имя файла.

Таблица 11. Различное представление имён файлов с карты памяти телефона Samsung

Имя файла	Короткое имя файла	Время создания	Байт сотых секунды	Время изменения
ГолосМ008.amr	_____M~6AMR	17:38:21.000 31/03/2014	100	17:38:24 31/03/2014
ГолосМ009.amr	_____M~7AMR	17:38:28.000 31/03/2014	000	17:38:44 31/03/2014
ГолосМ010.amr	ГОЛОСМ~1AMR	17:52:13.190 31/03/2014	119	18:30:42 11/04/2013

В таблице 11 отображена информация о файлах: в первом столбце отображается имя, полученное из блоков LFN; во втором столбце имя, полученное из SFN; далее время создания и «Байт сотых секунды». Первые два файла записаны на накопитель устройством и не изменялись, а третий файл был скопирован на данный накопитель с помощью другого устройства. К признакам изменения третьего файла можно отнести следующее: отличная от оригинальной кодировка короткого имени; отличное от 0 и 100 количество сотых секунд; время создания файла отличается в большую сторону от времени его изменения.

2.4. Файлы, оставляемые программными средствами редактирования видео- и аудиоданных

Зачастую программное обеспечение, предназначенное для редактирования аудио- и видеофонограмм, создаёт на носителе информации дополнительные файлы. Например, звуковой редактор Adobe Audition формирует рядом с открываемым файлом одноимённый файл с расширением «pk», а Sound Forge при сохранении файла формирует рядом с ним файл с расширением «sfk». Наличие таких файлов свидетельствует о том, что записи по крайней мере «открывались» указанными редакторами.

Обнаружить тот факт, что файл «открывался» с накопителя и сохранялся с тем же именем, можно также при анализе записей директорий, содержащих информацию об удалённых файлах.

Например, если в корневой директории накопителя размещён один файл с именем 1008.mp3, то в записях корневой директории будет содержаться только одна запись (рис. 11).

Смещение	Тип	^ Полный путь	Номер первого кластера	Размер
00046E00	Файл	\Root\1008.MP3	2	518687

Рис. 11. Записи директорий накопителя, содержащего один файл

Если звуковой сигнал из файла 1008.mp3 подвергнуть редактированию с помощью Sound Forge и сохранить результаты в том же файле, то в результате этих действий на накопителе по-прежнему будет находиться только один звуковой файл. При этом дата создания файла не изменится, а обновится только дата изменения. Но если проанализировать записи корневой директории носителя, то на нем будут обнаружены три записи (рис. 12). Особенностью функционирования Sound Forge в описанном случае является появление кроме записи удалённого файла ещё и записи с именем «frg001.tmp.tmp».

Смещение	Тип	^ Полный путь	Номер первого кластера	Размер
00046E80	Файл	\Root\1008.MP3	129	1171438
00046E60	Уд.Файл	\Root\frg001.tmp.tmp	2	518687
00046E00	Уд.Файл	\Root_008.MP3	2	518687

Рис. 12. Записи директорий накопителя после повторного сохранения файла с использованием Sound Forge

Если сигнал из файла 1008.mp3 редактировался средствами звукового редактора Audacity с последующим сохранением результата в том же файле, то после сохранения в области записей корневой директории будет содержаться две записи: одна – для нового сохранённого файла, вторая – для удалённого с добавлением к имени символа «0» (рис. 13).

^ Смещение	Тип	Полный путь	Номер первого кластера	Размер
00046E00	Уд.Файл	\Root_0080.MP3	2	518687
00046E20	Файл	\Root\1008.MP3	129	609383

Рис. 13. Записи директорий накопителя после повторного сохранения файла с использованием Audacity

Если звуковой сигнал из файла 1008.mp3 подвергнуть редактированию с помощью Adobe Audition и сохранить результаты в том же файле, то после сохранения в области записей корневой директории будет содержаться три записи: одна – для нового сохранённого файла, вторая – для удалённого с отсутствующим первым символом и третья – с именем, начинающимся со строки «test» и заканчивающимся набором цифр по формату, соответствующему GUID. При этом GUID каждый раз при сохранении будет прописываться разный (рис. 14).

Смещение	Тип	Полный путь	Номер первого кластера	Размер
00046E00	Уд.Файл	\Root_008.MP3	2	518687
00046EA0	Уд.Файл	\Root\test24618095-8803-49b3-ad57-3c417e0e95e3	0	0
00046EC0	Файл	\Root\1008.MP3	129	724080

Рис. 14. Записи директорий накопителя после повторного сохранения файла с использованием Adobe Audition

Следует отметить, что во всех трёх описанных случаях с применением разных звуковых редакторов область данных первичного файла остается свободной, что позволяет восстановить первичные файлы. Сравнивая фонограммы из имеющегося и восстановленного файлов, можно установить, какие изменения производились. А по имеющимся данным об удалённых файлах можно судить о программном обеспечении, которое использовалось для обработки фонограмм.

3. Рекомендуемое программное обеспечение

В исследованиях, результаты которых изложены выше, использовались методы анализа накопителей с файловой системой FAT16 или FAT32. Данные методы реализованы в специализированном программном обеспечении: Forensic ToolKit (разработчик «AccessData, Inc»), EnCase (разработчик «Guidance Software, Inc»), R-Studio (разработчик «R-Tools Technology, Inc»). При написании данной работы, в частности для получения информации о записях директорий и графического отображения размещения последовательности блоков файлов, использовался комплекс FAT-Expert, разработанный фирмой «ОТ-КОНТАКТ».

4. Область применения

Изложенные методы исследования применимы в тех случаях, когда видео- и звукозаписи предоставлены на накопителях, содержащих файловую систему FAT16 или FAT32. Это могут быть сменные накопители, например, карты памяти или внутренняя память устройства записи, поддерживающие подключение к ПК в качестве сменных носителей с файловой системой FAT16 или FAT32, например, память диктофонов, мобильных телефонов и других устройств записи. Накопители исследуются на предмет выявления признаков изменения видео- и звукозаписей и файлов, их содержащих: нарушения закономерностей размещения данных видео- и звукозаписей на цифровых накопителях, нарушения закономерностей формирования временных атрибутов файлов и их последовательностей, нарушения особенностей заполнения имён файлов, наличие удалённых файлов, свидетельствующих об использовании программ редакторов.

Следует отметить, что существуют и другие методы поиска на накопителях следов изменений видео- и звукозаписей. К таким методам можно отнести, например, поиск и анализ «сопутствующих» файлов, создаваемых устройствами записи, анализ журналов событий устройств и т.д. Данные методы выходят за рамки данной работы и требуют отдельного детального рассмотрения.

Применение описанных в работе методов расширяет возможности экспертов при проведении инструментальной части исследования видео- и звукозаписей при поиске признаков монтажа и других изменений, произведённых после завершения процесса записи, и позволяет в большем количестве случаев дать категорический вывод.

Литература

1. Вознюк М.А., Иванов И.Л. Экспертная диагностика технических обстоятельств и условий изготовления цифровых видео- и звукозаписей. Обобщение экспертной практики // Актуальные вопросы экспертизы видеозаписей: материалы всероссийского семинара, проходившего в г. Нижнем Новгороде 13–17 мая 2013 года / под ред. В.Н. Пронина, П.Г. Лесниковой. – Н. Новгород, 2014. С. 121–171 (в печати).

2. Кэрриэ Б. Криминалистический анализ файловых систем. – СПб.: Питер, 2007. – 480 с.