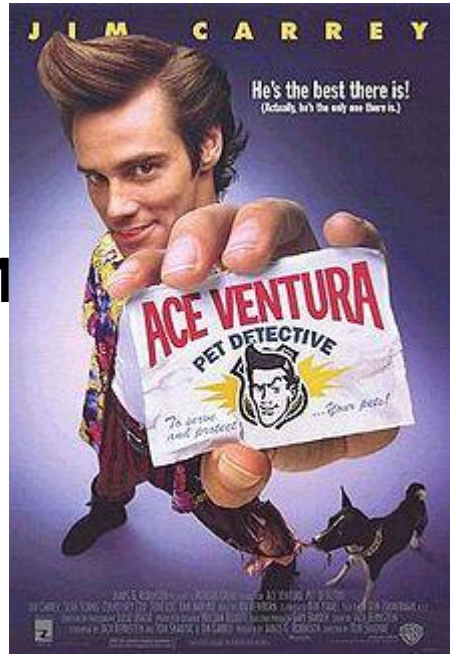
Защита информационных ресурсов компьютерных систем и сетей

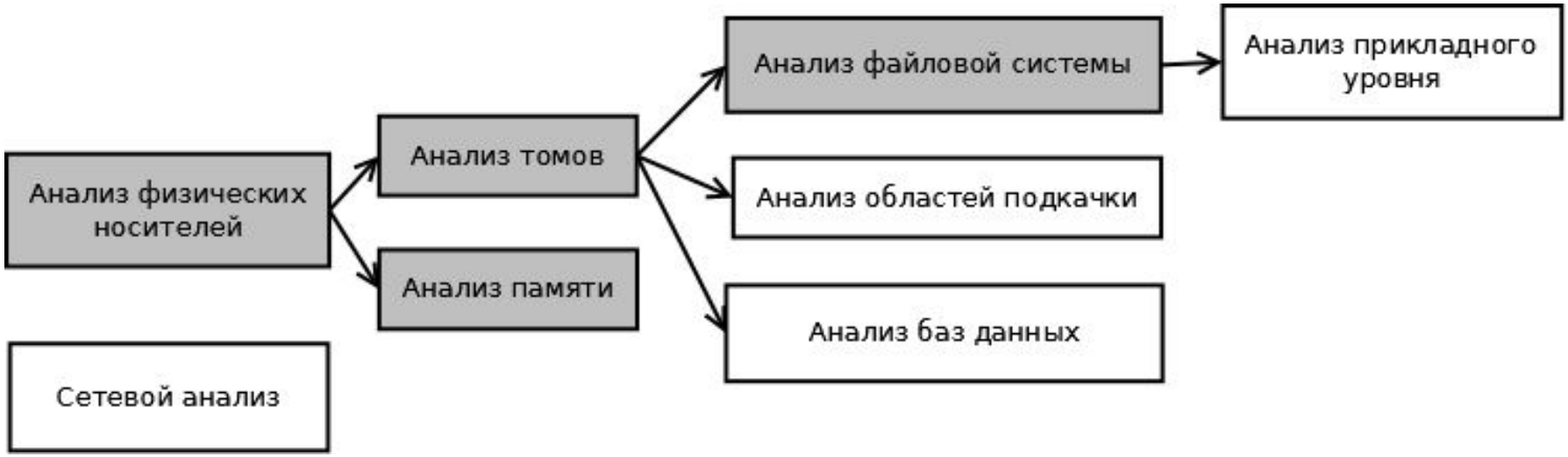
Компьютерная криминалистика

Что такое компьютерная криминалистика?

- Ответвление криминалистики, сочетающее в себе восстановление и расследование материалов, найденных на электронных носителях.
- Криминалистика – наука, исследующая закономерности приготовления, совершения и раскрытия преступлений



Разделы


Анализ физических носителей
Анализ томов
Анализ памяти
Сетевой анализ
Анализ файловой системы
Анализ областей подкачки
Анализ баз данных
Анализ прикладного уровня

Задачи

- Найди улику в образе диска
- Найди улику в дампе трафика
- Найди улику в дампе ОП
- Найди улику в бинарнике
- Найди улику в RAM
- …

Про анализ бинарников

- Бинарные файлы могут встречаться десятками в образе
- Каждый дизассемблировать смысла нет
- Проверить строки командой strings

Анализ оперативной памяти

- Volatility
- \\.\PhysicalMemory \\.\DebugMemory
- /dev/mem
- mdd
- Hex-editors (HxD, WinHex,..)

Загрузка ОС на примере Windows

- Включение питания
- Чтение команд из BIOS
- Анализ оборудования
- Поиск загрузочного носителя в порядке очереди
- Выполнение загрузочного кода из первого сектора диска
- Выполнение загрузочного кода раздела

Анализ файловых систем

- Данные файловой системы
- Данный содержимого
- Метаданные
- Данные имен файлов
- Прикладные данные

NTFS

- Наиболее распространенная файловая система для семейства ОС Windows
- Концепции
  - Безопасность
  - Надежность
  - Поддержка носителей больших объёмов

Основные понятия NTFS

- Все данные – файлы
- **MFT** (Master File Table ~ «Главная файловая таблица»)
- Пространство выделяется **кластерами** – (группы смежных секторов)

MFT (Master File Table)

- Запись в таблице для каждого файла и директории
- Все записи нумеруются. [0,1,…]
- Нулевая запись – запись на себя
- Может быть фрагментирована по секторам
- Расширяется системой, но не сужается

Запись MFT

- Занимает 1024 байта
- Первые 42 байта – фиксированный формат
- Остальное пространство под атрибуты

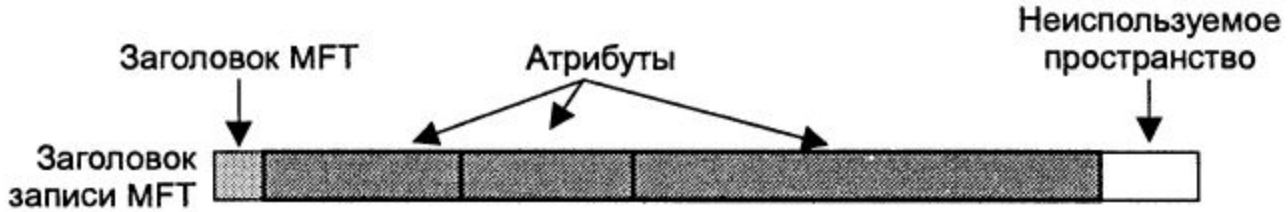


Рис. 11.1. Запись MFT содержит небольшой заголовок, а остальные байты предназначены для хранения различных атрибутов. Запись, показанная на рисунке, содержит три атрибута

Запись MFT

- Первая запись – **базовая**
- Если атрибуты не помещаются в запись, то создается ещё одна запись с ссылкой на базовую

Файлы метаданных

- Занимают зарезервированные первые 16 записей MFT
- Первые 12 записей выделены и содержат файлы метаданных
- 4 записи [12-15] выделены, но являются пустыми

Файлы метаданных

Номер	Название	Описание
0	$MFT	Запись для MFT
1	$MFTMirr	Резервная копия MFT
2	$LogFile	Журнал транзакций
3	$Volume	Информация о томе

Файлы метаданных

Номер	Название	Описание
4	$AttrDef	Информация о атрибутах
5	.	Корневой каталог
6	$BitMap	Маска выделения кластеров
7	$Boot	Загрузочный сектор и загрузочный код

Файлы метаданных

Номер	Название	Описание
8	$BadClus	Информация о поврежденных кластерах
9	$Secure	Информация о безопасности
10	$Upcase	Содержит uppercase Unicode символы
11	$Extend	Каталог с файлами необязательных расширений

Атрибуты

- Все атрибуты имеют заголовок и содержимое
- Структура содержимого может быть разная у разных атрибутов
- Заголовок хранит тип, размер, имя атрибута
- Запись может иметь несколько однотипных атрибутов (у каждого уникальный id)

Атрибуты

- Резидентные и нерезидентные
- Разреженные атрибуты
- Сжатые атрибуты($DATA)

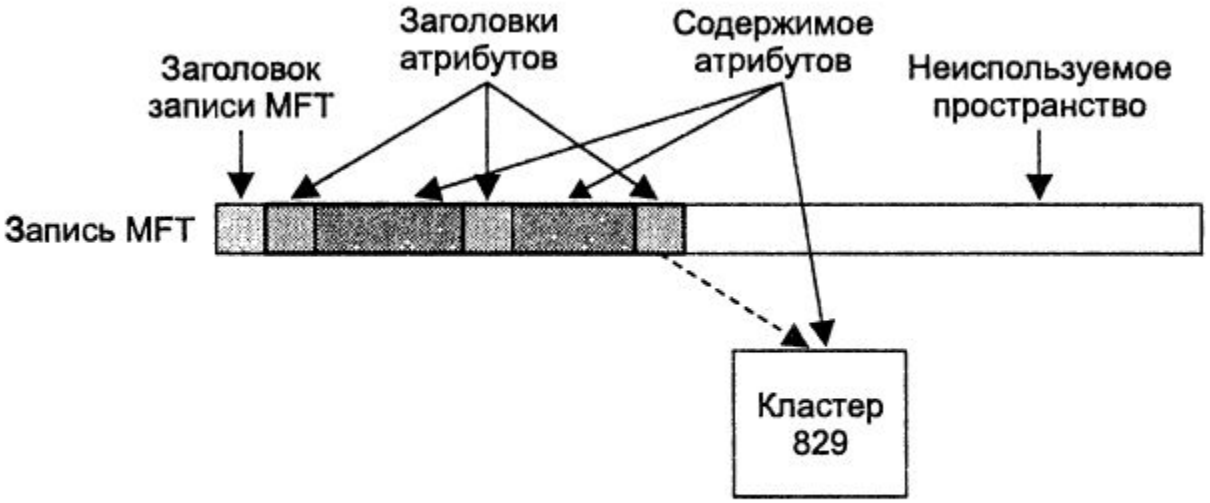


Рис. 11.5. Пример записи MFT: третий атрибут содержит слишком много данных, поэтому он преобразуется в нерезидентный

Сжатие

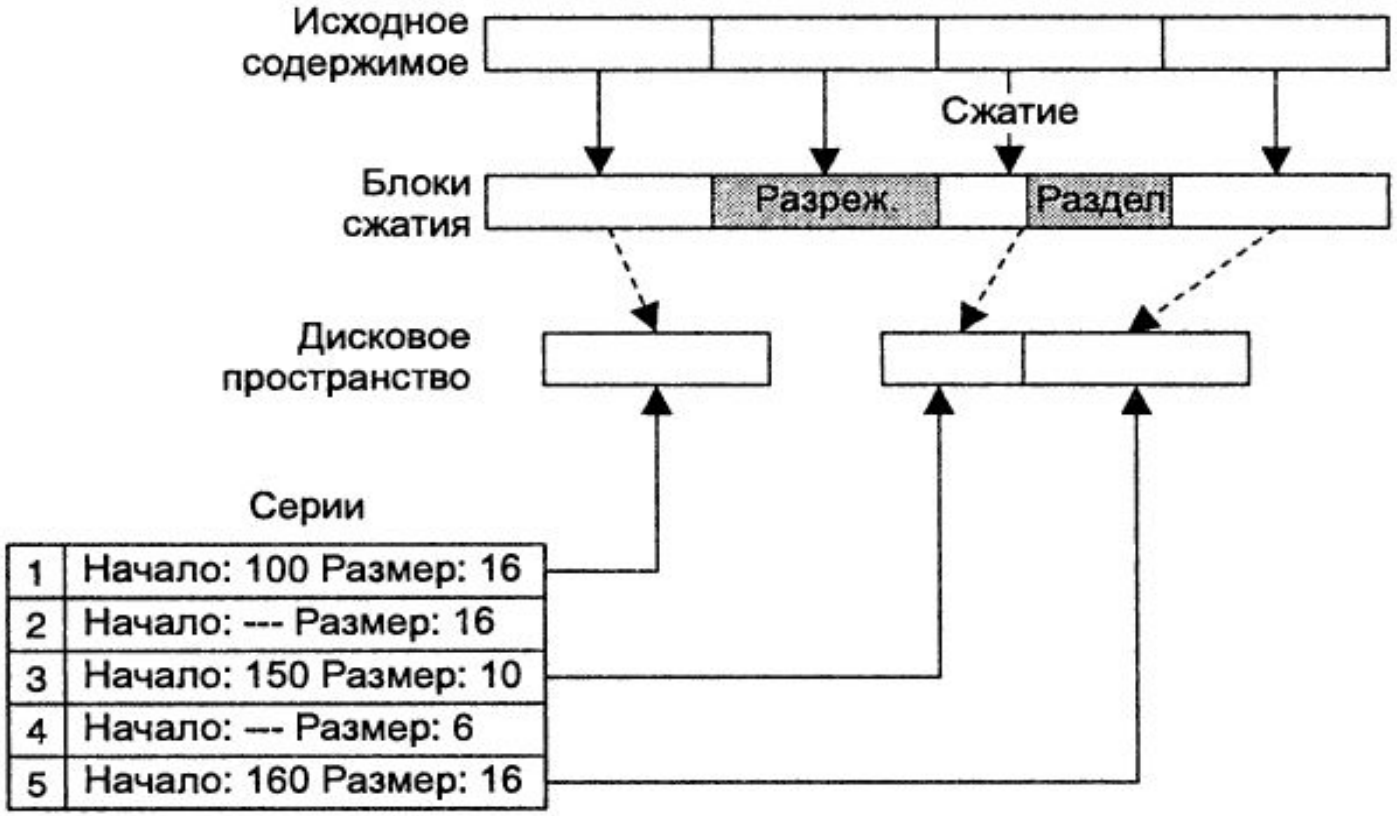


Рис. 11.9. Атрибут с двумя блоками, сохраняемыми без сжатия, одним разреженным блоком и одним блоком, сжимаемым до 10 кластеров

Типы атрибутов

- Все типы имеют идентификатор, имя
- По идентификатору происходит упорядочивание атрибутов в записи

Восстановление данных

1. Восстановление разрушенных данных
- **Аппаратные и программные сбои**
- **Воздействие вредоносного ПО**
- **Ошибки и намеренные действия пользователей**

2. Восстановление «закрытых» данных
- **Данные, закрытые паролем**
- **Кодированные и шифрованные данные**
- **Данные в «скрытых» областях**

3. Восстановление с систем хранения данных
- **RAID системы и внешние DAS системы**
- **Сетевые хранилища NAS**
- **Виртуальные и распределенные хранилища данных**

4. Разнообразие технологий хранения данных
- **Типы накопителей**
- **Интерфейсы**
- **Способы организации хранения данных**

Анализ данных и представление результатов

1. Анализ данных

- Выбор инструментария (ПО, утилиты)
- Интерпретация данных
- Корректная постановка вопросов эксперту

2. Представление результатов

- Доказательность собранных данных

Особенности Mobile forensics

1. Использование Flash, SSD в качестве основного носителя

- Работа с твердотельными носителями со сложной организацией памяти

2. Закрытость платформы

- Трудность обеспечения полноты копии из-за сложностей с организацией прямого доступа к памяти

3. Многообразие реализаций

4. Технические сложности из-за миниатюризации

Особенности Network forensics

1. Большое количество компьютеров

- Необходимо применение специальных средств мониторинга, анализа и хранения сетевых данных

2. Обмен данными с Интернет

- Необходимо предварительное накопление и хранение данных в специальных системах (аналогия - видеорегистраторы)

3. Беспроводные сети

- Проблемы Computer forensics

Проблемы хранения, передачи и обработки цифровых доказательств в компьютерной криминалистике. Предотвращение утечек информации.

Особенности:

- Предотвращение утечек цифровых доказательств (информационная безопасность)

- Предотвращение утечек информации (профилактика ИТ-инцидента)

-Применение средств информационной безопасности должно учитывать возможность проведения расследования методами компьютерной криминалистики

Предотвращение утечки информации и ИТ-инцидентов