Восстановление данных с дисков, поврежденных вредоносными программами

Выполнил:
Медведев А. А., 444 гр.

Научный руководитель:
ст. пр. **Губанов Ю. А.**

Научный консультант:
ст. пр. **Тимофеев Н. В.**

Рецензент:
ст. пр. **Ханов А. Р.**

Введение

Belkasoft Evidence Center - инструмент цифрового криминалистического анализа, который позволяет анализировать и восстанавливать данные.

При повреждении вредоносными программами системных структур носителя доступ к данным на носителях ограничивается. В результате, анализ данных становится недоступен.

Цели и задачи

Цель: разработать прототип инструмента для восстановления доступа к данным на устройствах хранения информации, поврежденных вредоносными программами.

Задачи:

- выполнить обзор наиболее уязвимых для атак вредоносными программами структур жёстких дисков
- исследовать способы восстановления доступа к данным при повреждении рассмотренных структур
- разработать архитектуру прототипа
- реализовать прототип
- провести тестирование разработанного прототипа

Обзор уязвимых структур

- Master Boot Record
  - Содержит исполняемый бинарный код и таблицу разделов
  - Не имеет внутреннего механизма защиты
    - Bootkit

- Master File Table
  - Содержит записи о каждом файле на томе файловой системы NTFS
  - Существует частичная копия MFT-таблицы, по которой нельзя восстановить данные всех файлов
    - The Petya

Способ восстановления MBR

Главная загрузочная запись может быть восстановлена непосредственно на поврежденном жестком диске.

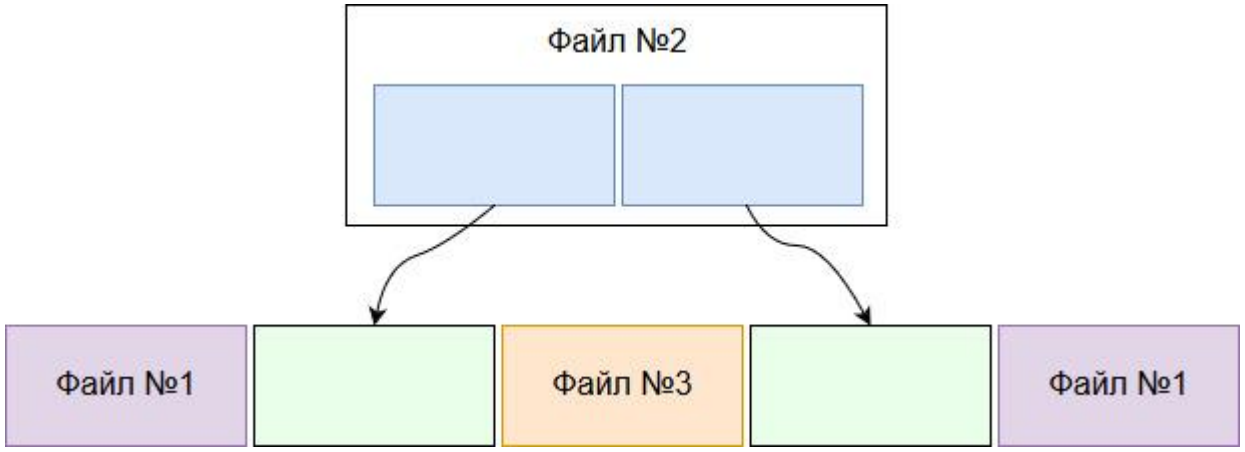
Составляющие MBR:

- исполняемый код
- таблица разделов
- сигнатура

Способ восстановления MFT

Восстановление главной таблицы файлов излишне трудозатратно. Есть возможность восстановить файлы с помощью метода сигнатурного поиска.

Существует проблема фрагментации файлов, которая многократно усложняет процесс восстановления файлов.



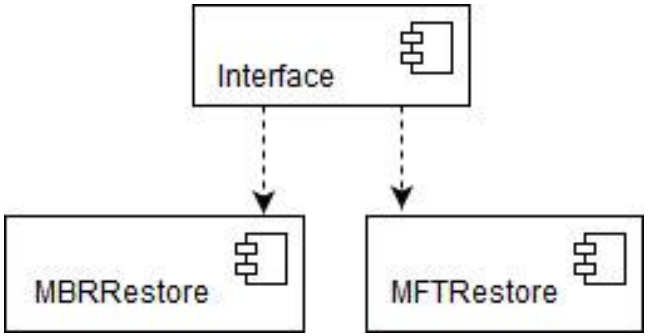
Архитектурные решения

Реализация на языке C# для упрощения дальнейшей апробации в продукте Belkasoft Evidence Center.

Целевая ОС - Windows.

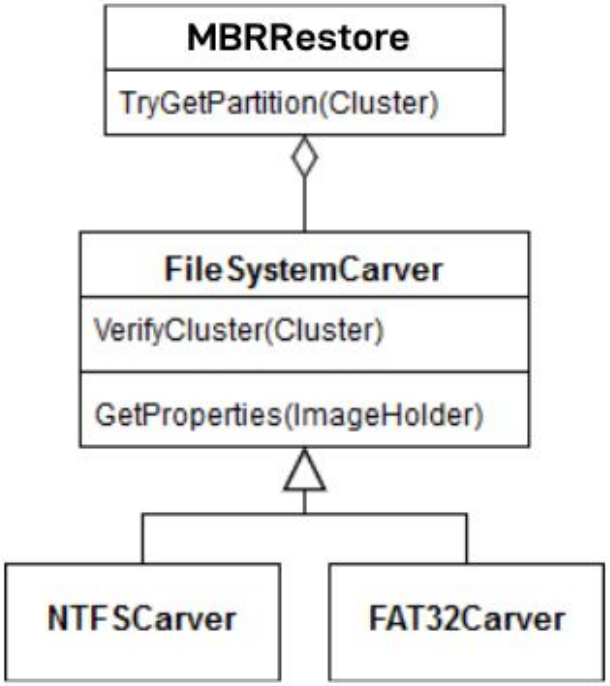
Основные компоненты:

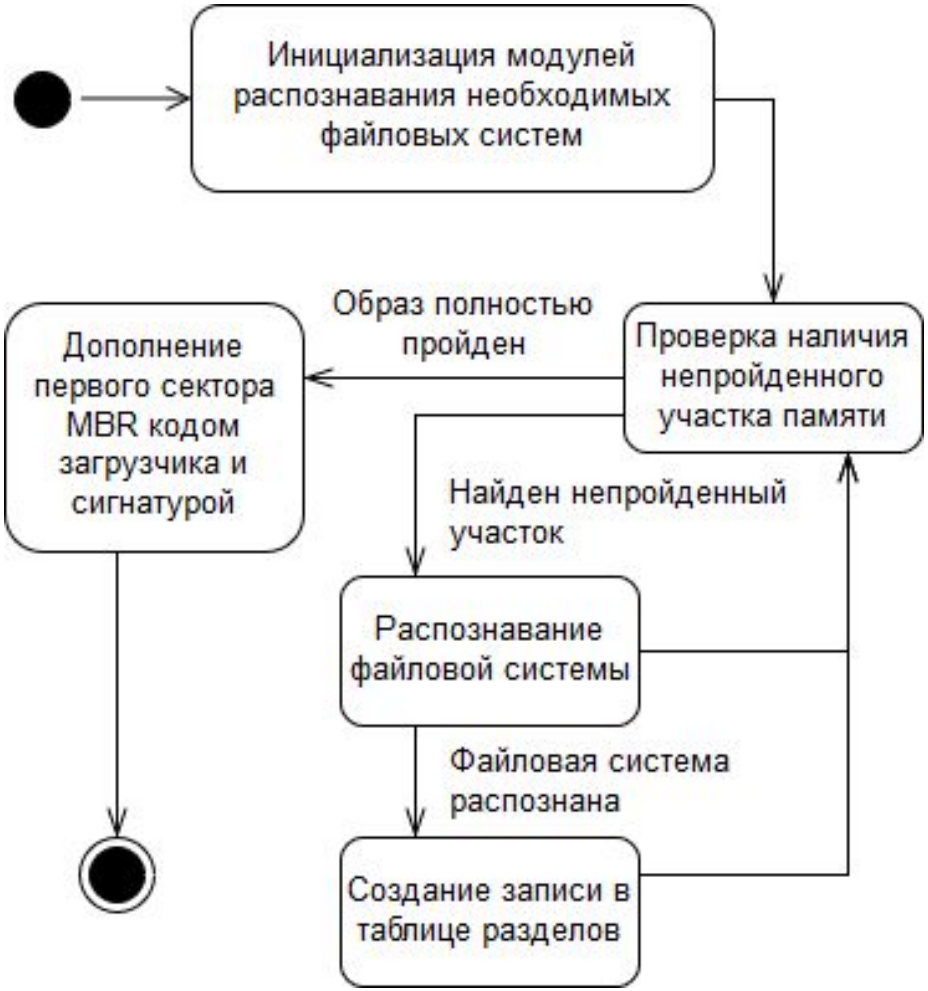
- Interface
- MBRRestore
  - NTFS и FAT32
- MFTRestore
  - JPEG



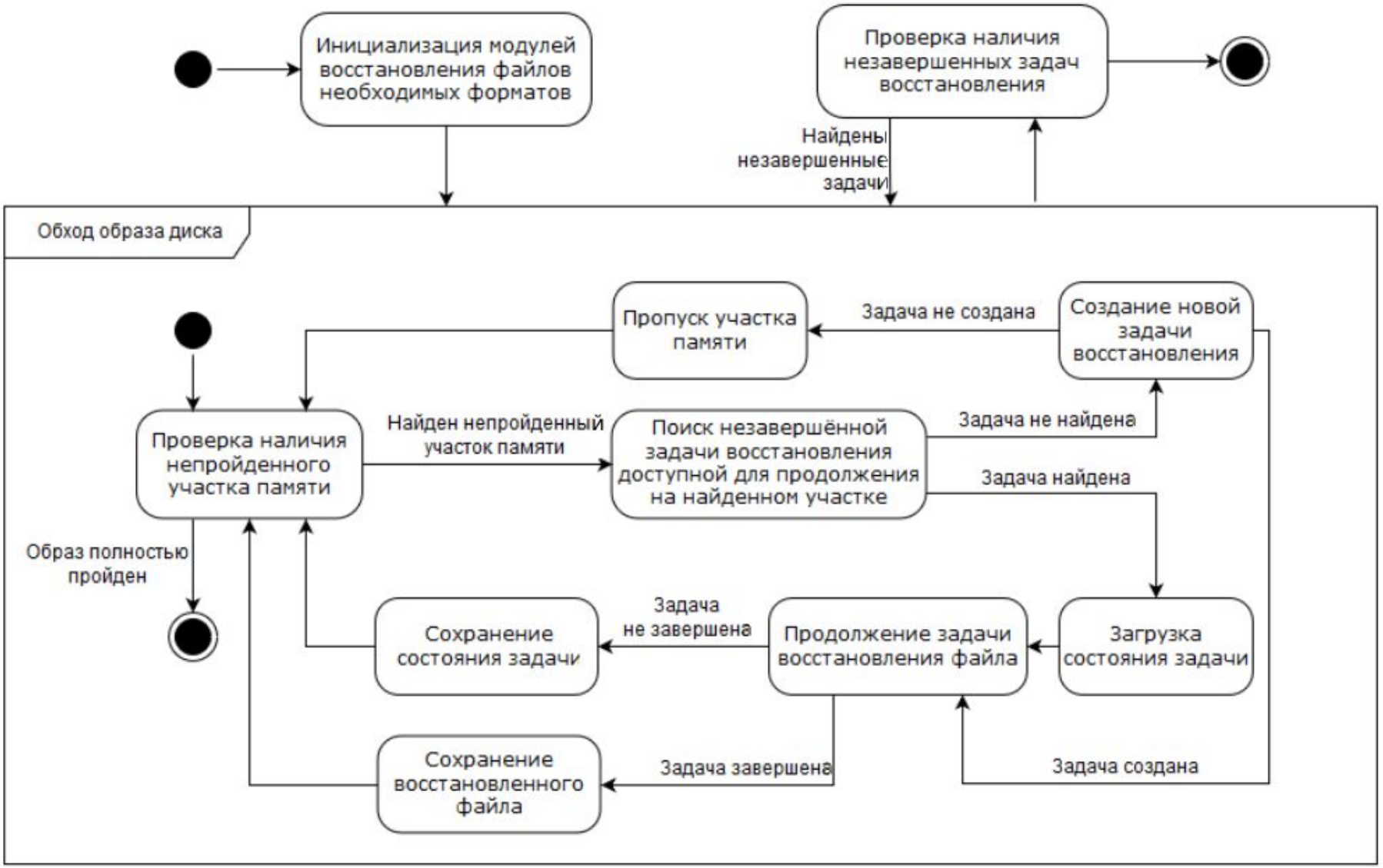
MBRRestore

Главная задача: восстановить главную таблицу разделов MBR.





Восстановление данных с образа диска с повреждённой MFT



Способ верификации фрагментов JPEG

- Структурный способ
- Контекстный способ

Для определения совместимости двух последовательных кадров JPEG необходимо сравнивать цвета на границах кадров.

Способы представления цвета:

- RGB (Red, Green, Blue)
  - Не соответствует человеческому восприятию
- LAB (Lightness, A: green–red, B: blue–yellow)

RGB	LAB
13 из 20	18 из 20

Количество успешно верифицированных файлов при использовании разных цветовых моделей

Тестирование MBRRestore

Создан набор образов жёстких дисков под управлением MBR.

С каждого образа жёсткого диска были удалены секторы в которых содержалась запись MBR.

Каждый из полученных образов был подан в качестве входных данных компоненту MBRRestore для восстановления.

В результате на каждом из образов была корректно воссоздана таблица разделов, доступ к разделам был восстановлен.

Сравнительный анализ восстановления JPEG

Аналоги:

- FTK, Encase, The Sleuth Kit, Foremost, Scalpel и т.д.
- Adroit Photo Forensic

Количество фрагментов JPEG	JPEGCarver	Adroit Photo Forensic
2 фрагмента	40 из 50	39 из 50
4 фрагмента	34 из 50	27 из 50

Результаты сравнительного анализа

Результаты

- Выполнен обзор MBR и MFT
- Исследованы способ восстановления MBR и способ восстановления файлов при повреждении MFT
- Разработана архитектура прототипа; определены основные компоненты
- Реализован прототип инструмента
- Проведено тестирование разработанного прототипа