Криминалистический анализ файловой системы XFS с восстановлением данных из журнала

Фунт Дина Дмитриевна, группа 18.Б11-мм

Научный руководитель: к.т.н. Ю.В. Литвинов, доцент кафедры программирования

Консультант: А. И. Цой, инженер-программист, ООО “Белкасофт“

Рецензент: С.М. Машарский, старший специалист по тестированию
ООО “Техцентр Дойче Банка”

Санкт-Петербург
2022

Введение

- Цифровой криминалистический анализ устройств
- Основной способ получения доказательств — изучение файловой системы устройства
- Существующие инструменты поддерживают чтение десктопных файловых систем, но не серверных
- Распространенность XFS возрастает

Постановка задачи

Цель: создание инструмента, позволяющего пользователю чтение и восстановление удаленных файлов из образов файловых систем XFS.

Задачи:

1. Провести обзор существующих решений для анализа образов памяти и изучить особенности файловой системы XFS
2. Исследовать возможность и предложить способы восстановления удаленных данных XFS
3. Реализовать инструмент для чтения файловой системы и восстановления удаленных данных
4. Проверить полученное решение на тестовых образах XFS

Обзор: инструменты анализа XFS

- UFS Explorer Standard Recovery
  - поддержано чтение и восстановление
  - коммерческий продукт
- ReclaiMe
  - чтение файловой системы
  - коммерческий продукт
- X-Ways Forensics
  - чтение данных
  - восстановление файлов путем карвинга
  - коммерческий продукт
- xfs_undelete
  - восстановление файлов

Обзор: The Sleuth Kit

- TSK — набор инструментов командной строки и библиотека C с открытым исходным кодом
- Анализ образов дисков и восстановление файлов из них
- Предоставляется API, удобное для поддержки других файловых систем
- не поддерживает XFS

Обзор: структура XFS

- группа выделения (AG)
- суперблок
- индексный дескриптор (inode)
  - local
  - extended
  - B-tree

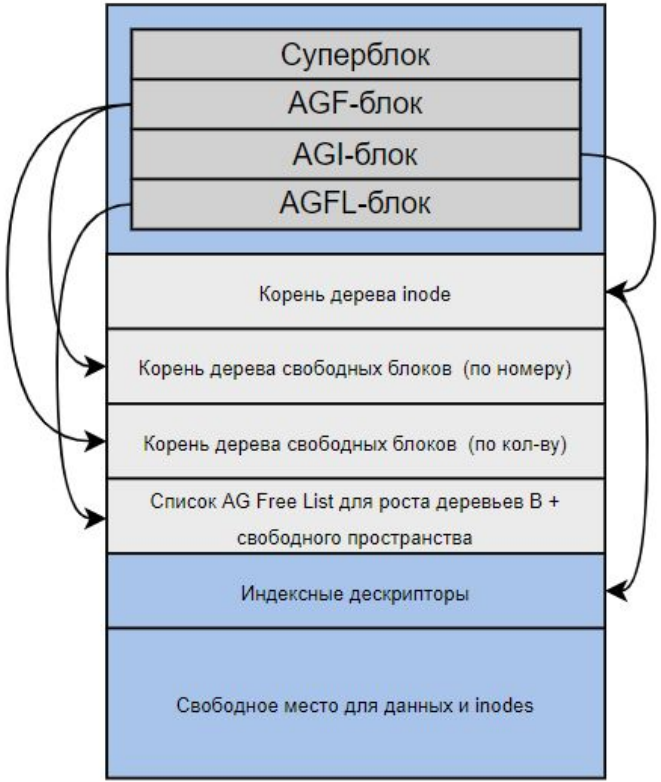


рис. Область памяти AG

Обзор: журналирование в XFS

- журнал цикличный
- состоит из транзакций
- транзакции состоят из операций
- изменение в inode, запись буфера

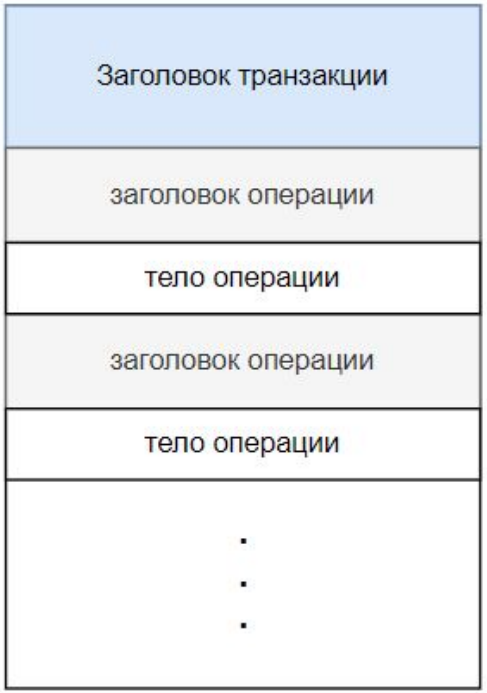
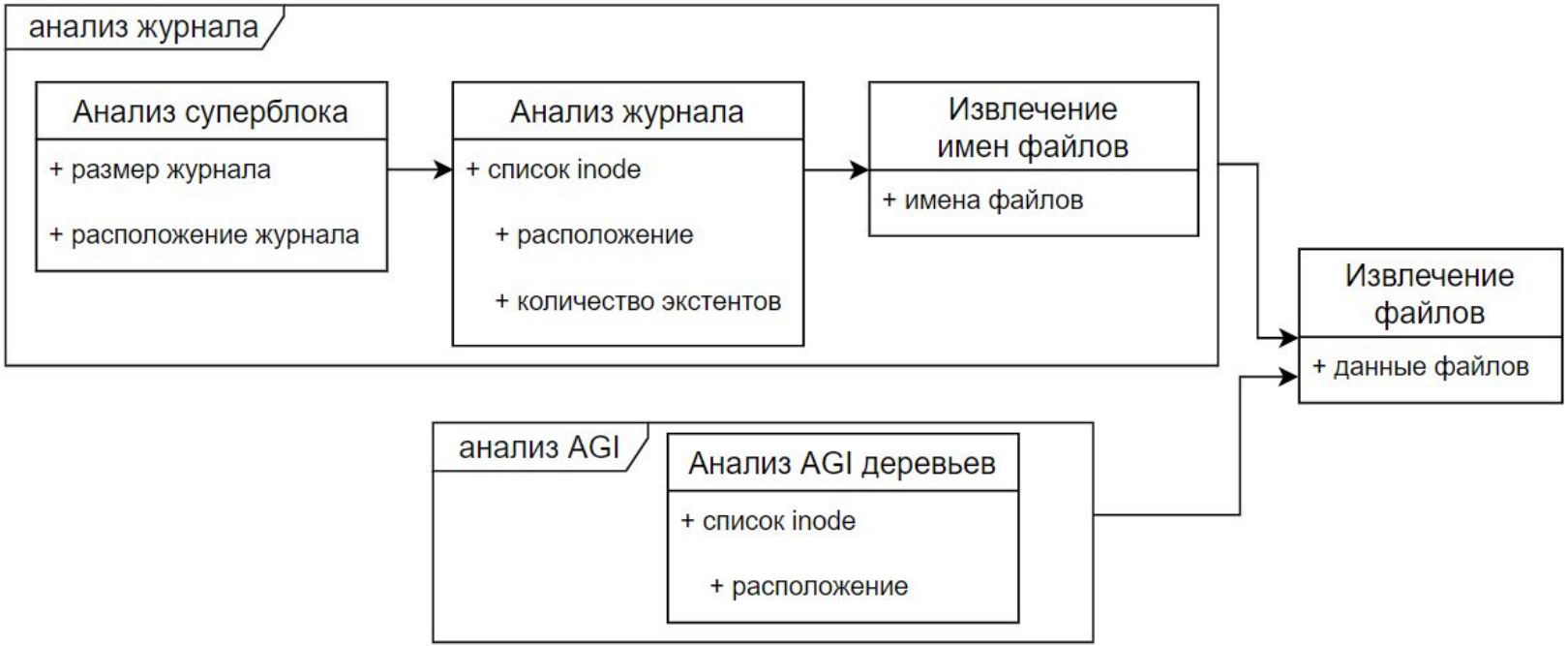


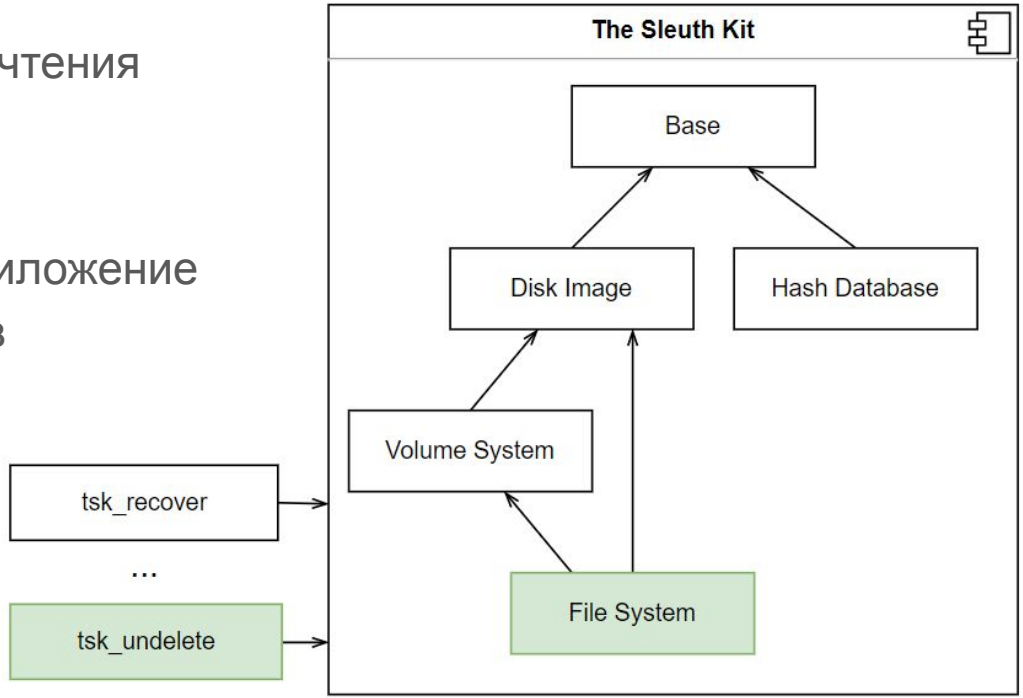
рис. Схема строения транзакции

Алгоритм восстановления файлов

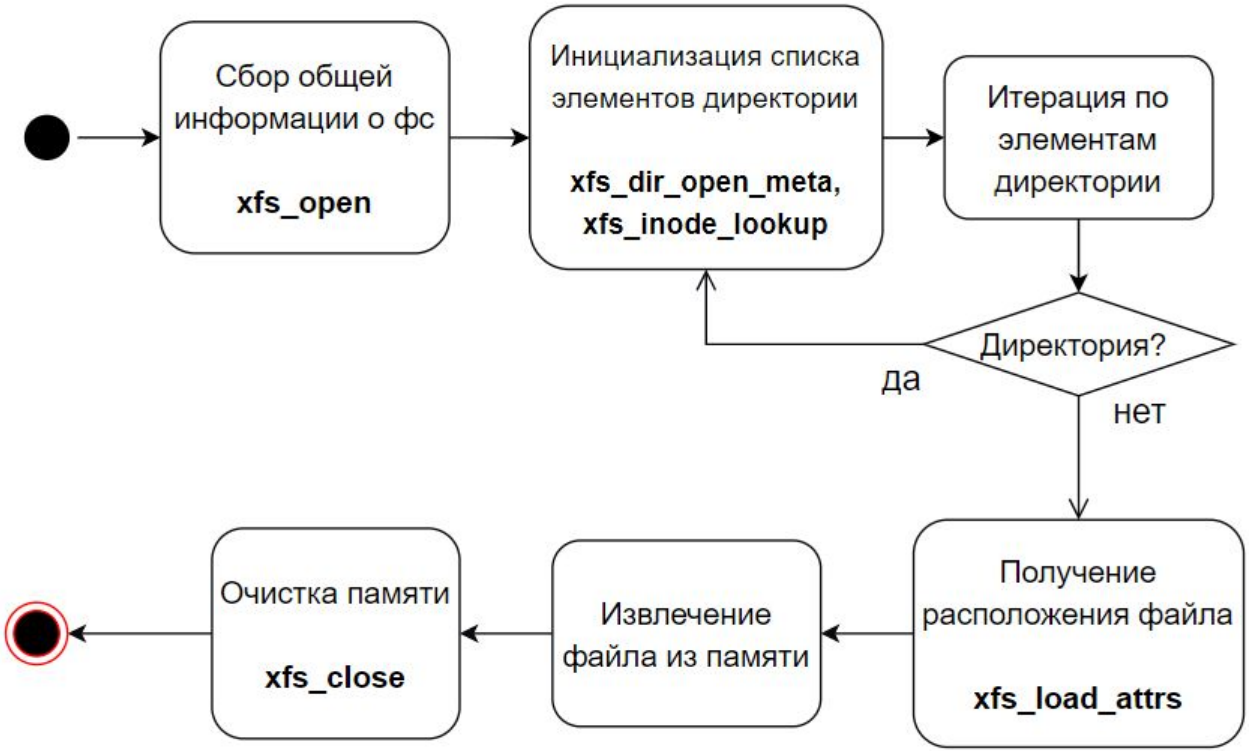


Детали реализации

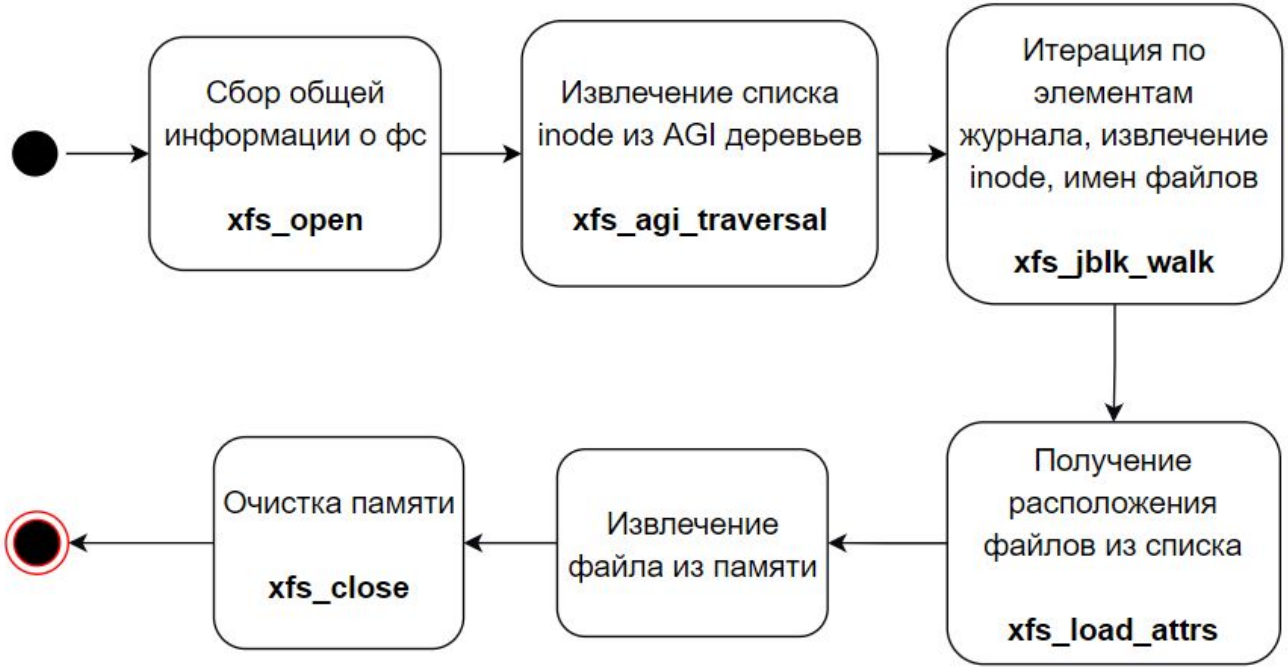
- язык C
- интерфейс для реализации чтения
  - xfs_open
  - dir_open_meta
  - xfs_load_attrs
- реализовано консольное приложение для восстановления файлов



Детали реализации: чтение



Детали реализации: восстановление



Эксперименты. Создание тестовых образов

- Oracle VirtualBox с установленным на нем дистрибутивом Linux Ubuntu 20.04 LTS. Хостовой ОС выступала Windows 10
- Диск отформатирован утилитой mkfs
- Было создано по образу для каждого типа директории, с 4, 256 и 2000 файлами
- Удалены файлы с различными ситуациями расположения, в корневой директории, на первом уровне вложенности и на втором, из различных типов директорий

Эксперименты. Результаты

№	удалено файлов, шт.	извлечено файлов всего, шт.	извлечено файлов без имени, шт.	извлечено файлов, AGI анализ	извлечено уникальных файлов, комбинация методов	примечание
1	1	1	0	1	1	файл из рутовой директории
2	3	3	0	2	3	удалено по файлу из каждого типа директорий
3	9	9	0	2	9	удалено 2 директории целиком
4	2	0	0	1	1	сбой в системе при удалении файла
5	неизвестно	4	0	0	4	предоставлен Belkasoft (тестовый)
6	неизвестно	4	2	240	242	предоставлен Belkasoft (тестовый)
7	неизвестно	212	10	16	220	предоставлен Belkasoft (тестовый)

Заключение

1. Проведен обзор существующих решений и файловой системы XFS
2. Разработан алгоритм восстановления файлов из образов дисков XFS
3. Реализовано расширение TSK для чтения и восстановления файлов из XFS
4. Проверены алгоритмы чтения и восстановления