Санкт-Петербургский государственный университет
Кафедра системного программирования

Извлечение данных SIM-карты с использованием считывателя карт

Даниил Федорович Степырев, 22.M04-мм

Научный руководитель: к.т.н. Ю.В. Литвинов, доцент кафедры системного программирования
Консультант: Н.М. Тимофеев, архитектор ООО «Цифровая Корпоративная Защита»

Санкт-Петербург
2024

Введение

- Цифровая криминалистика — наука, направленная на получение, обработку и анализ данных
  - Используется в судебной практике
- SIM-карта хранит данные о пользователе
  - Телефонная книга
  - SMS-сообщения
- Belkasoft X

Существующие способы извлечь данные SIM-карты

Существующие способы извлечения данных SIM-карты:

- Логический:
  - Использование телефона
  - Требуются ручные действия
  - Не все телефоны позволяют экспортировать данные SIM-карты
  - Проблемы совместимости с устройствами и протоколами
- Физический:
  - Использование считывателя карт
  - Автоматизация извлечения данных
  - Анализ артефактов
  - Не зависит от производителя и модели телефона

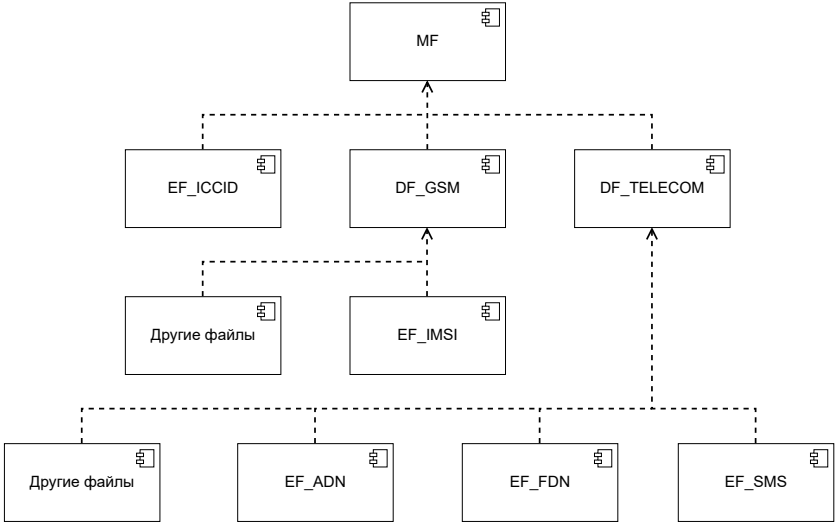
Постановка задачи

Целью работы является разработка модуля, предназначенного для извлечения данных SIM-карты с использованием считывателя карт

Задачи, поставленные в рамках учебной практики:

- Выполнить обзор предметной области — файловой системы SIM-карты, аналогов разрабатываемого модуля
- Выяснить принцип извлечения данных SIM-карты
- Спроектировать и реализовать модуль, извлекающий файловую систему SIM-карты с использованием считывателя карт
- Спроектировать и реализовать модуль, выполняющий разбор извлечённых данных SIM-карты
- Выполнить интеграцию в продукт Belkasoft X

Файловая система SIM-карты

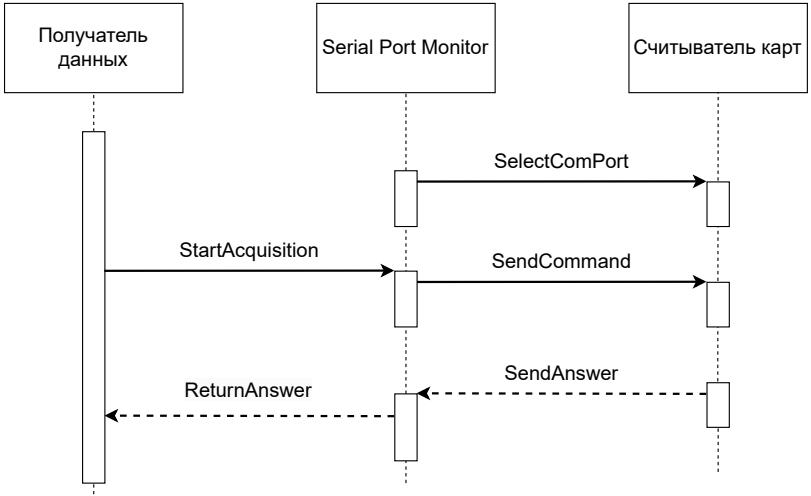


Обзор аналогов

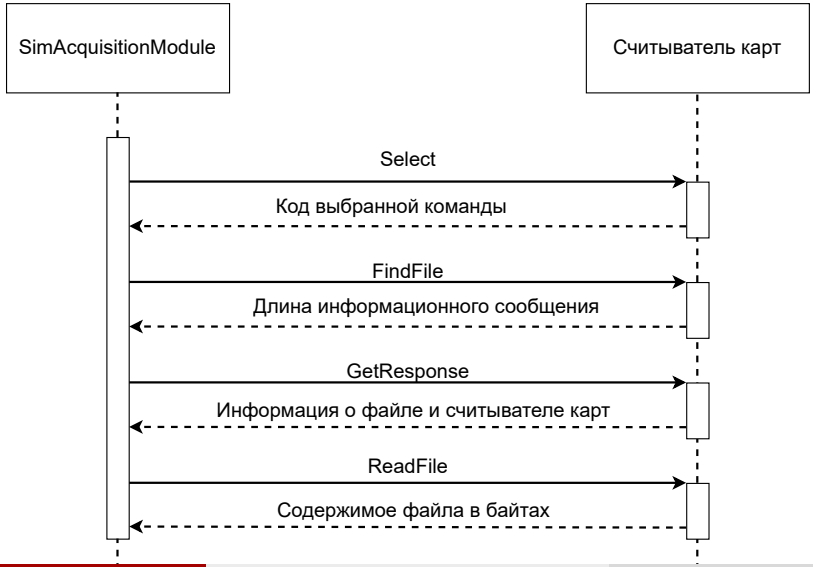
Название	Извлечение файловой системы	Разбор файловой системы	Верификация PIN-кода	Доступность
E3[1]	Есть	Есть	Есть	Триальная версия на 30 дней, 1850$ в год
Detective[2]	Есть	Есть	Есть	Триальная версия на 20 дней, 8090€ в год
SimLAB	Есть	Нет	Есть	В свободном доступе
Osmo-sim-auth	Есть	Нет	Есть	В свободном доступе
DualSim-Card	Есть[3]	Нет	Нет	В свободном доступе

[1] Полное название: E3: Electronic Evidence Examine
[2] Полное название: Oxygen Forensics Detective
[3] Доступно извлечение только данных оператора

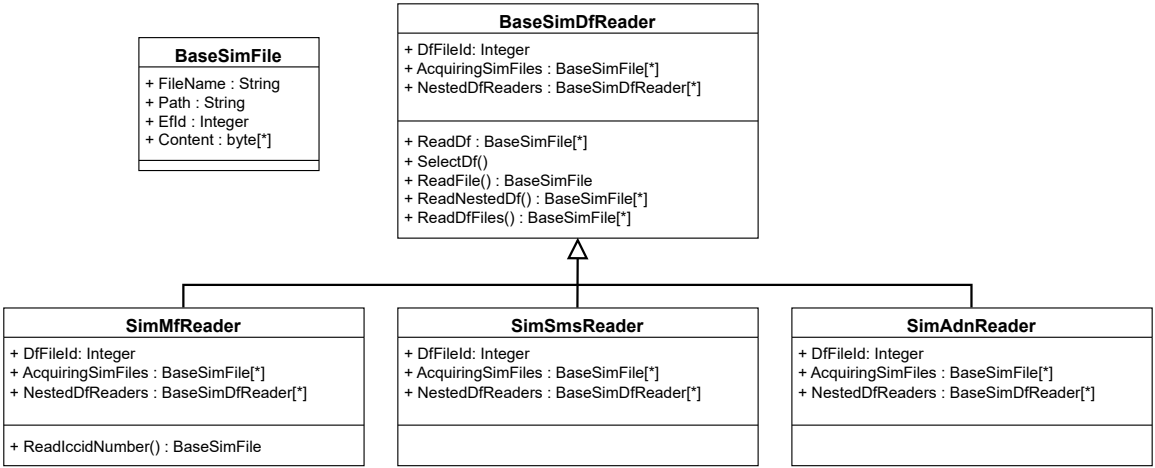
Принцип извлечения данных SIM-карты



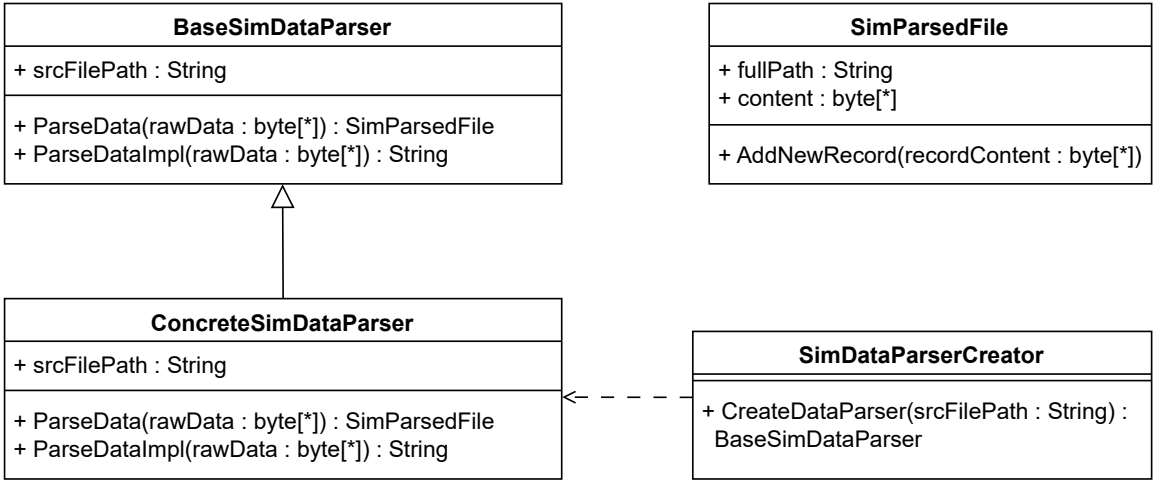
Алгоритм извлечения данных SIM-карты



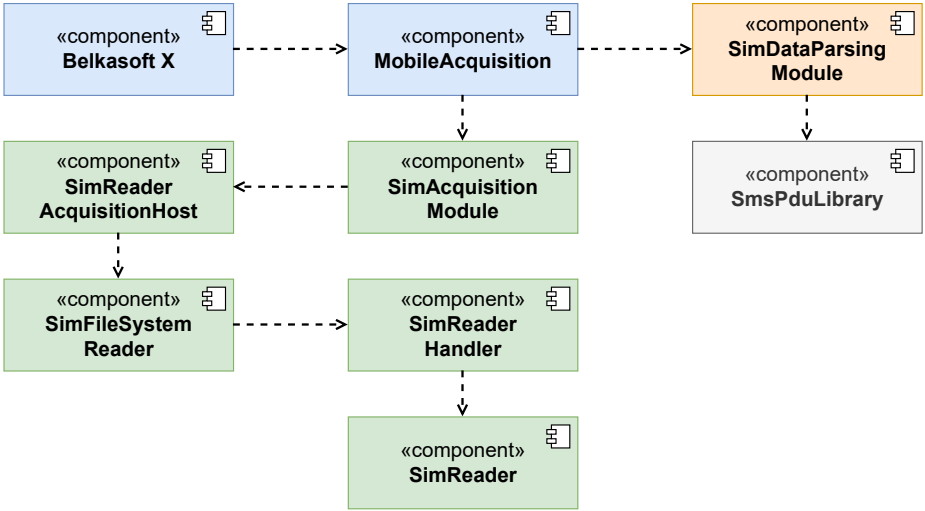
Извлечение файловой системы SIM-карты



Разбор извлечённой файловой системы SIM-карты



Интеграция в Belkasoft X



Апробация и тестирование

- Файловая система SIM-карты была успешно извлечена с SIM-карт различных операторов
  - Были использованы SIM-карты операторов Tele2, Megafon, Beeline, MTS
- Реализованный модуль выполнил разбор большего числа файлов, чем аналогичный доступный продукт
- Алгоритмы кодирования файлов для SIM-карт Tele2, Megafon и Beeline отличались
  - Разработанный модуль успешно выполнил разбор данных для всех алгоритмов
- Реализованная функциональность прошла проверку кода, была интегрирована в исходный код проекта Belkasoft X и была проверена командой тестирования компании «Цифровая Корпоративная Защита»

Результаты

Результаты:

- Проанализированы существующие аналоги разрабатываемого решения: E3: Electronic Evidence Center, Oxygen Forensics Detective, SimLab, Osmo-sim-auth, DualSimCard
- Выяснен принцип извлечения данных SIM-карты: команды и ответы на них отправляются в байтах согласно стандарту ISO 7816
- Спроектированы и реализованы модули, извлекающие и выполняющие разбор файловой системы SIM-карты (C++, C#, C++/CLI)
- Выполнена интеграция разработанного модуля в Belkasoft X: реализованная функциональность была добавлена в исходный код проекта