



Санкт-Петербургский государственный университет
Кафедра системного программирования

Извлечение данных SIM-карты с использованием считывателя карт

Даниил Федорович Степырев, 22.М05-мм

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

Консультант: Н.М. Тимофеев, архитектор ООО “Цифровая корпоративная защита”

Санкт-Петербург
2022

- 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:

- Использование телефона
 - ▶ Требуются ручные действия
 - ▶ Не все телефоны позволяют экспортировать данные SIM-карты
- Использование считывателя карт
 - ▶ Автоматизация извлечения данных
 - ▶ Анализ артефактов

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 ограниченное число файлов с SIM-карты с использованием считывателя карт
- Выполнить интеграцию в продукт Belkasoft X

Файловая система SIM-карты

- Древовидная структура
- Корневой элемент MF¹
- Элементарные файлы EF²
- Вложенные файлы DF³
 - ▶ Содержат файлы EF и DF

¹Master File

²Elementary File

³Dedicated File

Обзор аналогов

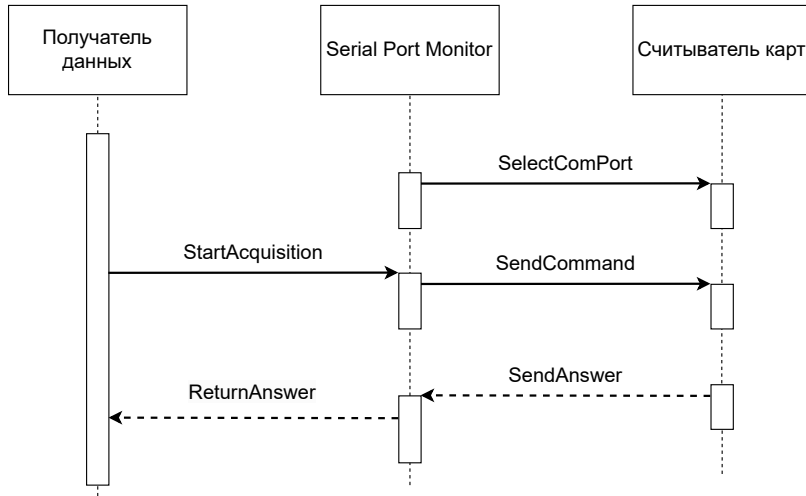
Название	Извлечение файловой системы	Разбор файловой системы	Верификация PIN-кода	Доступность
E3 ⁴	Есть	Есть	Есть	Триальная версия на 30 дней, 1850\$ в год
Detective ⁵	Есть	Есть	Есть	Триальная версия на 20 дней, 8090€ в год
SimLAB	Есть	Нет	Есть	В свободном доступе
Osmo-sim-auth	Есть	Нет	Есть	В свободном доступе
DualSim-Card	Есть ⁶	Нет	Нет	В свободном доступе

⁴ Полное название: E3: Electronic Evidence Examine

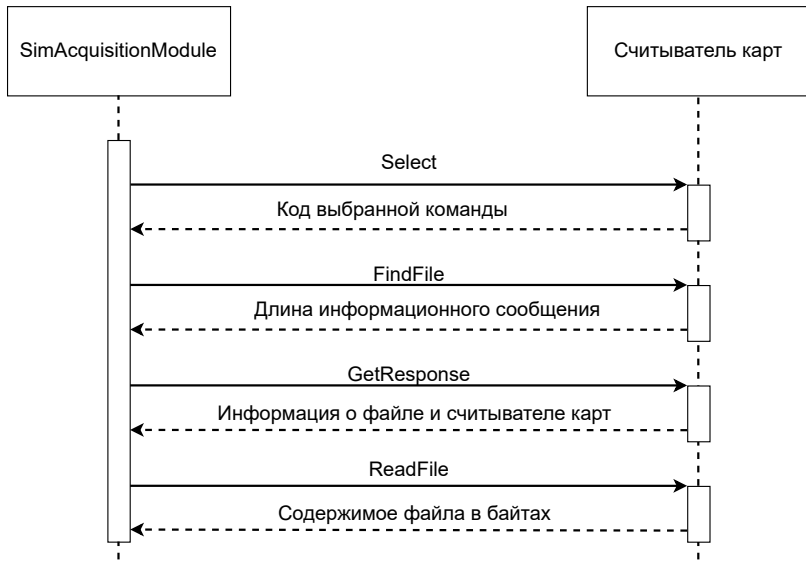
⁵ Полное название: Oxygen Forensics Detective

⁶ Доступно извлечение только данных оператора

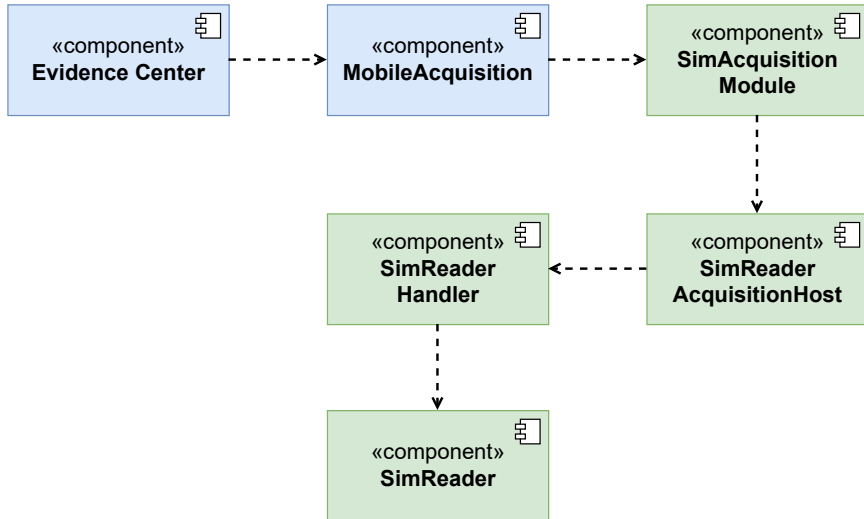
Принцип извлечения данных SIM-карты



Алгоритм извлечения данных SIM-карты



Интеграция в Belkasoft X



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
- Спроектирован и реализован модуль, извлекающий четыре файла SIM-карты с использованием считывателя карт: номер IMSI, книга ADN, сообщения SMS и оператор SIM-карты
- Выполнена интеграция разработанного модуля в Belkasoft X

Задачи, поставленные в рамках ВКР:

- Реализовать полное снятие файловой системы SIM-карты
- Реализовать разбор извлечённой файловой системы SIM-карты
- Реализовать верификацию PIN-кода и PUK-кода
- Провести тестирование и апробацию разработанного модуля