Санкт-Петербургский государственный университет
Кафедра системного программирования

Извлечение данных SIM-карты с использованием считывателя карт

Даниил Федорович Степырев, 22.M05-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

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:

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

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

Файловая система SIM-карты

- Древовидная структура
- Корневой элемент MF[1]
- Элементарные файлы EF[2]
- Вложенные файлы DF[3]
  - Содержат файлы EF и DF

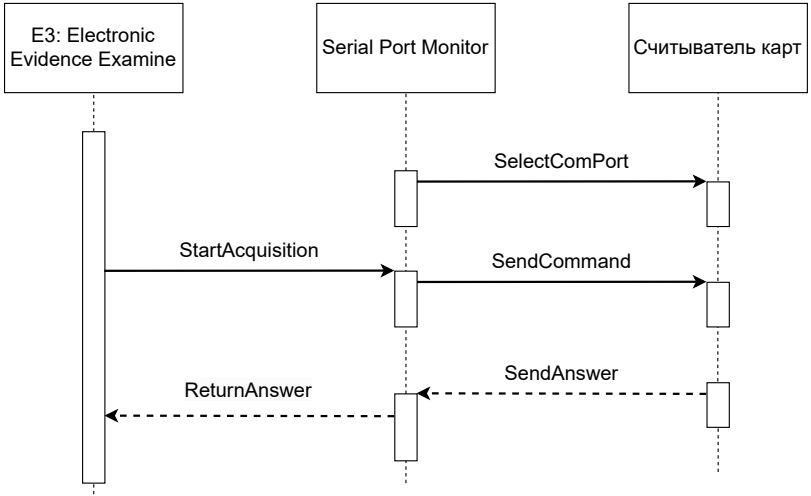
[1] Master File
[2] Elementary File
[3] Dedicated File

Обзор аналогов

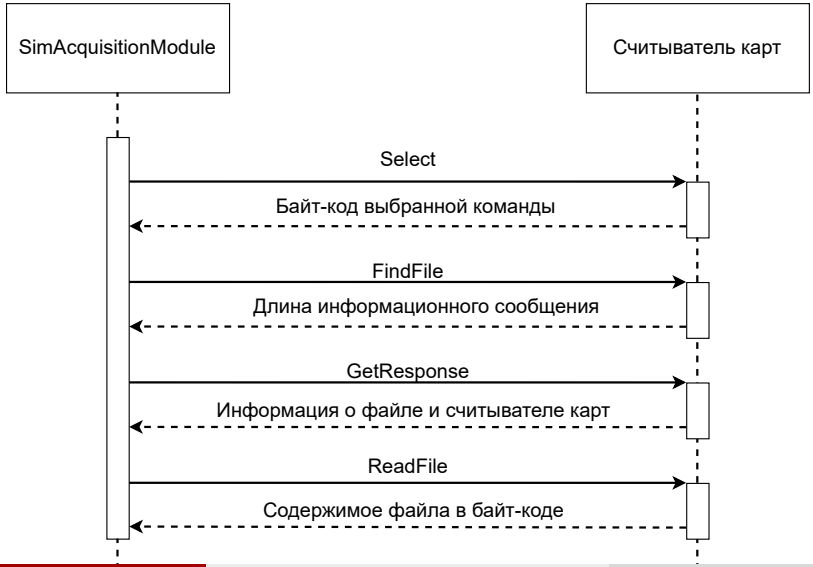
Название	Извлечение файловой системы	Разбор файловой системы	Верификация PIN-кода	Доступность
E3[4]	Есть	Есть	Есть	Триальная версия на 30 дней, 1850$ в год
Detective[5]	Есть	Есть	Есть	Триальная версия на 20 дней, 8090€ в год
SimLAB	Есть	Нет	Есть	В свободном доступе
Osmo-sim-auth	Есть	Нет	Есть	В свободном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

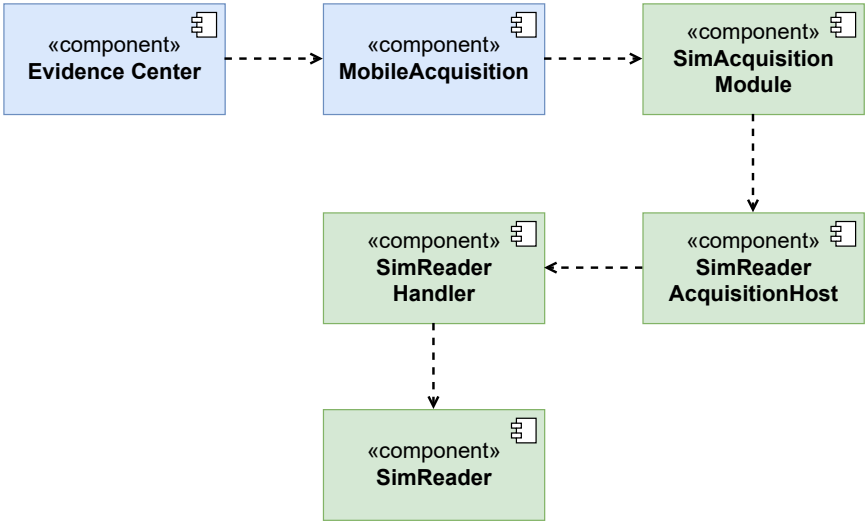
Принцип извлечения данных SIM-карты



Алгоритм извлечения данных SIM-карты



Интеграция в Belkasoft X



Результаты

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 BKP:

- 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