Санкт-Петербургский государственный университет

Степырев Даниил Федорович

Учебная практика

Извлечение данных SIM-карты с использованием считывателя карт

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

Консультант:
архитектор ООО «Цифровая корпоративная защита» Н.М. Тимофеев

Санкт-Петербург
2022

Оглавление

1. Введение

С развитием технологий в современном мире возрастает и число цифровых преступлений [1]. Примерами таких преступлений могут быть кражи личных данных, распространение противоправной информации, вмешательство в работу приложений и многое другое.

Цифровая криминалистика — наука, помогающая обнаружить, зафиксировать и исследовать компьютерные доказательства для подтверждения противоправных действий. Цифровая криминалистика не предназначена для противоправных действий, она используется только с разрешения суда.

Для обнаружения доказательств, подтверждающих цифровые преступления, эксперты цифровой криминалистики снимают данных с различных устройств [2]. Полезные для расследований данные могут находиться в памяти цифровых устройств, внешних запоминающих устройств, в облачных хранилищах данных. Одним из таких устройств является разновидность смарт-карт — SIM-карта.

На SIM-карте хранится идентификационная информация о пользователе: международный номер мобильного абонента (IMSI), ключ аутентификации пользователя (KI). Однако помимо идентификационной информации на SIM-карте также хранятся и данные о пользователе: телефонная книга, журнал звонков, принятые и отправленные SMS-сообщения [3]. Подобная информация может быть полезна экспертам в области цифровой криминалистики.

Чтение SIM-карт производится с помощью специальных устройств, называемых считывателями карт [4]. SIM-карта вставляется в специальный разъём устройства, которое затем подключается через USB-порт к компьютеру.

Интерес к снятию данных с SIM-карт возник у компании «Цифровая корпоративная защита» при разработке продукта Belkasoft X[1]. Belkasoft X — инструмент цифровой криминалистики, разработанный для снятия и анализа данных с компьютера, мобильных устройств, об-

[1]https://belkasoft.com/ru/x (дата обращения: 23.12.22).

лачных хранилищ.

На момент написания данной работы существует несколько работающих проектов, поддерживающих извлечение данных SIM-карты с использованием считывателя карт. Тем не менее эти проекты либо не позволяют выполнять полное снятие и разбор файловой системы SIM-карты, либо представляют собой условно-бесплатные ограниченные версии.

Однако с помощью инструментов обратной разработки можно выяснить принцип снятия данных с SIM-карты и реализовать модуль, позволяющий извлекать всю файловую системы SIM-карты с использованием считывателя карт. Реализация такой функциональности для коммерческого продукта Belkasoft X и стала целью данной работы.

2. Постановка задачи

Целью представленной работы является разработка модуля, предназначенного для извлечения данных SIM-карты с использованием считывателя карт. Для достижения цели были поставлены задачи.

- 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 разработанного модуля в продукт Belkasoft X.

3. Обзор

3.1. Файловая система SIM-карты

Файловая система SIM-карты имеет древовидную структуру. Корневым элементом файловой системы является главный файл (Master File). Он содержит в себе все остальные файлы, хранимые на SIM-карте [5]. Помимо главного файла существует ещё два типа файлов: элементарные и вложенные.

Элементарные файлы (Elementary File) содержат в себе только данные. Такие файлы не могут содержать внутри себя другие файлы. Данные в элементарных файлах хранятся в виде байтов с определённой в документации кодировкой. Пример элементарного файла — файл EF_IMSI [6]. Этот файл содержит в себе информацию об IMSI-номере SIM-карты.

Вложенные файлы (Dedicated File) содержат в себе другие файлы. Во вложенном файле могут находиться как элементарные файлы, так и другие вложенные файлы. Зачастую данные разбиваются на несколько элементарных файлов и хранятся в одном вложенном файле. Примером подобных файлов может являться телефонная книга номеров сокращённого набора ADN [7].

3.2. Считыватель карт

Считыватель карт — специальное устройство, предназначенное для взаимодействия с SIM-картой. Устройство имеет отдельное отверстие для подключения SIM-карты. Считыватель карт подключается через USB-порт компьютера и позволяет читать данные SIM-карты по COM-порту. Пример считывателя карт, используемого в данной работе, представлен рис. 1.

Рис. 1: Изображение считывателя карт.

3.3. Обзор аналогов

В обзоре описаны популярные инструменты, предназначенные для извлечения данных SIM-карты с использованием считывателя карт. Аналоги выбирались с помощью поисковой системы Google с использование ключевых слов «SIM card», «acquisition», «Reader», «tools».

3.3.1. E3: Electronic Evidence Examine

E3: Electronic Evidence Examine — продукт, распространяемый компанией Paraben, позволяющий извлекать данные с SIM-карты [8]. Инструмент ранее существовал как отдельный проект SIMCon, однако компания Paraben выкупила права на пользование и интегрировала его в качестве модуля продукта E3: Electronic Evidence Examiner. Инструмент позволяет извлекать и анализировать всю файловую систему SIM-карты, а также поддерживает верификацию PIN-кода. Проект поддерживается в настоящее время. Продукт E3: Electronic Evidence Examine платный, стоимость лицензии составляет 1895$ в год. Однако компания Paraben предоставляет бесплатную версию продукта на 30 дней.

3.3.2. Oxygen Forensics Detective

Oxygen Forensics Detective — продукт компании Oxygen Forensics, позволяющий извлекать данные с SIM-карты [9]. Инструмент помимо извлечения и анализа всей файловой системы SIM-карты, поддерживает верификацию PIN-кода. Проект поддерживается в настоящее время. Продукт платный, стоимость лицензии составляет 8090€ в год. Компания Oxygen Forensics предоставляют бесплатную версию продукта на 20 дней.

3.3.3. SimLAB

SimLAB — продукт с открытым исходным кодом, который позволяет извлекать файловую систему SIM-карты [10]. Инструмент также поддерживает верификцию PIN-кода. Инструмент simLAB не позволяет разбирать извлечённые файлы SIM-карты. В описании simLAB также указано, что SIM-карта может быть заблокирована, а автор не даёт никакой гарантии. Последние обновления в проекте были в 2016 году.

3.3.4. Osmo-sim-auth

Osmo-sim-auth — продукт с открытым исходным кодом, позволяющий извлекать файловую систему SIM-карты [11]. Инструмент помимо извлечения файловой системы SIM-карты также поддерживает верификцию PIN-кода. Osmo-sim-auth не позволяет проанализировать извлечённые с SIM-карты файлы. Последние обновления в проекте были в 2017 году.

3.3.5. DualSIMCard

DualSIMCard — продукт с открытым исходным кодом, предназначенный для извлечения данных SIM-карты [12]. Инструмент позволяет извлекать лишь часть файлов SIM-карты и не извлекает файлы, связанные с данными пользователя. DualSIMCard не поддерживает разбор извлечённых данных и верификацию PIN-кода. Последние обновления

в проекте были в 2019 году.

3.3.6. Сравнение аналогов

Рассмотренные аналоги представлены в таблице 1. Большинство рассмотренных аналогов позволяет извлекать файловую систему SIM-карты. Однако не все из них поддерживают полный разбор файловой системы. Только платные продукты E3: Electronic Evidence Examine [8] и Oxygen Forensics Detective [9] предоставляют такую возможность. Продукты simLAB, DualSIMCard [10, 12] позволяют только извлекать данные SIM-карты. С помощью доступных инструментов нельзя гарантированно извлечь и разобрать файловую систему SIM-карты.

Название	Извлечение файловой системы SIM-карты	Разбор файловой системы SIM-карты	Верификация PIN-кода	Актуальность	Доступность
E3: Electronic Evidence Examine	Есть	Есть	Есть	Поддерживается в настоящее время	Платная лицензия стоимостью 1895$ в год, триальная версия на 30 дней
Oxygen Forensics Detective	Есть	Есть	Есть	Поддерживается в настоящее время	Платная лицензия стоимостью 8090€ в год, триальная версия на 20 дней
SimLAB	Есть	Нет	Есть	Последнее обновление в 2016 году	В свободном доступе
Osmo-sim-auth	Есть	Нет	Есть	Последнее обновление в 2017 году	В свободном доступе
DualSIM Card	Только данные оператора	Нет	Нет	Последнее обновление в 2019 году	В свободном доступе

Таблица 1: Сравнительные характеристики аналогов

Продукты E3: Electronic Evidence Examine, Oxygen Forensics Detective [8,9] поддерживаются в настоящее время. Последняя модификация в проектах SimLAB, Osmo-sim-auth, DualSIMCard [10, 12] была в 2016, 2017 и 2019 годах.

Большинство продуктов поддерживают алгоритм верификации PIN-кода SIM-карты. Такая функциональность недоступна только в проекте DualSIMCard.

С помощью инструментов с открытым исходным кодом нельзя из-

влечь и разобрать всю файловую систему SIM-карты. Также с помощью продуктов SimLAB, Osmo-sim-auth, DualSimCard [10, 11, 12] не удалось извлечь данные с SIM-карты с использованием тестового считывателя данных.

Для исследования принципа извлечения данных SIM-карты был выбран продукт E3: Electronic Evidence Examine [8], поскольку он поддерживает полное извлечение и разбор файловой системы SIM-карты. Также этого инструмента больший срок бесплатной версии, чем у конкурента от компании Oxygen Forensics.

3.4. Перехват трафика E3: Electronic Evidence Examine

Исследование принципа извлечения данных SIM-карты проводилось с использованием средств обратной разработки. Был перехвачен трафик, передаваемый между продуктом E3: Electronic Evidence Examine [8] и считывателем карт. Для перехвата трафика использовалась бесплатная версия продукта Serial Port Monitor [13]. Архитектура решения представлена на рис. 2 (диаграмма последовательности UML).

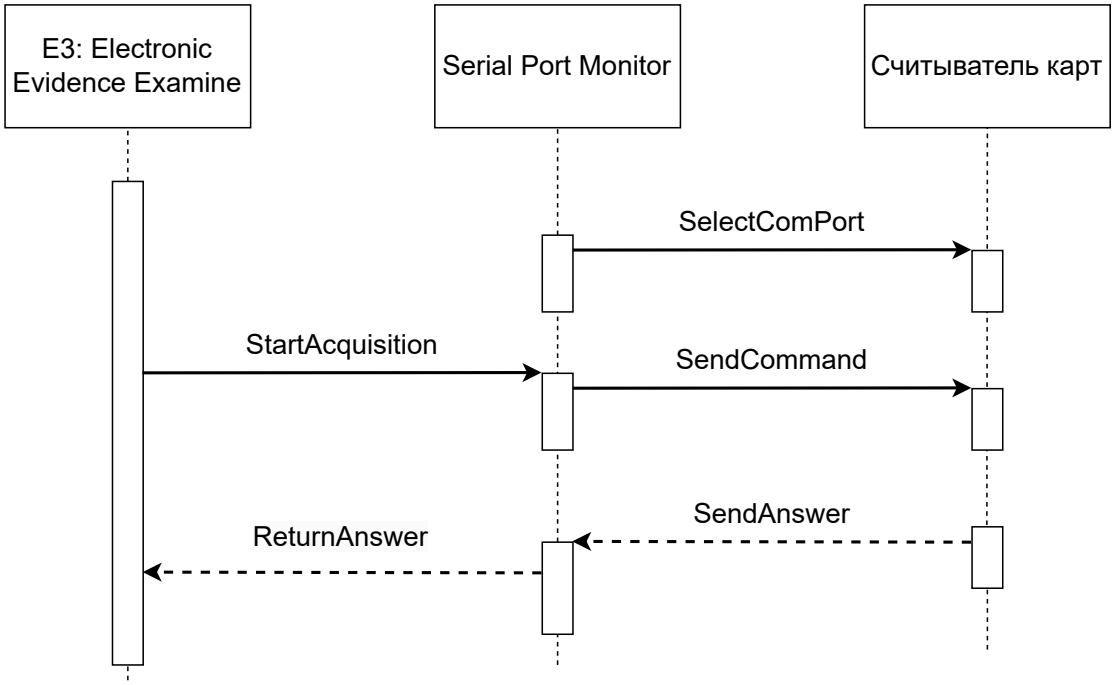

Рис. 2: Перехват трафика E3: Evidence Center Examine.

Перед началом извлечения данных на порт считывателя карт устанавливается перехватчик Serial Port Monitor (сообщение SelectComPort от SerialPortMonitor к считывателю карт). Это позволяет перехватить все отправляемые команды, а также получить ответы на них от считывателя карт.

Затем начинается извлечение данных SIM-карты продуктом E3: Electronic Evidence Examine (сообщение StartAcquisition от E3: Electronic Evidence Examine к считывателю карт). Отправляемые команды перехватываются Serial Port Monitor, записываются в файл и пересылаются считывателю карт (сообщение SendCommand от Serial Port Monitor к считывателю карт).

Полученные от считывателя карт ответы также перехватываются и записываются в файл (сообщение SendAnswer от считывателя карт к Serial Port Monitor). Затем перехватчик пересылает полученные ответы E3: Electronic Evidence Examine (сообщение ReturnAnswer от Serial Port Monitor к E3: Electronic Evidence Examine).

3.5. Извлечение данных SIM-карты

После перехвата трафика E3: Electronic Evidence Examine создаётся файл с перехваченными командами и ответами на них. Из данных этого файла было выяснено, что команды и ответы на них записываются в байтах. Также удалось определить, что взаимодействие со считывателем карт выполняется продуктом с использованием стандарта смарт-карт ISO 7816 [14].

Для доступа к файлу SIM-карты необходимо перейти в директорию, в которой находится файл. Переход в директорию осуществляется с помощью команды выбора файла. Для доступа во вложенную директорию необходимо сначала перейти в родительскую директорию.

Извлечение данных с SIM-карты может быть ограничено установленным PIN-кодом. Определить, установлен ли такой код на SIM-карту можно по полученному ответу от считывателя карт. Если PIN-код установлен, для доступа к данным SIM-карты необходимо пройти его вери-

фикацию.

На ввод PIN-кода предоставляется три попытки. После трёх неправильных попыток ввода PIN-кода, SIM-карта переходит в режим ввода PUK-кода. После десяти неправильных попыток ввода PUK-кода SIM-карта блокируется.

После считывания файла необходимо выполнить разбор полученного ответа от считывателя карт. Необходимо удалить из ответа информацию об исполненной команде и дополненные байты. Оставшиеся байты необходимо разобрать согласно алгоритму кодирования, указанному в стандарте ISO 7816.

4. Архитектура

4.1. Архитектура модуля

Архитектура модуля извлечения данных SIM-карты представлена на рис. 3 (диаграмма компонент UML). Синим цветом обозначены продукты компании «Цифровая корпоративная защита», зелёным цветом — реализованный модуль извлечения данных.

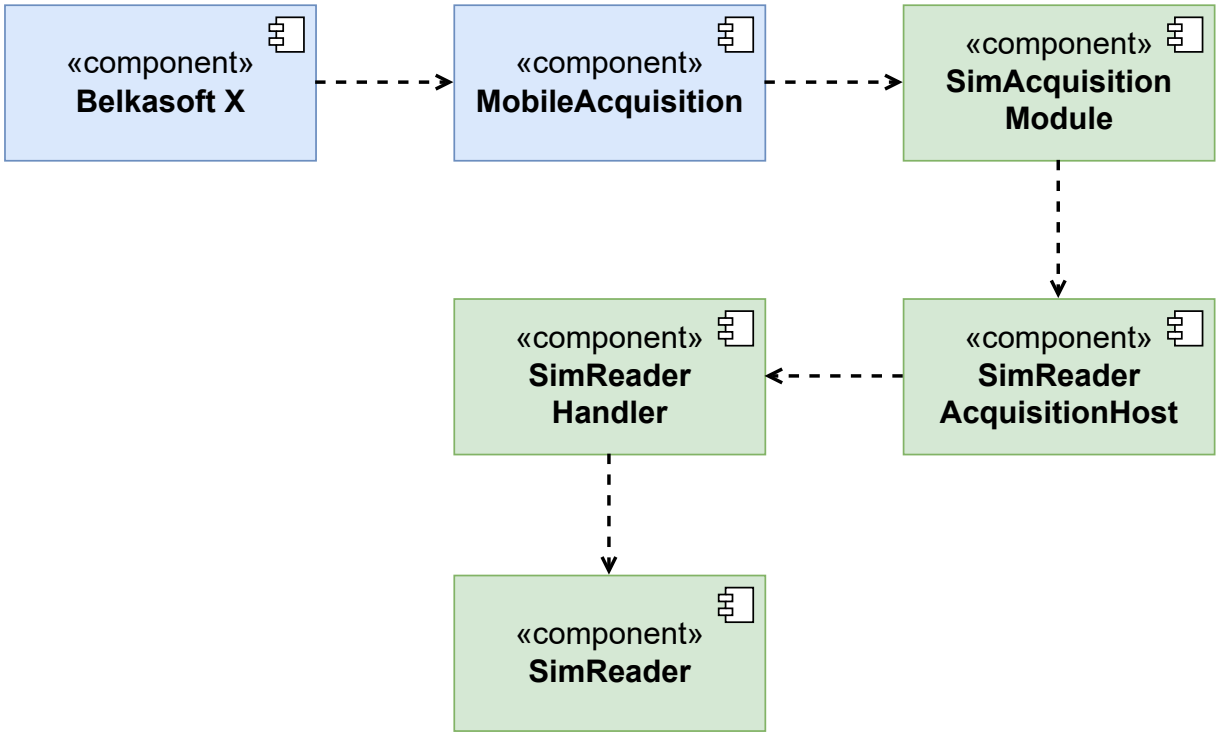

Рис. 3: Диаграмма компонент модуля.

Belkasoft X — инструмент цифровой криминалистики, разработанный для снятия и анализа данных с компьютера, мобильных устройств, облачных хранилищ. Реализован на C# и C++.

MobileAcquisition — модуль, используемый для анализа мобильных устройств и приложений в Belkasoft X. В MobileAcquition есть подмодули, предназначенные для извлечения данных и анализа различных мобильных устройств. Реализован на C#.

SimAcquisitionModule — подмодуль MobileAcquisition, предназначенный для извлечения данных SIM-карты. Модуль интегрирован в продукт Belkasoft X, поэтому реализован на языке программирования C#

и C++.

SimReaderAcquisitionHost используется для конфигурации и сохранения извлекаемых с SIM-карты файлов. На считыватель карт отправляются команды с помощью которых извлекаются данные SIM-карты. Полученные данные сохраняются их в бинарные файлы. SimReaderAcquisitionHost реализован на C#.

SimReaderHandler предназначен для взаимодействия с компонентой SimReader. SimReaderHandler является частью модуля извлечения данных SIM-карты SimAcquisitionModule. Реализован на C++/CLI для связи C# и C++ частей модуля.

SimReader предназначен для взаимодействия со считывателем карт. В SimReader реализованы функции выбора и считывания файла SIM-карты. Реализован на C++, поскольку взаимодействие со считывателем карт выполняется с помощью стандартных функций C++.

4.2. Пользовательский интерфейс

Перед извлечением данных SIM-карты пользователю необходимо выбрать COM-порт, к которому подключён считыватель карт. Программно такой порт нельзя определить заранее, потому что считыватели карт имеют разные названия, которые пользователь может изменять.

При выборе модуля извлечения данных SIM-карт в Belkasoft X пользователю демонстрируется окно с выбором COM-порта, представленное на рис. 4. В этом окне отображаются все подключённые по COM-порту устройства.

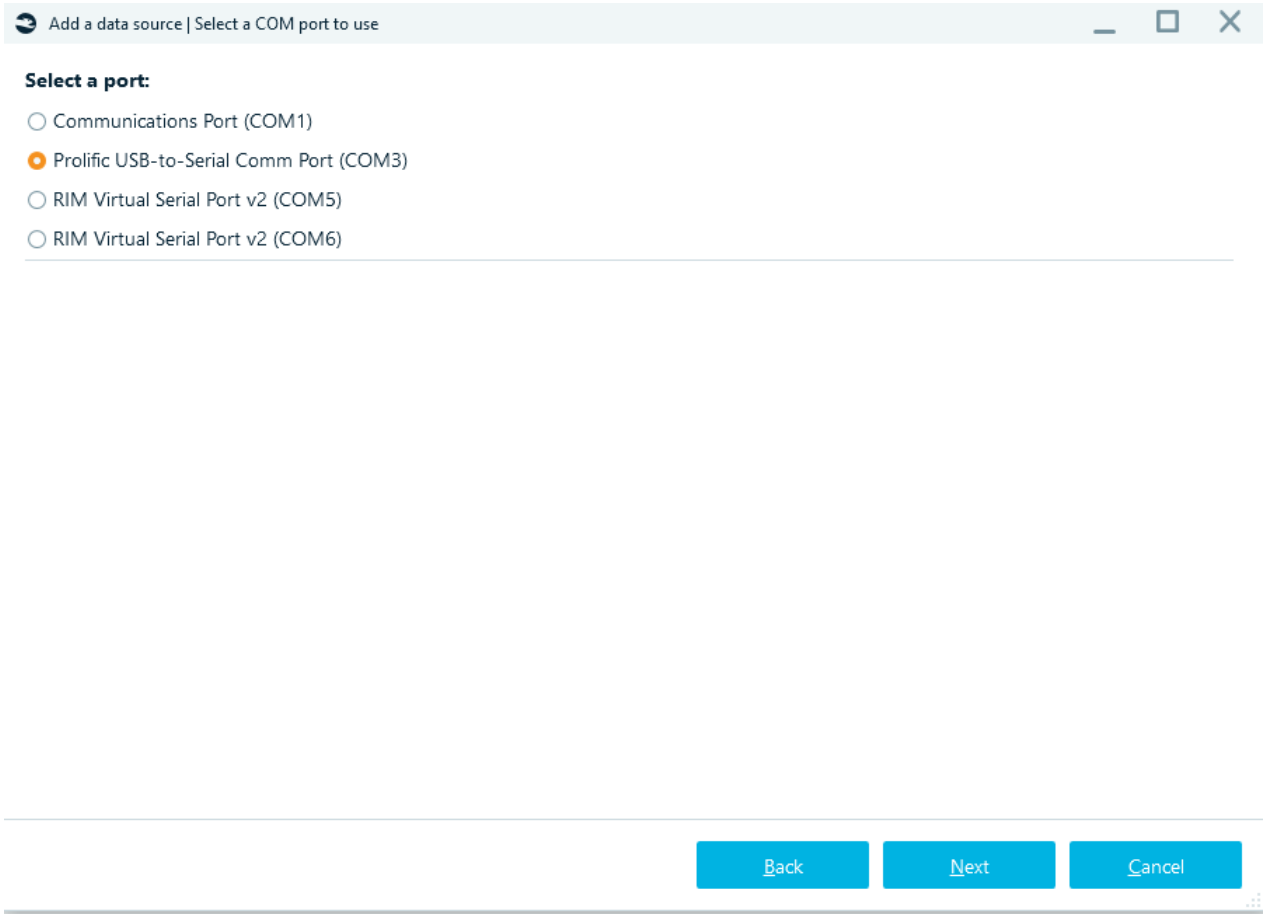

Рис. 4: Окно выбора COM-порта.

Многие считыватели карт в названии содержат значения «USB», «Serial», «Port». Среди всех подключённых по COM-порту устройств выполняется поиск таких значений. По умолчанию на окне выбора COM-порта выбирается устройство, содержащее в названии значения из такого списка. Если устройство не было найдено, выбирается первый элемент списка.

5. Особенности реализации

5.1. Реализация компоненты, взаимодействующей со считывателем карт

Разработанный модуль извлечения данных SIM-карты, представленный на рис. 3 (диаграмма компонент UML), состоит из нескольких частей. Первая часть SimReaderAcquisitionHost отвечает за выбор извлекаемых файлов и сохранение полученных данных в бинарные файлы. Вторая часть SimReader отвечает за взаимодействие со считывателем карт. Общение двух частей производится с помощью SimReaderHandler.

Для взаимодействия со считывателем карт необходимо установить обработчик на COM-порт, к которому подключён считыватель карт. Обработчик можно установить с помощью стандартной команды CreateFileA[2]. После открытия обработчика необходимо прочитать ATR-байты[3].

Отправить команду на считыватель карт можно с помощью стандартной функции WriteFile[4], а прочитать ответ с помощью функции ReadFile[5]. Между отправкой команды и получением ответа необходимо подождать некоторое время. По трафику, перехваченному во время анализа E3: Electronic Evidence Examine [8], было выяснено, что это значение составляет 500 миллисекунд.

Алгоритм извлечения данных SIM-карт представлен на рис. 5 (диаграмма последовательности UML).

[2]https://learn.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-createfilea
[3]https://www.cardlogix.com/glossary/atr-answer-to-reset-smart-card/
[4]https://learn.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-writefile
[5]https://learn.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-readfile

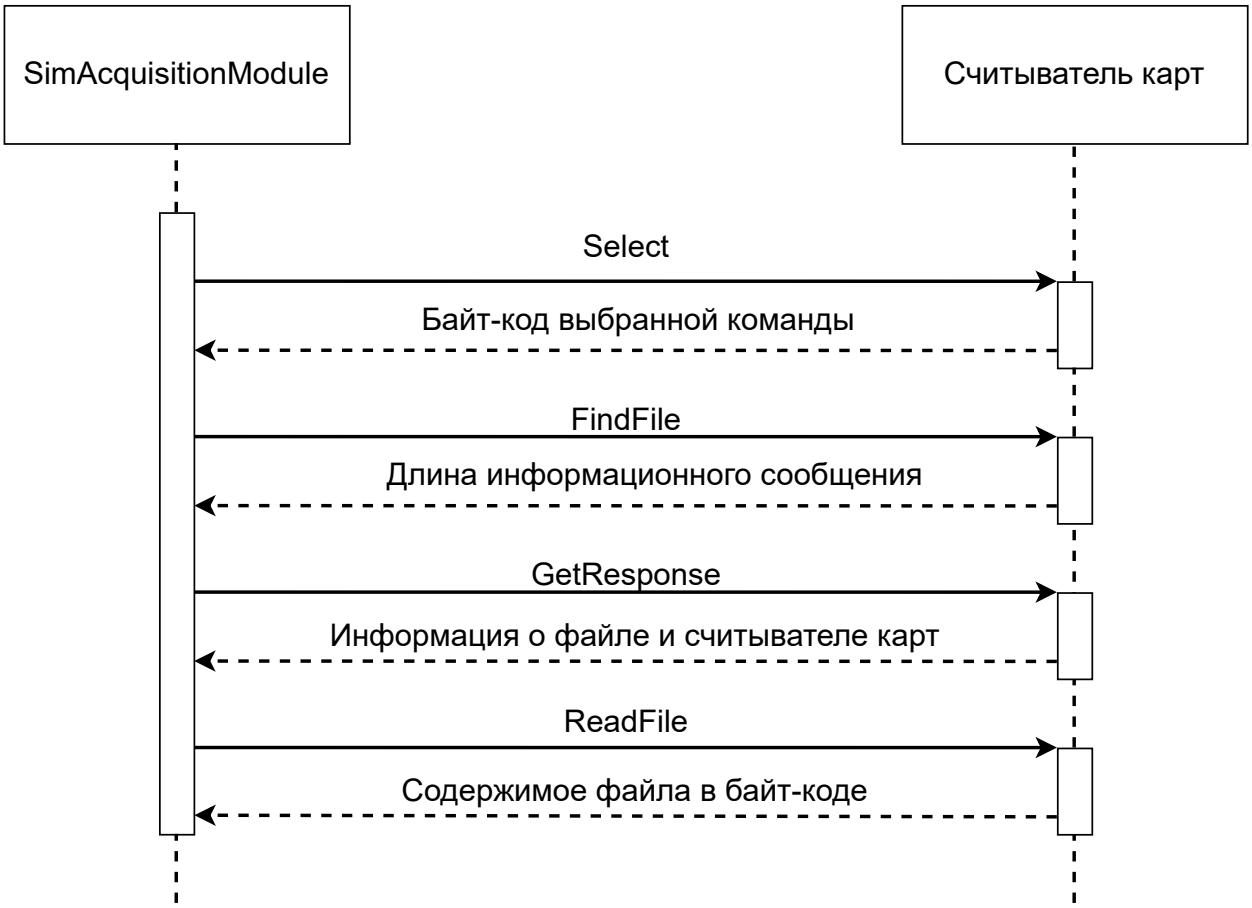

Рис. 5: Алгоритм чтения файла SIM-карты.

Для выбора файла для чтения на SIM-карт, необходимо отправить несколько комманд на считыватель карт. Первая команда Select предназначена для оповещения считывателя карт о том, что необходимо выбрать файл. В этом запросе указывается специальный код команды, описанный в документации. В ответ считыватель карт повторяет отправленную в байтах команду, добавляя в качестве последнего байта код установленной команды.

Для каждого файла на SIM-карте можно прочитать блок данных, содержащий информацию о считывателе карт: установлен ли PIN-код, число оставшихся попыток ввода PIN-кода, а также другие данные. Также такие блоки содержит длину считываемого файла.

Следующей запрос FindFile направлен на поиск считываемого файла. В запрос передаётся тип (EF или DF) и номер файла. В ответ считыватель карт повторяет отправленные байты, добавляя в качестве последних двух байтов результат исполнения команды и длину блока дан-

ных с информацией о считывателе карт и файле. Если файл не удалось найти, отправляются специальные байты.

Следующий запрос ReadInfoFile направлен на получение блока с данными для считываемого файла. В запросе указывается длина блока, полученная в ответ на предыдущий запрос. В ответ считыватель карт повторяет отправленный байты, добавляя содержимое информационного файла.

Последний запрос ReadFile направлен на считывание файла, который был выбран. В запросе указывается команда считывания файла, а также его длина, которую можно определить из информационного блока. В ответ считыватель карт повторяет отправленные байты, добавляя содержимое файла.

5.2. Внедрение C++ кода в C#

Компонента, позволяющая извлекать данные SIM-карты, реализована на языке программирования C++. Разработанный модуль извлечения данных SIM-карты, а также продукт Belkasoft X, в который производится интеграция, реализованы на языках программирования C# и C++.

Для использования C++ кода в C# проекте была реализована компонента SimReaderHandler. SimReaderHandler реализован на языке программирования C++/CLI, что позволяет вызывать код, написанный на C++, в C#-проекте.

Компонента SimReaderHandler реализована с использованием шаблона проектирования «Фасад». Доступны только две функции: выбрать файл, считать содержимое выбранного файла. Вся остальная логика скрыта внутри компоненты SimReader.

6. Тестирование и апробация

Апробация реализованного модуля извлечения данных SIM-карты проводилась с использованием тестового считывателя карт. Были извлечены данные с пяти SIM-карт различных операторов: две SIM-карты Tele2, одна SIM-карта Megafon, одна SIM-карта Beeline и одна SIM-карта MTS. Со всех SIM-карт удалось извлечь четыре файла: номер IMSI, телефонную книгу номеров сокращённого набора ADN, отправленные и полученные сообщения SMS, а также оператора SIM-карты.

Реализованная функциональность прошла проверку кода, была интегрирована в исходный код проекта Belkasoft X и была проверена командой тестирования компании «Цифровая корпоративная защита».

7. Заключение

В ходе данной работы были получены следующие 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 с использованием считывателя карт четыре файла SIM-карты: номер IMSI, книга ADN, сообщения SMS и оператор SIM-карты (C++, c#, C++/CLI).
- Выполнена интеграция разработанного модуля в Belkasoft X. Реализованная функциональность была добавлена в исходный код проекта.

Данную работу планируется продолжать в следующих семестрах и довести до уровня ВКР. В рамках ВКР поставлены задачи:

- 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.

Код проекта закрыт и принадлежит компании ООО «Цифровая корпоративная защита».

Список литературы

[1] Charles Griffiths. The Latest 2022 Cyber Crime Statistics. — AAG, 2022. URL: https://aag-it.com/the-latest-2022-cyber-crime-statistics/ (дата обращения: 23.12.22).

[2] How to Handle Data Acquisition in Digital Forensics. — EC-Council Cybersecurity Exchange, 2022. — URL: https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/data-acquisition-digital-forensics/ (дата обращения: 23.12.22).

[3] Manuel Rozewski. What Information Is Stored On A SIM Card? — SimOptions, 2021. URL: https://www.simoptions.com/sim-card-information/ (дата обращения: 23.12.22).

[4] Milan. What is SIM Card Reader and How Does it Work? — Hybrid Sim, 2021. URL: https://hybridsim.com/sim-card-reader/ (дата обращения: 23.12.22).

[5] Warlock. SIM card forensics: An introduction. — Infosec, 2013. — URL: https://resources.infosecinstitute.com/topic/sim-card-forensics-introduction/ (дата обращения 23.12.22).

[6] Content for TS 31.102. Tech-invite. — URL: https://www.tech-invite.com/3m31/toc/tinv-3gpp-31-102_c.html#e-4-2-2 (дата обращения: 23.12.22).

[7] Content for TS 31.102. Tech-invite. — URL: https://www.tech-invite.com/3m31/toc/tinv-3gpp-31-102_r.html#e-4-4-2-3 (дата обращения: 23.12.22).

[8] E3: Electronic Evidence Examine. — Paraben, 2022. — URL: https://paraben.com/ (дата обращения: 05.12.22).

[9] Oxygen Forensics Detective. — Oxygen Forensics, 2022. — URL: https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective (дата обращения: 05.12.22).

[10] SimLAB. — Kamil Wartanowicz, 2016. — URL: https://github.com/kamwar/simLAB (дата обращения: 05.12.22).

[11] Osmo-sim-auth. — Gerard Pinto, 2017. — URL: https://github.com/GerardPinto/osmo-sim-auth (дата обращения: 05.12.22).

[12] DualSIMCard. — Piotr Zerynger, 2019. — URL: https://github.com/ITger/DualSIMCard (дата обращения: 05.12.22).

[13] Free Serial Port Monitor — COM Port Monitoring, 2022 — URL: https://www.com-port-monitoring.com/#free-monitor (дата обращения: 23.12.22).

[14] Smart Card Standards. — QCard. — URL: https://www.q-card.com/about-us/smart-card-standards/page.aspx?id=1461 (дата обращения: 23.12.22).