Национальный Институт Стандартов и Технологий Экономического Департамента США (NIST)

Судебные программные средства для исследования SIM-карт

Уэйн Дженсен (Wayne Jansen)
Рик Эйерс (Rick Ayers)

Аннотация: Сотовые телефоны и другие портативные устройства, включающие в себя функции сотового телефона (например, смартфоны), повсеместно распространены. Помимо телефонных звонков, сотовые телефоны позволяют пользователям выполнять другие задачи, например: отправлять текстовые сообщения и управлять записями телефонной книги. Когда мобильные телефоны и устройства сотовой связи вовлечены в преступления или другие инциденты, судебным экспертам требуются инструментальные средства, которые позволяют провести надлежащий поиск и быстрое исследование данных, содержащихся в этих устройствах. Для устройств, соответствующих стандартам Глобальной Системы Мобильной Связи (Global System of Mobile communication), некоторые данные, типа набранных номеров, текстовых сообщений и записей телефонной книги, сохраняются на Модуле Идентификации Абонента (Subscriber Identity Module, SIM-карте). Эта статья дает представление о состоянии области судебных программных средств для исследования SIM-карт[1].

[1] В данной статье идентифицированы определённые названия продукции и торговых марок, чтобы проиллюстрировать технические понятия. Однако это не означает, что NIST рекомендует или одобряет их использование.

ОГЛАВЛЕНИЕ

Введение

Стандарты Глобальной Системы Мобильной Связи (GSM) для сотовых сетей, первоначально разработанные Европейской конференцией почтовых и телекоммуникационных ведомств (CEPT), были продолжены Европейским институтом телекоммуникационных стандартов (ETSI) и теперь поддерживаются проектом Партнерство третьего поколения (3GPP). Коммерческая служба GSM начала работу в середине 1991 года. К 1993 году, тридцать шесть сетей GSM работали в двадцати двух странах (Dechaux and Scheller 1993). Хотя система GSM была создана в Европе, она является международным эталоном для сетей, функционирующих в более чем 200 странах во всем мире (GSM World 2006).

Модули Идентификации Абонента (далее SIM- карты) синонимичны с мобильными телефонами и устройствами, которые взаимодействуют с сотовыми сетями GSM. Согласно структуре GSM, сотовый телефон означает «Мобильную Станцию» и состоит из двух различных компонентов: Модуль Идентификации Абонента (SIM- карты) и Мобильного Оборудования ("Mobile Equipment", далее "ME"). SIM- карта – сменный компонент, который содержит основную информацию об абоненте. ME - остальная часть радиотелефонной трубки, не может быть полнофункциональной без SIM- карты. Главная функция SIM- карты сопряжена с установлением подлинности пользователя сотового телефона в сети, чтобы он мог получить доступ к ее услугам. SIM- карта также обеспечивает хранение личной информации, такой как: записи телефонной книги, текстовых сообщений, а так же информации, связанной с услугами сети.

Стандарты GSM организованы различными способами, и разделяются по « фазам», которые они поддерживают. Эти « фазы» определены как: « Фаза 1», « Фаза 2», и « Фаза 2+», которые приблизительно соответствуют поколениям 1, 2 и 2,5 средств сети. SIM- карты часто классифицируются по уровню поддерживаемых спецификаций, которая записана в элемент ее файловой системы (EF Phase). Другой класс SIM- карт, который еще только получает распространение - UMTS SIM- карты (USIM- карты), используемые в третьем поколении (3G) сетей UMTS (Универсальная Система Мобильной Связи). USIM- карты - усовершенствованные версии современных SIM-карт, содержащие совместимую с предыдущими версиями информацию.

Некоторые из первых судебных средств, для исследования сотовых телефонов, предназначались для исследования SIM- карт, не только из-за подробных спецификаций, доступных для них, но также и из-за очень важных и полезных данных, которые можно было бы из них извлечь.

Данная статья предлагает обзор современных судебных программных средств для исследования SIM-карт и типов данных, которые они могут из этих карт считать, а также оценку способностей и ограничений этих средств.

Характеристики SIM-карты

Разделение сотового телефона на SIM- карту и ME, оговорённое в стандартах GSM, привело к портабельности подобных устройств. Перемещение SIM- карты между совместимыми сотовыми телефонами автоматически переносит вместе с ней идентификационные и аутентификационные данные об абоненте и связанную с ним информацию. Напротив, современные телефоны CDMA не используют SIM-карту. Вместо этого, сходные функциональные элементы, обеспечивающие возможности SIM- карт, непосредственно встроены в такие устройства. В то время как SIM- карты наиболее широко используются в системах GSM, сопоставимые модули также используются в телефонах iDEN (улучшенная интегрированная цифровая сеть) и в пользовательском оборудовании UMTS (то есть, USIM). Из-за гибкости, которую SIM- карта предлагает пользователям телефонов GSM для переноса их личной информации, идентификационных и аутентификационных данных между устройствами, в конечном счете, все сотовые телефоны, как ожидается, будут включать (U)SIM- подобные элементы. Например, требования для Сменного Модуля Идентификации Пользователя (R-UIM), обладающего расширенными возможностями по сравнению с SIM- картой, были определены для сотового окружения в соответствии со спецификаций TIA/EIA/IS-95-A и -B, которые включают CDMA на основе технологии широкополосного сигнала (3GPP2 2001).

По своей сути, SIM- карта – это специальный тип смарт-карты, которая обычно содержит микропроцессор и около 16 - 128 Кбайт электрически стираемой, программируемой, постоянной памяти (ЭСППЗУ). Она также включает оперативное запоминающее устройство (ОЗУ) для выполнения программ, и постоянное запоминающее устройство (ПЗУ) для операционной системы, данных аутентификации пользователя, алгоритмов кодирования данных и других приложений. Иерархически организованная файловая система SIM- карты находится в постоянной памяти и хранит такие данные, как записи имен и телефонных номеров, текстовые сообщения и настройки сетевых услуг. В зависимости от используемого телефона, некоторая информация на SIM-карте может быть продублирована в памяти телефона. Альтернативно, информация может находиться полностью в памяти телефона, а не в SIM-карте.

Хотя было стандартизировано два размера SIM-карт, только меньший размер, показанный на Иллюстрации 1, широко используется сегодня в телефонах GSM. Модуль имеет ширину 25 мм, высоту 15 мм и толщину 0,76 мм, и приблизительно равен площади, занимаемой почтовой маркой. Хотя SIM-карты схожи по размерам со сменными картами памяти MiniSD или MMCmobile, поддерживаемыми некоторыми сотовыми телефонами, она придерживается иного набора спецификаций с совсем другими характеристиками. Например, их 8- контактные разъёмы не выровнены вдоль нижнего края, как у сменных карт памяти, а вместо этого образуют округлую контактную площадку, являющуюся основанием чипа смарт-карты, который вставлен в пластиковый каркас. Также, слот для SIM-карты обычно не доступен с внешней стороны телефона, чтобы облегчить частую установку и извлечение, как в случае с картой памяти. Вместо этого, он обычно расположен внутри телефона, в отсеке питания под батареей.

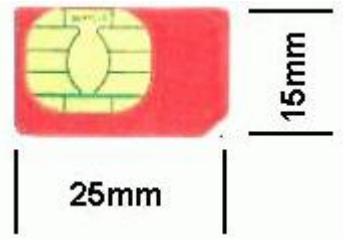


Иллюстрация 1: Геометрические размеры SIM-карты

Когда SIM- карта вставлена в телефонную трубку, для установления связи между ними используется последовательный интерфейс. SIM- карту можно извлечь из телефона и прочитать, используя специализированное устройство и ПО для считывания SIM- карт через тот же самый интерфейс. Для SIM- карт доступны адаптеры, позволяющие вставлять их в стандартное устройство для считывания смарт-карт.

Организация файловой системы

Как показано на Иллюстрации 2, файловая система SIM- карты организована в виде иерархической древовидной структуры, составленной из следующих трёх типов элементов (3GPP 2005a):

- «**Главный Файл**» (“Master File”, далее “**MF**”) – корневая директория файловой системы, которая содержит специальные и элементарные файлы.

- «**Выделенный Файл**» (“Dedicated File”, далее “ **DF**”) – каталог, подчинённый корневой директории, который содержит специальные и элементарные файлы.

- «**Элементарный Файл**» (“Elementary File”, далее “ **EF**”) – файл, который содержит различные типы форматированных данных, структур в виде: либо последовательности байтов данных, либо последовательности записей установленного размера, либо фиксированного набора записей установленного размера, используемых циклически.

Стандарты GSM определяют несколько важных выделенных файлов, расположенных ниже MF: DFGSM, DFDCS1800, и DFTELECOM. Для MF и этих DF определены несколько EF, включая многие обязательные. Файлы EF под DF GSM и DF DCS1800 содержат, главным образом, информацию, имеющую отношение к сети, соответственно для диапазона GSM 900 МГц и DCS (Цифровая Система Сотовой Связи) 1800 МГц. EF для диапазона США 850 МГц и 1900 МГц также расположены, соответственно, под этими DF. Файлы EF под DFTELECOM содержат информацию, относящуюся к услугам. Содержание определенных EF обсуждается далее в статье.

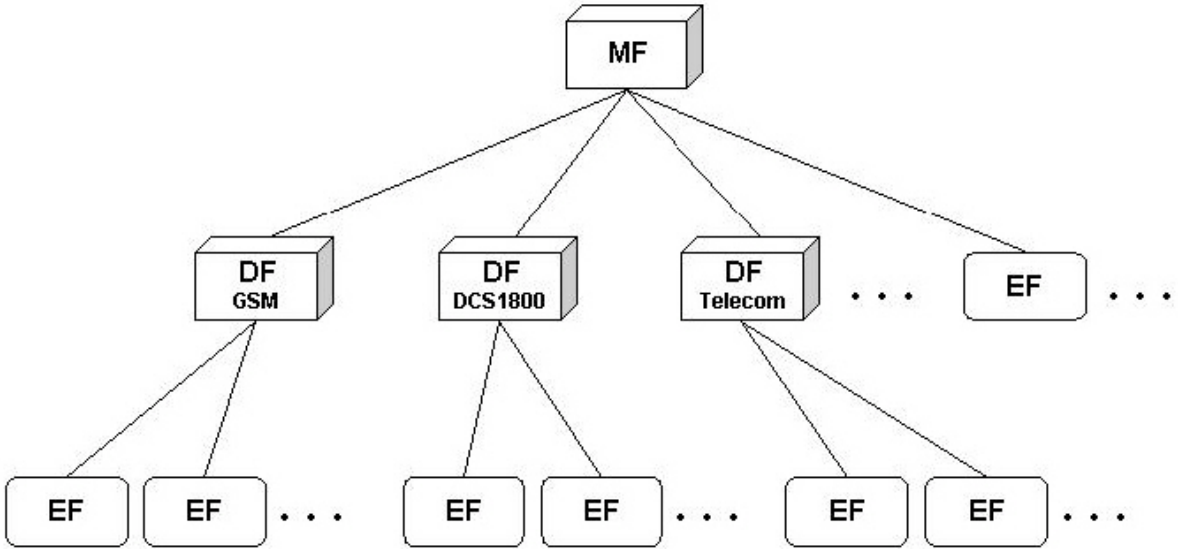


Иллюстрация 2: Файловая система SIM-карты

Хотя файловые системы SIM-карт стандартизированы, стандарты позволяют некоторую гибкость, чтобы можно было менять их содержание среди сетевых операторов и поставщиков услуг. Например, сетевой оператор может не использовать дополнительный элемент файловой системы, а может создать отдельный дополнительный элемент на SIM-карте для использования в своих операциях или может установить встроенную функцию, чтобы предоставить специализированную услугу.

Обеспечение безопасности

Смарт-карты, включая SIM-карты, используют ряд методов, защищающих информацию, которую они содержат, от несанкционированного вмешательства. Кроме того, существуют различные уровни привилегий, которые назначены файлам DF или EF для управления условиями доступа (3GPP 2005a):

- «**Всегда**» (“**Always**”) - Доступ может быть выполнен без всякого ограничения.
- «**Верификация Владельца Карты 1**» (“**CHV1”**) - Доступ может быть выполнен только после успешной проверки личного идентификационного номера (PIN) пользователя или если проверка PIN заблокирована.
- «**Верификация Владельца Карты 2**» (“**CHV2**”) - Доступ может быть выполнен только после успешной проверки PIN2 пользователя или если проверка PIN2 заблокирована.
- «**Права Администратора**» (“ **Administrative**”) - Доступ может быть выполнен только после того, как будут выполнены предписанные требования для доступа с правами администратора.
- «**Никогда**» (“**Never**”) - Доступ к файлу через интерфейс SIM/ME запрещается.

Операционная система SIM-карты контролирует доступ к элементу файловой системы, основанный на ее условиях доступа и типе предпринимаемого действия (3GPP 2005a).

Например, действия над EF включают: поиск, чтение и обновление содержания. Тогда как чтение и поиск содержания отдельного EF могут быть разрешены без проверки CHV1,т.е. условие доступа « Всегда» (“Always”); для обновления содержания необходимым условием, вероятно, будет проверка CHV1,т.е. условие доступа (CHV1). В общем, CHV1 защищает основные данные SIM- карты против несанкционированного чтения и обновления выборочно, тогда как CHV2 защищает, главным образом, дополнительные данные. Оба условия доступа CHV содержат 4-8 цифр и могут быть изменены или отключены пользователем.

Операционная система SIM- карты позволяет только заданное число попыток, обычно в пределах трёх, для ввода правильного CHV, прежде чем дальнейшие попытки будут блокированы. Представление правильного значения для разблокирования CHV, также известного как PUK (ключ разблокировки PIN), восстанавливает в исходное состояние CHV и счетчик попыток. Если известен идентификатор SIM- карты, т.е. её « Номер идентификации чип-карты» (Integrated ChipCard IDentification) , далее “ICCID”, то значения для разблокирования либо CHV1, либо для CHV2, могут быть получены от поставщика услуг или сетевого оператора. ICCID обычно фиксируется в SIM-карте вместе с именем сетевого оператора. Если необходимо, то идентификатор может быть прочитан из EF, EFICCID с помощью инструментальных средств для SIM- карт, так как для него условие доступа “Always” применяется по определению. Если количество попыток правильно ввести значения для разблокирования CHV превышает установленный лимит (обычно десять попыток),то карта блокируется навсегда.

Безопасное подтверждение подлинности устройства в сети – важная функция, выполняемая через SIM- карту. Информация о криптографическом ключе и алгоритмах в модуле, защищенном от несанкционированного вмешательства, обеспечивают устройство возможностью участвовать в диалоге «отклик - отзыв» с сетью и отвечать правильно, не показывая ключевых данных и другую информацию, которую можно было бы использовать для клонирования SIM- кары и получения доступа к услугам абонента. Информация о криптографическом ключе в SIM- карте также поддерживает потоковое шифрование для защиты от подслушивания в радиоинтерфейсе (Vedder 1993, Willassen 2003).

Исследование данных

С SIM- карты можно извлечь различные типы цифровых данных. Эти данные могут быть расположены вразброс по всей файловой системе, в EF- файлах, в MF, а также в вышеупомянутых DF.

Несколько общих категорий исследуемых данных, которые могут быть идентифицированы:

- Информация, связанная с услугами
- Телефонная книга и информация о звонках
- Информация об обмене сообщениями
- Информация о расположении.

Оставшаяся часть этого раздела рассматривает файлы EF, обычно исследуемые экспертами, которые подпадают под одну из вышеперечисленных категорий (Dearsley 2005, Willassen 2003). Стандартизированные имена и аббревиатуры EF, хотя иногда и необычные, используются в течение этого обсуждения.

Информация, связанная с услугами

ICCID (Integrated ChipCard Identification, « Номер идентификации чип-карты») – уникальный числовой идентификатор для SIM-карты, который может быть длиной до 20 цифр. Он состоит из приставки идентификатора отрасли промышленности (89 для электросвязи), за которым следует код страны, идентификационный номер издателя и идентификационный номер личного счёта (ITU-T, 2006). Кроме приставки, компоненты ICCID являются изменяемыми, что иногда делает их трудными для интерпретации. ICCID можно прочитать с SIM- карты, не предоставляя PIN и он никогда не может быть обновлён. Код страны и издателя могут использоваться для определения сетевого оператора, предоставляющего услуги, и для получения записей данных о звонках абонента.

IMSI (Internatonal Mobile Subscriber Identity, « Международный идентификатор абонента мобильной связи», далее "IMSI") - уникальный числовой личный номер, назначенный абоненту. Он имеет структуру до некоторой степени подобную ICCID: Международный код страны в сети мобильной связи (MCC), Код сети мобильной связи (MNC), и Личный номер абонента мобильной связи (MSIN), назначенный сетевым оператором. MCC состоит из 3-х цифр, в то время, как MNC может иметь 2 или 3 цифры. Четвёртый бит другого EF, Административные данные (AD), дает длину MNC. Сети используют номера IMSI, чтобы установить сеть, абонентом которой является владелец устройства, и, если это не их сеть, позволить ли этим сетевым абонентам получать доступ к услугам.

ICCID и IMSI могут использоваться, чтобы определить абонента и сетевого оператора, предоставляющего услуги. Однако так как эти идентификаторы могут быть неверно истолкованы, другие данные SIM- карты могут помочь в подтверждении полученной информации.

MSISDN (Mobile Station International Subscriber Directory Number, «Международный номер ISDN мобильной станции», далее "MSISDN") предназначен для того, чтобы передавать номер телефона назначенному абоненту; для получения звонков на телефон. Однако в отличие от ICCID и IMSI, MSISDN является дополнительным EF . Если он присутствует, абонент может модифицировать его значение, делая его менее надежным источником данных, так как он затем станет несовместимым с фактически назначенным номером.

SPN (Service Provider Name, « Наименование службы провайдера», далее "SPN") – дополнительный EF, который содержит имя поставщика услуг. Если он присутствует, то он может быть модифицирован только администратором, т.е. разрешён доступ с правами администратора. Точно так же EF $_{SDN}$ (Service Dialling Numbers, « Сервисные номера», далее "SDN") содержит номера специальных служб, например, поддержки абонентов и, если он присутствует, это может помочь установить, в какой сети зарегистрирована SIM-карта.

Телефонная книга и информация о звонках

EF $_{ADN}$ (Abbreviated Dialling Numbers, « Ускоренный набор номеров», далее "ADN") сохраняет список имен и телефонных номеров, введенных абонентом. Память позволяет выбрать по имени часто набираемые телефонные номера, изменять эти номера и звонить по ним, используя меню или специальные кнопки телефона, обеспечивая упрощенную работу с телефонной книгой. Большинство SIM-карт предоставляют приблизительно 100 слотов для записей ADN.

EF $_{LDN}$ (Last Numbers Dialled, « Последние набранные номера», далее "LND") содержит список самых последних телефонных номеров, набранных устройством. Имя также может быть связано с записью и сохраненным номером (например, набранная запись телефонной книги). Хотя номер появляется в списке, соединение, возможно, не было успешным, только осуществлена попытка соединения. Большинство SIM-карт предоставляют только ограниченное количество слотов (например, десять) для таких записей. Некоторые телефоны не хранят набранные номера на SIM- карте, а вместо этого записывают эти данные в свою память.

Информация об обмене сообщениями

Обмен текстовыми сообщениями – это средство связи, в котором сообщения, введенные в один сотовый телефон, отправляются на другой через сеть мобильной связи. EF $_{SMS}$ (Short Message Service, « Служба коротких сообщений», далее "SMS") содержит текстовые и сервисные параметры для сообщений, полученных или посланных по сети, или, которые должны быть отосланы как сообщение с сотового телефона. Записи SMS содержат другую информацию, помимо самого текста, например, время отправки входящего сообщения, зарегистрированного сетью мобильной связи, телефонный номер отправителя, адрес центра SMS и состояние записи. Состояние записи сообщения может быть отмечено как свободное пространство или занятое, одним из следующего: непрочитанное полученное сообщение, прочитанное полученное сообщение, исходящее сообщение, которое надо отправить, или отправленное исходящее сообщение. Сообщения, удаленные через интерфейс телефона, часто просто отмечаются как свободное пространство и сохраняются на SIM- карте, пока не будут перезаписаны. Когда новое сообщение записывается в доступный слот, неиспользуемая часть заполняется незначащей информацией, перезаписывая любые оставшиеся части предыдущего сообщения, которое могло бы быть там.

SIM-карты имеют различную ёмкость для сохраненных сообщений. Многие сотовые телефоны также используют свою собственную внутреннюю память для сохранения текстовых сообщений. Выбор памяти для сохранения сообщений (то есть, SIM-карта или телефон) может отличаться в зависимости от программного обеспечения телефона и пользовательских параметров настройки (Willassen 2005). Например, по умолчанию все входящие сообщения могут сохраняться в памяти SIM- карты до использования внутренней памяти телефона, тогда как исходящие сообщения сохраняются только по явному требованию. Модели телефонов одного поколения и изготовителя часто работают согласованно в этом отношении (Willassen 2005).

Максимальная длина одной записи SMS- сообщения – 160 символов текста. Сообщения, превышающие эту длину, должны быть разбиты передающим телефоном на меньшие

части и повторно собраны принимающим телефоном. Эта функция особенно полезна для наборов символов иностранных языков, таких, как китайский или арабский, кодирование которых занимает в два раза большее число битов на символ, чем в английском языке. Параметр номера для ссылки устанавливает записи, части которых требуют повторной сборки. Такие сообщения называются соединёнными сообщениями. SMS- сообщения могут быть созданы другими способами, помимо сотового телефона, например, отправлены через SMS-сервер в Интернете или через электронную почту.

SMS-сообщение может быть кодировано различными способами. Первая и самая обычная схема кодирования – 7- битный набор символов, специфичный для GSM. Такое кодирование не может быть легко интерпретировано непосредственно из необработанных данных, с использованием шестнадцатеричного редактора. Кроме того, оно поддерживает не все языки. Поддержка других наборов символов, таких, как 16- битный Unicode, была добавлена для языков, алфавит которых не может быть представлен, используя исходный западноевропейский набор символов (3GPP 2005b).

EMS (Enhanced Messaging Service, « Служба передачи расширенных сообщений») была определена как способ расширения содержания SMS- сообщений чтобы позволить передавать простые мультимедиа-сообщения. EMS-сообщения могут содержать не только отформатированный текст с различными стилями шрифта и различными шрифтами, но также черно-белые растровые изображения и монофонические мелодии (3GPP 2005b). Содержание EMS- сообщений находится в EF SMS наряду с содержанием SMS-сообщений. Передача EMS- сообщений - по своей сути - это расширение прикладного уровня SMS, который соответствует основной структуре SMS-сообщений и поддерживает соединённые сообщения. Устройства с поддержкой EMS обратно совместимы по определению с устройствами с поддержкой SMS.

Информация о расположении

Сеть GSM состоит из отдельных радиосот, используемых для установления связи с мобильными телефонами. Соты группируются в определенные зоны, используемые для управления связью. Телефоны отслеживают зону, в которую они попадают, для передачи данных и речи. EF $_{LOCI}$ (Location Information, « Информация о местонахождении», далее “LOCI”) содержит LAI (Location Area Information, « Идентификация зоны местонахождения») для передачи речи. LAI состоит из MCC, MNC (зоны местонахождения), LAC (Location Area Code, « Код зоны местонахождения»), идентификатора для группы сот. Когда телефон выключен, LAI сохраняется в памяти, позволяя определить общее место, где телефон работал последний раз. Поскольку зона местонахождения может содержать сотни или больше сот, место действия может быть довольно обширным. Тем не менее, это может быть полезным для сужения области, в которой произошло определённое событие.

Точно так же EF $_{LOCIGPRS}$ (GPRS Location Information, « Информация о местонахождении GPRS», далее “LOCIGPRS”) содержит RAI (Routing Area Information, «Информация о зоне маршрутизации», далее “RAI”) для передачи данных через GPRS (General Packet Radio Service, «Служба пакетной передачи данных в радиоканале», далее “GPRS”). RAI состоит из MCC, MNC зоны маршрутизации, LAC, а также RAC (Routing Area Code, « Код зоны маршрутизации»), идентификатора зоны маршрутизации в пределах LAC. Зоны маршрутизации могут быть определены так же, как и зоны расположения, или они могут включать меньше сот, обеспечивая большую разрешающую способность.

Судебные инструментальные средства

Главная цель судебного инструмента для исследования SIM-карт состоит в том, чтобы извлечь цифровые данные, присутствующие в файловой системе. Помимо клонирования, большая часть подобных судебных инструментов поддерживают ряд функций по исследованию данных и составлению отчётов. Некоторые инструментальные средства работают только с SIM-картами, тогда как другие являются частью полного комплекта инструментов, который также исследует сами телефоны.

Самая важная характеристика судебного инструмента – его способность сохранить целостность клонируемого оригинального источника данных, а также сохранение целостности извлеченных данных. Первое достигается блокированием, или иным способом устранением запросов записи на устройство, содержащее данные. Последнее достигается вычислением криптографического хэша содержания исследуемых файлов и рекуррентной проверкой того, что это значение остается неизменным на всем протяжении времени существования этих файлов. Сохранение целостности не только поддерживает достоверность с юридической точки зрения, но также позволяет любым последующим расследованиям использовать те же самые объекты для последующих исследований.

Доступен целый ряд программ для управления данными пользователя на SIM-карте. Они позволяют считывать некоторые данные на персональный компьютер, модифицировать их и перезаписывать назад на SIM-карту. Инструментальные средства такого типа ненадёжны, так как они специально не предназначены для судебных целей. Учитывая количество доступных судебных средств, следует избегать подобных программ.

Чтобы клонировать SIM-карту, её нужно извлечь из телефона и вставить в соответствующее считывающее устройство. В отличие от судебного дублирования НЖМД, прямое обращение к данным, находящимся на SIM-карте, не допустимо из-за механизмов защиты, встроенных в нее. Вместо этого, необходимо использовать команды, которые называются APDU (Application Protocol Data Units, « Пакеты данных протокола прикладного уровня », далее “APDU”), которые посылаются на SIM-карту, чтобы извлечь данные, без их модификации, из каждого EF файловой системы. Протокол APDU - простой обмен « команда-ответ». Каждый элемент файловой системы, определенный в этом стандарте, имеет уникальный назначенный числовой идентификатор, который может использоваться для ссылки на элемент и для выполнения некоторой операции, например, чтение содержимого при работе с инструментом клонирования.

Судебные средства для исследования SIM-карт требуют либо специализированного устройства для считывания, в которое SIM-карта вставляется непосредственно, либо считывающее устройство для полноразмерной смарт-карты. Для последнего устройства, чтобы вставить в него SIM-карту, необходим адаптер. Таблица №1 предоставляет список нескольких судебных программных средств для исследования SIM-карт и список их основных поддерживаемых функций – клонирование, исследование и составление отчёта. Первые четыре перечисленных инструмента: Cell Seizure, GSM .XRY, Mobiledit! и TULP2G, также могут дублировать данные SIM-карты через телефон. Обратите внимание, что используя эти инструментальные средства, при дублировании SIM-карты через телефон, не все ее доступные данные могут быть считаны. При клонировании данных SIM-карты через телефон могут возникнуть некоторые проблемы криминалистического характера. Самая обычная проблема – это то, что состояние SMS сообщения может быть изменено с «непрочитанного» на «прочитанное».

Таблица №1: Инструментальные средства для исследования SIM-карт

Инструмент	Функция
1	2
Cell Seizure	Клонирование, Исследование, Отчёт[2]
GSM .XRY	Клонирование, Исследование, Отчёт[3]
Mobiledit! Forensic	Клонирование, Исследование, Отчёт[4]
TULP 2G	Клонирование, Отчёт[5]
Forensic Card Reader	Клонирование, Отчёт[6]
ForensicSIM	Клонирование, Исследование, Отчёт[7]
SIMCon	Клонирование, Исследование, Отчёт[8]
SIMIS	Клонирование, Исследование, Отчёт[9]

Доступные данные

В то время как все данные, хранящиеся на SIM- карте, могут потенциально иметь доказательную ценность, многие данные относятся к сетевым службам и имеют мало прямой доказательственной силы. Как правило, судебные инструментальные средства для работы с SIM- картами имеют доступ не ко всем данным, находящимся на SIM- карте. Количество доступных данных также зависит от используемого судебного средства. Таблица №2 предоставляет краткий обзор данных SIM- карт, перечисленных слева, доступных различным судебным инструментам, перечисленным вверху.

Таблица №2: Доступность данных SIM-карт различным судебным инструментальным средствам

	Cell Seizure	GSM .XRY	Mobiledit!	TULP 2G	FCR	Forensic SIM	SIMCon	SIMIS
1	2	3	4	5	6	7	8	9
IMSI	X	X	X	X	X	X	X	X
ICCID	X	X	X	X	X	X	X	X
MSISDN	X	X		X	X	X	X	X
SDN	X			X		X	X	X
SPN	X			X		X	X	X
Phase	X	X	X			X	X	X
ADN	X	X	X	X	X	X	X	X
LND	X	X	X	X	X	X	X	X
SMS/EMS								

[2] Версия 2.0.0.33660, смотри www.paraben-forensics.com
[3] Версия 2.5, смотри www.msab.com/en
[4] Версия 1.95, смотри www.mobiledit.com
[5] Версия 1.1.0.2, смотри tulp2g.sourceforge.net
[6] Версия 1.0.1, смотри www.becker-partner.de/forensic/intro_e.htm
[7] Версия 1.3.0.0, смотри www.radio-tactics.com/forensic_sim.htm
[8] Версия 1.1, смотри www.simcon.no
[9] Версия 2.0.13, смотри www.crownhillmobile.com

•Состояние: прочитано/ не прочитано	X	X	X	X	X	X	X	X
•Удаленные	X	X		X		X	X	X
LOCI	X	X		X	X	X	X	X
GPRSLOCI	X					X	X	X

Декодирование и преобразование

Судебные инструментальные средства могут представить пользователю клонируемые данные несколькими способами, как это изображено на Иллюстрации 3. Каждая стадия, однако, может вносить ошибки. Самая основная форма – это необработанные закодированные данные, полученные в ответ на запрос APDU. Как было упомянуто ранее, текст, закодированный в 7- битный алфавит GSM, требует много усилий и времени для расшифровывания вручную. Другой менее тяжёлый способ расшифровки включает в себя двоично-десятичные (BCD) числовые идентификаторы. Большинство, но не все, из инструментальных средств, по возможности, декодируют необработанные данные в форму, удобную для ее интерпретации пользователем.

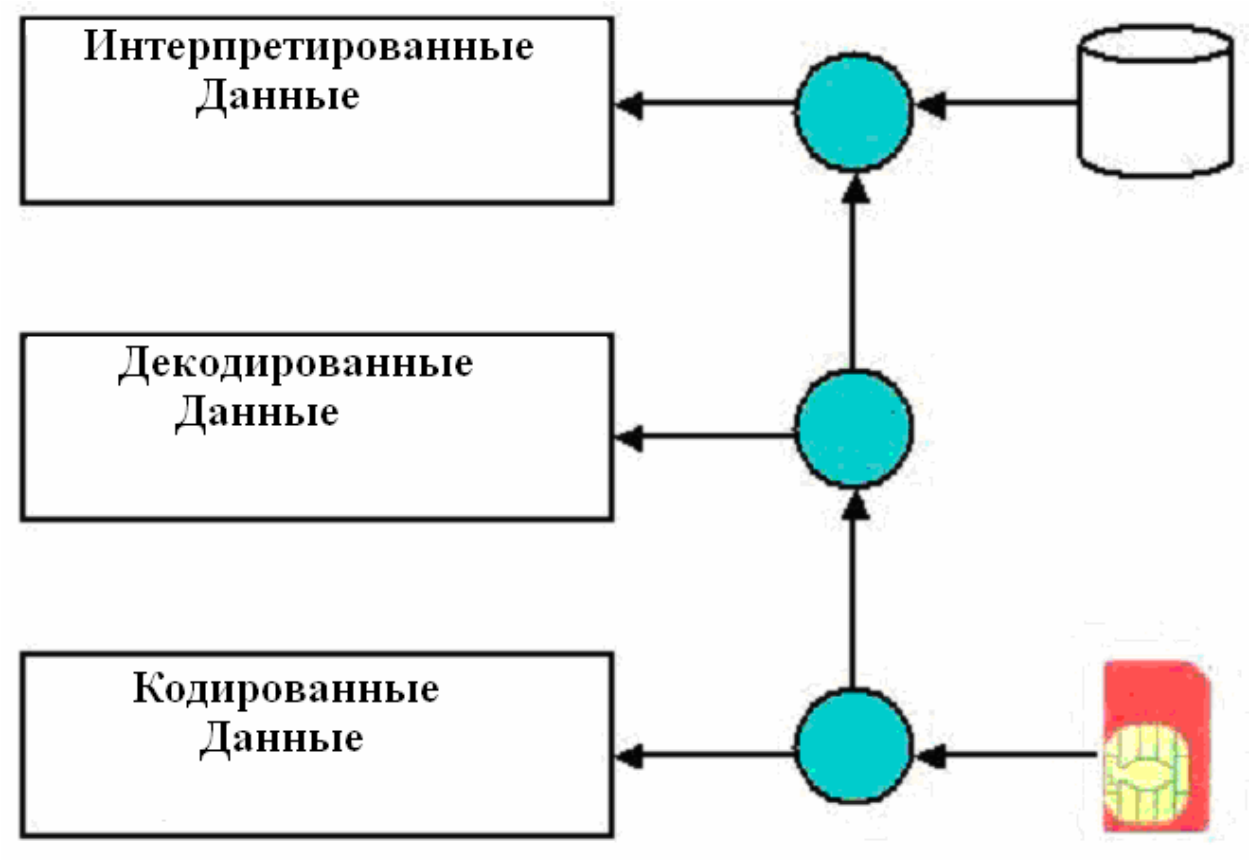


Иллюстрация 3: Декодирование и преобразование данных

Несколько инструментальных средств выходят за рамки декодирования и пытаются преобразовывать декодированные данные в форму, более доступную для восприятия пользователя. Это особенно касается числовых данных. Например, двоично-десятичное закодированное значение части MCC и MNC LAI, “130014”, декодируется в “310410”, где

310 - значение MCC, а 410 - значение MNC. Код страны 310 назначен Соединенным Штатам, тогда как сетевой код 410 назначен оператору Cingular.

Оценка судебных инструментов

SIM-карты – высоко стандартизированные устройства, чей интерфейс, поведение и содержание однородны. Вообще говоря, все инструментальные средства для SIM- карт поддерживают клонирование любой SIM- карты через внешнее считывающее устройство (карт-ридер). Чтобы измерить способности судебного инструмента получать информацию с SIM-карты, заполненной данными, использовались специально разработанные сценарии. Акцент в сценариях делался на заполнение SIM-карты определенным видом информации. Как только сценарий был выполнен, с использованием подходящего телефона GSM или программы для работы с SIM- картами, эта карта использовалась для оценки судебных инструментов.

Эти сценарии не предназначены быть исчерпывающими или служить формальной оценкой программы. Однако они пытаются охватывать область данных, с которыми обычно сталкиваются при исследовании SIM- карт, и они полезны в определении возможностей, предоставленных эксперту. Таблица №3 дает краткий обзор этих сценариев. Обратите внимание, что ни один из сценариев не пытается подтвердить, сохранена ли целостность данных на SIM- карте при применении инструмента - эта тема выходила за пределы данного исследования.

Таблица №3: Сценарии

Сценарий	Описание
1	2
Основные данные	Определяет, может ли инструмент восстановить информацию с SIM-карты, связанную с основным абонентом (то есть, элементарные файлы IMSI, ICCID и SPN), PIM (то есть, элементарный файл ADN), телефонными звонками (то есть, элементарный файл LND), SMS-сообщениями, включая записи удалённых SMS, и правильно ли декодированы и отображены все данные.
Данные о местонахо-ждении	Определяет, может ли инструмент восстановить информацию с SIM-карты, связанную с местонахождением (то есть, элементарные файлы LOCI и LOCIGPRS), и правильно ли декодированы и отображены все данные.
Данные EMS	Определяет, может ли инструмент восстановить EMS- сообщения длиной более 160 символов и содержащие нетекстовые данные, и правильно ли декодированы и отображены все данные, как для активных, так и для удалённых сообщений.
Данные об иностранных языках	Определяет, может ли инструмент восстановить с SIM- карты SMS-сообщения и данные PIM на иностранном языке, и правильно ли декодированы и отображены все данные.

Результаты тестов, для каждого инструмента, сравнивались с предопределенными ожиданиями, и устанавливалось ранжирование. Запись « Соответствует» (“Meet”), указывает, что программное обеспечение соответствует ожиданиям сценария для данного устройства. Так как сценарии ориентируемы на клонирование, это ранжирование обычно означает, что все идентифицированные данные были успешно считаны. Точно так же

запись « Ниже» (“Below”) указывает, что программное обеспечение не полностью соответствует ожиданиям.

Ранжирование « Ниже» (“Below”) часто является следствием того, что инструмент выполнил логическое клонирование, но не смог восстановить удаленные данные, что понятно. Однако это ранжирование может быть также обусловленным тем, что активные данные на устройстве не были успешно считаны, что вызывает большее беспокойство. Хороший пример этого является случай, когда SMS- сообщения были удалены, но не перезаписаны другим сообщением. Запись « Неудачно» (“Miss”) указывает, что программное обеспечение не соответствовало каким-либо ожиданиям и требует дальнейшего совершенствования.

Таблица №4 даёт краткий отчёт о результатах для каждого инструмента, использованного в нескольких тестах SIM- карт: 5343 от T-Mobile, 8778 от Cingular, и 1144 от AT&T. Обратите внимание на малое количество неудачных совпадений. Главные проблемы возникали из-за трудностей, которые испытали инструменты Cell Seizure и Forensic SIM при клонировании любых данных с SIM-карты Cingular. Остальные являлись результатом ограниченного масштаба охвата доступных данных SIM- карт, у инструмента Mobiledit!, как было отмечено ранее в Таблице №2.

Таблица №4: Отчёт

Программа	**Сценарий**	**SIM-карта**		
		5343	**8778**	**1144**
1	2	3	4	5
Cell Seizure	Основные данные	Соответствует	Неудачно	Соответствует
	Данные о местонахождении	Соответствует	Неудачно	Соответствует
	Данные EMS	Ниже	Неудачно	Ниже
	Данные об иностранных языках	Ниже	Неудачно	Ниже
GSM .XRY	Основные данные	Соответствует	Соответствует	Соответствует
	Данные о местонахождении	Ниже	Ниже	Ниже
	Данные EMS	Соответствует	Соответствует	Соответствует
	Данные об иностранных языках	Ниже	Ниже	Ниже
Mobiledit! Forensic	Основные данные	Ниже	Ниже	Ниже
	Данные о местонахождении	Неудачно	Неудачно	Неудачно
	Данные EMS	Ниже	Ниже	Ниже
	Данные об иностранных языках	Ниже	Ниже	Ниже
TULP 2G	Основные данные	Соответствует	Соответствует	Соответствует
	Данные о местонахождении	Ниже	Ниже	Ниже
	Данные EMS	Соответствует	Соответствует	Соответствует
	Данные об иностранных языках	Соответствует	Соответствует	Соответствует
	Основные данные	Ниже	Ниже	Ниже

Forensic Card Reader	Данные о местонахождении	Ниже	Ниже	Ниже
	Данные EMS	Ниже	Ниже	Ниже
	Данные об иностранных языках	Ниже	Ниже	Ниже
ForensicSIM	Основные данные	Соответствует	Неудачно	Ниже
	Данные о местонахождении	Соответствует	Неудачно	Ниже
	Данные EMS	Ниже	Неудачно	Ниже
	Данные об иностранных языках	Ниже	Неудачно	Ниже
SIMCon	Основные данные	Соответствует	Ниже	Ниже
	Данные о местонахождении	Соответствует	Соответствует	Соответствует
	Данные EMS	Соответствует	Соответствует	Соответствует
	Данные об иностранных языках	Соответствует	Соответствует	Соответствует
SIMIS	Основные данные	Соответствует	Соответствует	Соответствует
	Данные о местонахождении	Соответствует	Ниже	Ниже
	Данные EMS	Ниже	Ниже	Ниже
	Данные об иностранных языках	Ниже	Ниже	Ниже

В остальной части от этого раздела обсуждаются области, где результаты судебных инструментальных средств были ниже ожидаемых и приводятся некоторые характерные примеры.

Основные данные

Как правило, восстановление основных данных не вызывает больших проблем у большинства судебных инструментов (за исключением удаленных SMS- данных). Некоторые инструментальные средства не считывают отдельные полезные данные, как это было отмечено в Таблице №2. Большее беспокойство вызвало то, что несколько инструментальных средств совсем не смогли клонировать SIM-карту. Один инструмент не смог отобразить полное имя записи телефонной книги максимального размера, а другой сократил все имена на один символ. В обоих случаях для просмотра недостающих символов можно использовать другие считываемые данные, предоставляемые инструментальными средствами. Один инструмент последовательно присоединил впереди IMSI четырехразрядный байт чётности.

Интересная проблема имела место при преобразовании значений IMSI SIM- карты. Нескольким европейским инструментальным средствам не удалось преобразовать IMSI правильно. Они игнорировали значение AD, содержащее размер части MNC, которое нужно использовать при декодировании значения в сетевое имя, и вместо этого устанавливали по умолчанию 2 цифры. Поскольку размер Североамериканского MNC – 3 цифры, происходила ошибка преобразования. Однако можно было выполнить правильное преобразование вручную, так как также были предоставлены декодированные данные, используемые для преобразования.

Данные о местонахождении

Как было отмечено в Таблице №2, несколько инструментальных средств считывают LOCI, но не считывают LOCIGPRS. Один инструмент не считал ни то, ни другое. Одно из инструментальных средств, которое считало данные, не смогло сообщить о частях MCC/MNC информации о зоне местонахождения (LAI), в то время как другой инструмент неправильно представил значение компонента LOCI.

Часть MNC от LAI, трёхзначное значение, была неправильно расшифрована одним инструментом. Несколько инструментальных средств не пытались преобразовать коды LAI и RAI в сетевое имя и избежали этой проблемы. Одно из них даже не пыталось декодировать необработанные данные, чтобы упростить ручное преобразование.

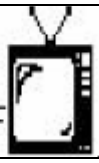
Данные EMS

Восстановление текстовых EMS-сообщений больших, чем 160 символов, не представляло собой большой проблемы для большей части инструментальных средств, за исключением двух инструментов, которые имели проблемы при считывании удаленных EMS-сообщений. Как отмечено в Таблице №2, это те же самые инструменты, которые имели проблемы со считыванием удаленных SMS- сообщений. Другие результаты получились при считывании EMS- сообщений с изображениями. В текст было вставлено два изображения разного размера: маленького - 16x16 пикселей, и большого - 32x32 пикселей. Результаты показаны в Таблице №5.

Только два инструмента, GSM .XRY и SIMCon, успешно клонировали и отобразили оба размера вложенных изображений. Ещё один инструмент, TULP 2G, смог успешно клонировать только маленькие изображения. Для большого изображения этот инструмент не смог сообщить о присутствии сообщения, полностью его пропуская. Два других инструментальных средства успешно восстановили текст, но неверно истолковывали значение изображения, в то время как еще одни инструмент восстановил текст и предоставил уведомление о наличии изображения.

Таблица №5: Сообщения с текстом и картинками

Про-грамма	Текст и изображение маленького размера	Текст и изображение большого размера
1	2	3
Cell Seizure	Неудачное Клонирование – SIM-карта Cingular	lßiOß&/Ψà
GSM XRY	Picture msg 	Emspictur 
Mobiledit!	Picture msg	Emspictur
TULP 2G	Picture msg 	Полностью Отсутствует
SIMIS	@@@@@@@x?P¡K?□□□□00@@ @@@@@@**Picture msg**	?@@@□@@□□@??@@?@(@$@? @?@?□□?4p@@D□?(Xq?x7□ @q,?@p□@ba?@@D? @??P?@x□@?@p□@??@$?????8x □@□□□S□□**mspictur**
Forensic	Неудачное Клонирование – SIM-карта	Заголовок – Большое Изображение

SIM	Cingular	Пользовательские Данные - **Emspictur**
Forensic CR	#"èY@@@@@@@@@@x£Pò BaK?ààààlÆ??00@@@@@@@@@@**Picture msg**	¥!èL@@p£@@@ß@@@?è@@@££@@ò @@¡@ò@@è@$@¿@¿@üààààààààà àà?4p@@DàøÆ¡(Xq¥x7? @q¸¥@på7@@baù@¿Él@@D¥ @¡?P£@xì?@@à@¥@på0@@ü£ù@ ¿É¿@$ö¥ø¿¡?¡£8xìÆ@@àààààààààSà ààà?**Emspictu**
SIMCon	Picture msg 	Emspictur 

Данные об иностранных языках

Данные об иностранных языках встречались как в телефонной книге AND, так и в записях SMS-сообщений. Использовались французский и японский языки. Таблица №6 показывает результаты для SMS- сообщений. Только одному инструменту не удалось правильно отобразить сообщения на французском языке. Однако, используя особенность дампа, можно найти правильные данные. Для сообщений на японском языке, только один инструмент, SIMCon, правильно отобразил сообщение. Большинство других были близки, но добавили в конце ложные символы. Оставшиеся исказили содержание сообщений, хотя отметка даты/времени и другая информация заголовков были представлены правильно.

Результаты для записей ADN на французском и японском языках, в целом, соответствуют результатам для SMS- сообщений. Однако один из инструментов показал худшие результаты для записей AND на французском языке, чем для записей SMS-сообщений, в то время как другой показал худшие результаты для записей AND на японском языке, чем для записей SMS-сообщений

Таблица №6: Сообщения на иностранных языках

Программа	**Французский язык**	**Японский язык**
1	2	3
Cell Seizure	Il est entété mais sincère	Заголовки – ОК, Сообщение - Искажённо
GSM XRY	Il est entété mais sincère	阿婆家里面对于是否则的确实现在家里面对于—□□
Mobiledit!	Il est entété mais sincère	阿婆家里面对于是否则的确实现在家里面对于 啟签
TULP 2G	Il est entété mais sincère	阿婆家里面对于是否则的确实现在家里面对于—??
SIMIS	Il est ent鴆 mais sinc肮	阿婆家里面对于是否则的确实现在家里面对于—
Forensic SIM	Il est entété mais sincère	Заголовки – ОК, Сообщение - Искажённо
Forensic CR	Il est entété mais sincère	Заголовки – ОК, Сообщение - Искажённо

SIMCon	Il est entété mais sincère	阿婆家里面对于是否则的确实现在家里面对于

Выводы

Судебная экспертиза сотовых устройств – развивающаяся предметная область компьютерно-технической экспертизы. Инструментальные средства судебной экспертизы преобразовывают данные в формат и структуру, которые являются понятными для экспертов и могут эффективно использоваться для идентификации и восстановления исследуемых объектов. Однако инструментальные средства могут содержать некоторую степень погрешностей. Например, реализация инструмента может содержать ошибку программирования; спецификация, используемая инструментом для преобразования кодированных битов в данные, понятные эксперту, может быть неточной или устаревшей; или протокол, поддерживаемый SIM- картой, может быть неверным, являясь причиной неправильного функционирования инструмента в некоторых ситуациях.

Со временем, опыт работы с инструментом даёт понимание его ограничений, позволяя эксперту компенсировать, где это возможно, любые недостатки или обращаться к другим инструментальным средствам. Практика пробных экспертиз может помочь получить глубокое понимание возможностей инструмента и ограничений, которые часто включают в себя тонкие различия, а также предоставляет возможность настроить средства инструмента для последующего использования.

Судебные программные средства для исследования SIM-карт находятся на средней стадии развития. В то время как инструментальные средства, обсужденные в этой статье, в целом работали хорошо и имели адекватные функциональные возможности, новые версии, как ожидается, будут совершенствоваться и лучше отвечать требованиям проводимых расследований. Например, во время подготовки этого отчёта, почти для каждого инструмента были выпущены новые версии, которые включают в себя усовершенствованные функциональные возможности.

Литература:

3GPP, 2005a, Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface, 3rd Generation Partnership Project, TS 11.11 V8.13.0 (Release 1999), Technical Specification, (2005-06).

3GPP, 2005b, Technical Realization of the Short Message Service (SMS), 3rd Generation Partnership Project, TS 23.040 V6.6.0 (Release 6), Technical Specification Technical (2005-12).

3GPP2, 2001, Removable User Identity Module for Spread Spectrum Systems, 3rd Generation Partnership Program 2, 3GPP2 C.S0023-0, Version 4.0, June 15.

Dearsley, T., 2005, Mobile Phone Forensics – Asking the Right Questions, New Law Journal, July 29, pp. 1164-1165.

Dechaux, C., Scheller, R., 1993, What are GSM and DECT?, Electrical Communication, 2nd Quarter, pp. 118-127.

GSM World, 2006, GSM Global Networks on Air, <URL: http://www.gsmworld.com/news/statistics/networks_complete.shtml>.

ITU-T, 2006, Automatic International Telephone Credit Cards, International Telecommunications Union, Telecommunication Standardization Sector (ITU-T), Recommendation E.118, (02/01).

Vedder, K., 1993, Security Aspects of Mobile Communications, in Computer Security and Industrial Cryptography - State of the Art and Evolution, Lecture Notes in Computer Science, Vol. 741, pp. 193-210.

Willassen, S., 2003, Forensics and the GSM Mobile Telephone System, International Journal of Digital Evidence, Volume 2, Issue 1.

Willassen, S., 2005, Forensic Analysis of Mobile Phone Internal Memory, IFIP International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, February 13-16, in Advances in Digital Forensics, Vol. 194, Pollitt, M.; Shenoi, S. (Eds.), XVIII, 313 p., 2006.

Перевод:
Бочков Дмитрий Сергеевич
Капинус Ольга Валерьевна
Михайлов Игорь Юрьевич