Извлечение информационных улик из телефонов, смартфонов и КПК

2010

Рост рынка смартфонов

По данным FutureSource Consulting

Рынок смартфонов растет даже на фоне общего падения продаж

Смартфон это небольшой ПК

- Сотовый телефон
- Адресная книга
- Планировщик и органайзер
- Обмен сообщениями
- Фото и видео камера
- GPS навигатор
- Веб-клиент
- Установка новых приложений

Смартфон: сотовый телефон

Основная информация	• IMEI • Версия прошивки и оборудования • Информация о сети
Журнал событий	• История входящих, исходящих и пропущенных вызовов • История отправленных и полученных сообщений • История GPRS & Wi-Fi соединений
SIM карта	• IMSI • Телефонные номера* • SMS сообщения*

* - Обычно этот функционал не используется смартфонами

Смартфон: Адресная книга

Данные контакта

- Поля имени: имя, отчество, фамилия, обращение, полное имя, прозвище, префикс, суффикс
- Фотография и персональная мелодия
- Телефонные номера: общий, мобильный, факс, видео, пейджер, VoIP, push-to-talk
- Почтовые адреса
- Веб-сайты и e-mail адреса
- Компания, отдел, должность
- Текстовые заметки
- Личные данные: день рождения, супруга, дети
- Пользовательские метки полей
- Множественные поля одного типа
- Дата последнего сохранения

Группы

- Список групп абонентов и их состав

Быстрые наборы

- Список назначенных быстрых наборов

Смартфон: Планировщик

События календаря

- Встречи, напоминания, годовщины
- Дата и время начала
- Дата и время окончания
- Дата и время тревоги
- Повторения
- Дата последнего сохранения

Задачи

- Описание задачи
- Крайний срок
- Приоритет
- Дата и время тревоги
- Дата и время выполнения

Заметки

- Текст заметки и дата

Смартфон: Обмен сообщениями

Система обмена сообщениями

- Текстовые сообщения (SMS)
- Мультимедиа сообщения (MMS)
- E-mail сообщения с вложениями
- BIO сообщения: vCard, vCal, конфигурации и прочее
- Файлы полученные через Bluetooth, Инфракрасный порт или по USB
- Стандартные папки сообщений
- Пользовательские папки сообщения
- Дата и время
- Дата и время СЦ
- Информация об удаленных SMS сообщениях

Смартфон: GPS-навигатор

GPS-навигатор	• Последние зафиксированные GPS координаты • История поиска • История маршрута • Последняя просмотренная карта • Сохраненные карты • Список любимых мест
Гео-информация	• GPS координаты в фотоснимках* • Координаты сот в фотоснимках* • Координаты сот для фотоснимков** • Координаты сот для видеороликов** • Координаты сот для SMS сообщений**

* - Доступно в заголовке EXIF для большинства новых моделей
** - Доступно в смартфонах с установленным приложением Nokia LifeBlog

Смартфон: Web-клиент

Web браузер	• Временные файлы интернет • Закладки • История просмотров страниц • Последняя открытая страница • История поиска • Куки (Cookies)
Клиент мгновенных сообщений	• IP, логин (UID, e-mail) и пароль* • Список контактов • История переписки • История звонков

* - Доступны для некоторых клиентов мобильных сообщений

Смартфон: компьютер

Стандартные приложения

- Снимки фотокамеры
- Видеоклипы
- Записи диктофона
- Мелодии и подкасты
- Список сетей Wi-Fi
- Список подключений по Bluetooth
- Список подключенных SIM карт
- VPN профили

Сторонние приложения

- Список установленных приложений
- Офисные документы
- Журналы и файлы данных приложений

Способы извлечения данных

Существует 2 стандартных способа получить информацию из смартфона: логический и физический анализ

Логический анализ

- Данные извлекаются через протоколы обмена данными между ПК и телефоном: AT, OBEX, SyncML
- Смартфон подключен к ПК через стандартный кабель (или Bluetooth/ИК адаптер)

Физический анализ

- Данные извлекаются прямым чтением памяти телефона (hex дамп)
- Смартфон (или только чип памяти) подключен к специальному оборудованию

Логический анализ смартфонов

•- Доступный набор данных ограничен и зависит от производителя телефона

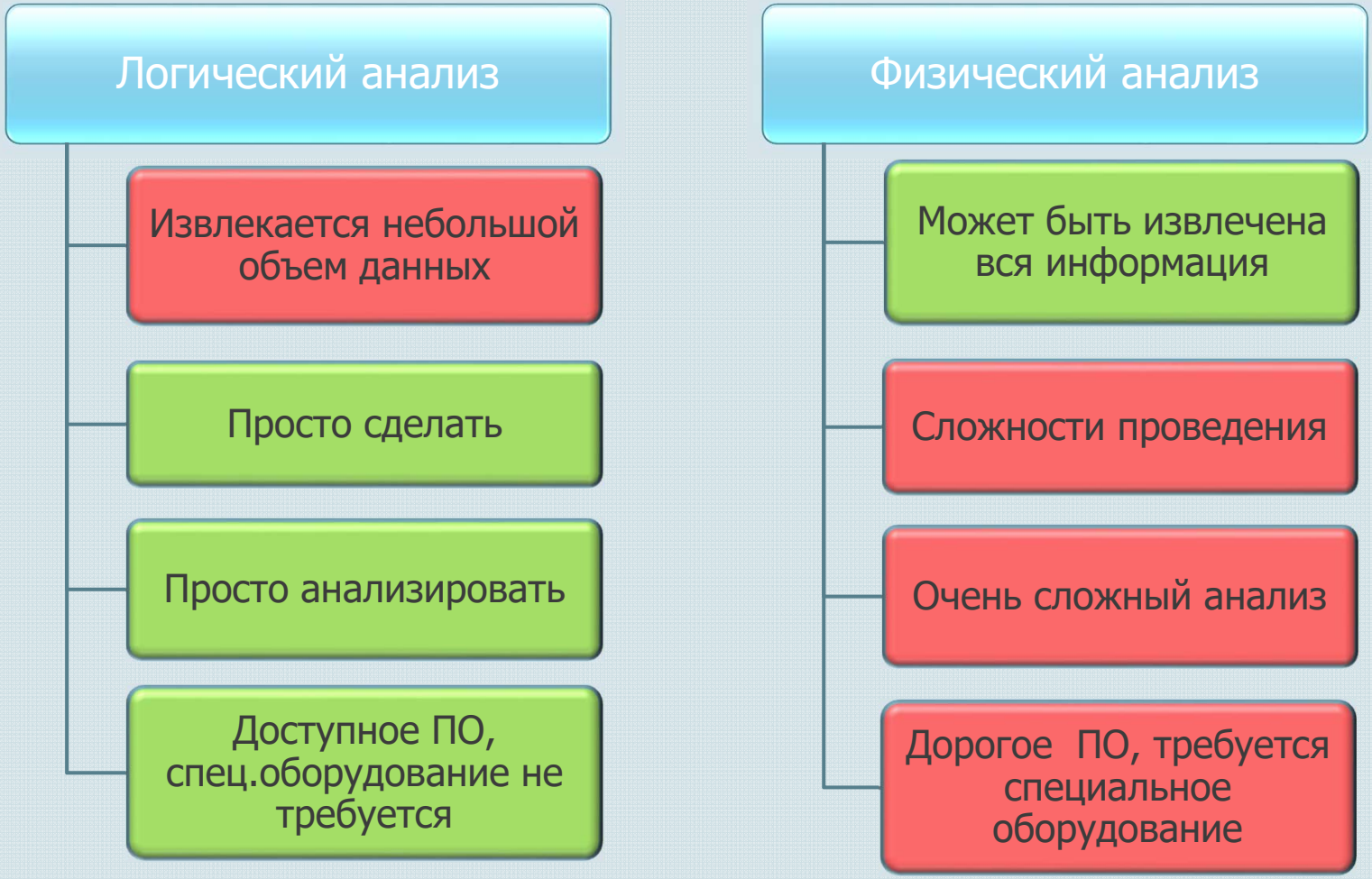
1) Информация извлекаемая логическими протоколами является лишь вершиной айсберга
2) Все логические протоколы разработаны для синхронизации данных

Физический анализ смартфонов

```
00000090: 17 00 9A 82 05 00 01 00  00 00 9E 01 00 00 9D 82  ..љ,.....ћ...ќ,
000000A0: 05 00 01 00 00 00 A6 01  00 00 27 88 03 00 01 00  ......¦...'€....
000000B0: 00 00 7D 00 00 00 00 90  07 00 04 00 00 00 30 32  ..}....ђ......02
000000C0: 32 30 03 90 02 00 14 00  00 00 AE 01 00 00 04 90  20.ђ......®....ђ
000000D0: 02 00 14 00 00 00 C2 01  00 00 01 91 07 00 04 00  ......В....'....
000000E0: 00 00 01 02 03 00 01 92  0A 00 01 00 00 00 D6 01  .......'......Ц.
000000F0: 00 00 02 92 05 00 01 00  00 00 DE 01 00 00 08 92  ...'......Ю....'
00000100: 03 00 01 00 00 00 00 00  00 00 09 92 03 00 01 00  ...........'....
00000110: 00 00 18 00 00 00 0A 92  05 00 01 00 00 00 E6 01  .......'......ж.
00000120: 00 00 7C 92 07 00 B0 09  00 00 EE 01 00 00 00 A0  ..|'..°...о.... 
00000130: 07 00 04 00 00 00 30 31  30 30 01 A0 03 00 01 00  ......0100. ....
00000140: 00 00 01 00 00 00 02 A0  04 00 01 00 00 00 00 08  ....... ........
00000150: 00 00 03 A0 04 00 01 00  00 00 00 06 00 00 01 A4  ... ...........¤
00000160: 03 00 01 00 00 00 00 00  00 00 02 A4 03 00 01 00  ...........¤....
00000170: 00 00 00 00 00 00 03 A4  03 00 01 00 00 00 00 00  .......¤........
00000180: 00 00 04 A4 05 00 01 00  00 00 9E 0B 00 00 06 A4  ...¤......ћ....¤
00000190: 03 00 01 00 00 00 00 00  00 00 07 A4 03 00 01 00  ...........¤....
000001A0: 00 00 01 00 00 00 00 00  00 00 48 71 00 00 40 42  ..........Hq..@B
000001B0: 0F 00 1C 00 00 00 0A 00  00 00 32 30 30 39 3A 30  ..........2009:0
000001C0: 34 3A 32 31 20 31 32 3A  30 37 3A 30 35 00 32 30  4:21 12:07:05.20
000001D0: 30 39 3A 30 34 3A 32 31  20 31 32 3A 30 37 3A 30  09:04:21 12:07:0
000001E0: 35 00 F3 13 00 00 E8 03  00 00 29 01 00 00 64 00  5.у...и...)...d.
000001F0: 00 00 38 00 00 00 0A 00  00 00 41 06 06 06 AB 17  ..8.......A...«.
00000200: 8E E2 10 74 56 DC 7D 2A  9C 5F 0B BC 61 1A E8 DA  Ћв.tVЬ}*њ_.ja.иЪ
00000210: 5C B9 B4 48 B2 FF 97 AA  DE 01 E7 D3 89 7E 41 10  \№ґHІя—Єю.зУ‰~A.
00000220: 08 35 6E 4E 79 63 50 1A  23 E3 44 07 6B A8 C0 54  .5nNycP.#гD.kЁАТ
00000230: 08 ED DF CF 34 D0 B9 B7  14 BE 65 52 42 4F 17 3F  .нЯП4Р№·.ѕeRBO.?
00000240: F2 27 3F B3 59 5C 01 2B  BB 58 A7 B6 4D 1C 30 03  т'?іY\.+»X§¶M.0.
00000250: C0 35 71 36 80 65 65 C5  C9 06 6D DF 1D 38 5E 6C  А5q6ЂeeЕЙ.mЯ.8^l
00000260: 46 77 07 47 FE 7F 3C 70  F1 27 66 8D 54 B6 0E 6E  Fw.Gю<pc'fЌT¶.n
00000270: 8B 8A 8A AA 82 21 1D 32  D7 07 4A 5A AA 31 B1 2D  ‹ЉЉЄ‚!.2Ч.JZЄ1±-
00000280: A9 9C E8 79 93 61 B7 2C  42 7F CB 5E FC 7E 2E EB  ©њиу“а·,ВЛ^ь~.л
00000290: 85 5F 55 C8 26 C1 EA C4  1D 0B 3D 53 8F 14 22 BA  …_ИИ&БкД..=SЏ."є
000002A0: FE E9 37 6D D1 8D 48 02  46 5B DA 09 EF 75 E3 E8  юй7mСЌН.F[Ъ.пuги
000002B0: BF C6 88 9A 1B 19 6B 84  0A 77 40 86 A0 9F E4 05  їЖЂљ..k„.w@† џд.
000002C0: AB 3E 18 BF 41 96 AD 6E  94 A4 6F FD 83 A1 28 7A  «>.їA–-n”¤oэѓЎ(z
000002D0: A3 F4 7C 29 76 47 C7 42  B7 79 BF F1 5E CB 10 7D  Јф|)vGЗВ·yїc^Л.}
000002E0: E7 A2 58 90 E4 95 11 3F  50 F5 86 35 CC 43 EC 6D  зўXђд•.?Рх†5МСмm
```

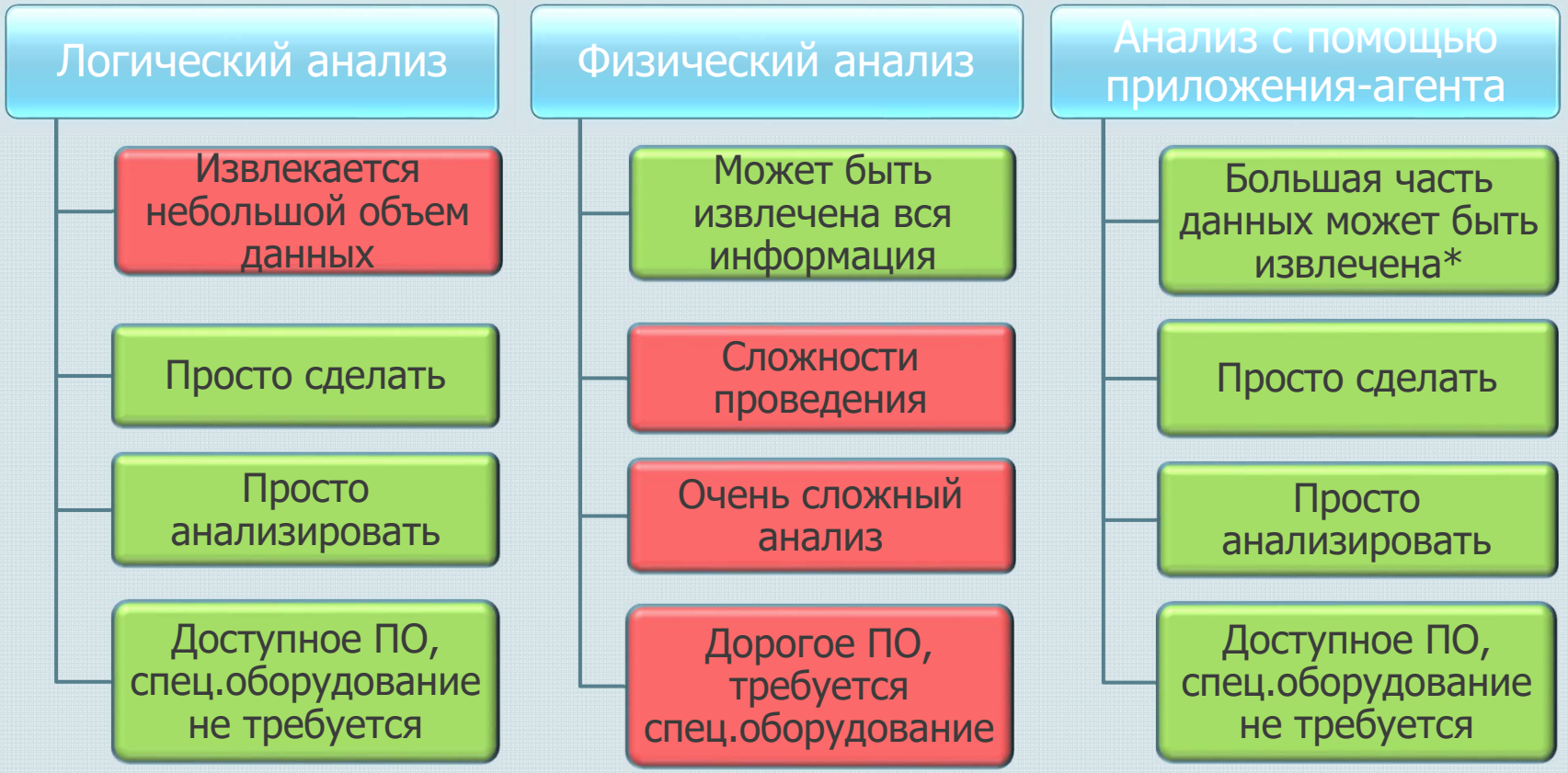
И что делать с ГИГАБАЙТАМИ этого добра?

Стандартные методы: Резюме



Как без проблем извлечь данные?

В 2002 специалистами ЗАО «Оксиджен Софтвер» был изобретен 3й путь – анализ при помощи приложения-агента, работающего внутри смартфона



* - Агент может извлечь всю информацию, доступную приложениям операционной системы

Использование приложения-агента

- ✓Общая информация телефона и SIM карты
- ✓Контакты со всеми полями и частными метками
- ✓Группы абонентов и Быстрые наборы
- ✓Журнал событий
- ✓События календаря
- ✓Дела и Заметки
- ✓Сообщения из стандартных и пользовательских папок
- ✓Информация об удаленных сообщениях
- ✓Дата и время сервисного центра сообщений
- ✓Фотоснимки, видеоролики и голосовые записи
- ✓Файловая система
- ✓Данные GPS и Гео-информация
- ✓Временные файлы и закладки интернет
- ✓Данные клиентов мгновенных сообщения
- ✓Сторонние приложения и их данные

- Защищённые системные файлы
- Дамп памяти

Опасаетесь изменений в телефоне?

Сравнение вносимых в телефон изменений при использовании различных методов анализа

Использование SyncML

- Установка параметров синхронизации
- Установка дополнений для проведения синхронизации*
- Запуск сервера SyncML
- Сервер SyncML создает журналы синхронизации

Использование агента

- Загрузка приложения-агента в устройство
- Установка агента
- Запуск Агента
- Удаление Агента**

* - Установка дополнений может понадобиться для извлечения дополнительной информации (напр. MMS)
** - Агент не создает никаких журналов своей работы

В отличие он Агента, сервер SyncML не предназначен для проведения экспертиз и не предоставляет эксперту полного контроля. В дополнение, он производит больше модификаций данных, чем Агент.

Резюме

Смартфоны занимают значительную долю на рынке мобильных устройств
FutureSource Consulting прогнозирует рост продаж смартфонов на 95% ежегодно в период 2008 – 2013 гг. Объем достигнет 300 миллионов штук. Доля новых смартфонов на рынке достигнет уровня 37%, против 13% в 2008г.

Смартфоны хранят намного больше представляющей интерес информации, чем простые сотовые телефоны
Будучи продвинутым устройством «всё-в-одном» под управлением операционной системы с открытым API смартфоны становятся небольшими ПК с достаточным объемом памяти для хранения и работы как предустановленных, так и сторонних приложений.

Стандартные средства извлечения информации менее эффективны для смартфонов
Все логические протоколы разработаны для синхронизации, поэтому они извлекают только небольшую часть данных. Физический анализ гигабайтов дампов памяти занимает слишком много времени.

Использование приложения-агента является золотой серединой
Метод извлечения данных с использованием Агента, предложенный ЗАО «Оксиджен Софтвер» в 2002 году практически достигает полноты физического анализа. В то же время, для подключения аппартов используются стандартные кабели и адаптеры, а также информация извлекается и представляется для анализа в читаемом формате, что свойственно логическому анализу.

Хотите узнать больше?

www.oxygen-forensic.com

+7 (495) 222-92-78

support@oxygensoftware.com

www.ddf.ru

ЗАО «Оксиджен Софтвер» было основано в 2000 году и с тех пор мы занимаемся разработкой продуктов для работы с мобильными устройствами на ПК