



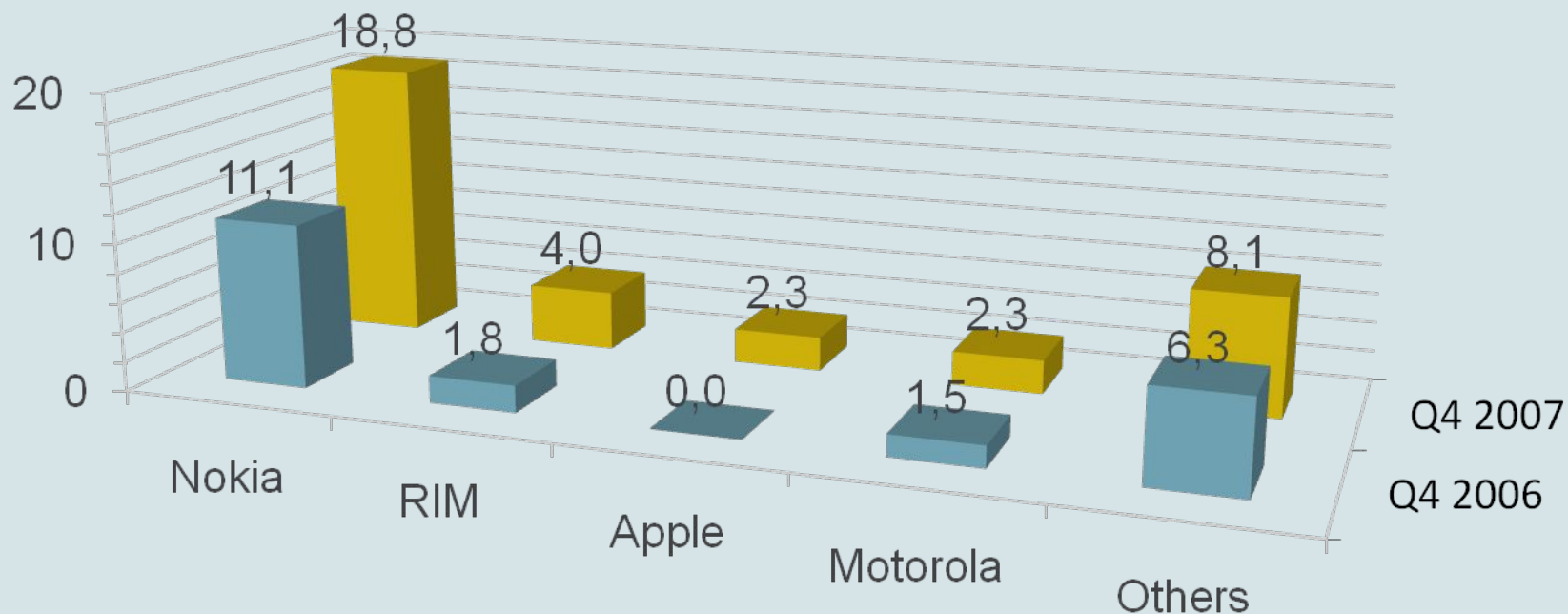
Извлечение информационных улик из телефонов, смартфонов и КПК

Цели исследования телефонов

- ⦿ Извлечение максимально полной и неизменённой информации из сотовых телефонов, смартфонов и КПК.
- ⦿ Анализ информации и нахождения улик.
- ⦿ Подготовка отчётов, которые могут служить доказательством в суде.
- ⦿ Гарантия подлинности извлечённых данных.

Рост рынка смартфонов

Продано устройств, М
Рост продаж Q4 2006/2007 составил 71.9%



Источник: Canalys estimates , © canalys.com ltd, 2008

Эволюция сотовых телефонов

8 лет назад



Nokia 5110

Список контактов

Быстрые наборы

История звонков

SMS сообщения

Мелодии вызова

Общая информация

Сейчас



Современный смартфон

Список контактов

Календарь

Список дел

Заметки

Группы абонентов

Быстрые наборы

Журнал событий

Персональные настройки контакта

Галерея и файлы

Приложения и игры Java

Множественные однотипные поля контакта

Режимы

Папки сообщений

Сообщения

Общая информация

LifeBlog

GPS

Эволюция коммуникационных протоколов



2000

AT+

- Контакты (простые), звонки, SMS, файлы*, настройки*
- Очень медленный
- Зависит от реализации
- Синхронизация

Nokia FBUS

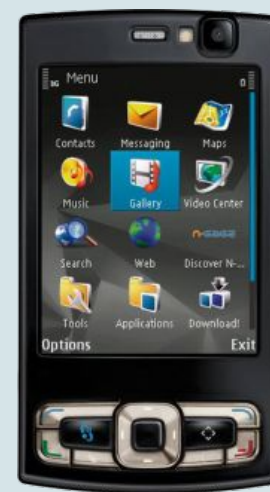
- Почти вся информация
- Не документирован
- Не для смартфонов
- Зависит от реализации
- Синхронизация

OBEX

- Контакты, календарь, файлы
- Зависит от реализации
- Обмен файлами и объектами

SyncML

- Контакты, календарь, настройки, сообщения*
- Зависит от реализации
- Синхронизация



2009

Все стандартные протоколы были разработаны для синхронизации!

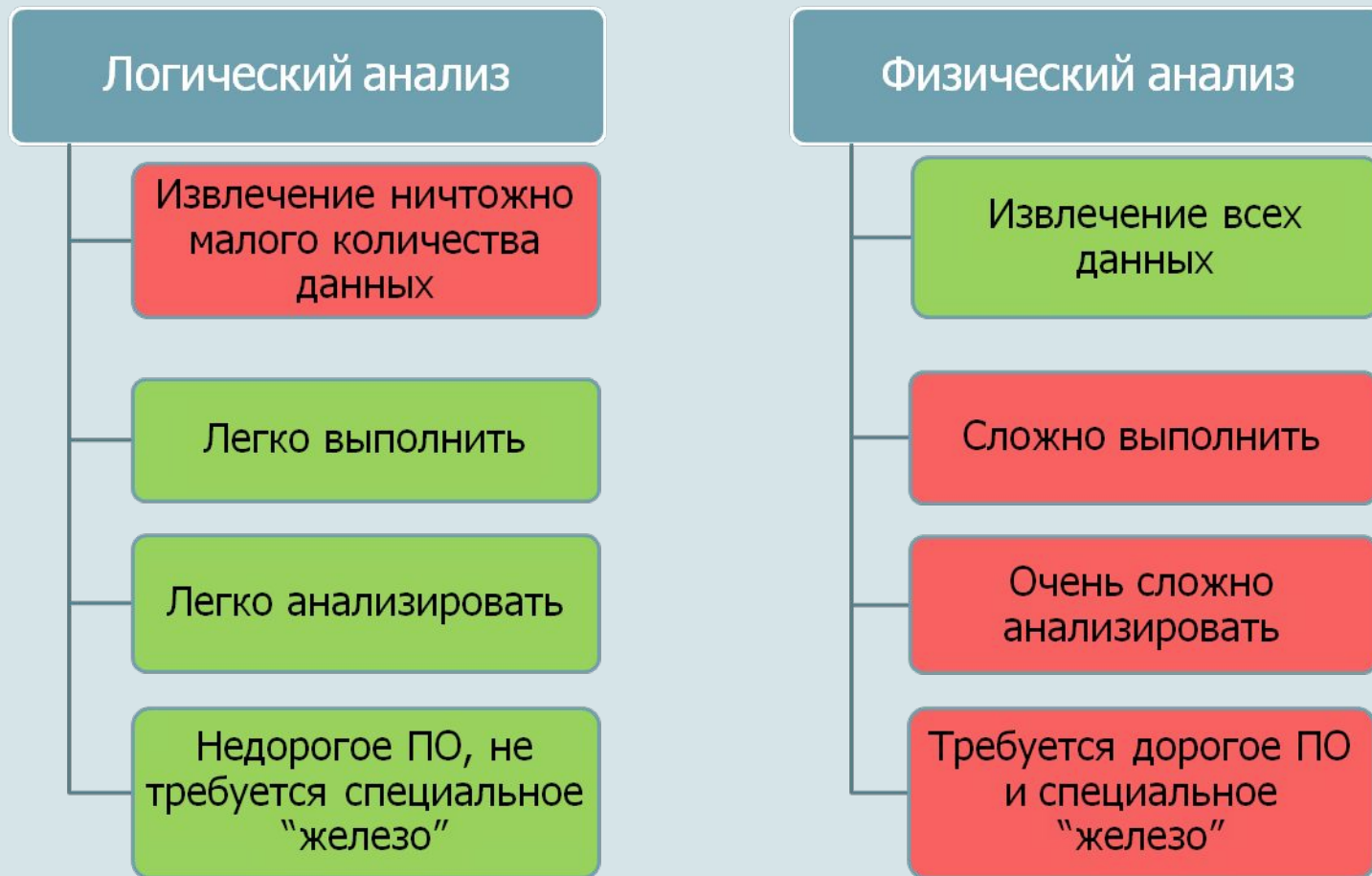
Смартфоны и стандартные протоколы

На текущий день возможности современных смартфонов по части хранения данных сильно превосходят возможности стандартных протоколов по части их извлечения.



Способы извлечения данных

Есть два стандартных способа извлечения информации из смартфонов: логический анализ и физический анализ



Как извлечь все данные?

Мы в Oxygen Software придумали третий способ извлечения данных – с помощью специальной программы-агента, загружаемой непосредственно в смартфон



Использование программы-агента

Программа-агент работает внутри аппарата, соответственно она может извлечь всю информацию, которая доступна для приложений ОС смартфона



Запись в телефон?

Изменяется ли персональная информация в телефоне при записи агента?

Нет. Смартфоны имеют разделённые области памяти для программ и данных.



Противоречит ли такой метод принципу "исследования без вмешательства"?

Теоретически - да. Но это оправдано объёмом и полнотой извлекаемых данных.

Главные преимущества использования Агента

Доступ к журналу LifeBlog смартфонов на платформе Symbian S60

LifeBlog – это предустановленное приложение, которое ведёт журнал отправки и приёма SMS, фотоснимков и других событий, сохраняя их географические координаты (MCC, MNC, LAC, Cell ID). На текущий момент только “Мобильный Криминалист” способен читать эту информацию.

Чтение SMS, MMS и E-mail сообщений из пользовательских папок

Пользователи часто создают отдельные папки для хранения определённых сообщений (например, от конкретного абонента). Стандартные протоколы тут бессильны.

Чтение журнала событий

Смартфоны хранят не только историю звонков, но и историю сообщений, а также журнал GPRS и Wi-Fi сессий.

Извлечение информации об удалённых сообщениях

Многие программы декларируют возможность чтения удалённых сообщений с SIM-карты. Но эта функция бесполезна для смартфонов. “Мобильный Криминалист” – единственный, кто умеет читать удалённые SMS из встроенной памяти телефона.

Сочетание преимуществ логического и физического анализа

“Мобильный Криминалист” вычитывает практически все данные, не требуя дорогого оборудования, и при этом представляет их в читаемом и удобном для анализа виде.

Журнал LifeBlog: список событий

Oxygen Forensic Suite 2

Device View Tools Help

Desktop Search Export Print Help

Life Blog

Gallery item

Name: 20092007055
GMT time: 20.09.2007 11:53:45

Local time: 20.09.2007 13:53:32
Description: e:\images\200709\200709a

Country Code: Germany (262)
Network Code: 02 (7)
Local Area Code / Cell ID: 51038 / 30001



Device Info
Phonebook
Calendar
Messages
Event Log
File Browser
Life Blog

Local time	GMT time	Local Area Code	Cell ID	Country Code	Network Code
28.09.2007 13:38:18	28.09.2007 10:38:18	4804	2748	Finland (244)	Sonera Carrier Networks O
26.09.2007 18:32:24	26.09.2007 15:32:24	1502	15237	Finland (244)	Finnnet Networks Ltd. (12)
24.09.2007 14:44:39	24.09.2007 11:44:39	1502	15245	Finland (244)	Finnnet Networks Ltd. (12)
23.09.2007 12:01:34	23.09.2007 08:01:34	1502	15245	Finland (244)	Finnnet Networks Ltd. (12)
22.09.2007 17:44:57	22.09.2007 13:44:57	6110	4784	Russian Federation (250)	Mobile Telesystems (1)
22.09.2007 17:03:18	22.09.2007 13:03:18	6100	2462	Russian Federation (250)	Mobile Telesystems (1)
22.09.2007 17:01:49	22.09.2007 13:01:49	6100	2462	Russian Federation (250)	Mobile Telesystems (1)
22.09.2007 14:20:23	22.09.2007 10:20:23	6110	4785	Russian Federation (250)	Mobile Telesystems (1)
22.09.2007 04:42:13	22.09.2007 00:42:13	6350	5234	Russian Federation (250)	Mobile Telesystems (1)
22.09.2007 02:38:52	22.09.2007 00:38:52	6350	5232	Russian Federation (250)	Mobile Telesystems (1)
22.09.2007 02:38:43	22.09.2007 00:38:43	6350	5232	Russian Federation (250)	Mobile Telesystems (1)
21.09.2007 15:21:20	21.09.2007 13:21:20	870	31593	Germany (262)	Vodafone (2)
21.09.2007 11:58:40	21.09.2007 09:58:40	893	9682	Germany (262)	Vodafone (2)
21.09.2007 09:37:15	21.09.2007 07:37:15	821	19891	Germany (262)	Vodafone (2)
20.09.2007 20:26:31	20.09.2007 18:26:31	51038	10029	Germany (262)	O2 (7)
20.09.2007 20:17:10	20.09.2007 18:17:24	51038	10029	Germany (262)	O2 (7)
20.09.2007 20:16:50	20.09.2007 18:16:50	51038	10029	Germany (262)	O2 (7)
20.09.2007 20:16:34	20.09.2007 18:16:46	51038	10029	Germany (262)	O2 (7)
20.09.2007 20:16:14	20.09.2007 18:16:28	51038	10029	Germany (262)	O2 (7)
20.09.2007 20:13:07	20.09.2007 18:13:07	51038	10029	Germany (262)	O2 (7)
20.09.2007 19:16:52	20.09.2007 17:17:05	51038	10029	Germany (262)	O2 (7)
20.09.2007 14:23:12	20.09.2007 12:23:13	51038	50103	Germany (262)	O2 (7)
20.09.2007 13:53:32	20.09.2007 11:53:45	51038	30001	Germany (262)	O2 (7)
20.09.2007 13:52:38	20.09.2007 11:52:51	51038	50103	Germany (262)	O2 (7)
20.09.2007 10:52:19	20.09.2007 08:52:19	51047	31134	Germany (262)	O2 (7)
19.09.2007 21:55:12	19.09.2007 19:55:12	51038	30002	Germany (262)	O2 (7)
19.09.2007 16:56:05	19.09.2007 14:56:05	192	1374	France (208)	Bouygues Telecom (20)
19.09.2007 14:54:49	19.09.2007 12:54:49	256	32540	France (208)	Bouygues Telecom (20)
19.09.2007 13:30:54	19.09.2007 11:30:54	256	32540	France (208)	Bouygues Telecom (20)

Total count: 2001 Filtered: 2001 No filter

Журнал LifeBlog: определение положения

The screenshot displays the Oxygen Forensic Suite 2 interface. The main window shows a 'Life Blog' section with a list of items. The left sidebar contains a 'Desktop' view and a 'Nokia N95 (442-60/02)' device selection. The bottom of the sidebar lists various device features like 'Device Info', 'Phonebook', 'Calendar', 'Messages', 'Event Log', 'File Browser', and 'Life Blog'. The main window shows a table of Life Blog items with columns for UID, Description, Name, Folder, and Log. The table lists several items, including photos and text messages. A Google Maps window is open in the foreground, showing a map of Munich, Germany, with a red pin indicating a location. The map window title is '48.140534,11.564909 - Google Maps - Windows Internet Explorer'. The map shows streets like Nymphenburger Str., Marsstraße, and Amulfstraße, and landmarks like the Hofgarten and Prinzregentenstraße. A search bar in the map window contains the coordinates '48.140534,11.564909'.

UID	Description	Name	Folder	Log
4664	e:\images\2008 10\2008 10a0\23102008 147.jpg	23102008 147	e:\images\2008 10\2008 10a0\	
4662	e:\images\2008 10\2008 10a0\23102008 146.jpg	23102008 146	e:\images\2008 10\2008 10a0\	
4660	Finished training. Going to sauna.	Маша	Sent	
4658	e:\images\2008 10\2008 10a0\21102008 145.jpg	21102008 145	e:\images\2008 10\2008 10a0\	
4656	I'm waiting.	Федоров Олег	Sent	
4654	Money delivered.	Федоров Олег	Sent	
4652	e:\images\2008 10\2008 10a0\21102008 144.jpg	21102008 144	e:\images\2008 10\2008 10a0\	
4650	Almost reached point of destination.	Горюнов Сергей	Sent	
4648	Ok \$ delivered	Горюнов Сергей	Inbox	

Чтение сообщений из папок пользователя

The screenshot displays the Oxygen Forensic Suite 2 application window. The interface includes a menu bar (Device, View, Tools, Help), a toolbar (Desktop, Search, Export, Print, Help), and a sidebar with navigation options (Desktop, Suspect (N95 8GB), N95-1 (445-34)/05, Nokia N95 (442-60/02)). The main area shows a list of messages with columns for Type, Folder, Remote party, Time Stamp, and Text. A 'Quick Filter' and 'Message information' panel are also visible.

Messages

Quick Filter: For example, John Doe

Message information: Folder: Sleasy business, Remote party: Text: 29.10.2008 13:48:55 +79852229278, Time Stamp: 29.10.2008 13:48:34, Text: He ordered 5lb. Must deliver next Th.

Type	Folder	Remote party	Time Stamp	Text
SMS	Sleasy business	Slims Scott	29.10.2008 13:48:34	He ordered 5lb. Must deliver next Th.
SMS	Sleasy business	Slims Scott	29.10.2008 13:39:44	Ok it's deal.
SMS	Sleasy business	Slims Scott	29.10.2008 13:37:44	He's ready to take more if price is just.
SMS	Sleasy business	Slims Scott	29.10.2008 13:26:43	Where are you? He disagrees with the price.
SMS	Sleasy business	Slims Scott	29.10.2008 13:23:42	Still waiting for the client...
SMS	Sleasy business	Федоров Олег	21.10.2008 16:33:11	Money delivered.
SMS	Sleasy business	Горюнов Сергей	21.10.2008 16:28:42	Almost reached point of destination.
SMS	Sleasy business	Горюнов Сергей	21.10.2008 16:24:14	Ok \$ delivered
SMS	Sleasy business	Федоров Олег	21.10.2008 16:23:10	To the Turkey? ;)
SMS	Sleasy business	Федоров Олег	21.10.2008 16:21:53	I'm late for Zenit live :-(Still driving home...
SMS	Sleasy business	Горюнов Сергей	21.10.2008 16:07:20	I'm in Helsinki now.
SMS	Sleasy business	Федоров Олег	21.10.2008 14:22:23	No dude. Gone to Turkey. Will be back next week.
SMS	Sleasy business	Федоров Олег	21.10.2008 14:20:04	Are you in Moscow? I need drugs.
SMS	Sleasy business	Alfa-Bank	20.10.2008 8:43:02	Dlya oplaty interneta na summu 1000 RUR na schet 7
Email		atN95@gmail.com "Oleg Fedorov" \Ox\ 21.08.2008 11:17:04		----- Original Message ----- From: Michael O
Email		atN95@gmail.com "Oleg Fedorov" \Ox\ 21.08.2008 11:17:02		
Email		atN95@gmail.com "Nikolay Golubev" <20.09.2007 7:55:40		Для ОФ. Вчера позвонил дяденька (Кирилл Фрол
Email		atN95@gmail.com Олег Фёдоров <of_06.08.2007 22:55:49		У меня твоё письмо в спам упало :-). 1. Ок, беру E-

Total: 1935 Filtered: 14

Журнал событий

Oxygen Forensic Suite 2

Device View Tools Help

Desktop Search Export Print Help

Event Log

Quick Filter
For example, John Dow

Event info
Slims Scott
+79852229278
Type: SMS
Duration: 00:00:00
Time Stamp: 29.10.2008 16:48:34

Device Info
Phonebook
Calendar
Messages
Event Log
File Browser
Life Blog
Desktop

Suspect (N95 8GB)
N95-1 (445-34)/05
Nokia N95 (442-60/02)

Full event log | Answered calls | Missed calls | Dialed calls | SMS | Packet Data | Wi-Fi

Type	Number	Subject	Description
SMS	+79852229278	He ordered 5lb. Must deliver next Th.	Short message
SMS	+79852229278	Ok it's deal.	Short message
SMS	+79852229278	He's ready to take more if price is just.	Short message
SMS	+79852229278	Where are you? He disagrees with the price.	Short message
SMS	+79852229278	Still waiting for the client...	Short message
Voice	+79852229278		Voice call
WiFi	<no number>	Traffic in: 1,89 MB, out: 383,86 KB	Wlan
WiFi	<no number>	Traffic in: 3,04 KB, out: 1,35 KB	Wlan
WiFi	<no number>	Traffic in: 55,75 KB, out: 5,65 KB	Wlan
WiFi	<no number>	Traffic in: 1,29 KB, out: 1,75 KB	Wlan
WiFi	<no number>	Traffic in: 42,56 KB, out: 5,77 KB	Wlan
WiFi	<no number>	Traffic in: 93,78 KB, out: 7,13 KB	Wlan
WiFi	<no number>	Traffic in: 3,45 KB, out: 3,55 KB	Wlan
WiFi	<no number>	Traffic in: 2,25 KB, out: 3,02 KB	Wlan
SMS	Alfa-Bank	Dlya oplaty mobilnoi svyazi na summu 1000 RUR za nomer +79166272	Short message
Voice	+798521		Voice call
SMS	+7916185	И куда оно кладёт то, что прочитало?	Short message
Packet	<no number>	Traffic in: 44,43 KB, out: 5,78 KB	Packet Data
WiFi	<no number>	Traffic in: 355,24 KB, out: 60,29 KB	Wlan
SMS	Alfa-Bank	5*5459; Postupleniye; Summa: 90i	Short message
SMS	Alfa-Bank	Spisanie so scheta 4.	Short message
SMS	Alfa-Bank	Dlya oplaty mobilnoi svyazi na summu 500 RU	Short message
WiFi	<no number>	Traffic in: 563,27 KB, out: 87,06 KB	Wlan
WiFi	<no number>	Traffic in: 0 B, out: 0 B	Wlan
Packet	<no number>	Traffic in: 24,85 KB, out: 18,26 KB	Packet Data
Packet	<no number>	Traffic in: 26,43 KB, out: 18,83 KB	Packet Data
Packet	<no number>	Traffic in: 39,52 KB, out: 25,86 KB	Packet Data

Total: 293 Filtered: 293

Список телефонов

Oxygen Forensic Suite 2

Устройство Просмотр Инструменты Справка

Поиск Справка Демо-тур Выйти

Мой телефон

Общие задачи

Подключить новое устройство

Действия устройства

Открыть устройство

Закреть устройство

Удалить устройство

Показать информацию устройства

Сохранить в архив

Загрузить из архива

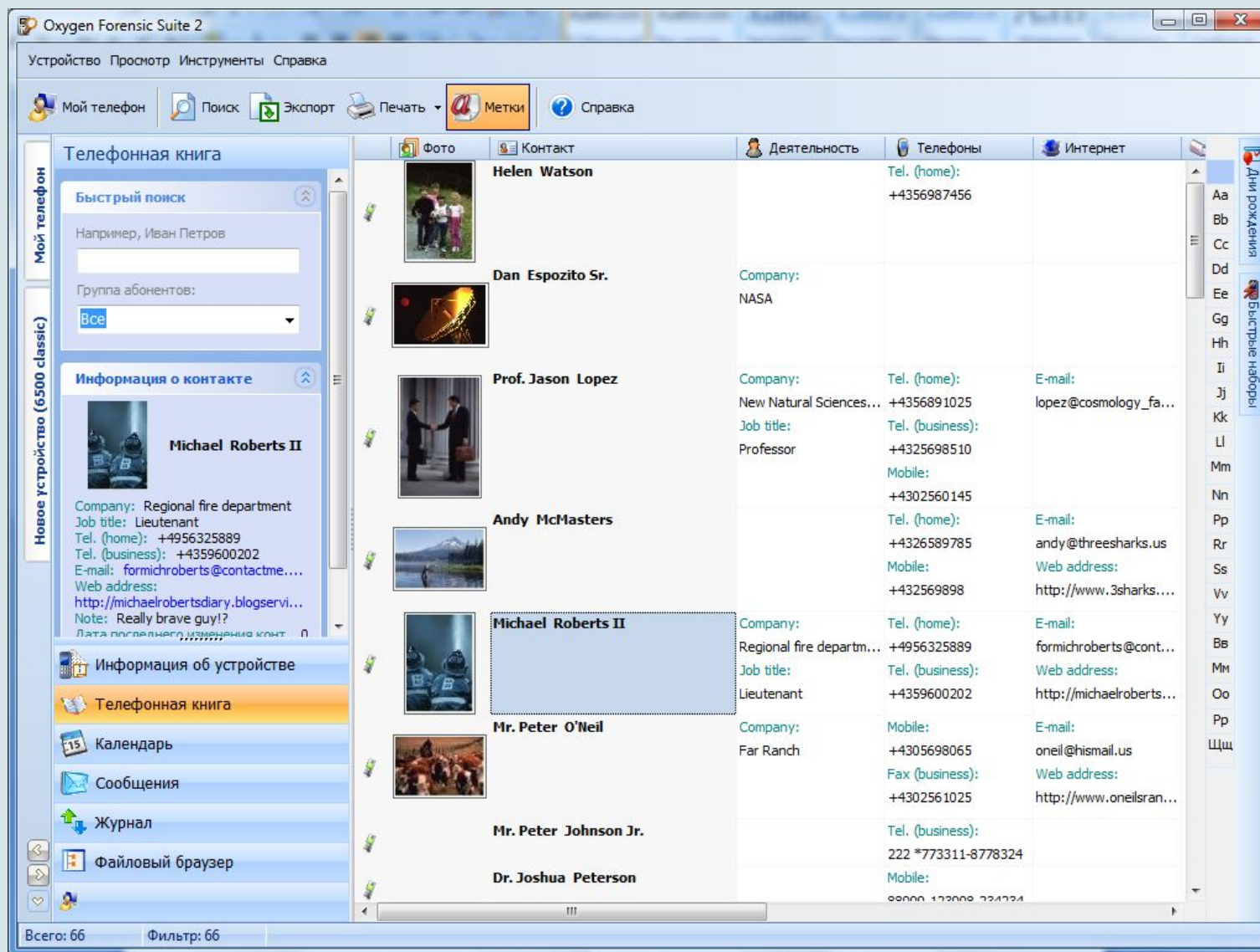
Новое устройство (6500 classic)

№	Устройства	Детали	Извлечение	Статус
	 Модель: Nokia 6500 classic IMEI: 358667011979568 Владелец: <Нет>	Новое устройство (6500 classic) Дело: <Нет>	Инспектор: John Smith 30.10.2008 23:57:49	Открыто
	 Модель: Nokia 6500 classic IMEI: 358667011979568 Владелец: <Нет>	Новое устройство (6500 classic) Дело: <Нет>	Инспектор: John Smith 30.10.2008 1:31:03	Открыто
	 Модель: BlackBerry 8800 IMEI: 354672013206659 Владелец: <Нет>	Tom Hagen (8800) Дело: Corleone family	Инспектор: Unknown User 08.05.2008 17:11:31	Открыто
	 Модель: Nokia 7610 IMEI: 353387000326920 Владелец: <Нет>	Bruno Tattaglia (Nokia 7610) Suspected in secret communications with Corleone f Дело: Tattaglias	Инспектор: Unknown User 06.05.2008 10:37:20	Открыто
	 Модель: Windows Mobile WM ph IMEI: 352994019542982 Владелец: <Нет>	Santino Corleone (Eten Glofish) New York, May 05, 2008. Found at Santion Corleon Дело: Corleone family	Инспектор: Unknown User 06.05.2008 10:29:04	Открыто
	 Модель: Sony Ericsson K530i IMEI: 353500021126711 Владелец: <Нет>	Jules Segal (K530i) Taken from Jules Segal suspected in relations with C Дело: Corleone family	Инспектор: Unknown User 06.05.2008 10:25:15	Открыто

Всего устройств: 6, открыто: 6

Авторизировано

Телефонная книга



Календарь

Oxygen Forensic Suite 2

Устройство Вид Инструменты Справка

Мой телефон Поиск Экспорт Печать Справка

Календарь

Быстрый поиск

Например, Иван Петров

Информация о событии

Напоминание
Начало: 19.11.2008
Сигнал: В тот же день в 12:00
Повторение: Каждую неделю, Среда.
Текст: Поливать цветы
MD5 Hash:
3ec202ca0a16861cdbee45b1f8cec51c

Информация об устройстве

Телефонная книга

Календарь

Сообщения

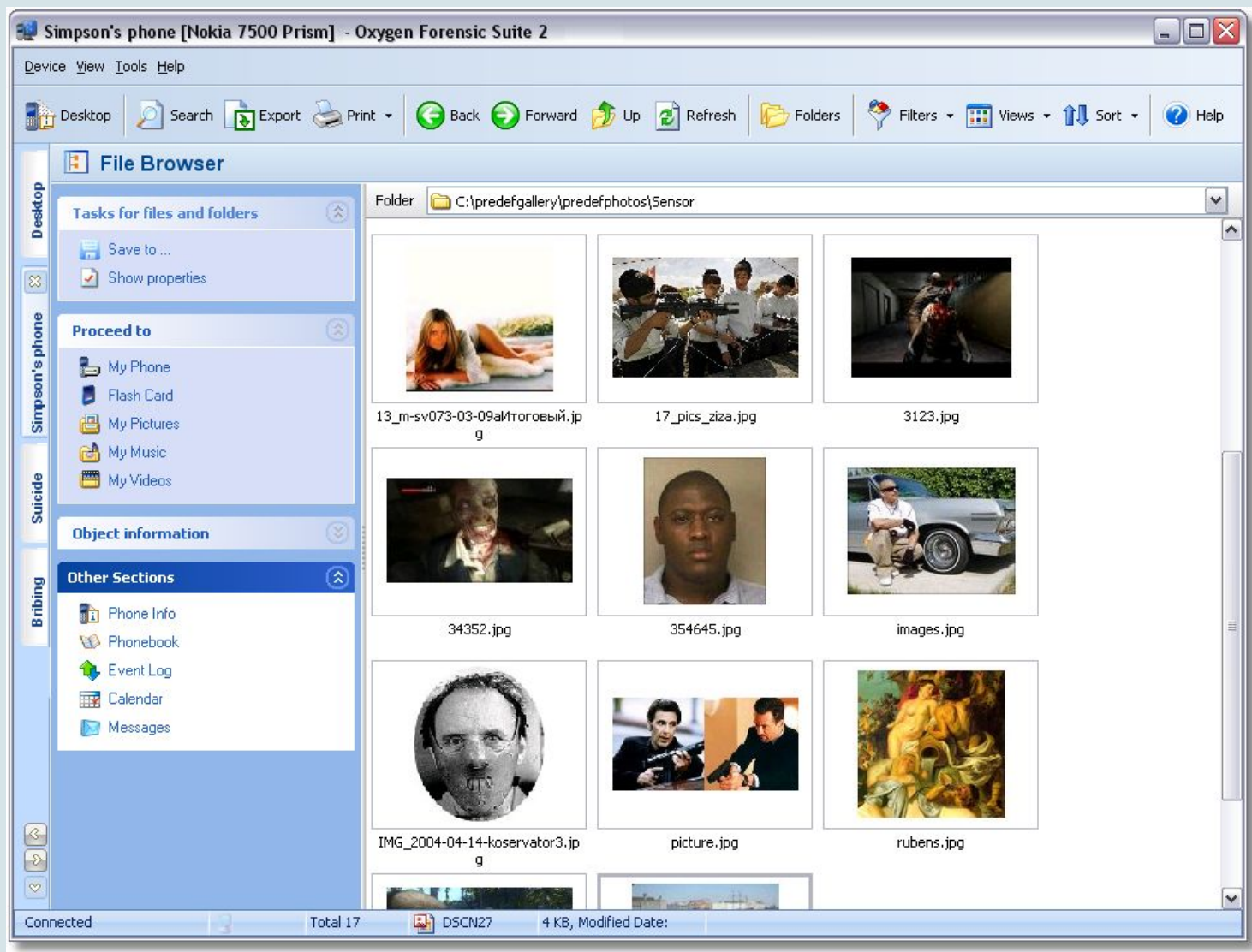
Журнал

Файловый браузер

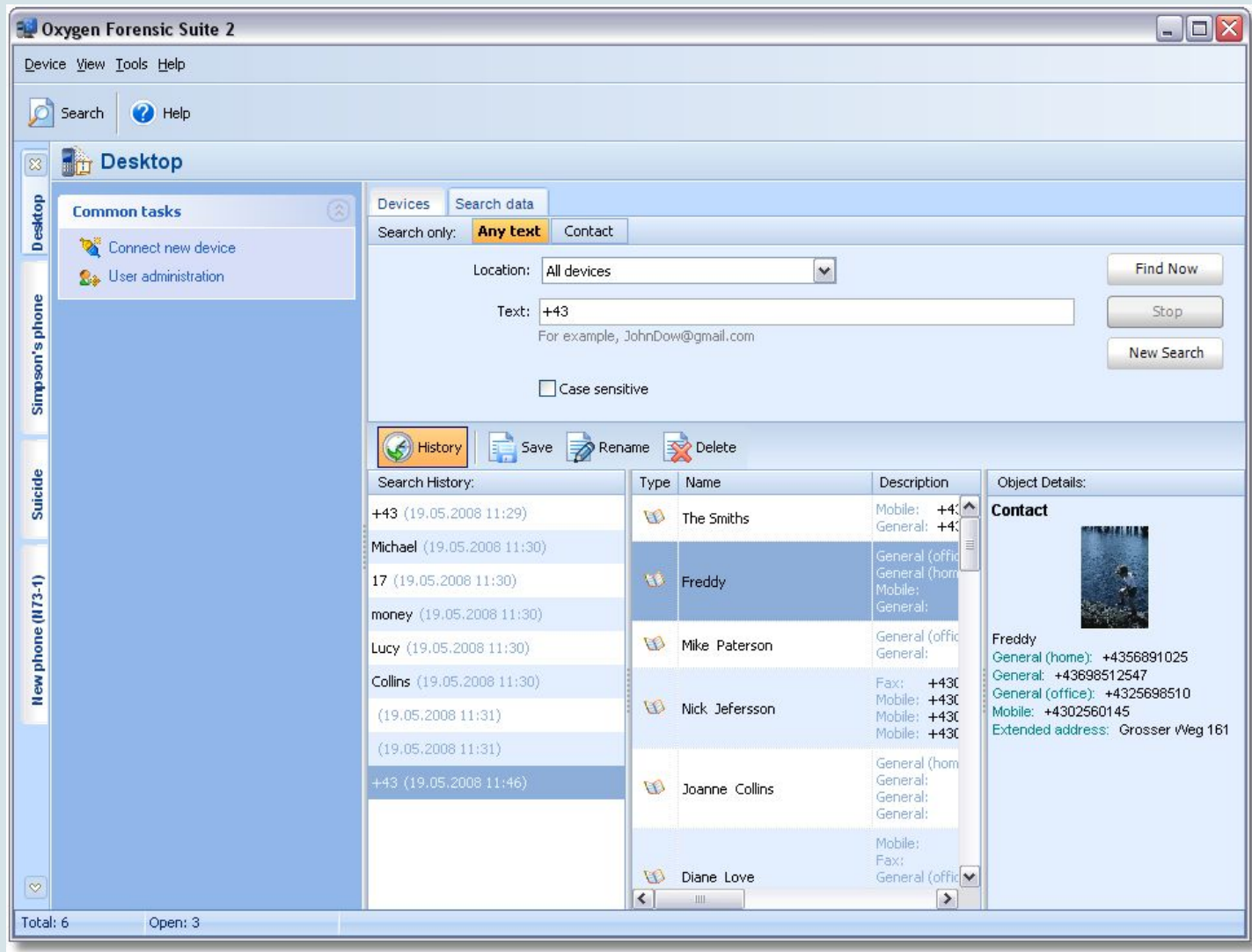
Время	Описание	MD5 Hash
Начало: 27.09.1982 Сигнал: В тот же день в 10:00	Текст: Евдокимова Софья	9f4e0c42ffbd35bfc766a43e1f68ba0
Начало: 25.01.1983 Сигнал: В тот же день в 10:00	Текст: Панкова Татьяна	fa286a333c2eb48f406df34eb5938980
Начало: 19.11.2008 Сигнал: 61 дня(ей) до в 11:00	Текст: Парикмахерская	c2ff3e08aea262b873715d7d56569296
Начало: 21.11.2009 Окончание: 22.11.2009	Текст: Позвонить Андрею	90e9f7ae3380eda079f11890c7ea90de
Начало: 01.11.2008 Сигнал: В тот же день в 21:30	Текст: Напомнить	5ffaaf0549fe3dbfd3ac13433daf05a6
Начало: 19.11.2008 Сигнал: В тот же день в 12:00	Текст: Поливать цветы Повторение: Каждую неделю, Среда.	3ec202ca0a16861cdbee45b1f8cec51c
Начало: 21.11.2008 Сигнал: В тот же день в 10:00	Текст: Планерка Повторение: Каждую неделю, Пятница.	eac8957f0603b7b827a2e3935865c3df
Начало: 22.11.2008 Сигнал: В тот же день в 12:00	Текст: Поливать цветы Повторение: Каждую неделю, Суббота.	65eebfd9d701a0427364306bad3563d4
Начало: 24.11.2008 Сигнал: В тот же день в 10:00	Текст: Планерка Повторение: Каждую неделю, Понедельник.	d3bd3b240c1f7e1c88e4d236d5545ffc
Начало: 24.11.2008 Сигнал: В тот же день в 12:00	Текст: Поливать цветы Повторение: Каждую неделю, Понедельник.	f54164d126cc9cbcf64ce619e22dd95

Всего: 20 Фильтр: 20

Галерея телефона



Поиск данных по нескольким телефонам



Частые вопросы и ответы на них

Какие способы соединения с телефоном поддерживает OxyAgent?

Кабель, Bluetooth, ИК – обычно любые методы, поддерживаемые самим телефоном.

Используется ли Microsoft ActiveSync для чтения данных их устройств на платформе Windows Mobile?

Нет. ActiveSync – это приложение для синхронизации, которое способно внести изменения в данные телефона. Поэтому мы используем прямую связь через Bluetooth.

Может ли “Криминалист” считать информацию из заблокированного с помощью ПИН-кода телефона?

К сожалению, ни одна программа не может преодолеть блокировку ПИН-кодом.

Какая информация может быть прочитана Агентом?

Вся информация, которая доступна приложениям для ОС смартфона.

Работает ли “Мобильный Криминалист” с обычными телефонами?

Конечно. На данный момент он поддерживает более 1000 моделей.

Нужен ли Агент для анализа обычных телефонов (например Nokia 6500)?

Нет. Агент нужен только для смартфонов. Для обычных телефонов “Криминалист” использует комбинацию из стандартных низкоуровневых протоколов.

О нас

ЗАО "Оксиджен Софтвр"
Россия, 117216, Москва, ул.
Феодосийская, 1

Телефоны:

+7-495-222-9278 (Россия)

+1 (877) 9-OXYGEN (USA)

+44 020 8133 8450 (UK)

www.oxygensoftware.ru

www.oxygen-forensic.com

