Юрин Игорь Юрьевич
ООО «Национальный центр по борьбе
с преступлениями в сфере высоких технологий» (Россия)

Forensic Assistant - программное обеспечение для экспертно-криминалистического исследования компьютерных носителей информации

Программный комплекс «Forensic Assistant» («Помощник эксперта»)

Предназначен для автоматизации работы эксперта судебной компьютерной и компьютерно-технической экспертиз при проведении исследования носителей информации.

Возможности:

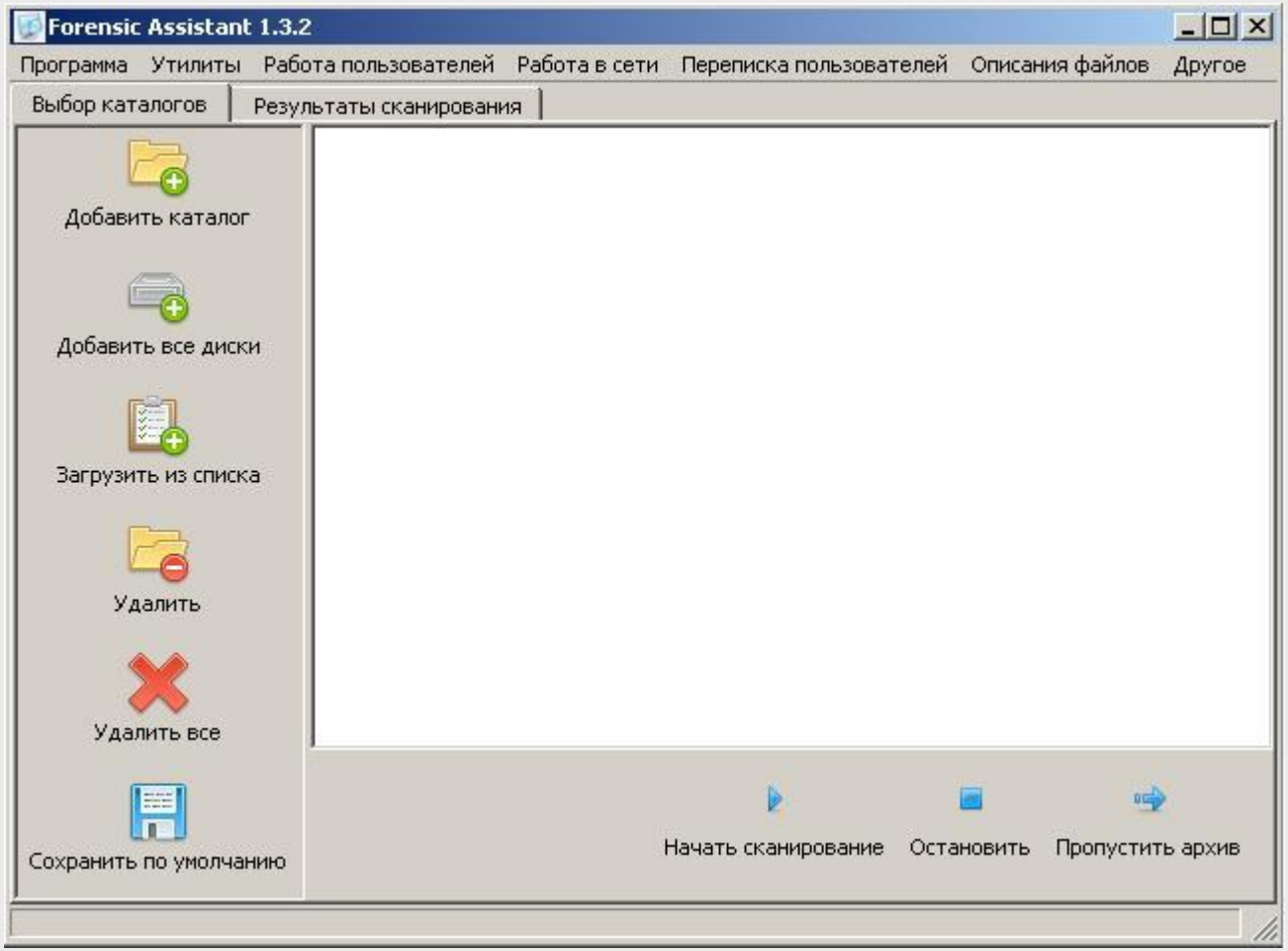
1. Исследование файловой структуры носителя информации;
2. Анализ файлов;
3. Составление текстовых фрагментов, включаемых в справки специалиста и заключения эксперта.

Основные направления исследования:

1. Обстоятельства работы пользователя в сети Интернет;
2. Обстоятельства работы пользователя за локальным компьютером;
3. Переписка пользователя;
4. Описание характеристик файлов;
5. Определение подключения сменных носителей, обстоятельств подготовки документов, и др.

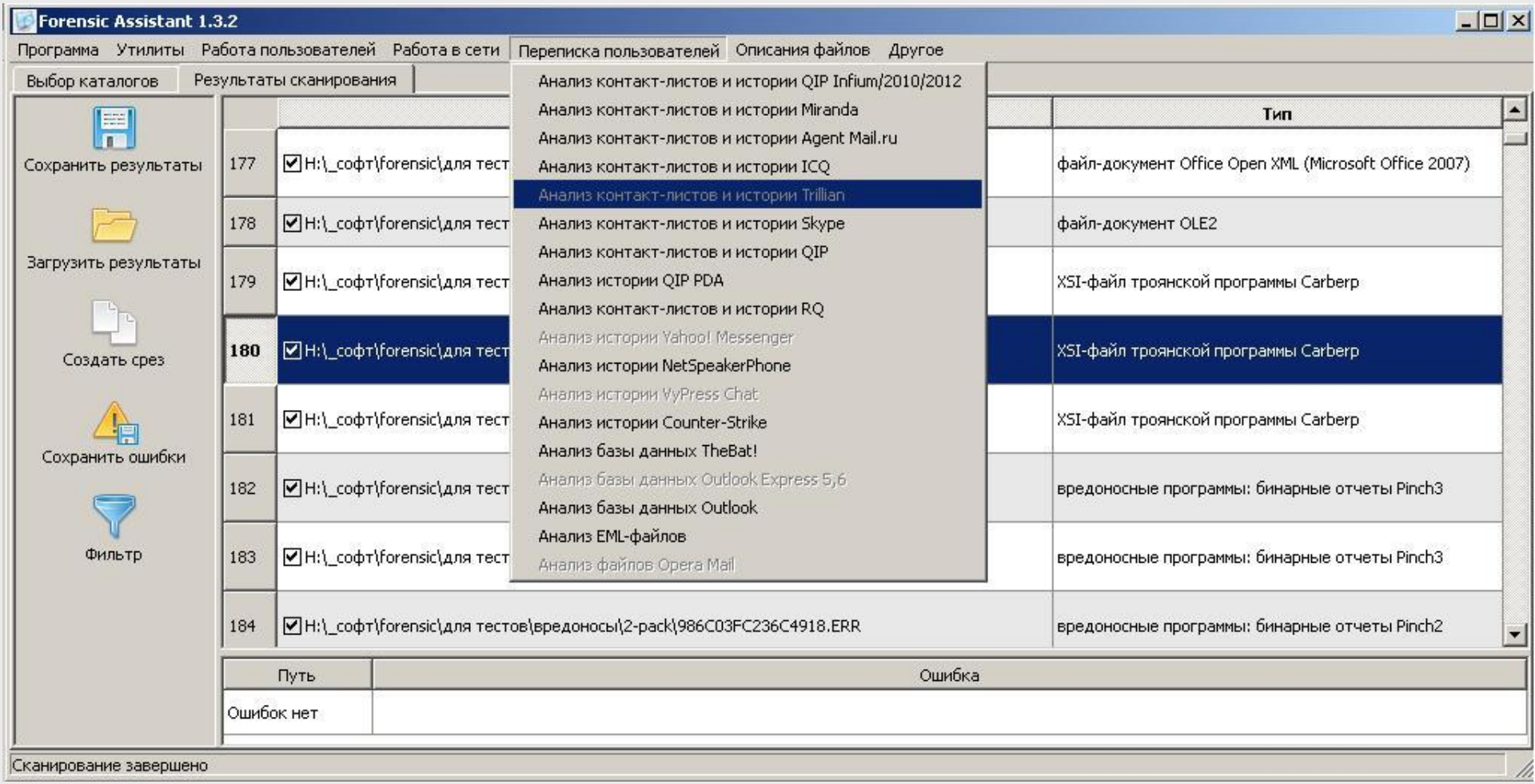
0xFA:
Forensic Assistant

Пользовательский интерфейс



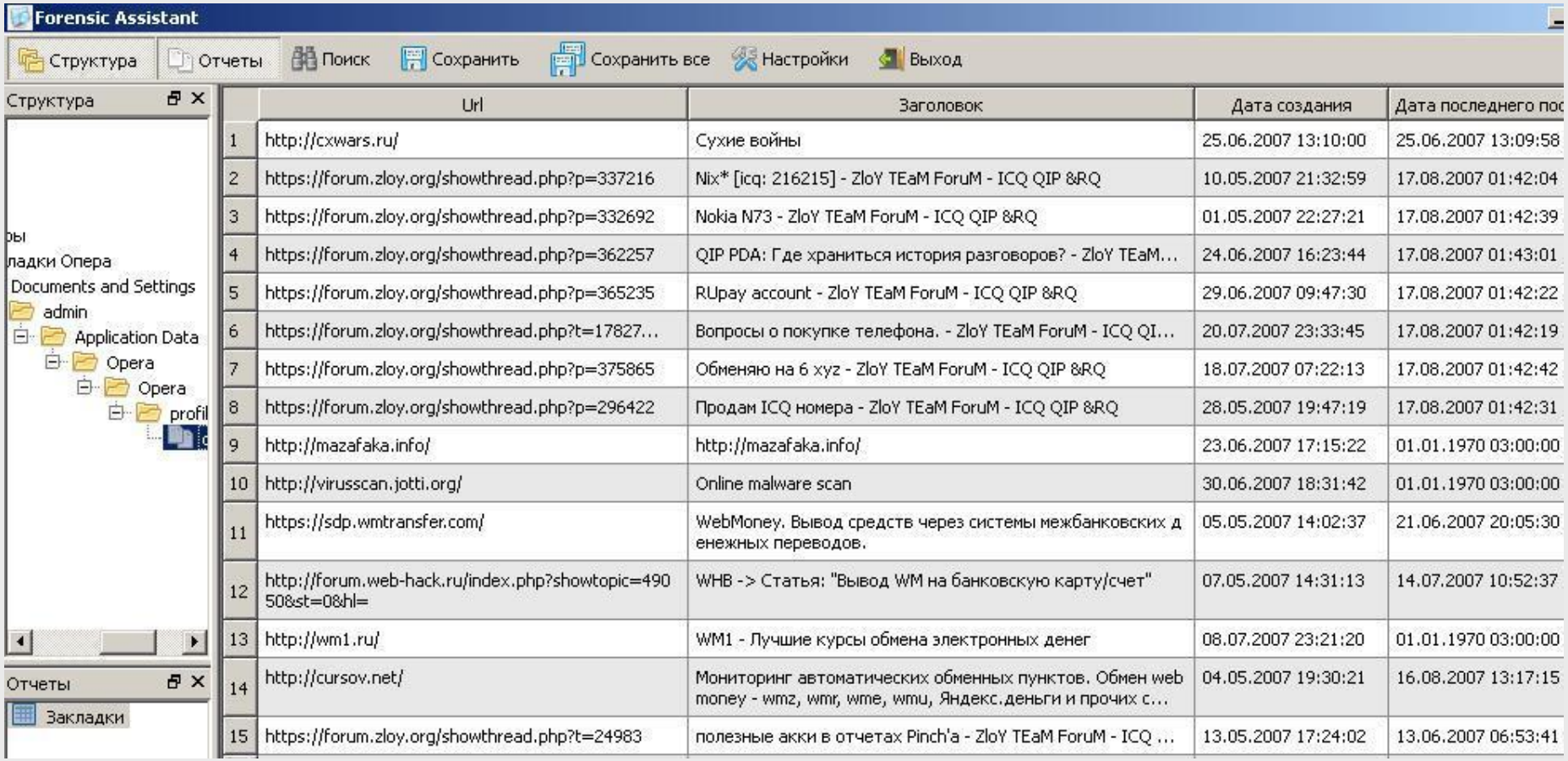
0xFA:
Forensic Assistant

Пользовательский интерфейс



0xFA:
Forensic Assistant

Пользовательский интерфейс



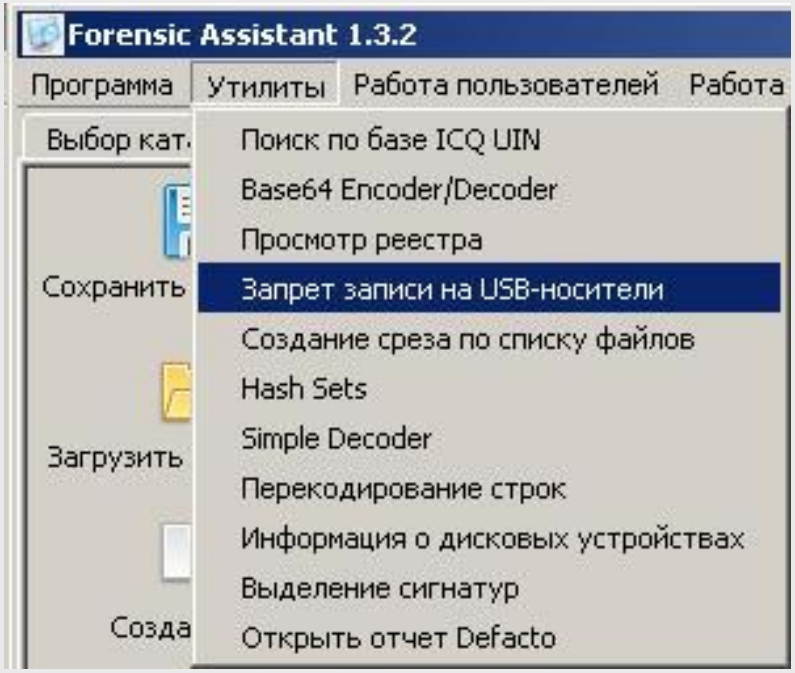
	Url	Заголовок	Дата создания	Дата последнего пос
1	http://cxwars.ru/	Сухие войны	25.06.2007 13:10:00	25.06.2007 13:09:58
2	https://forum.zloy.org/showthread.php?p=337216	Nix* [icq: 216215] - ZloY TEaM ForuM - ICQ QIP &RQ	10.05.2007 21:32:59	17.08.2007 01:42:04
3	https://forum.zloy.org/showthread.php?p=332692	Nokia N73 - ZloY TEaM ForuM - ICQ QIP &RQ	01.05.2007 22:27:21	17.08.2007 01:42:39
4	https://forum.zloy.org/showthread.php?p=362257	QIP PDA: Где храниться история разговоров? - ZloY TEaM...	24.06.2007 16:23:44	17.08.2007 01:43:01
5	https://forum.zloy.org/showthread.php?p=365235	RUpay account - ZloY TEaM ForuM - ICQ QIP &RQ	29.06.2007 09:47:30	17.08.2007 01:42:22
6	https://forum.zloy.org/showthread.php?t=17827...	Вопросы о покупке телефона. - ZloY TEaM ForuM - ICQ QI...	20.07.2007 23:33:45	17.08.2007 01:42:19
7	https://forum.zloy.org/showthread.php?p=375865	Обменяю на 6 xyz - ZloY TEaM ForuM - ICQ QIP &RQ	18.07.2007 07:22:13	17.08.2007 01:42:42
8	https://forum.zloy.org/showthread.php?p=296422	Продам ICQ номера - ZloY TEaM ForuM - ICQ QIP &RQ	28.05.2007 19:47:19	17.08.2007 01:42:31
9	http://mazafaka.info/	http://mazafaka.info/	23.06.2007 17:15:22	01.01.1970 03:00:00
10	http://virusscan.jotti.org/	Online malware scan	30.06.2007 18:31:42	01.01.1970 03:00:00
11	https://sdp.wmtransfer.com/	WebMoney. Вывод средств через системы межбанковских д енежных переводов.	05.05.2007 14:02:37	21.06.2007 20:05:30
12	http://forum.web-hack.ru/index.php?showtopic=49050&st=0&hl=	WHB -> Статья: "Вывод WM на банковскую карту/счет"	07.05.2007 14:31:13	14.07.2007 10:52:37
13	http://wm1.ru/	WM1 - Лучшие курсы обмена электронных денег	08.07.2007 23:21:20	01.01.1970 03:00:00
14	http://cursov.net/	Мониторинг автоматических обменных пунктов. Обмен web money - wmz, wmr, wme, wmu, Яндекс.деньги и прочих с...	04.05.2007 19:30:21	16.08.2007 13:17:15
15	https://forum.zloy.org/showthread.php?t=24983	полезные акки в отчетах Pinch'a - ZloY TEaM ForuM - ICQ ...	13.05.2007 17:24:02	13.06.2007 06:53:41

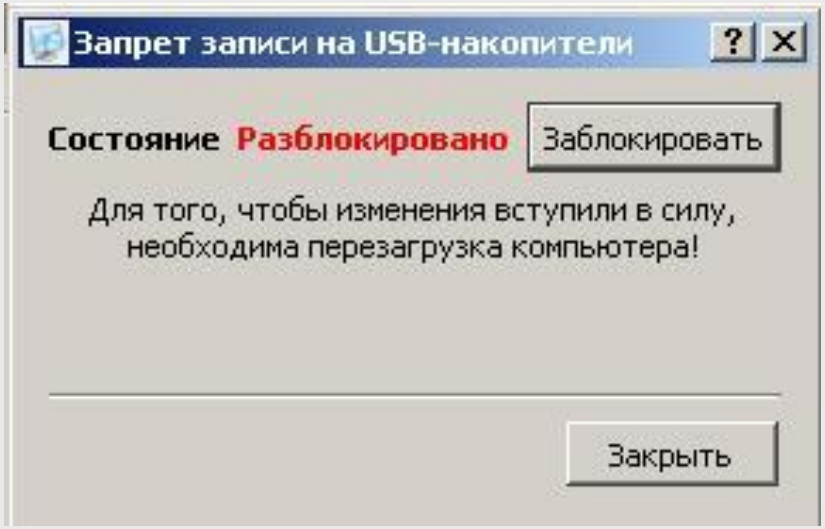
0xFA:
Forensic Assistant

Работа в режиме «только чтение»

Блокирование записи на USB:

Исследуемые носители информации подключаются к компьютеру эксперта в режиме «только чтение» для предотвращения модификации данных в процессе исследования.





Позволяет искать и анализировать криминалистически значимую информацию из:

- баз программ обмена сообщениями по протоколу OSCAR (ICQ, ICQ Lite, &RQ, R&Q, Trillian, QIP, QIP Infium, QIP PDA, Miranda) - контакт-листы и переписка пользователей;
- баз программ обмена сообщениями (Mail.ru Agent, Skype, Skype 4, VyPress Chat, Yahoo! Messenger) - контакт-листы и переписка пользователей;
- баз обмена сообщениями игровых программ (NetSpeakerPhone, Counter-Strike);
- баз почтовых программ (Outlook, Outlook Express, TheBat!, Opera Mail, *.eml) - письма и почтовые вложения, в том числе - в удаленном виде;
- индексных файлов ОС Windows (index.dat) - все блоки, включая LEAK;
- системных журналов событий (Event Logs) ОС Windows, включая Windows Vista/7 (*.evt, *.evtx) - информация о работе компьютера в сети, о подключении сменных носителей;
- служебных файлов ОС Windows (Prefetch - *.pf, Link - *.lnk, setupapi.log, *.pbk, modemlog*, *.xml DataColl);
- служебных файлов программ-браузеров (Internet Explorer, Opera, Firefox);
- кэша виртуальной машины Java;
- документов в форматах OLE2, ODF (Open Office), Office Open XML (Microsoft Office 2007), PDF - все необходимые метаданные в корректном виде;
- графических файлов распространенных форматов - метаданные и миниатюры изображений;
- резервных копий адресных книг и сообщений мобильных телефонов (Nokia, Samsung и др.);

0xFA:
Forensic Assistant

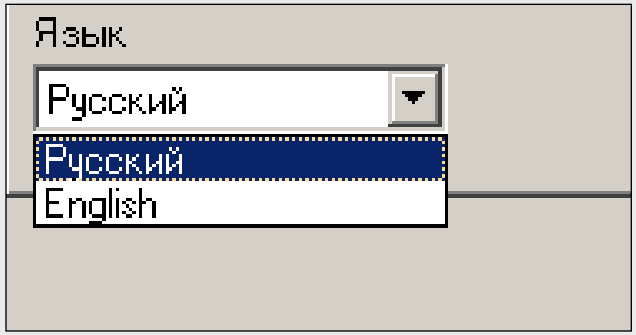
Возможности

Модульная архитектура

Программа имеет модульную структуру с гибким интерфейсом (API), что позволяет выпускать дополнения и новые модули, в том числе разработанные сторонними авторами. Загрузка обновлений может быть осуществлена через сеть Интернет.

Многоязычный интерфейс

Поддержка нескольких языков делает возможным применение данного комплекса и в других странах. Перевод интерфейса на любой язык не требует вмешательства автора программы и может быть осуществлен любым пользователем.



Встроенные утилиты:

- создание среза файлов по списку файлов ("чистый" список, отчет "Антивируса Касперского", отчеты программ "AvSearch" и "Архивариус 3000");
- кодирование/декодирование информации в формате base64 (MIME);
- кодирование/декодирование информации простейшими алгоритмами (для извлечения настроек вредоносных программ);
- криминалистический учет номеров ICQ;
- блокировка записи на USB-устройства (для Windows XP SP2+/Vista/7/8);
- утилита "RegWalker", позволяющая осуществлять работу с неактивным реестром ОС Windows;
- утилита "Hash Sets", позволяющая создавать базы хэшей, проводить детектирование файлов с их использованием, сравнивать группы файлов (в том числе - программу и ее дистрибутив).
- сбор информации о подключенных дисковых устройствах;
- автоматизированное выделение сигнатур из произвольного числа файлов;
- модуль для инвентаризации программного обеспечения "Defacto";
- декодирование паролей программы "Mail.ru Agent";

Дополнительные возможности:

- результаты представляются в табличной форме, доступна сортировка по любому полю таблицы и поиск текстовых строк (в том числе - по списку);
- результаты можно экспортировать в текстовый файл (RTF) или файл программы Excel (CSV);
- экспортируемые результаты адаптированы для включения в текст заключения эксперта;
- поиск и анализ информации осуществляется, в том числе, внутри архивов 14-ти форматов;
- обнаружение архивов, защищенных паролем, и файлов некоторых криптографических программ;
- предпросмотр найденных файлов с использованием внешних утилит;
- проверка целостности подключаемых модулей программы;
- возможность добавления пользователями собственных сигнатур для детектирования файлов;
- обновление через сеть Интернет, в том числе через прокси-сервер.

Наши пользователи

«Forensic Assistant» применяется на практике в ряде экспертных учреждений России (ЭКЦ МВД, ЛСЭ Минюста, ЭКО ФСКН, Следственного Комитета, ФСБ), правоохранительных органах других стран (МВД Республики Беларусь, КГБ Республики Беларусь, КНБ Республики Казахстан, Полиции Республики Молдова), а также в независимых экспертных организациях.

Программный комплекс «Forensic Assistant» использовался при обучении экспертов судебной компьютерной экспертизы органов МВД России в Саратовском юридическом институте МВД России.

Наши контакты

http://www.nhtcu.ru

info@nhtcu.ru