САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Математико-механический факультет
Кафедра системного программирования

Дмитриева Дарья Алексеевна

Создание triage-инструмента для цифровой криминалистики

Курсовая работа

Научный руководитель:
ст. преп. Губанов Ю. А.

Санкт-Петербург
2015

Оглавление

Введение

В современной криминалистке для доказательства вины или причастности какого-либо человека к преступлению используются личные вещи подозреваемого. Важной уликой может стать содержимое персонального компьютера, так как на нем могут содержаться личные переписки, документы, фотографии, история посещенных сайтов и др. Также можно установить местоположение человека по данным его устройств.

Поиском и анализом улик такого рода занимается цифровая криминалистика.

Лучше всего проводить анализ в специальных лабораториях, куда можно принести устройства для обследования. Но может возникнуть ситуация, когда надо быстро определить наличие улик на компьютере подозреваемого и нет времени или возможности перевозить его куда-либо. Или в составе команды, прибывшей на место преступления, нет опытного программиста, который умеет проводить анализ устройств без установки дополнительных программ на компьютер.

В таких случаях используется специальное программное обеспечение, позволяющее провести быстрый поиск улик (в цифровой криминалистики для этого процесса используется термин triage анализ), не обладая навыками цифровой криминалистики.

Такое ПО запускается со съемного носителя, который заранее готовит программист в лаборатории. При включении в целевой компьютер достаточно просто запустить нужный исполняемый файл и подождать, пока программа сама найдет все нужные улики и сохранит их на носитель. Причем переносимые данные не теряют информативность и сохраняют свою значимость как возможные улики.

Далее данные с этого носителя можно передать специалистам, чтобы исследовать на любом другом компьютере всему доступными средствами.

Постановка задачи

- Провести исследование существующих средств.
- Реализовать возможность эффективного захвата данных определенного пользователем типа с возможностью их использования для компьютерной криминалистики. Для этого нужно создать инструмент, работающий по следующему алгоритму:

1) На рабочей машине эксперта запускается интерфейс, в котором задать параметры поиска интересующих файлов и фильтры, например:

- Быстрый или подробный поиск
- Типы интересующих данных
- Делать захват RAM или нет
- Осуществлять поиск с копированием данных или без

2) Создается XML-документ с конфигурацией поиска файлов с заданными раннее параметрами и записывается на какое-либо съемное устройство вместе со специальной версией программы.
3) Это устройство вставляется в целевой компьютер, запускается и осуществляет поиск и копирование значимых файлов. Одна из сложностей заключается в том, что необходимо скопировать файлы с мета-информацией.
4) При подключении устройства в рабочий компьютер пользователь может извлечь файлы для последующего анализа, если был выбран поиск с копированием.

Существующие средства

EnCase Portable

EnCase Portable[3] является автономным устройством, содержащим следующие компоненты, описанные ниже:

- Загрузочный ключ безопасности (Bootable Security Key**,** 4 Гб карманный USB Device). Он содержит в себе EnCase, Encase Portable, EnCase Portable Management EnPack и некоторое свободное пространство, которое можно использовать для хранения собранных доказательств.
- EnCase Portable Boot CD.
- EnCase Portable установочный DVD.

На рабочей машине должен быть установлен продукт EnCase, поверх которого устанавливается EnCase Portable. В EnCase Portable можно работать через EnCase с помощью Portable Management EnPack.

Работу на целевой машине осуществляется с помощью bootable Security Key(входит в комплект EnCase Portable), separate Security Key(можно создать из любого USB флэш-носителя) или bootable CD(входит в комплект EnCase Portable). При больших объемах собираемых данных можно заранее добавить дополнительные устройства хранения.

Перед началом работы на целевой машине, надо на рабочей машине создать дело(Job), которое можно экспортировать из EnCase или с диска, где указываны фильтры для данных или конкретный набор данных, которые нужно будет собрать, и добавить на съемное устройство, которое будет использовано.

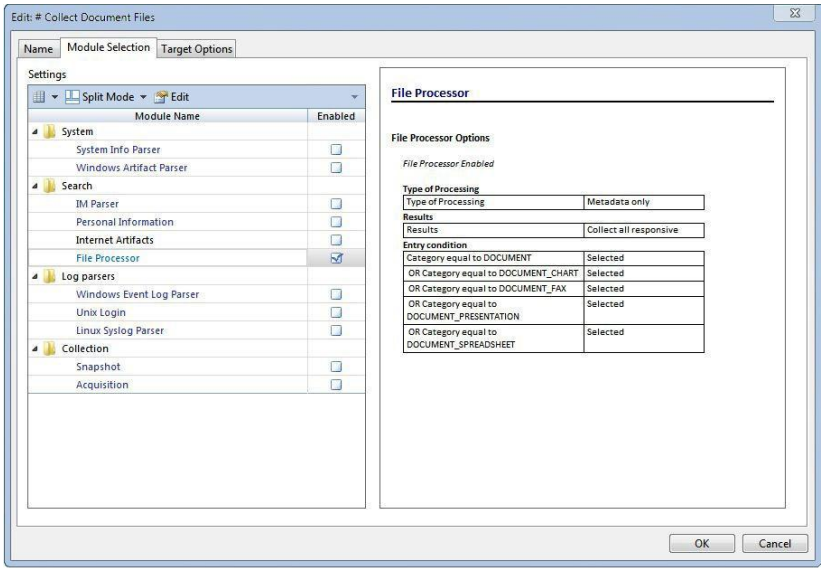

Рис. 1. Окно настройки модулей при создании дела.

Дело состоит из модулей.

Каждый модуль отвечает за свой тип инструкций, которые можно конфигурировать.

Также можно выбрать типы данных, которые будут сканироваться:

- системная информация,
- артефакты, оставленные клиентами мгновенного обмена сообщениями,
- все документы, базы данных и файлы Интернета
- история посещенных веб-сайтов, кэш пользователя, закладки, печенье и загруженных файлов.
- события Windows, зарегистрированных в системные журналы, в том числе приложения, системы и журналов безопасности
- snapshot соответствующей информации машины
- любые файлы, используя метаданные, ключевые слова или наборы хэшей, или найти данные изображения

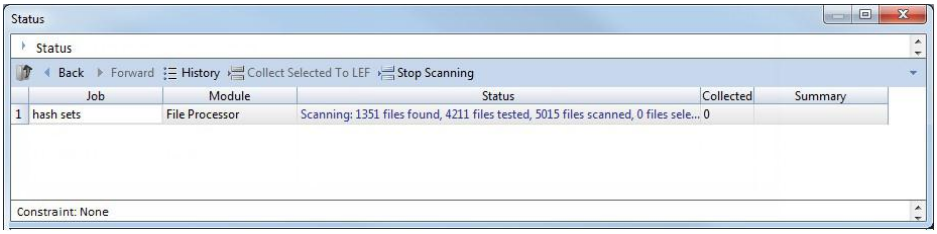

Рис. 2. Отсеивание данных с помощью хэш-функций

1. Запуск EnCase Portable на целевой машине:
   - Для работающего компьютера надо вставить съемный носитель с EnCase Portable в целевую машину, далее автоматически запустится диалогое окно EnCase Portable.
   - Для выключенного компьютера включить компьютер, зайти в настойки BIOS, выбрать тип устройства, которое будет использовать(USB или CD), далее надо подключить сначала bootble CD(если требуется), потом bootable security key и дополнительные хранилища.
   - Сохранить настройки BIOS и продолжить загрузку с использованием bootble CD или bootable security key. Потом произойдет загрузка операционной системы WinPE и откроется стандартное диалоговое окно EnCase Portable.

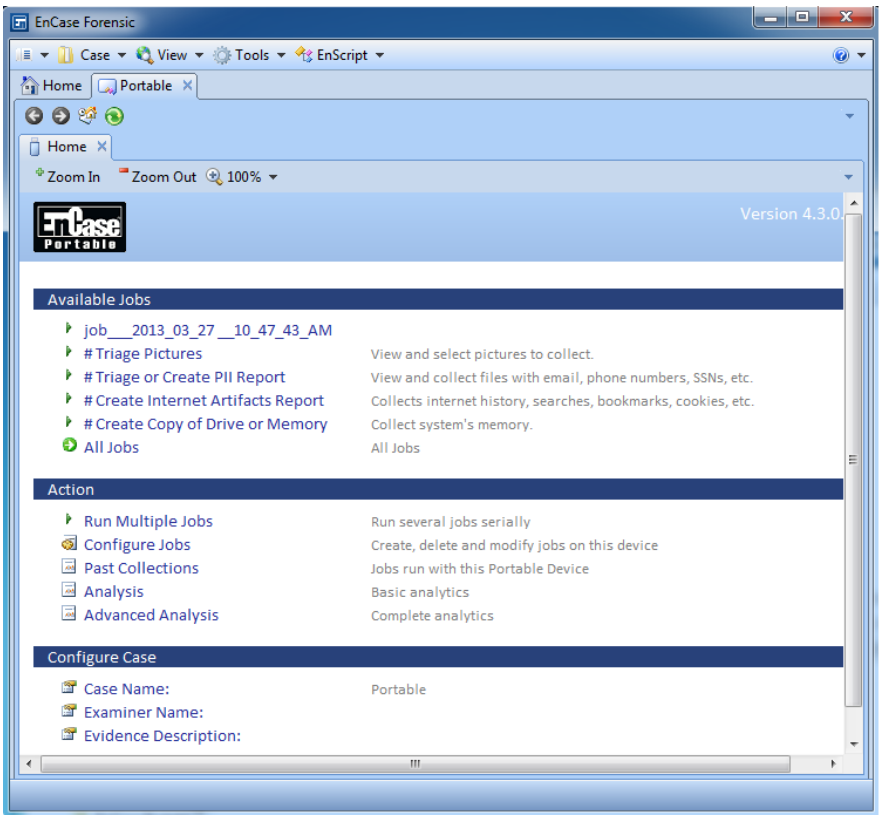

Рис. 3. Окно EnCase Portable при запуске на целевой машине.

2. Надо выбрать нужные Jobs и запустить их в Action.

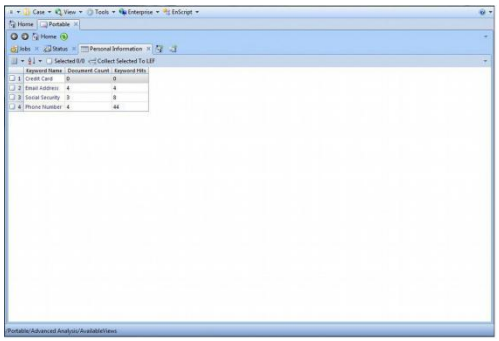

Рис. 4. Окно при завершении job или остановке процесса с результатами

3. После завершения или остановки всех Jobs можно импортировать данные или сгенерировать отчет или посмотреть фактически отобранные данные и убрать все лишнее, просматривая каждый файл отдельно или отсевая с определенным фильтром. Собранные доказательства будут храниться в хранилищах типа .E01 или .L01.
4. Извлечь bootable Security Key или separate Security Key и все дополнительные хранилища.

Internet Evidence Finder Frontline

IEF Frontline[2] - простой инструмент предварительного просмотра для нетехнического персонала, желающего провести первоначальный осмотр на компьютере подозреваемого. IEF Frontline запускается с USB-носителя и быстро просматривает потенциальные доказательства, чтобы помочь определить, нужно ли изымать устройство для полной судебно-медицинской экспертизы.

Пользователю предоставляется USB-накопитель, на котором находится IEF Frontline.

Для запуска надо вставить USB-накопитель в интересующий компьютер и запустить с него “Run IEF Frontline.cmd”.

Далее надо выбрать интересующие данные(Internet, Photo&Video, Chat или All) и ждать результаты поиска.

Рис. 5. Окно выбора интересующих категорий информации.

По завершению поиска можно посмотреть найденные файлы по категориям и отфильтровать фотографии на предмет порнографии.

Можете отметить интересующие файлы и создавать HTML отчет. Также есть возможность сохранения результатов в PDF, Excel или HTML формате непосредственно на IEF Frontline USB-ключ.

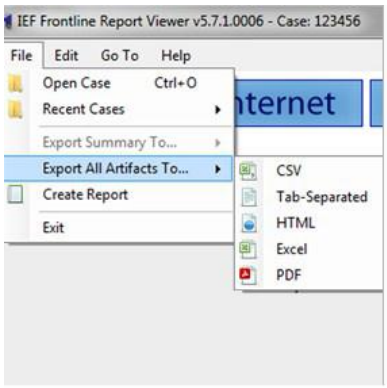

Рис. 6. Окно генерации отчета

Internet Evidence Finder Triage

IEF Triage[2] предлагает ту же функциональность, что и IEF Standard, а также обеспечивает возможность запуска непосредственно с USB флэш-накопителя в режиме "Стелс", не оставляя цифровых треков на компьютере. IEF Triage имеет возможности захвата RAM и проверки шифрования диска.

AccessData Triage

AD Triage[4] является инструментом для просмотра и извлечения данных с компьютера без установки на него специальных программ или изъятия в лабораторию. Возможно считывание сетевых, системных и данных из оперативной памяти(последнее только при включенном компьютере).

На рабочем компьютере должна быть установлена программа AD Triage Admin, в которой можно создавать Custom Triage Device(это может быть USB флэш-накопитель, CD/DVD диск или съемный жесткий диск), который и будет осуществлять сбор и сохранение данных на целевом компьютере. Для одного устройства дается одна лицензия и один профиль сбора данных, который нужно создать и добавить в устройство с лицензией.

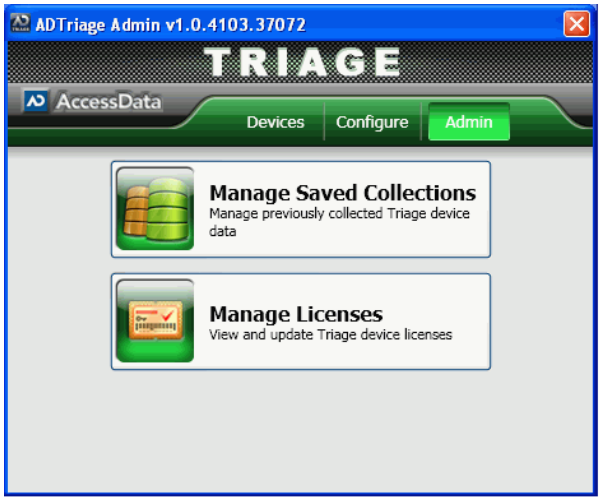

Рис. 7. Стартовое окно AD Triage Admin.

Создание профиля:

1. Во вкладке «Configure» создать новый профиль.
2. В открывшемся окне выбрать типы данных, который будет собирать профиль.

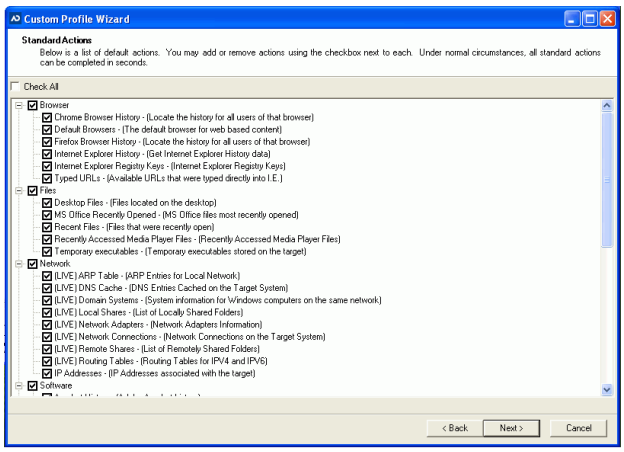

Рис. 8. Окно выбора типа данных.

3. Далее можно создать фильтры для данных по дате и времени, размеру, ключевым словам, MD5 хэш-функции, незаконным фото, регулярным выражениям, расположению и расширению. Относительно друг друга фильтры можно объединять в группы по пересечению и объединению результатов.
4. В финальном окне можно посмотреть все действия, назначенные для текущего профиля и удалить лишнее, если понадобится.

В конце создания Custom Triage Device можно установить такие параметры как:

- Автоматический запуск поиска файлов
- Автоматический экспорт файлов
- Включение удаленных файлов
- Включение slack-space файлов

Запуск Custom Triage Device на целевом компьютере:

1. Запустить AD Triage:

- Для включенного компьютера просто вставить устройство и запустить AD Triage
- Для выключенного компьютера запустить его, зайти в BIOS, изменить тип запускаемого устройства на тот, который совпадает с Custom Triage Device. После перезапуска автоматически откроется AD Triage Agent.

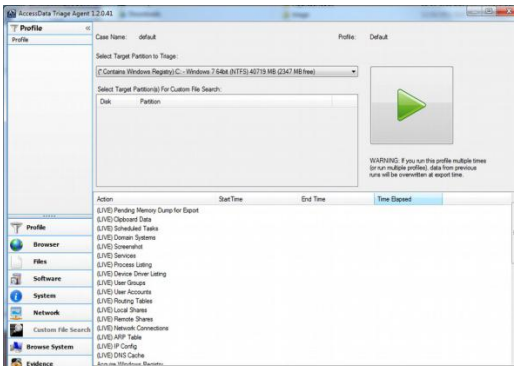

Рис. 9. Окно AD Triage Agent при запуске на целевой машине.

2. Если при создании не был выбран пункт «Автоматический запуск поиска файлов», то запустить его вручную нажатием на кнопку.Если при создании не был выбран пункт «Автоматический экпорт файлов», то после завершения поиска файлов запустить его вручную нажатием на кнопку «Export now» во вкладке «Evidence».
3. Далее на рабочем компьютере можно посмотреть и изменить собранные файлы, сделать отчет, извлечь файлы на рабочий компьютер или экспортировать собранные данные в AD1, E01, RAW или SMART образ.

Реализация

Общая структура

Работа состоит из двух этапов – разработка алгоритма создания конфигурации для поиска с последующей записью на USB-носитель вместе с требуемым программным обеспечением и создание triage режима для BelkaSoft Evidence Center[1](далее BEC).

BEC – это продукт цифровой криминалистики, чьи алгоритмы поиска данных будут использованы в triage-программе.

На первом этапе нужно определить, как будет храниться triage-программа и запускаться на USB носителе, создать визард, который будет форматировать и записывать все нужные файлы.

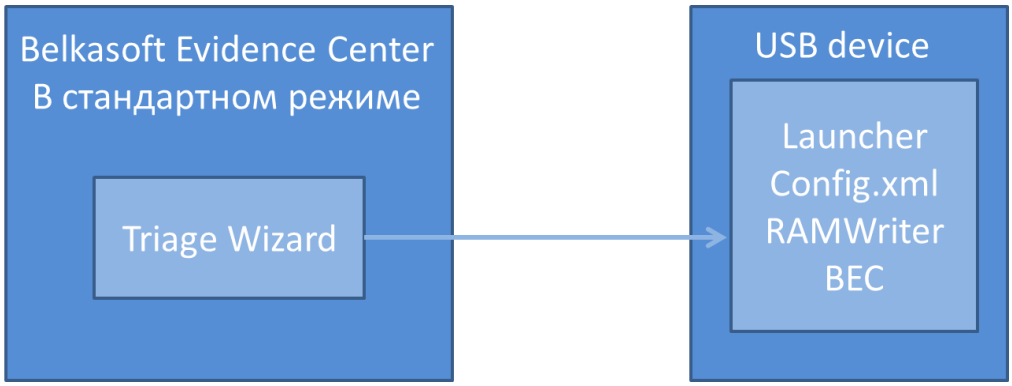

Рис. 10. Схема работы мастера создания triag конфигурации

Второй этап предполагает создание специального режима BEC, который будет запускаться на целевой машине.

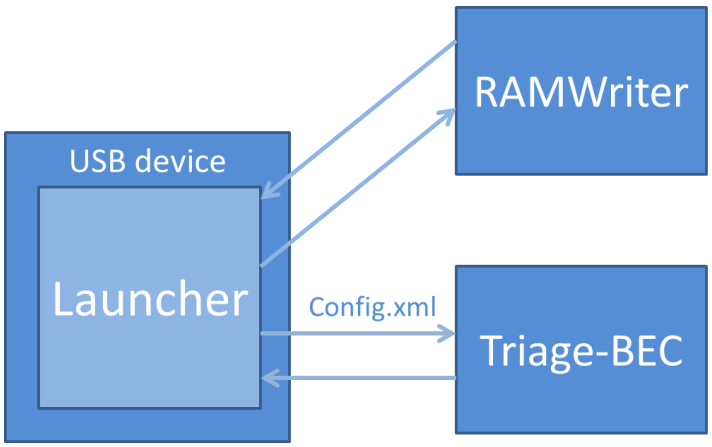

Рис. 11. Схема работы продукта на целевом компьютере

Создание конфигуратора BelkaSoft Evidence Center

Launcher – небольшой exe-файл для запуска BEC в triage режиме с нужной конфигурацией.

Он должен быть как можно проще, чтобы не занимать много оперативной памяти, так как мы может делать ее захват.

Алгоритм его работы:

- Определить, надо ли делать дамп оперативной памяти. Если надо, то запускает RAMReader, ждет завершения, сохраняет результат в папку экспорта.
- Запустить BEC через командную строку с нужным ключом, который и регулирует работу BEC в triage режиме.

Создание мастера настроек для BEC-triage

Для создания визарда в BEC были реализованы:

- Форма Windows самого визарда. Она включала в себя панель для вывода пользовательского элемента страницы, кнопки Next, Back, Finish, текстовое поле с названием, а также опцию текущих настроек визарда.
- Пользовательский элемент управления Страница, который может размещать на себе визард и менять содержимое в зависимости от нажатий на элементы управления, а также генерировать опции специального вида, хранящие в себе настройки текущей страницы, для последующего их использования.

Для визарда создания конфигурации BEC-triage потребовалось создать 2 типа страниц, из которых он и состоит.

Первый тип - это страница настроек, включающая в себя возможность выбора:

- USB носителя из активных на данный момент для записи на него triage-программы
- Тип поиска
- Возможность сделать захват оперативной памяти

Для каждой из этих настроек в соответствующей опции для данной страницы есть специальное поле(для первой настройки – строка с адресом, для 2 и 3 свои перечисляемые типы).

Второй тип – страница выбора нужных типов данных, которая содержит лист выбора анализаторов, представленных в виде дерева, существующих в BEC. В ее опции

есть 2 перечисляемые структуры – список анализаторов и список структур, в которых хранятся простые данные, позволяющие по ним однозначно получать анализатор.

Списки между собой синхронизированы, второй нужен для создания несложного xml-документа, опираясь на который, BEC-triage сможет получить список анализаторов, которые были выбраны для поиска.

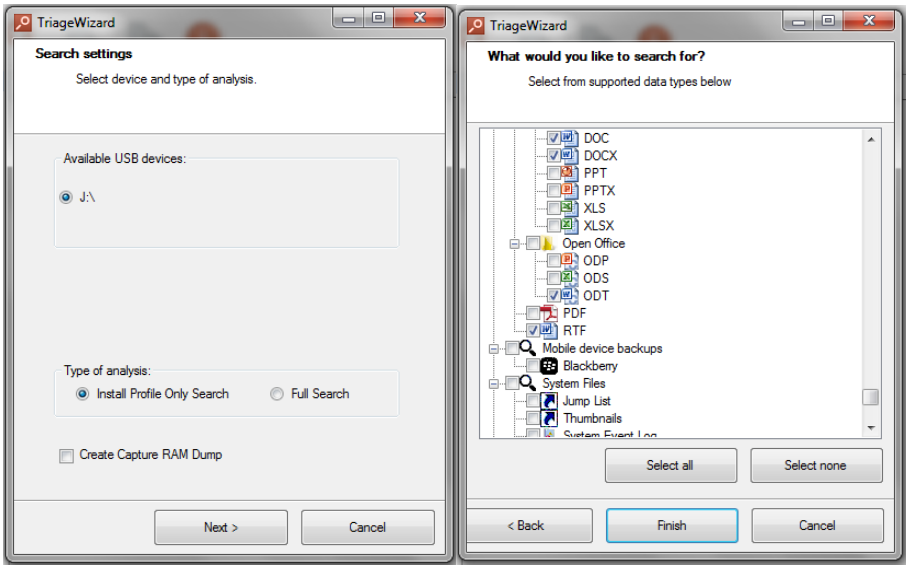

Рис. 12. Страницы мастера настроек для BEC-triage

При нажатии кнопки «Finish» Triag-визард производит следующие действия:

- форматирует выбранный USB носитель
- создает файл конфигурации, в котором содержится сериализованный объект опции текущего визарда
- Записывает на отформатированное USB-устройство BEC, RAMReader(если есть соответствующая настройка), файл конфигурации, Launcher для запуска.

Создание triage-режима для BelkaSoft Evidence Center

В BEC есть 3 возможных режима работы:

- Default – стандартный режим со всеми возможностями.
- Embedded – режим автоматического сканирования в заданной директории
- Triage – режим автоматического сканирования анализаторами, восстановленными из конфигурационного файла, по всем найденным локальным дискам.

В каком именно режиме будет работать BEC определяет(а также поддерживает этот его) статический класс EmbeddedHelper. Он умеет определять режим по аргументам командой строки при запуске BEC.

При запуске triage режима надо убрать все лишние возможности BEC, такие как работа с делами(для поиска будет использоваться дело по умолчанию(Default Case)), вкладки для работы при анализе файлов, экспорт результата, вызов визарда выбора данных для анализа и анализаторов(в triage режиме сканировать надо все локальные диски, а анализаторы будут восстановлены из конфигурационного файлов) и пр.

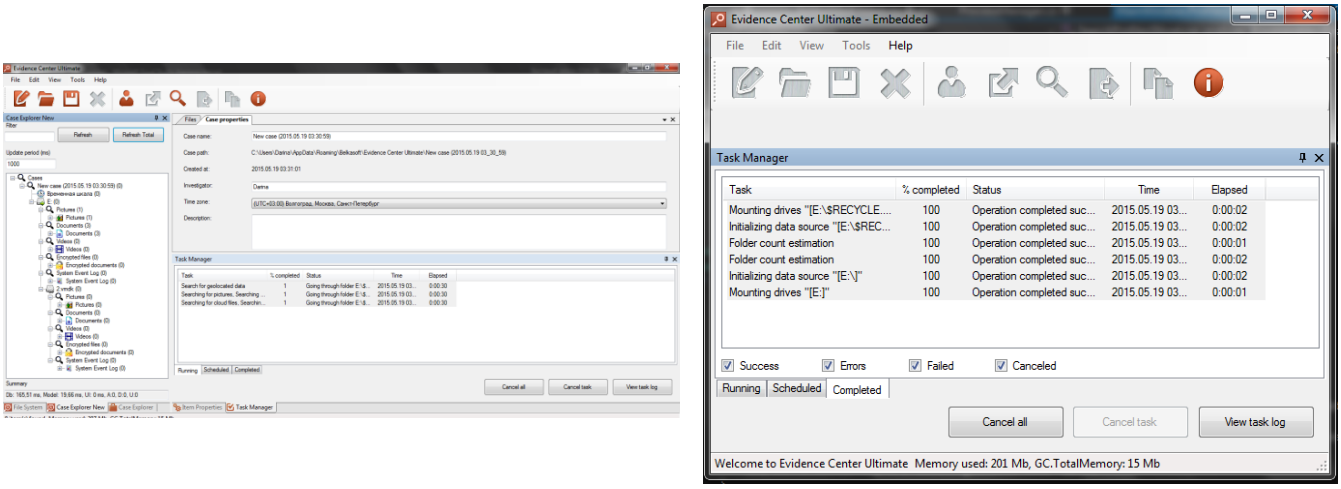

Рис. 13. Внешняя разница между стандартным и triage режимами

Поиск в BEC происходит по профайлам(это класс, хранящий и предоставляющий инструменты для работы с файлами, найденными определенным анализатором).

Профайлом может оказаться единственный файл, папка или массив файлов. В одном поиске должно быть не больше одного профайла каждого типа данных.

После загрузки основной формы в нужном режиме, надо запускать поиск профайлов, для которого EmbeddedHelper сначала осуществляет:

- поиск всех локальных дисков
- извлечение и десериализацию опции triage-визарда из конфигурационного файла, где содержится опция страницы выборов нужных типов данных. Потом из последней указанной опции по списку структур восстанавливается список анализаторов.

Эти данные передаются в менеджер процессов, а оттуда в контроллер поиска профайлов. Далее для каждого из дисков происходит следующая последовательность действий.

Сначала из оригинальной опции для поиска с нужным списком анализаторов создается новая с указанием, какой именно диск нужно сканировать. Потом последовательно создаются, помещаются в TaskManager и запускаются следующие процессы – инициализация диска, оценка его файловой структуры и запуск нужных

анализаторов. По завершению поиска каждого профайла все найденные файлы сохраняются на USB носитель, предварительно добавляя хеш-функцию, а также время создания, изменения и открытия(при копировании файлов эти времена изменяются, а следователю важны изначальные данные. Хеш-функция же является гарантией, что файл не был изменен и его можно использовать как улику). Все эти процессы пользовать может отслеживать в менеджере задач, а так же смотреть отчет по каждому из них.

Заключение

Было проведено исследование существующих средств.

Реализован инструмент, обладающий возможностью эффективного захвата данных определенного пользователем типа с возможностью их использования для компьютерной криминалистики.

Работа над данной задачей может быть продолжена. Так, может быть интересной возможность сохранения данных в стандартизированное хранилище (например L01) для возможности их анализа в любом продукте для криминалистического анализа или создание загружаемого решения для возможности анализа выключенной или заблокированной машины. Помимо того планируется сделать быстрый сигнатурный поиск с сохранением некоторой окрестности блока для возможности разбора на машине эксперта.

Список литературы

[1] Belkasoft. Ресурс сайта производителя // http://ru.belkasoft.com/.

[2] Internet Evidence Finder Frontline. Ресурс сайта производителя // http://www.magnetforensics.com/

[3] EnCase Portable v4.pdf //https://www.guidancesoftware.com/resources/Pages/doclib/Document-Library/EnCase-Portable-v4.aspx - 2009.

[4] AccessData Triage User Guide // https://ad-pdf.s3.amazonaws.com/Triage%202.4.0%20User%20Guide.pdf – 2013.

.