САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Математико-механический факультет

Кафедра системного программирования

ВИЗУАЛИЗАЦИЯ ДАННЫХ ЦИФРОВОГО КРИМИНАЛИСТИЧЕСКОГО АНАЛИЗА

Дипломная работа студентки 545 группы

Золотухиной Алины Игоревны

Научный руководитель	…… / подпись /	ст. преп. Губанов Ю.А.
Рецензент	…… / подпись /	ст. преп. Луцив Д.В.
“Допустить к защите” заведующий кафедрой,	…… / подпись /	д.ф.-м.н., проф. Терехов А.Н.

Санкт-Петербург

2012

SAINT-PETERSBURG STATE UNIVERSITY

Mathematics and Mechanics Faculty

Software Engineering Department

DIGITAL FORENSIC ANALYSIS DATA VISUALIZATION

Graduate paper by

Alina Zolotukhina

545 group

Supervisor	……	Senior Lect. Yu.A. Gubanov
Reviewer	……	Senior Lect. D.V. Luciv
"Approved by" Head of Department	……	Dr. Sci., Prof. A.N. Terekhov

Saint-Petersburg

2012

Оглавление

1. Введение

С развитием компьютерных технологий многие сферы человеческой деятельности переносятся в виртуальные пространства, в интернет. Разговоры в многочисленных интернет-пейджерах, общение в социальных сетях, переписка по электронной почте, обмен файлами заменяют телефонное и личное общение. Эта тенденция затрагивает разнообразные слои населения — интернетом пользуются все, начиная с детей и домохозяек и заканчивая наркодилерами, распространителями детской порнографии и другими преступниками. Для предотвращения и раскрытия преступлений органы охраны правопорядка заинтересованы в получении информации, передаваемой и получаемой незаконопослушными гражданами. Поскольку практически от любой деятельности на компьютере остаются какие-либо следы, существует возможность обнаружить их и далее на их основе предпринимать действия по доказательству виновности или невиновности подозреваемого [14].

Компьютерная криминалистика (computer forensics) занимается нахождением и анализом "цифровых" улик — файлов и файловых систем, данных реестра, сетевых соединений, вирусов и вредоносных программ вообще, исследованием баз данных и мобильных устройств [3]. Заниматься такого рода исследованиями вручную представляется довольно сложным. Прежде всего, весьма затруднительно знать все необходимые для исследования особенности структуры памяти и другие тонкости исследуемого устройства вследствие разнообразия таких устройств. Ручной поиск отнимает много времени. Использование специальных приложений, извлекающих необходимую информацию быстро и без изменения исследуемых данных, позволяет смягчить все эти трудности. Кроме того, при предоставлении найденных доказательств в суде факт использования таких приложений автоматически гарантирует то, что ни один бит информации не

был изменён.

Приложения, предназначенные для проведения цифровой компьютерной экспертизы, облегчают задачи нахождения и анализа артефактов, оставшихся от работы пользователя на компьютере и прочих цифровых устройствах, таких как мобильные телефоны, смартфоны, игровые консоли и т.п. Артефакты могут представлять собой как файлы (например, файлы истории интернет-пейджеров или файлы, содержащие базы данных браузера со списком посещённых в интернете страниц), так и данные оперативной памяти компьютера (например, данные, оставшиеся после посещения сайтов — личные сообщения и сообщения ленты новостей социальных сетей, письма почтовых сервисов и т.п.). Данные могут быть найдены в нераспределённых областях жёсткого диска, где могли сохраниться удалённые файлы или куда специально могли быть спрятаны временные данные программ, представляющие интерес для экспертов. Можно исследовать как внутренние жёсткие диски или внешние носители, так и отдельные файлы, содержащие образ памяти или файловой системы.

В некоторых случаях время на поиск улик или доказательств очень ограничено, поскольку необходимо предоставить информацию в предельно сжатые сроки. Таким образом, учитывая, что в наши времена объём используемой дисковой памяти может достигать нескольких терабайт даже у простого пользователя на домашнем компьютере, программы цифровой криминалистики должны предоставлять возможность сравнительно быстро работать с больши́ми объёмами данных.

Ещё одной проблемой является сложность работы с данными, полученными в результате анализа. В некоторых случаях недостаточно только найти данные. На диске может храниться множество писем, сообщений и файлов, среди которых необходимо выделить те, которые помогут в расследовании. Самостоятельный анализ такого количества информации будет долгим, неудобным и подчас даже невозможным в условиях ограниченности времени. Необходим способ автоматизации,

позволяющий структурировать найденные данные и предоставлять их в понятном для пользователя виде.

Эксперту-криминалисту зачастую необходим лишь некоторый срез данных, содержащий важные улики или свидетельства. Его могут интересовать какие-то конкретные типы данных или данные за определённый промежуток времени. Возникает необходимость в определённых фильтрах (по времени, по имени, по встречающимся словам и т.п.). В некоторых случаях криминалист обладает информацией о конкретном пользователе и хочет изучить взаимодействие этого пользователя с другими. Также ввиду ограниченности времени исследования необходимо уметь быстро анализировать найденную информацию.

Для решения этой задачи в некоторых продуктах используется визуализация данных. Визуализация данных в криминалистических продуктах является новой тенденцией, и в данный момент во многих продуктах цифровой криминалистики происходит переход от обычных плоских списков к графическому представлению данных. В качестве объектов визуализации могут быть выбраны разные типы связей — к примеру, можно визуализировать связи между пользователями или изменения во времени и т.п.

Задача данной дипломной работы заключается в разработке модуля визуализации для программного продукта цифрового криминалистического анализа, описываемого в следующей главе.

2. Обзор

Несмотря на быстрое развитие технологий и инструментов в области цифрового криминалистического анализа, лишь некоторые из них позволяют наглядно изобразить связи между извлеченными данными. В данной работе проведён обзор наиболее известных способов визуализации данных и приложений, предоставляющих соответствующие средства визуализации. Отдельное внимание уделяется визуализации временной шкалы. Также рассматриваются основные характеристики продукта Belkasoft Evidence Center [15], визуализация данных в котором и является задачей, поставленной перед автором данного диплома.

2.1. Обзор типов визуализации криминалистических данных

Рассмотрим основные типы визуализации криминалистических данных.

1. Визуализация связей между людьми.

   Существует большое количество инструментов, предоставляющих визуализацию связей между людьми, к примеру, в социальных сетях. Такой способ визуализации помогает выявить, насколько тесно люди связаны друг с другом, кто является ключевыми фигурами, как по сети распространяется информация. Одним из инструментов, предоставляющих такой тип визуализации, является Sentinel Visualizer [10]. Помимо предоставления общей картины связей в сети, данный инструмент также помогает вычислить людей, имеющих наибольшее количество связей с другими людьми или могущих связаться с наибольшим количеством пар и групп людей и т.п.

2. Визуализация связей между людьми и объектами.

   Данный способ визуализации очень похож на предыдущий и отличается от него только тем, что помимо людей в рассматриваемой сети также могут присутствовать местоположения, объекты (например, телефоны) или метаданные — любые данные, которые могут состоять в

каком-либо отношении с другими данными. Такой способ визуализации позволяет выявить неочевидные соотношения между связанными элементами. Примером инструмента, предоставляющего такой способ визуализации данных, является Analyst's Notebook [6]. Помимо представления связей в виде графа, данный инструмент также позволяет отследить движение данных: существует возможность посмотреть, в какой последовательности и когда те или иные связи были активны.

3. Визуализация передаваемых данных сети.

   Такой способ визуализации предоставляет, к примеру, The Network Visualizer [11]. Данный инструмент на основе заранее записанных данных показывает связи между удалёнными и локальными машинами. При выборе определённой машины предоставляется информация о данных передаваемых пакетов или деятельности портов.

4. Визуализация временной шкалы.

   Некоторые инструменты в качестве визуализации данных предоставляют так называемую временную шкалу данных — события, расположенные определённым образом согласно времени, в которое они произошли. Подробнее такие инструменты рассмотрены в следующем параграфе.

2.2 Обзор способов визуализации временной шкалы

Рассмотрим существующие способы визуализации временной шкалы.

1. Analyst’s Notebook [6] предоставляет данные в виде графика, в котором по горизонтали указано время, с шагом в неделю или день, по вертикали — активность (количество сообщений, писем, звонков, передаваемых в данный промежуток времени). Помимо такого графика инструмент предоставляет таблицу, с помощью которой наглядно показываются наиболее интенсивные точки общения, т.е. моменты, в которые было активно наибольшее количество связей или произведено

наибольшее количество обменов данными. Ячейки этой таблицы представляют собой промежутки времени, каждый из которых выделен цветом в зависимости от активности. Пример такой таблицы представлен на рисунке 1.

Рисунок 1. Временная шкала в программе Analyst's Notebook.

2. Adroit Photo Forensics [4] используется для обнаружения и восстановления фотографий. Продукт строит графическое представление фотографий на временной шкале, группируя фотографии по некоторым критериям и располагая их в виде окружностей разных диаметров на отрезке с начальной меткой времени самой ранней фотографии и конечной меткой самой поздней фотографии. Чем больше диаметр окружности, тем больше фотографий найдено в данный период времени. На рисунке 2 показано, как выглядит временная шкала в Adroit Photo Forensics.
3. Ещё один графический редактор временной шкалы — Zeitline [1] — позволяет группировать события в суперсобытия. Основной структурой данных является событие. Любое событие состоит из промежутка времени, в течение которого оно происходило, источника для определения происхождения события и описания события. Каждое событие может содержать список подсобытий или являться элементом списка подсобытий у суперсобытия. События могут группироваться в иерархию событий. Недостатком Zeitline с точки зрения цифровой

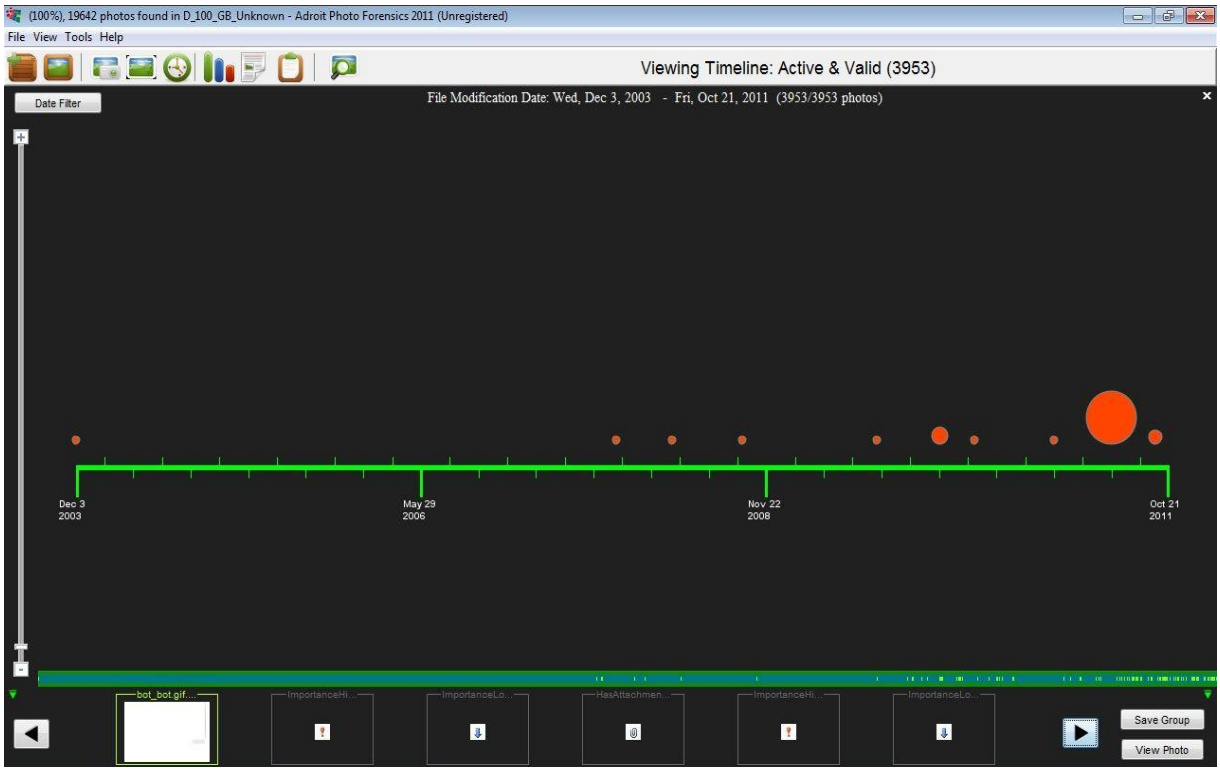

Рисунок 2. Временная шкала в программе Adroit Photo Forensics.

криминалистики является то, что он не обрабатывает истории разговоров и другую интернет-активность.

4. log2timeline [8] — инструмент для автоматического создания временной шкалы на основе данных из файлов журналов и найденных артефактов. Наглядной визуализации этот инструмент не предоставляет, но в нём реализована возможность экспорта данных в разные форматы, такие как XML, TLN, SQLite и др., для последующего использования в инструментах визуализации данных, например, в SIMILE [7] или CFTL [2].
5. EnCase [5] предлагает временную шкалу в виде календарной таблицы. К примеру, по горизонтали в ней расположены дни месяца, по вертикали — часы. В ячейках таблицы либо отмечено цифрой количество артефактов, относящихся к данному периоду времени, либо изображены прямоугольники, относящиеся непосредственно к определённому артефакту. Снимок экрана с примером работы EnCase представлен на рисунке 3.

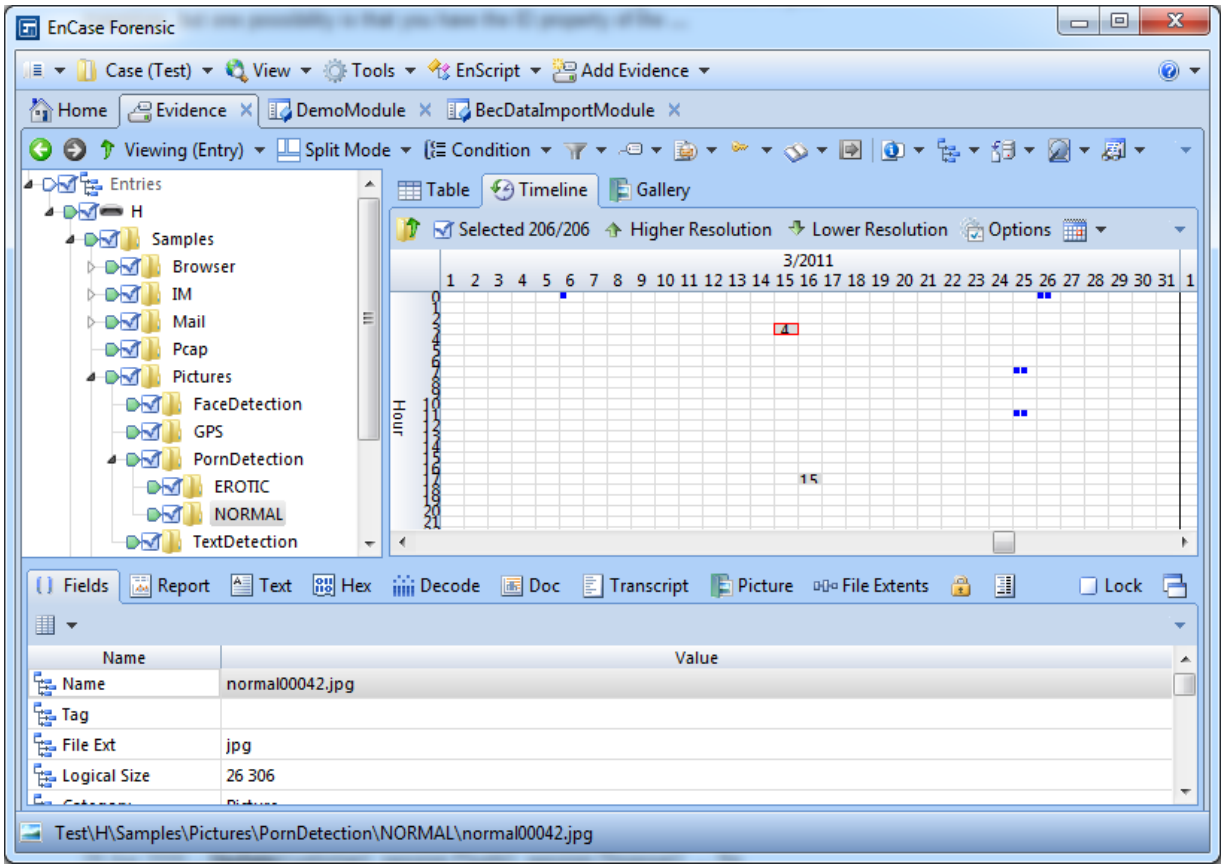

Рисунок 3. Временная шкала в программе EnCase.

2.3. Belkasoft Evidence Center

Belkasoft Evidence Center [15] — продукт отечественной компании, появившийся на рынке в 2010 году. Belkasoft Evidence Center предоставляет возможность поиска сообщений, писем, активности в социальных сетях, P2P-программах, разговоров в онлайн-играх и т.п. в целях проведения цифровой криминалистической экспертизы и с учётом её специфики, обсуждавшейся выше. Поиск может осуществляться на разных источниках — на жёстком диске или на других носителях (компакт-диски, USB-флеш-накопители и т.п.), на образах оперативной памяти, файлах подкачки и гибернации и т.д.

Помимо всего прочего, в продукте существует возможность добавлять закладки на найденные артефакты, осуществлять по ним поиск и строить отчёты.

В Belkasoft Evidence Center существует два типа поиска: поиск по файловой системе и поиск по всему диску либо на образе памяти. Найденные

данные отображаются списком, при этом навигация осуществляется с помощью дерева, отображающего типы искомых данных (например, историю Skype, ICQ, письма Gmail, Outlook, сообщения Facebook и т.п.).

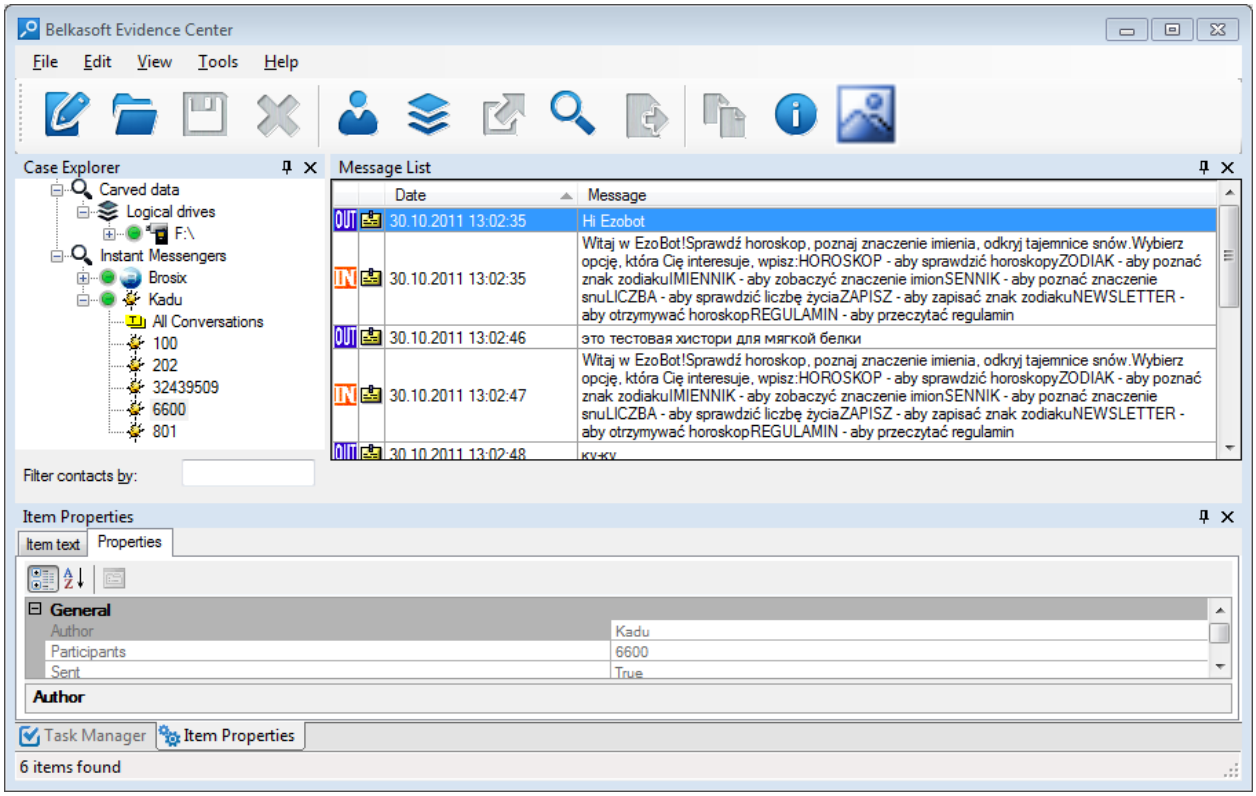

Рисунок 4. Представление данных в Belkasoft Evidence Center.

На рисунке 4 представлен пример работы Belkasoft Evidence Center. Здесь можно видеть как данные, найденные в результате поиска по файловой системе (это профили Brosix и Kadu в разделе Instant Messengers), так и данные, найденные в результате карвинга — побайтового анализа носителя информации (профиль диска F с найденными данными типа Torrent File в разделе Carved Data). Как видно на снимке экрана, Belkasoft Evidence Center предоставляет возможность просмотра данных только в табличном виде и только отдельно по профилям и не предоставляет возможность просмотреть все данные вместе взятые, что является его недостатком.

3. Постановка задачи

Перед автором дипломной работы была поставлена задача улучшить визуализацию данных в продукте Belkasoft Evidence Center:

1. Разработать подход к визуализации данных цифрового криминалистического анализа и реализовать разработанную концепцию.
2. Реализовать возможность визуализации на разных уровнях — как на уровне данных одного типа, так и на уровне всех исследуемых артефактов.
3. Реализовать визуализацию найденных артефактов на временной шкале с возможностью изменения масштаба рассматриваемого промежутка.

4. Предлагаемое решение

Существуют разные типы визуализации данных криминалистического анализа: временная шкала, граф общения, показывающий связи между участниками коммуникаций, всевозможные сводные таблицы и т.п. Для улучшения визуализации данных в Belkasoft Evidence Center была выбрана временная шкала. Этот способ визуализации является одним из наиболее наглядных, поскольку предоставляет информацию в виде, наиболее удобным для анализа. Согласно исследованиям, проведённым в [2], эксперты-криминалисты, работающие с инструментом, предоставляющим визуализацию временной шкалы, быстрее и с меньшим количеством ошибок справляются с задачей, нежели эксперты-криминалисты, работающие с обычным инструментом.

Предлагаемое решение заключается в построении временной шкалы по запрошенной выборке данных:

- эксперт-криминалист выделяет интересующий его блок данных анализа;
- по выделенным данным строится список событий, при этом событием является любой артефакт, имеющий одну или несколько временных меток;
- по списку событий строится временная шкала в виде оси с метками, относящимися к событиям.

Для удобства визуализации большого количества данных предлагается возможность задавать различный масштаб просмотра временной шкалы:

- просмотр данных о конкретных артефактах при увеличенном масштабе
- просмотр данных о количестве артефактов разных типов при уменьшенном масштабе

Помимо удобства восприятия данных с экрана, такой подход позволяет наглядно продемонстрировать развитие событий преступления в суде.

Поскольку задача дипломной работы состояла в разработке подхода и

реализации визуализации в конкретном продукте, отдельную сложность представляла интеграция спроектированного модуля в существующее окружение.

Разработка велась на языке C# в среде Microsoft Visual Studio 2008.

5. Архитектура

5.1. Существующая архитектура Belkasoft Evidence Center

Рассмотрим основные элементы архитектуры Belkasoft Evidence Center. Основным объектом при взаимодействии с пользователями является «дело» (case), в котором пользователь, задавая необходимые параметры, объединяет диски, папки и файлы для последующего поиска артефактов.

В каждом деле имеется список профилей (profile), относящихся к найденным данным разных типов. Каждый профиль отвечает отдельному типу данных — например, профиль программы обмена мгновенными сообщениями, профиль изображений, видео, данных карвинга, почты и т.п. Такое разделение профилей на типы необходимо из-за того, что данные являются разнородными. Схема профилей представлена на рисунке 5.

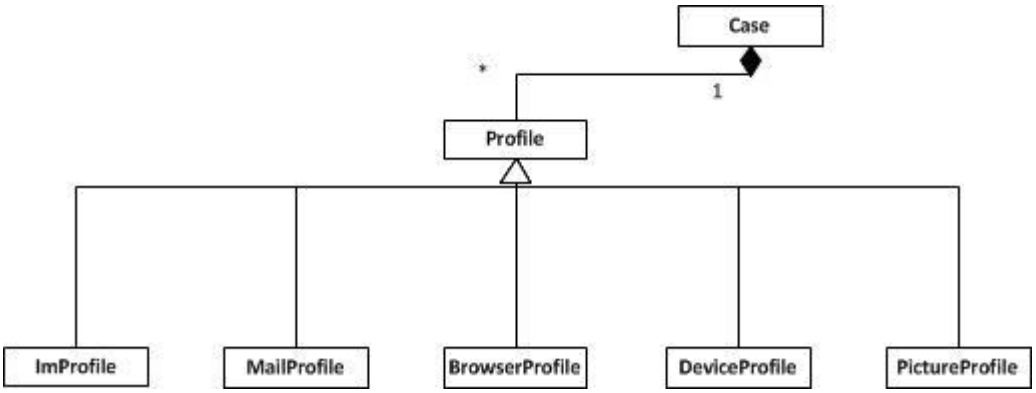

Рисунок 5. Схема профилей.

5.2. Интерфейс временной шкалы

Опишем основные элементы, используемые для построения временной шкалы.

Для реализации возможности просмотра временной шкалы были добавлены интерфейсы для элементов временной шкалы и для создания списка этих элементов: ITimelineable и ITimelineProvider соответственно.

Интерфейс ITimelineProvider реализуют все классы, являющиеся

наследниками класса Profile. Необходимо уметь визуализировать данные любого профиля, а эти данные предоставляют как раз классы, имеющие предком Profile. Кроме того, этот интерфейс реализует класс Case — это необходимо для возможности построения временной шкалы по всем найденным артефактам.

Интерфейс ITimelineProvider представлен на рисунке 6.

```
interface ITimelineProvider : IKeyAbstraction
{
   void ConstructTimeline();
   IList<ITimelineable> TimelineableItems { get; }
   bool HasTimeline { get; }
}
```

Рисунок 6. Интерфейс ITimelineProvider

- Метод ConstructTimeline строит временную шкалу по имеющимся объектам профиля, помещая при этом создаваемые объекты временной шкалы в коллекцию.
- Доступ к этой коллекции осуществляется с помощью свойства TimelineableItems.
- Свойство HasTimeline указывает, построена ли временная шкала для данного профиля.

Интерфейс ITimelineable реализуют классы меток временной шкалы. Каждый такой класс соответствует определённому типу профиля. Схема интерфейса и реализующих его классов представлена на рисунке 7.

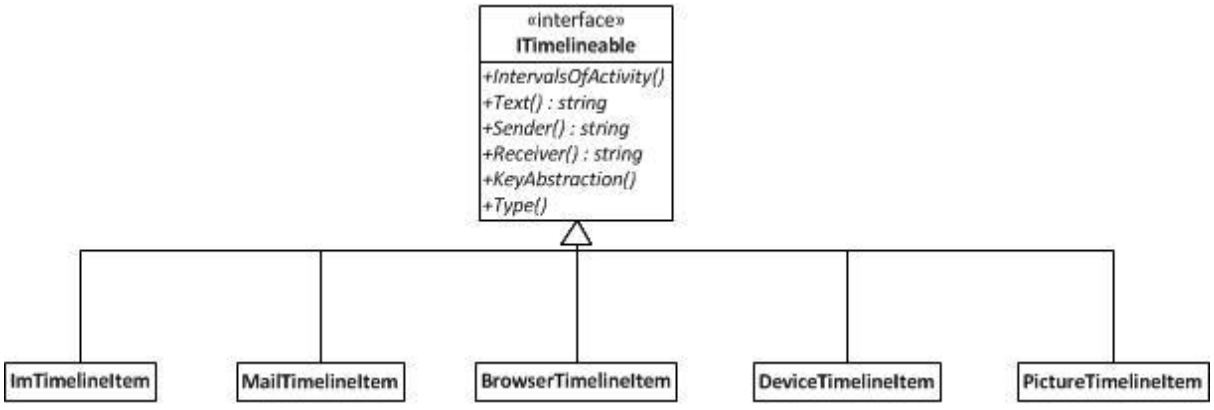

Рисунок 7. Схема ITimelineable и реализующих его классов

Интерфейс ITimelineable представлен на рисунке 8.

```
interface ITimelineable : IKeyAbstraction
{
   IEnumerable <Pair<DateTime, DateTime>>
IntervalsOfActivity { get; }
   string Text;
   string Sender;
   string Receiver;
   IKeyAbstraction KeyAbstraction { get; }
   TimelineType Type { get; }
}
```

Рисунок 8. Интерфейс ITimelineable

У каждой метки временной шкалы есть текст, отправитель и получатель. В связи с разнообразием типов данных эти поля будут иметь смысл не для всех меток (например, у ссылки нет получателя и отправителя), однако в большинстве случаев они будут нести смысловую информацию.

- IntervalsOfActivity — это интервалы времени, относящиеся к метке (он может обозначать, например, дату создания какого-либо файла или дату получения какого-либо сообщения). В основном, началом и концом интервала будет являться одна и та же дата (сообщение не имеет продолжительности, у него есть только одна дата — дата отправки), но, например, для звонка даты начала и конца будут разные. К одной метке может относиться несколько интервалов времени. Например, для изображения там будет содержаться дата создания и дата изменения изображения.
- KeyAbstraction — это ссылка на профиль или дело, по которому строилась временная шкала. При этом IKeyAbstraction — это интерфейс, отвечающий любому элементу, который может быть представлен пользователю.
- Text — текст метки. Для сообщений и писем это будет текст сообщения и письма, для изображений и видео-файлов – их название.
- Sender — отправитель (указывается только для сообщений и писем)
- Receiver — получатель (указывается только для сообщений и писем)
- TimelineType — это структура, перечисляющая возможные типы

временных меток. Метки могут иметь тип сообщения, письма, артефакта карвинга, артефакта браузера, изображения или видео-файла. Структура выглядит следующим образом:

```
enum TimelineType
{
  Message,
  Mail,
  CarvedArtifact,
  Picture,
  Video,
  Browser
}
```

Рисунок 9. Структура TimelineType

Для проверки работоспособности добавленных интерфейсов и классов был реализован просмотр меток временной шкалы в табличном виде. На уровне профиля просмотр меток ничем не отличается от просмотра самих артефактов. Однако метки временной шкалы, в отличие от артефактов, можно также просмотреть на уровне всего дела. При этом помимо данных метки ещё указывается и её тип.

При запросе на построение временной шкалы соответствующие классы строят список из элементов ITimelineable, далее этот список передаётся для предоставления в виде таблицы и для визуализации. При этом в деле дерева появляется новый узел — Timeline, — либо на уровне конкретного профиля, либо на уровне всего дела. При просмотре данных этого узла показывается табличное представление меток временной шкалы.

6. Визуализация

6.1. Выбор библиотеки

Для визуализации временной шкалы по данным анализа было необходимо выбрать библиотеку, которая предоставляет возможность отрисовки временной шкалы, отрисовки и раскладки вершин-меток с информацией и возможность изменения масштаба всех отображаемых данных. Кроме того, библиотека должна предоставляться с открытыми исходными кодами для возможности её настройки под нужды конкретного проекта, связанные со спецификой отображаемых данных, и её лицензия должна давать право использовать её в коммерческих продуктах.

Библиотеки, идеально подходящей требуемым параметрам, найдено не было. Библиотека WPF Toolkit [12] обладает многими возможностями, однако она не предоставляет возможности работы с масштабированием. Более того, последнее обновление библиотеки было в начале 2010 года, что вызывает опасения по поводу поддержки библиотеки её авторами.

WPF Draw Tools [13], наоборот, предоставляет возможность работы с масштабированием, но не специализируется на работе с графами.

Наиболее подходящей библиотекой оказалась библиотека NodeXL [9]. Данная библиотека обладает больши́м количеством функций и свойств, которые могут быть полезны для визуализации графов. Она предоставляет возможность масштабирования и интерактивного взаимодействия с пользователем и имеет лицензию Microsoft Public License, которая позволяет её использование в коммерческих продуктах.

6.2. Настройка библиотеки NodeXL

Поскольку NodeXL не предоставляет возможности расположения узлов на временной шкале, эту функциональность было необходимо реализовывать самостоятельно.

NodeXL — библиотека для WPF (Windows Presentation Foundation).

Поскольку Belkasoft Evidence Center для отображения пользовательского интерфейса использует технологию Windows Forms, элемент управления NodeXL для построения временной шкалы пришлось адаптировать для возможности использования с Windows Forms.

Для непосредственной визуализации временной шкалы был добавлен класс TimelineView, который в методе PopulateAndDraw() по списку элементов временной шкалы строит списки вершин и рёбер графа, представляющего собой временную шкалу. В этом же методе указывается тип раскладки графа, определяющий, каким образом вершины будут расположены по отношению друг к другу и вызывается метод, строящий граф (временную шкалу).

Для добавления возможности раскладки вершин в виде временной шкалы был реализован класс TimelineLayout. В этом классе вычисляются непосредственные координаты каждой вершины. В данном случае необходимо было использовать два типа вершин — временны́е вершины (расположенные на линии времени) и вершины с информацией, не имеющей отношения ко времени (далее — информационные вершины). Временны́е вершины расположены в нижней части элемента управления и соединены обычной линией, каждая вершина подписана соответствующей ей датой. Информационные вершины расположены выше, и к ним идут рёбра от соответствующих временны́х вершин.

6.3. Масштабирование

Масштабирование реализовано следующим образом:

- Существует несколько планов просмотра — посекундный, поминутный, почасовой, ежедневный, ежемесячный и годовой.
- При каждом варианте просмотра перемещение по шкале времени происходит с помощью полосы прокрутки.
- Переключение между вариантами просмотра происходит с помощью колеса мыши.

Артефакты группируются в соответствии с масштабом просмотра (т.е. по минутам, по дням и т.д.). На линии времени указывается соответствующая дата, при вершине с информацией указывается, сколько артефактов относится к данному периоду времени. При наведении курсора на вершину пользователю показывается, какие артефакты были найдены (например, 20 сообщений, пять писем, три ссылки). Данную функциональность можно наблюдать на рисунке 10, где представлены данные с масштабом в год.

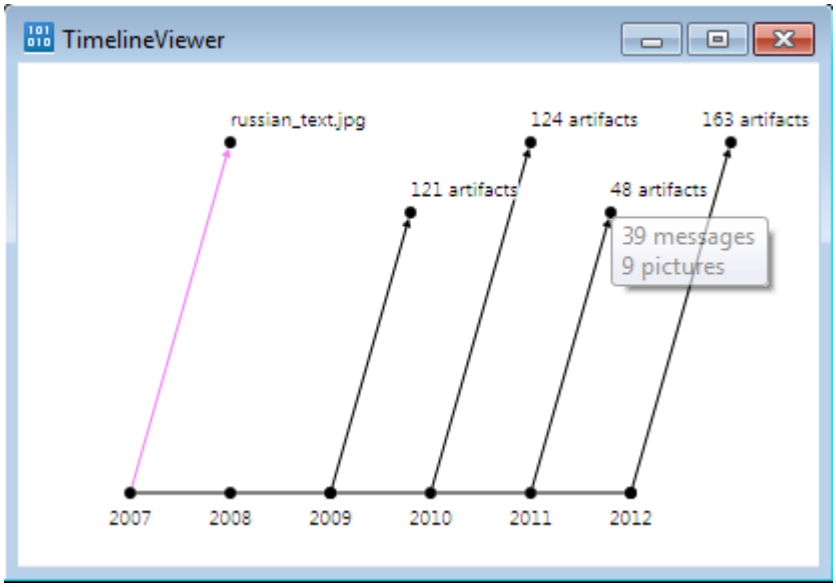

Рисунок 10. Временная шкала Belkasoft Evidence Center с масштабом в год

Если к определённому времени относится один артефакт, то у информационных вершин указывается краткая информация об артефакте (название изображения, отправитель сообщения и т.п.). При наведении курсора на вершину пользователю показывается дополнительная информация об артефакте (к примеру, для сообщения показывается от кого, кому и что было отправлено). Каждому типу артефакта соответствует ребро определённого цвета. На рисунке 11 наглядно представлено, как выглядит поминутный просмотр артефактов.

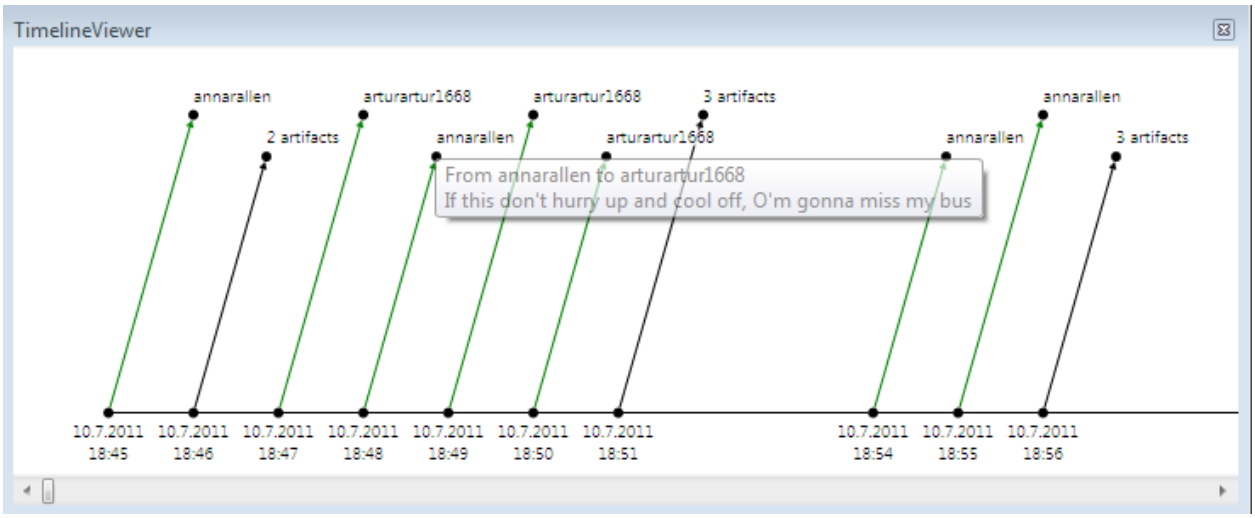

Рисунок 11. Временная шкала Belkasoft Evidence Center с масштабом в минуту

По умолчанию данные показываются с таким масштабом, что все вершины видны без использования полосы прокрутки.

Для удобства просмотра отдельных разговоров на общей линии времени была добавлена возможность выделения разговора. При нажатии на вершину с сообщением или письмом выделяются все рёбра, относящиеся к вершинам этого разговора. Снимок экрана, иллюстрирующий эту функциональность, представлен на рисунке 12. На рисунке видны три выделенные стрелки, относящиеся к разговору пользователей с номерами icq 601288382 и 644654052. При этом также видно, что сообщение, отправленное с номера 644654052 на номер 63373309 не было выделено.

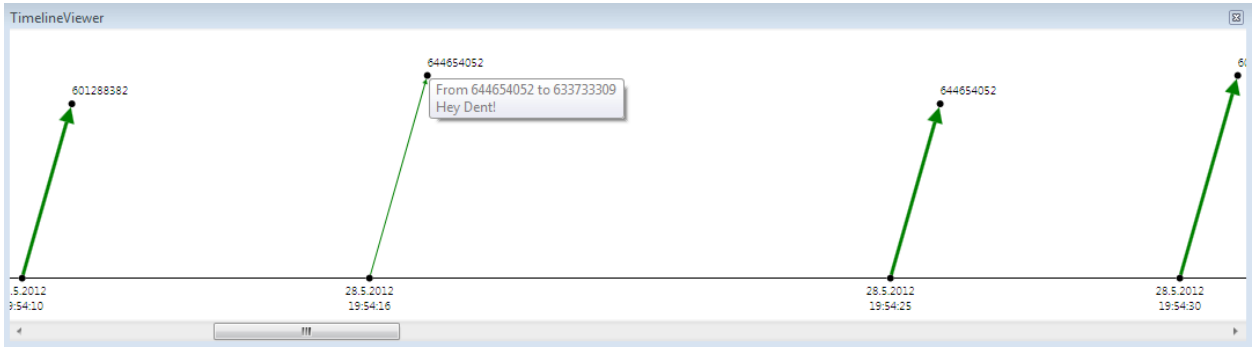

Рисунок 12. Временная шкала Belkasoft Evidence Center с выделенным разговором

7. Апробация

Разработчиками Belkasoft Evidence Center было проведено тестирование функциональности временной шкалы на разных данных. В качестве набора тестовых данных использовались как персональные данные разработчиков, так и данные, предоставляемые пользователям в качестве примера, выложенные на сайте компании. В результате тестирования было обнаружено небольшое количество незначительных ошибок, которые были исправлены автором работы. Дальнейшая апробация результатов дипломной работы планируется в Федеральной службе Российской Федерации по контролю за оборотом наркотиков.

8. Заключение

В рамках данной дипломной работы выполнены следующие задачи:

1. Разработан и реализован механизм графической визуализации данных криминалистического анализа в виде временной шкалы в продукте Belkasoft Evidence Center с использованием библиотеки NodeXL.
2. Реализована возможность визуализации на уровне данных одного типа и на уровне всех исследуемых артефактов.
3. Реализована возможность динамического масштабирования временной шкалы с изменением отображаемых на ней данных: непосредственно самих артефактов в случае наибольшего масштаба и статистических данных по количеству артефактов в остальных случаях.

В дальнейшем планируется собрать пользовательские отзывы о реализованной функциональности и на основании этих отзывов совершенствовать наглядность интерфейса и увеличивать набор предлагаемых возможностей. Также предполагается реализация других типов визуализации (например, визуализации графов общения пользователей).

9. Список литературы

1. CERIAS — Zeitline: a forensic timeline editor http://projects.cerias.purdue.edu/forensics/timeline.php [27.05.2012]
2. Computer forensic timeline visualization tool http://www.dfrws.org/2009/proceedings/p78-olsson.pdf [27.05.2012]
3. Computer Forensics — Wikipedia, the free encyclopedia http://en.wikipedia.org/wiki/Computer_forensics [27.05.2012]
4. Digital Assembly — A smart choice for photo forensics http://digital-assembly.com/products/adroit-photo-forensics/ [27.05.2012]
5. EnCase Forensic — Computer Forensic Data Collection for Digital Evidence Examiners http://www.guidancesoftware.com/forensic.htm [27.05.2012]
6. IBM — IBM i2 Analyst's Notebook http://www.i2group.com/us/products/analysis-product-line/analysts-notebook [27.05.2012]
7. IR and forensic talk >> Using SIMILE for timeline visualization http://blog.kiddaland.net/2009/09/using-simile-for-timeline-visualization/ [27.05.2012]
8. Log2timeline http://log2timeline.net/ [27.05.2012]
9. NodeXL: Network Overview, Discovery and Exploration for Exel http://nodexl.codeplex.com/ [27.05.2012]
10. Social Network Analysis (SNA) Software with Sentinel Visualizer Diagrams http://www.fmsasg.com/SocialNetworkAnalysis/ [27.05.2012]
11. tnv: computer network traffic visualization tool http://tnv.sourceforge.net/ [27.05.2012]
12. Windows Presentation Foundation (WPF) http://wpf.codeplex.com/ [27.05.2012]
13. WPF Draw Tools — CodeProject http://www.codeproject.com/Articles/22776/WPF-DrawTools [27.05.2012]

14. Интервью с Юрием Губановым, основателем и владельцем компании Belkasoft: любой действие с компьютером оставляет следы, и их можно обнаружить — Интервью — Anti-Malware.ru http://www.anti-malware.ru/node/8767 [27.05.2012]
15. Официальный сайт компании Belkasoft http://belkasoft.com [27.05.2012]