УДК 343.982:004.4 + 004.4:343.98 Вестник УрФО № 3(21) / 2016, с. 16–23

Антясов И. С., Уфимцев М. С.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И МЕТОДЫ ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ КОМПЬЮТЕРНЫХ ЭКСПЕРТИЗ

При проведении компьютерных криминалистических экспертиз одним из ключевых этапов является поиск присутствующих на исследуемом носителе объектов, которые впоследствии смогут выступить основой для доказательной базы расследуемого инцидента. В статье исследованы используемые методы восстановления, проанализированы имеющиеся на рынке решения, обеспечивающие возможность восстановления удаленной и скрытой информации. Рассмотрено наиболее часто используемое в компьютерных экспертизах программное обеспечение, проведены сравнительные тесты коммерческих и бесплатных продуктов. Представлена оценка возможностей о применимости каждого инструмента, выделены достоинства и недостатки.

Ключевые слова: *восстановление данных, карвинг, компьютерная экспертиза, криминалистика, метаданные, форензика.*

Antyasov I. S., Ufimtcev M. S.

SOFTWARE AND METHODS OF RECOVERY OF INFORMATION IN THE PROCESS OF COMPUTER FORENSICS

Search for information objects in the investigated media is the main step in conducting forensic examinations. Found objects are subsequently become the basis for the evidence of the incident. In the article the use of data recovery techniques. We analyzed the available solutions on the market that provide the ability to recover deleted and hidden information. We describe the software that is used in computer forensics. We also conducted comparative tests of commercial and free products. Evaluate the merits and disadvantages of each tool.

Keywords: *data recovery, carving, computer forensics, criminology, metadata.*

Форензика - прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании цифровых доказательств, методах поиска, получения и закрепления таких доказательств. Форензика является подразделом криминалистики[1]. Ключевым вопросом в проведении компьютерной экспертизы помимо получения материала для исследования является процесс восстановления и поиска информации, которая способна выступить в качестве доказательной базы для расследования тех или иных инцидентов.

На рынке представлено довольно значительное количество продуктов по восстановлению и поиску информации, поэтому было принято решение проанализировать рынок коммерческого программного обеспечения для проведения компьютерных экспертиз в разрезе восстановления удаленной или скрытой на носителе информации. Также произведена оценка возможностей бесплатных альтернативных решений и сделаны выводы об их применимости в процессе проведения экспертиз.

В обзоре были исследованы ведущие программные продукты:

- Belkasoft Evidence Center,
- Мобильный Криминалист Детектив.

В качестве свободных аналогов выбрана связка, которая входит в состав дистрибутива KaliLinux:

- Foremost,
- RegRipper,
- BulkExtractor.

В рамках данной работы будем исходить из того, что в результате определенных действий был получен образ носителя информации, который подвергается анализу. Процесс получения данного образа весьма трудоемок, так как требуется соблюсти условие целостности носителя, которое подразумевает сохранение содержащейся на нем информации и ее неизменность на протяжении всей экспертизы.

Стоит заметить, что восстановление данных в форензике принципиально ничем не отличается от обычного восстановления утерянных файлов. Однако представляют интерес различные данные, вводившиеся подозреваемым (номера кредитных карт, данные геолокации, телефонные номера, посещаемые сайты, почтовые адреса).

Подавляющее большинство современных файловых систем содержит метаданные, которые описывают их структуру. Как минимум хранится информация об иерархии папок и файлов, а также их имена. Для каждого файла также хранится физический адрес на жестком диске, а для фрагментированных файлов еще и информация о фрагментах для последующей возможности считывать такого рода файлы.

Процесс восстановления файлов без метаданных называют карвингом. Основная идея заключается в анализе исходного содержимого файла и определении того, что найденный на носителе фрагмент информации принадлежит к определенному типу файлов. Варианты подобного анализа довольно разнообразны. В самом простом случае можно искать заголовки файлов, проходя объем исследуемого носителя байт за байтом. К примеру, графические файлы в формате png имеют в качестве первых четырех байтов заголовок вида «89 50 4E 47» (рис. 1). Некоторые файлы также содержат информацию о конце файла (футер) или о начале следующего фрагмента. Простейшие карверы данных вырезают последовательность байт между заголовком и футером, более сложные алгоритмы задействуются для сборки фрагментированных файлов.

Процесс карвинга позволяет найти помимо удаленных или скрытых файлов много полезной информации, которую можно исполь-

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG IHDR
00000010	00	00	06	D9	00	00	04	D8	08	06	00	00	00	7A	18	A8	Щ Ш z Ё
00000020	83	00	00	01	2F	69	43	43	50	49	43	43	20	50	72	6F	ѓ /iCCPICC Pro
00000030	66	69	6C	65	00	00	28	15	63	60	60	32	70	74	71	72	file (c``2ptqr
00000040	65	12	60	60	C8	CD	2B	29	0A	72	77	52	88	88	8C	52	e ``ИН+) rwR€€ЊR
00000050	60	BF	C0	C0	C1	C0	CD	20	CC	60	CC	60	9D	98	5C	5C	`їАААБАН М`М` \\
00000060	E0	18	10	E0	C3	00	04	79	F9	79	A9	20	1A	15	7C	BB	а аГ ущу© |»
00000070	C6	C0	08	12	B9	AC	0B	32	0B	55	8E	20	8F	2B	B9	A0	ЖА №¬ 2 Uћ +№
00000080	A8	04	A8	EA	0F	10	1B	A5	A4	16	27	33	30	30	1A	00	Ё Ёк Ґ¤ '300

Рис. 1. Пример файлового заголовка

зовать в интересах криминалистики. Обычные средства восстановления, не направленные на поиск специфичной информации, с такой задачей справиться не смогут.

В качестве критерия для сравнения имеющихся на рынке программных продуктов была поставлена задача извлечь максимальное количество файлов и любой другой полезной информации из слепка оперативной памяти работающего компьютера, папки пользователя операционной системы семейства Windows и бэкапа мобильного устройства на операционной системе Android 4.4, полученного средствами технологии Android Debug Bridge (ADB).

Проведем краткий обзор выбранных средств для проведения компьютерных экспертиз.

Belkasoft Evidence Center[2] представляет собой коммерческое решение для криминалистов, способное обнаруживать большое количество потенциальных улик. Программный комплекс способен работать с образами дисков, файлами, каталогами, физическими и логическими дисками. Удобный интерфейс и грамотно сконфигурированные базы данных агрегируют в удобном виде информацию об артефактах (в терминологии BelkaSoft артефакты – это найденные на носителе информации объекты, которые могут быть использованы в качестве улик) реестра, системных журналах, программах мгновенного обмена сообщениями. Также данный продукт извлекает файлы всех указанных при начальной конфигурации расширений, анализирует файлы подкачки и гибернации.

Мобильный Криминалист[3] в редакции «Детектив» представляет весьма узкоспециализированное коммерческое решение для исследования мобильных устройств. Программный комплекс содержит ценную информацию о тысячах присутствующих на рынке мобильных устройств максимального количества производителей. Среди ключевых особенностей стоит выделить возможность получать доступ к заблокированным телефонам, используя различные уязвимости для некоторых платформ. Однако, данная возможность распространяется на ограниченный ряд устройств, список которых постоянно пополняется. Кроме всего прочего, программный комплекс способен извлекать из устройства системные данные, информацию о звонках и переписках, восстанавливать данные приложений, социальных сетей, историю сетевых подключений, геолокационные данные. Вся полученная информация структурируется в виде удобной базы данных. Выбранные данные возможно структурировать в виде графов, отображающих информацию о связях между субъектами, которые теми или иными средствами связывались с владельцем исследуемого устройства.

Bulk Extractor[4] представляет собой инструмент компьютерной криминалистики для сканирования образов дисков, файлов и каталогов. Также, как и большинство программного обеспечения подобного класса, извлекает данные без информации о структуре файловой системы. Из-за того, что Bulk_ Extractor игнорирует структуру файловой системы, становится возможным параллельная обработка нескольких областей жесткого диска. Инструмент формирует удобные отчеты в виде текстовых файлов, в которых описывает найденную информацию и место ее нахождения на диске. Также имеются встроенные базовые методы анализа собранной информации. Примером может служить построение гистограмм для ключевых модулей, например, периодичность упоминания на исследуемом носителе какого-либо адреса электронной почты. Из возможностей стандартных модулей можно выделить сбор информации о кредитных картах, почтовых адресах, номерах телефонов, URL-адресах и Exif-информации фото- и видеофрагментов.

Foremost[5]. Принцип работы инструмента Foremost заключается в сканировании предоставленного на вход материала и распознавании файловых структур известных типов файлов на основе присущих только им признаков. Одним из таких признаков является уникальный для многих файлов заголовок и следуемая за ним служебная информация. На основе этой информации вырезается последовательность байт между заголовком и предполагаемым концом файла и отдается на исследование соответствующему модулю программы. Обычно таким образом удается восстановить уже удаленные и частично перезаписанные данные. Инструмент поддерживает шаблоны файловых структур, написанных пользователем, что существенно расширяет его функционал в долгосрочной перспективе.

RegRipper[6] включен в обзор, как альтернатива мощному обработчику файлов реестра Windows, который содержится в составе программного комплекса Belkasoft Evidence

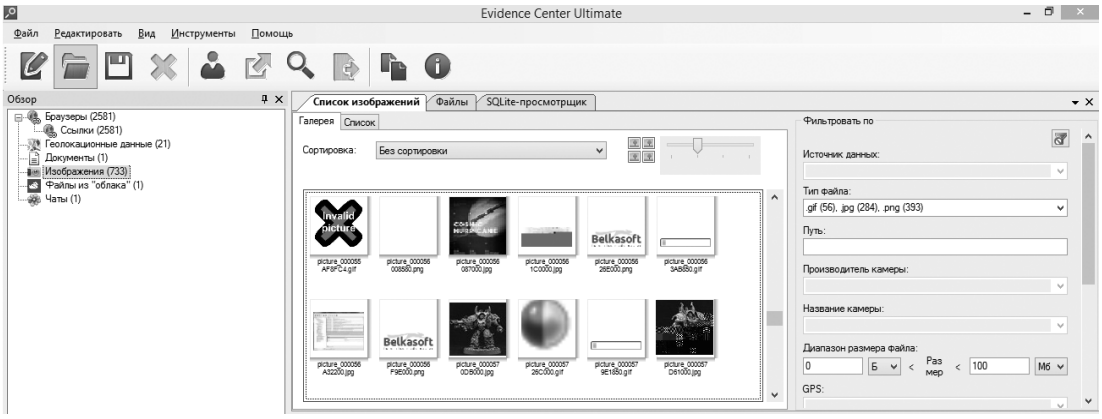

Рис. 2. Belkasoft Evidence Center и извлеченные данные

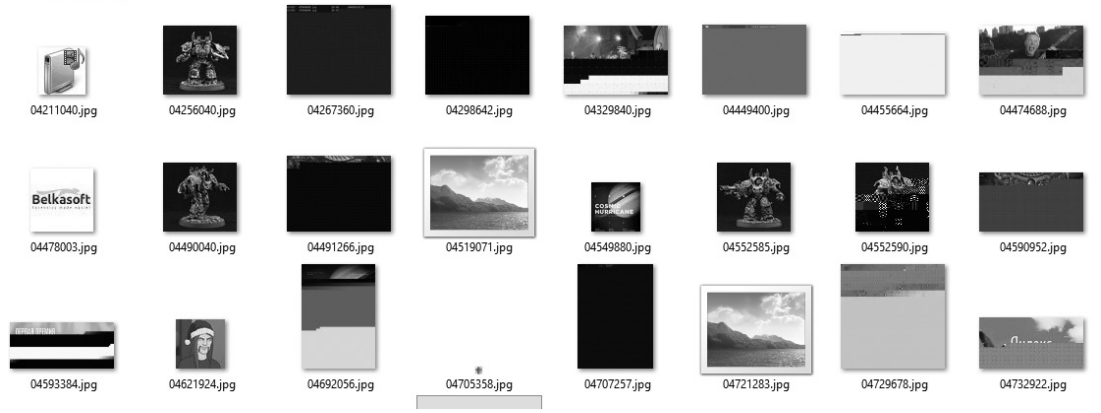

Рис. 3. Изображения, извлеченные с помощью Foremost

Center. Программа поддерживает сторонние плагины, синтаксис которых достаточно прост, что позволяет расширять возможности инструмента.

Первый этап тестирования было решено провести на максимально быстро меняющемся источнике данных. Примером тому может служить оперативная память. В зависимости от контекста задачи пользователя, оперативная память расходуется под запись огромного количества данных, которые постоянно подвергаются удалению и перезаписи. Образ оперативной памяти получен с помощью бесплатной утилиты Belkasoft Live RAM Capturer.

Программный комплекс от Belkasoft извлек из образа оперативной памяти большое количество изображений. Часть найденного материала была повреждена и не открывалась вовсе (рис. 2). Некоторые изображения удалось восстановить лишь частично. Также были получены ссылки на ресурсы, которые посещал пользователь в браузере. Подобный перечень информации довольно точно отображает недавнюю активность пользователя.

Бесплатные инструменты справились с задачей со схожими результатами. Некоторые различия в результатах обусловлены различными алгоритмами работы инструментов. Foremost смог извлечь схожий по объему и качеству список изображений (рис. 3). Были найдены также отрывки аудиозаписей и фрагменты веб-страниц. Большое количество файлов не открывается штатными средствами, некоторые открываются с нарушением целостности. Но тем не менее, общую тенденцию рабочего процесса пользователя проследить возможно (рис. 4).

Bulk_Extractor нашел почтовые адреса, которые были помещены в память в результате загрузки списка контактов почтового ящика в браузере. Также были найдены ссылки на поисковые запросы (рис. 5), посещаемые ресурсы (рис. 6, 7) и телефонные номера.

Анализ содержимого папки пользователя операционной системы Windows выявил различие между бесплатными и коммерческими продуктами. Как и ожидалось, Bulk_Extractor извлек большое количество информации об активности пользователя, характер и вид ко-

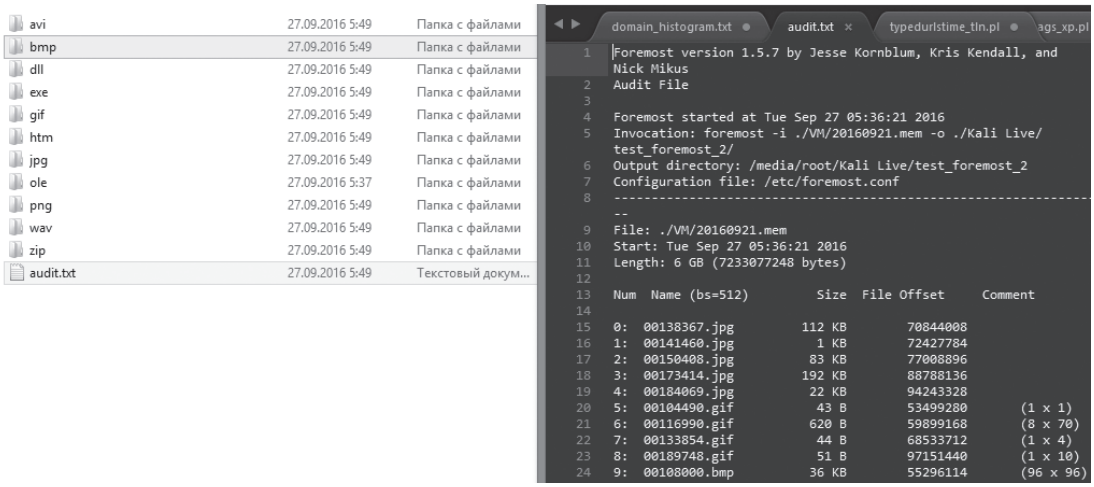

Рис. 4. Сформированные списки найденных файлов и места их нахождения

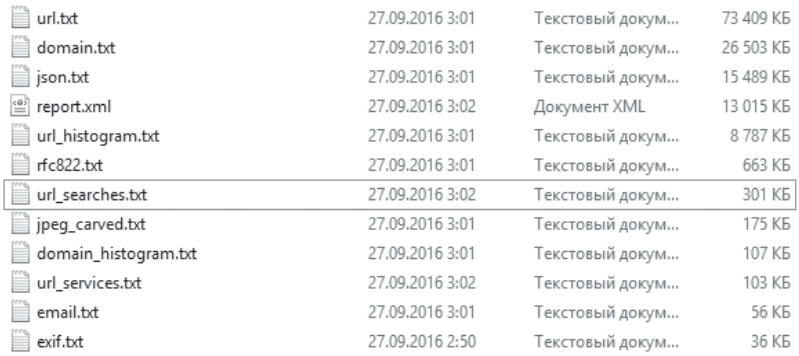

Рис. 5. Текстовые файлы с извлеченной информацией

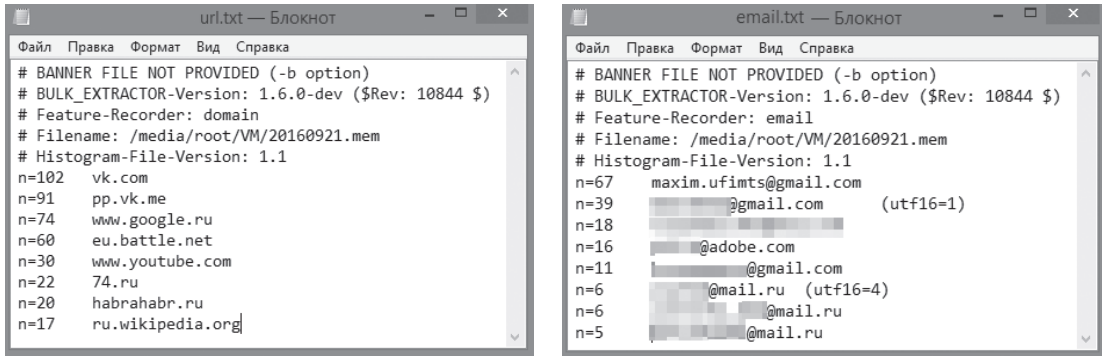

Рис. 6. Информация о посещаемых ресурсах и почтовые адреса

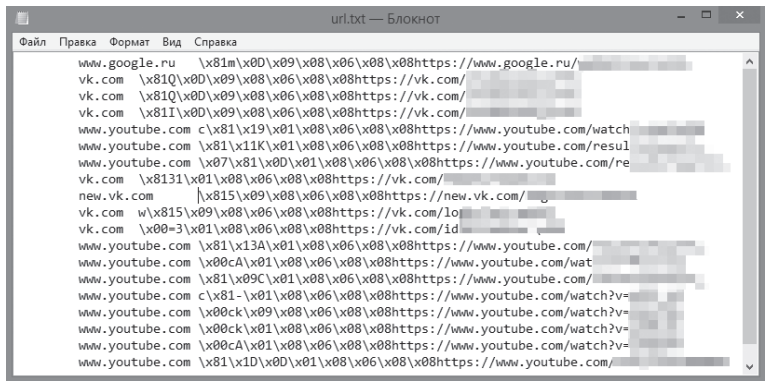

Рис. 7. Подробная информация о найденных ссылках

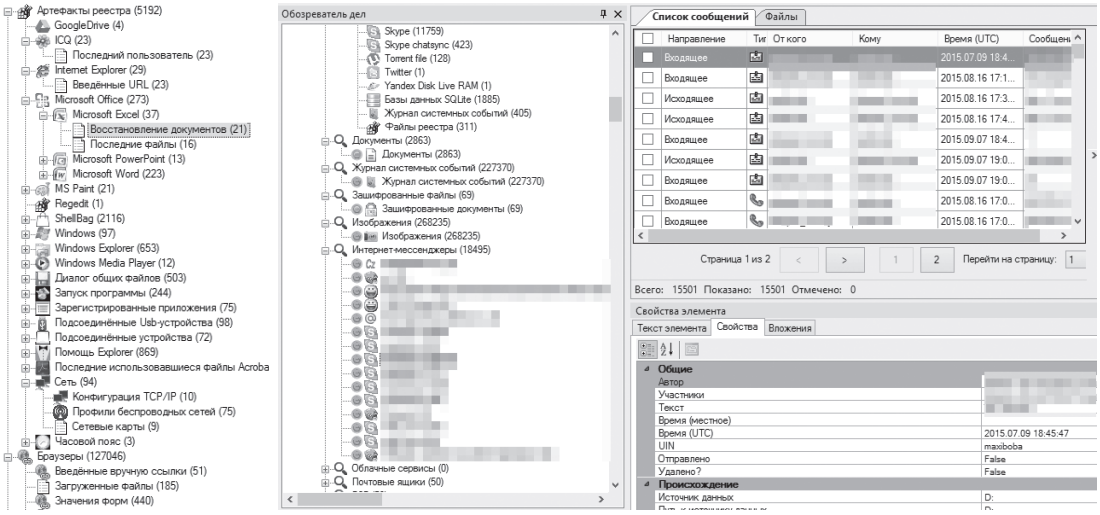

Рис. 8. Информация, извлеченная с помощью Belkasoft Evidence Centre

торой был описан в предыдущем разделе. Также, был составлен список найденных SQLite баз данных, в которых содержится информация об активности пользователя в браузерах и мессенджерах. Однако, данный подход требует отдельного программного обеспечения для просмотра баз данных. В свою очередь, Belkasoft Evidence Centre справился с этой задачей и в удобной структурированной форме предоставил данные (рис. 8).

Емкую картину о содержимом реестра способен дать инструмент RegRipper с необходимыми плагинами. На вход программе подавался найденный файл ntuser.dat, в котором содержится информация из ветки HKEY_CURRENT_USER, после анализа которого, мы получаем удобный отчет в текстовом виде (рис. 9).

Последним исследуемым объектом стал backup-файл телефона на операционной системе Android 4.4. Образ бэкапа получен средствами ADB и разархивирован для удобства работы. Полученные файлы были переданы для анализа инструменту Bulk_Extractor. В текстовом виде программа извлекла уже рассматриваемые в предыдущих разделах данные, однако не удалось достать файлы с смс-сообщениями, были лишь частично восстановлены телефонные номера без какой-либо связи с лицами из телефонной книги. Полученный объем информации почти не позволял с ним работать, кроме всего прочего, отдельной проблемой стало подключение телефона к компьютеру и аккуратное снятие резервной копии.

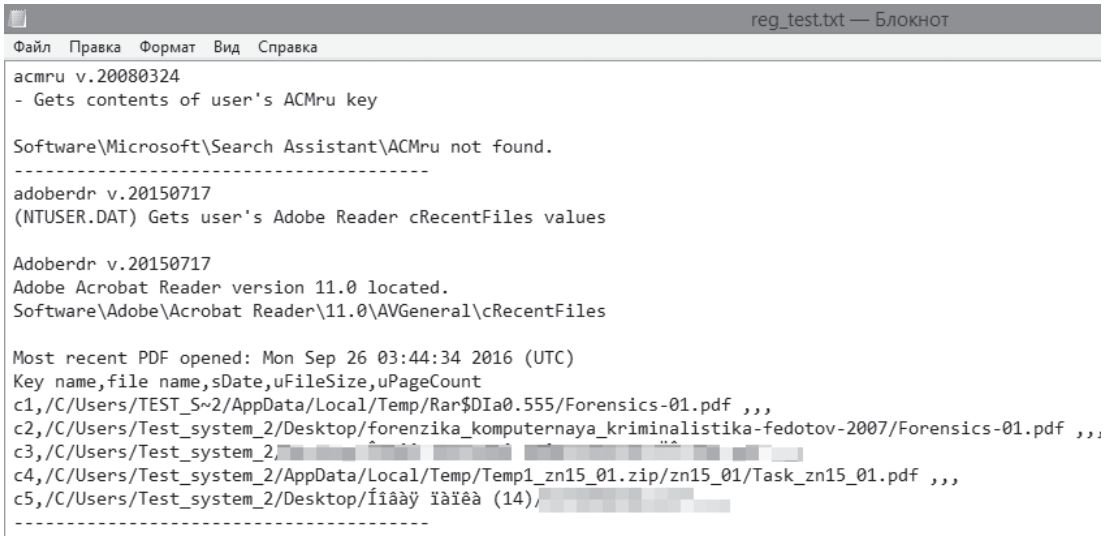

Рис. 9. Текстовый вывод программы RegRipper. Результат работы первого плагина. Открываемые ранее PDFфайлы.

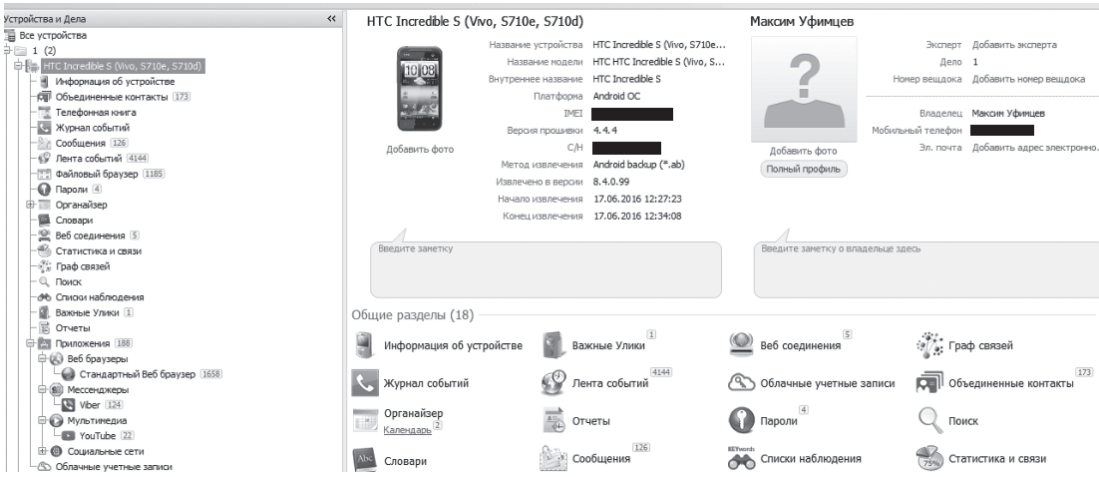

Рис. 10. Главное окно программы с доступными уликами

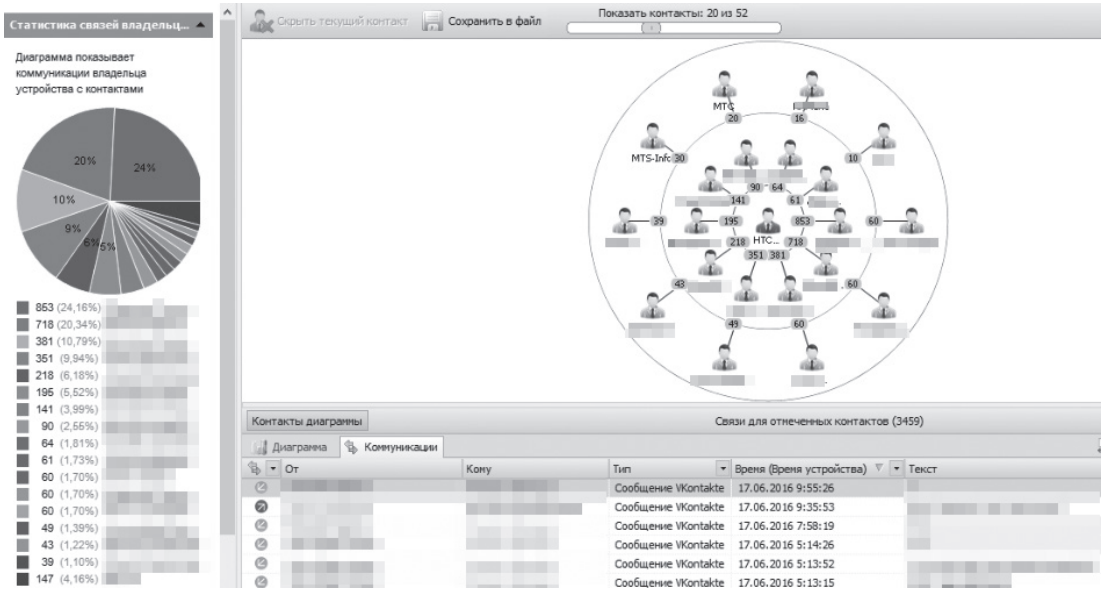

Рис. 11. Граф частоты связей

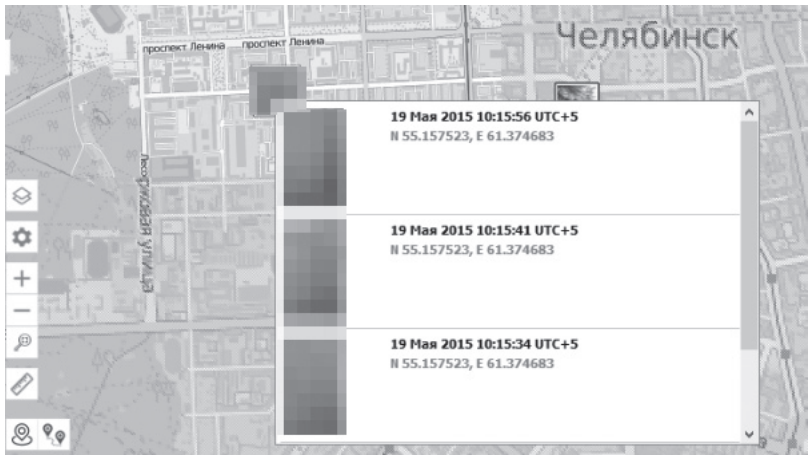

Рис. 12. Карта с отмеченными точками геолокации

Мобильному криминалисту удалось не только обнаружить все требуемые улики, но и в очень удобном виде предоставить информацию для анализа пользователю (рис. 10). В частности, были построены диаграммы активности владельца устройства, графы связей с другими телефонными номерами и аккаунтами в социальных сетях (рис. 11), геометки, полученные из EXIF-данных фотографий сразу помещены на загруженные карты (рис. 12). Стоит отметить, что телефон был подключен напрямую к компьютеру, Мобильный Криминалист подобрал необходимые драйверы для устройства и, используя свои закрытые алгоритмы, произвел извлечение всей информации. Отличительной особенностью программы является постоянная поддержка от производителя, которая включает в себя регулярное обновление списков доступных мобильных устройств и исследуемых приложений. Если телефон или его аналог загружен в базу доступных устройств, то программный комплекс имеет всю необходимую информацию, о том, в каких местах и каким образом, проводить поиск улик.

Таким образом, сравнительный анализ бесплатных и коммерческих продуктов выявил дружелюбность к конечному пользователю последних: удобный интерфейс для быстрого анализа информационных объектов, автоматический поиск и формирование отчетов обо всех найденных уликах. Платные решения позволяют без траты лишнего времени эффективно собирать доказательную базу даже лицам, не понимающим сути процессов, в которых участвует исследуемая информация. Бесплатные аналоги, несмотря на наличие недостатков (необходим высокий уровень эксперта, имеются риски пропустить ценную информацию, требуется дополнительная обработка для сортировки и упрощения восприятия), имеют открытый исходный код, а также возможности по быстрой модернизации. Интернет-сообщество регулярно улучшает функционал бесплатных инструментов, выкладывая в открытый доступ новые плагины и конфигурации, что позволяет при грамотном использовании извлекать на порядок больше информации и вмешиваться эксперту в процесс своей работы на любом этапе исследования.

Примечания

1. Федотов Н.Н. Форензика – компьютерная криминалистика –М.: Юридический Мир, 2007. – 432 с.

2. Официальный сайт производителя программы Belkasoft Evidence Centre. URL: http://ru.belkasoft.com/ru (дата обращения: 21.09.2016)

3. Официальный сайт производителя программы Мобильный Криминалист. URL: http://www.oxygensoftware.ru (дата обращения: 21.09.2016)

4. Официальный репозиторий программы Bulk_Extractor. URL: https://github.com/simsong/bulk_extractor (дата обращения: 21.09.2016)

5. Официальный сайт программы Foremost. URL: http://foremost.sourceforge.net (дата обращения: 21.09.2016)

6. Официальный репозиторий программы RegRipper. URL: https://github.com/keydet89/RegRipper2.8 (дата обращения: 21.09.2016)

Антясов Иван Сергеевич, ассистент кафедры защиты информации, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)», Россия, 454080 Челябинск, проспект Ленина, 76. E-mail: antiasovis@susu.ru

Уфимцев Максим Сергеевич, студент кафедры защиты информации, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)», Россия, 454080 Челябинск, проспект Ленина, 76. E-mail: ufimtcevms@susu.ru

Antyasov Ivan Sergeevich, assistant of Information Security department, Federal State Autonomous Educational Institution of Higher Education «South Ural State University (national research university)» FSAEIHE SUSU (NRU), 76, Lenin prospekt, Chelyabinsk, Russia, 454080. E-mail: antiasovis@susu.ru

Ufimtcev Maxim Sergeevich, student of Information Security department, Federal State Autonomous Educational Institution of Higher Education «South Ural State University (national research university)» FSAEIHE SUSU (NRU), 76, Lenin prospekt, Chelyabinsk, Russia, 454080. E-mail: ufimtcevms@susu.ru