УДК 004.49:519.81

К ВОПРОСУ СОВЕРШЕНСТВОВАНИЯ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ ПРАВООХРАНИТЕЛЬНЫМИ ОРГАНАМИ

[1]Иванов В.Ю., [2]Жигалов К.Ю.

[1]Московский университет МВД им. В.Я. Кикотя, Москва, e-mail: ivsl71@mail.ru;
[2]ФГБУН «Институт проблем управления Российской академии наук им. В.А. Трапезникова», Московский технологический институт, Москва, e-mail: kshakalov@mail.ru

Расследование следов преступлений в сфере высоких технологий предполагает поиск доказательств противоправных цифровых действий пользователя в информационной системе. В качестве объектов исследования для формирования доказательной базы, используются всевозможные устройства способные хранить в себе цифровую информацию. В данной статье рассмотрены различные программные, аппаратные и аппаратно-программные комплексы, используемые органами внутренних дел и другими организациями для расследования преступлений в области информационных технологий. Кроме того, показаны способы получения информации с накопителей на жестких магнитных дисках, SSD и мобильных устройств. В дополнение к стандартным способам и методам получения цифровых следов, в качестве полезного источника дополнительной информации указывается на образ оперативной памяти вычислительной системы. В ходе исследований выявлена возможность получения из оперативной памяти следующей информации: перечень запущенных процессов; сведения о сетевых соединениях; пароли для доступа к файлам; расшифрованные файлы, находящиеся в зашифрованном виде в файловой системе; ключи шифрования; буфер обмена; переписку пользователя; вредоносный код. Применение описанной в статье информации позволит как эффективно защищать данные от злоумышленников, так и проводить доказательную базу и поиск доказательств осуществления незаконной деятельности.

Ключевые слова: киберпреступление, следы на информационных носителях, образ оперативной памяти, мобильные устройства, органы внутренних дел

TO THE QUESTION OF IMPROVING THE ANTI CYBERCRIME LAW ENFORCEMENT

[1]Ivanov V.Yu., [2]Zhigalov K.Yu.

[1]Moscow University of the Ministry of the Interior of Russia, Moscow, e-mail: ivsl71@mail.ru;
[2]V.A. Trapeznikov Institute of control Sciences of the Russian Academy of Sciences, Moscow Technological Institute, Moscow, e-mail: kshakalov@mail.ru

Investigation of traces of crimes in the field of high technology involves the search for evidence of illegal digital actions of the user in the information system. As the objects of research to form the evidence base, using all kinds of devices capable of storing digital information. This article discusses the various software, hardware and hardware-software systems used by the Internal Affairs Bodies and other organizations to investigate crimes in the field of information technology. In addition, the methods of obtaining information from hard disk drives, SSDS and mobile devices are shown. In addition to the standard methods and techniques for obtaining digital traces, as a useful source of additional information is indicated on the image of the RAM of the computer system. In the course of research, the possibility of obtaining the following information from the RAM: the list of running processes; information about network connections; passwords to access files; decrypted files that are encrypted in the file system; encryption keys; the clipboard; the correspondence of the user; the malicious code. The use of the information described in the article will allow both to effectively protect data from intruders and to conduct evidence base and search for evidence of illegal activities.

Keywords: cybercrime, traces on information carriers, the computer's memory, a mobile device, police

Все громкие преступления в настоящее время совершаются при помощи вредоносных программ. Разработчики вредоносного программного обеспечения уже не развлекаются, выводя компьютер из строя, а все свои усилия направляют в сторону получение прибыли от созданного им программного кода.

Есть четкое разграничение обязанностей в преступном мире: одни люди занимаются разработкой вредоносных программ, другие люди их распространяют, третьи люди умеют только зайти в административную панель бот-сети и отправлять команды управления вредоносной программой, которая стоит на тысячах зараженных компьютерах, другие умеют только обналичивать полученные финансовые средства и так далее.

В связи с этим разделением очень сложно привлечь данных людей к уголовной ответственности. Только в ходе рассмотрения дела в рамках преступной группы задачи каждого члена становятся понятными.

Сложностью расследования еще является то, что каждый член группы, как правило, знает только одного или двух своих подельников, причем не настоящие имена, а «ники». Поэтому установить связи преступного сообщества очень сложно и доказать это в суде довольно затруднительно.

В связи с этим преступность в цифровом мире очень развита; чувствуя безнаказанность, злоумышленники продолжают нарушать закон, посягая на чужие права.

Цифровые доказательства

В качестве доказательств при расследовании преступлений в сфере высоких технологий выступают, как правило, цифровые данные. В отличие от вещественных доказательств они находятся в памяти электронных устройств и могут быть зафиксированы только при помощи специальных аппаратно-программных криминалистических комплексов.

Носители информации можно разделить на энергонезависимые и энергозависимые. Энергонезависимый носитель информации способен хранить записанные данные в течение длительного времени без необходимости подключения к источнику питания. Энергозависимый носитель информации не способен после отключения от источника питания в течение длительного времени хранить данные.

На этапе сбора и фиксации информации об инциденте необходимо понимать, что цифровые доказательства находятся не только на жестких дисках, но и имеются в оперативной памяти и дампах сетевого трафика. Это очень важно сейчас, когда вредоносные программы работают в основном в оперативной памяти, чтобы не оставлять следов на жестком диске.

В оперативной памяти можно найти: перечень запущенных процессов; сведения о сетевых соединениях; пароли для доступа к файлам; расшифрованные файлы, которые в обычном состоянии находятся на диске в зашифрованном виде; ключи шифрования; буфер обмена; переписку пользователя; вредоносный код.

Выключение компьютера, подвергшегося инциденту без снятия дампа оперативной памяти, приведет к потере очень важных цифровых доказательств, без которых наказать злоумышленника порой будет практически невозможно.

Зачем нужен сетевой трафик? Допустим, мы нашли вредоносную программу на жестком диске, и, если она не очень сложная, можно попытаться найти ссылки на сервер управления, куда отсылаются данные. Однако на момент исследования эти ссылки могут оказаться неактуальными, в связи с тем, что злоумышленники меняют адреса сервера как минимум два раза в день и реальные ip-адреса сервера мы не получим.

На основании вышеизложенного, можно предложить следующий порядок сбора информации:

1. Создание копии содержимого оперативной памяти.
2. В случае необходимости создание копий энергонезависимых носителей информации.
3. Выключение работающих компьютеров одним из следующих методов:
   3.1. Штатной процедурой выключения;
   3.2. Прерыванием электропитания.
4. Извлечение энергонезависимых носителей информации (НЖМД, флеш-накопители) и создание их копии.
5. Копирование лог-файлов сетевого оборудования.
6. Запрос лог-файлов у интернет-провайдера и других сервисов в случае надобности.

Для сбора данных с энергозависимых носителей информации необходимо иметь flash-накопитель или переносной жесткий магнитный диск, на который предварительно должны быть записаны специальные программы.

Для операционной системы Windows: Mandiant «Memoryze» [1], AccessData «FTK Imager» [2]. Для операционной системы Linux: LiME, Fmem [3, 4]. Для операционной системы OS X: Mac Memory Reader [5]. Эти программы условно-бесплатные и находятся в свободном доступе.

```
C:\Mem>MemoryDD.bat -output RAM
Memoryze.exe by MANDIANT (c) 2011 - http://www.mandiant.com/products/free_software/memoryze/
   Usage: C:\Mem\MemoryDD.bat
     -offset   optional offset into physical memory. Exclude for all.
     -size     optional size of physical memory to acquire. Exclude for all.
     -output   directory to write the results. Default .\Audits

C:\Mem\RAM\Audits\TESTVM\20121010164436>dir /l
 Том в устройстве C не имеет метки.
 Серийный номер тома: B088-DA9C

 Содержимое папки C:\Mem\RAM\Audits\TESTVM\20121010164436

10/10/2012  09:44 AM    <DIR>          .
10/10/2012  09:44 AM    <DIR>          ..
10/10/2012  09:44 AM            20,047 batchresults.xml
10/10/2012  09:44 AM               286 issues.batchresults.xml
10/10/2012  09:44 AM             1,008 issues.memory.213f5926.img.xml
10/10/2012  09:44 AM       536,805,376 memory.213f5926.img
```

Рис. 1. Результаты работы программы Memoryze

Исследование оперативной памяти

Для снятия копии содержимого оперативной памяти можно воспользоваться утилитой Memoryze [1]. С помощью командной строки необходимо запустить следующий файл из директории программы Memoryze:

MemoryDD.bat –output <out_dir>,

где <out_dir> – папка для сохранения образа.

В результате работы данной утилиты сохраняется образ оперативной памяти в виде файла с расширением .img (рис. 1).

Альтернативной программой по созданию копии оперативной памяти является программа AccessData FTK Imager. В отличие от предыдущей утилиты, она имеет более дружественный интерфейс и позволяет при создании копии включить в создаваемый образ файл подкачки, содержащий дополнительную системную информацию (рис. 2).

Исследуя оперативную память, можно получить список запущенных процессов и сервисов. Появление в этом списке неизвестного процесса позволит более тщательно рассмотреть этапы его запуска и работы (рис. 3).

Список установленных в системе драйверов. Здесь можно получить информацию о том, какие внешние устройства были подключены к компьютеру и в каком состоянии они находились на момент изъятия оперативной памяти. Наряду с этим исследование оперативной памяти позволяет получить журнал посещенных пользователем сайтов. На рис. 4 можно увидеть их названия и реальные ip адреса. Так, например, сайт www.openrce.org имеет ip-адрес 96.126.125.53 [6].

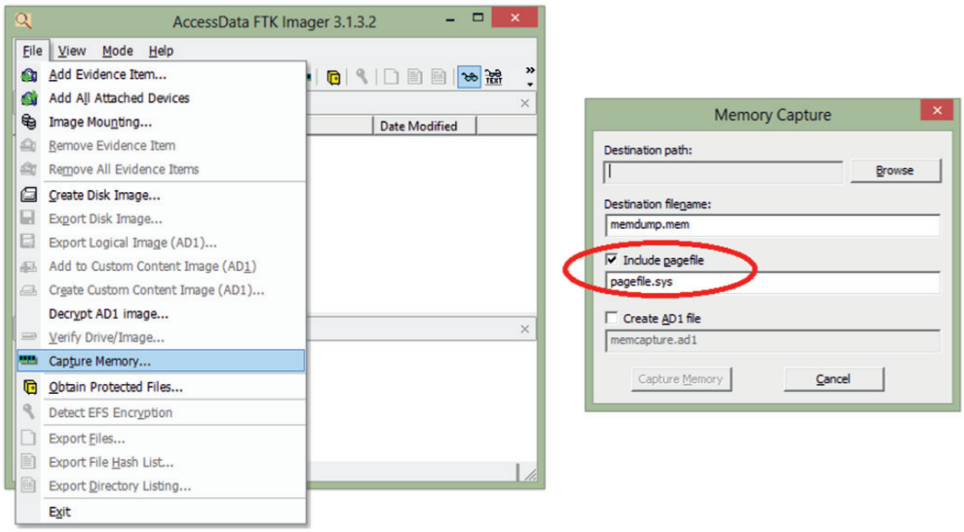

Рис. 2. Снятие копии содержимого оперативной памяти с помощью AccessData FTK Imager

```
>tasklist  /SVC >tasklist.txt
```

```
Image Name                     PID Services
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       616 N/A
csrss.exe                      808 N/A
wininit.exe                    868 N/A
csrss.exe                      888 N/A
services.exe                   932 N/A
lsass.exe                      956 KeyIso, Netlogon, ProtectedStorage, SamSs
lsm.exe                        964 N/A
winlogon.exe                   648 N/A
svchost.exe                    684 DcomLaunch, PlugPlay, Power
nvvsvc.exe                     996 nvsvc
svchost.exe                    816 RpcEptMapper, RpcSs
svchost.exe                   1116 AudioSrv, Dhcp, eventlog, lmhosts, wscsvc
svchost.exe                   1160 AudioEndpointBuilder, Netman, SysMain,
                                   TrkWks, UxSms, WPDBusEnum, wudfsvc
svchost.exe                   1188 BITS, Browser, gpsvc, IKEEXT, iphlpsvc,
                                   LanmanServer, MMCSS, ProfSvc, Schedule,
                                   SENS, ShellHWDetection, Themes, Winmgmt,
```

Рис. 3. Список запущенных процессов и сервисов

```
>ipconfig /displaydns    >DNScache.txt
```

```
www.openrce.org
----------------------------------------
Record Name . . . . . : www.openrce.org
Record Type . . . . . : 1
Time To Live  . . . . : 71897
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 96.126.125.53


www.ic3.gov
----------------------------------------
Record Name . . . . . : www.ic3.gov
Record Type . . . . . : 1
Time To Live  . . . . : 58520
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 65.201.175.137
```

Рис. 4. Журнал посещенных сайтов

Список текущих открытых соединений позволяет определить, к каким сетевым ресурсам в момент снятия оперативной памяти был подключен компьютер и с какими ресурсами он взаимодействует.

Исследование накопителей на жестких магнитных дисках

Сбор данных с энергонезависимых носителей информации несколько отличается от рассмотренного выше. Это связано с тем, что объемы жестких магнитных дисков гораздо больше, чем размер оперативной памяти, и если есть необходимость в процессе выемки создать образ жесткого магнитного диска, то надо понимать, что на это уйдет гораздо большее количество времени.

Немаловажным фактором является то, что без специального оборудования нельзя на работающем компьютере создать копию интересующего нас диска. Любая операции копирования вносит изменения в атрибуты исследуемых файлов, что не позволит использовать их в качестве доказательства в суде.

В соответствии со статьей 57 Уголовно-процессуального кодекса Российской Федерации эксперт не вправе без разрешения дознавателя, следователя или суда проводить исследование, которое может повлечь полное или частичное уничтожение объектов либо изменение их внешнего вида или основных свойств.

Поэтому для осуществления копирования данных по секторам жесткого магнитного диска необходимо использовать программные или аппаратные блокираторы записи.

Блокираторами записи называются программы или аппаратные устройства, которые на физическом уровне предотвращают какие-либо изменения в процессе копирования данных. Данные устройства позволяют гарантированно создавать аутентичные образы исследуемых дисков.

Наряду со встроенными блокираторами записи эксперты могут использовать автономные устройства, которые называются дубликатами или копирами. Эти устройства также имеют возможность блокирования записи, но, в отличие от предыдущих, позволяют создавать копии исследуемых дисков без использования персонального компьютера.

Сам процесс создания копии диска осуществляется при помощи специальных программ, например AccessData FTK Imager, и занимает продолжительное время (рис. 5).

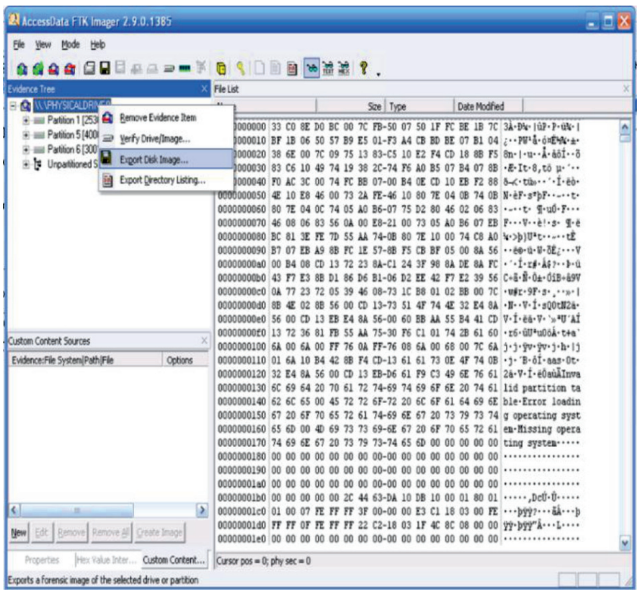

Рис. 5. Создание копии диска программой AccessData FTK Imager

После получения образов запоминающих устройств, их исследование уже проводится на стендовом оборудовании в лабораторных условиях.

Для проведения компьютерных экспертиз наиболее часто используются следующие аппаратно-программные комплексы:

– Paraben's P2C,
– EnCase Forensic
– Belkasoft Evidence Center.

Данные комплексы способны восстановить удаленную информацию, осуществить контекстный поиск по различным критериям внутри файлов, отсортировать информацию в удобном для восприятия виде и автоматически составить отчет, который можно использовать в приложениях к экспертному заключению. Так же имеется возможность просмотреть содержимое всех основных интернет-чатов, по которым можно определить собеседников и прочитать их сообщения. Поддерживаются все известные браузеры, работающие под операционную систему Windows, что позволяет получить хронологию посещения сайтов на исследуемом компьютере. Имеется возможность анализировать изображения и видеофайлы на наличие порнографии, лиц и отсканированного текста. Поддерживается излечение удаленной истории. Доступен анализ образа оперативной памяти [7].

При фотографировании мобильными устройствами или фотоаппаратами с GPS модулем, внутри фотографий могут помещаться данные о геолокации. Если на диске имеются такие графические файлы, аппаратно-программный комплекс покажет все места, где были сняты выбранные фотографии на картах Google внутри окна встроенного веб-браузера.

Если навести мышь на изображение места на карте, то можно будет получить информацию об изображении, снятом в данном месте (рис. 6).

Исследование мобильных устройств

Мобильные устройства, такие как смартфоны и планшеты, наряду с оперативной памятью и жесткими магнитными дисками компьютера также содержат в себе цифровую информацию, которую можно использовать в качестве доказательства в суде.

Количество полезной информации о повседневной жизни злоумышленника здесь гораздо больше. Это связано с тем, что сотовым телефоном человек пользуется гораздо чаще и он всегда находится при нем [2, 8].

Наиболее популярными аппаратно-программными комплексами для исследований мобильных устройств являются комплексы: UFED; XRY; Мобильный Криминалист (Oxygen Forensic Suite).

UFED – израильская разработка, XRY – разработка шведской компании, Мобильный Криминалист – создан российскими специалистами.

Основными местами хранения данных в мобильных устройствах являются: внутренняя память; внешняя память; SIM-карта; оператор сотовой связи (NSP); «облачное» хранилище.

Для получения доступа к хранимой информации необходимо соединить телефон с аппаратно-программным комплексом с помощью интерфейсных кабелей, входящих в комплект, либо используя Bluetooth или инфракрасный порт.

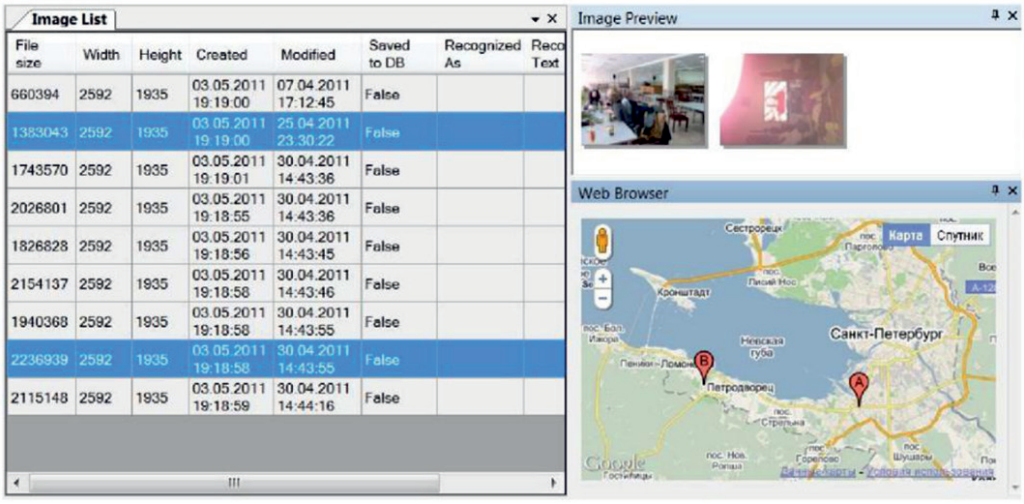

Рис. 6. Belkasoft Evidense Center

Комплексы иногда позволяют обходить блокировку экрана или снимать пароли, защищающие устройства. Также возможен подбор пароля на зашифрованных резервных копиях.

Аппаратно-программные комплексы извлекают все данные: контакты, сообщения, звонки, файловую систему, данные из приложений – и восстанавливают удаленные данные [9, 10].

В удобном для восприятия виде можно получить все отправленные и полученные SMS сообщения. Каждое сообщение сопровождается информацией о получателе и отправителе, времени отправления и текстом.

Программа извлекает данные геолокации из различных источников: мобильные устройства, облачные сервисы, карты памяти и так далее [11, 8]. Пространственные координаты отображаются на онлайн- и оффлайн-картах.

Встроенный модуль карт позволяет:

– посмотреть посещенные пользователем места;

– построить маршруты передвижения пользователя;

– найти общие места пребывания нескольких пользователей.

Комплексы имеют ряд программных аналитических разделов, таких как «лента событий» – показывающая все события в хронологическом порядке, «граф связей» – указывающий связи между владельцами устройств и их контактами.

Заключение

В заключение хотелось бы отметить, что в последнее время борьба с компьютерными преступлениями становится все более актуальной. Наиболее перспективным направлением этой борьбы, по мнению авторов, является исследование мобильных устройств. Практически каждый человек сегодня имеет подобное устройство. А что касается молодёжи, то большая часть свободного времени их связана с общением через интернет-приложения, посещением сайтов, созданием селфи и др. А это связи, местонахождение и интересы.

Список литературы

1. Жигалов К.Ю. Подготовка техники к использованию в системах автоматизированного управления строительства автодорог // Естественные и технические науки. 2014. № 1 (69). С. 62–65.

2. Бобкин Д.В., Жигалов К.Ю. Исследование надежности распознавания речи системой Google Voice Search // Cloud of Science. 2015. Т. 2. № 3. С. 465–472.

3. Effective Email Borne Ransomware Responses // Сайт компании FireEye [Электронный ресурс]. URL: https://www.fireeye.com (дата обращения: 27.09.2018).

4. Empowering Collection to Analysis Excellence // Сайт компании AccessData [Электронный ресурс]. URL: http://www.accessdata.com/product-download (дата обращения: 27.09.2018).

5. Computer Forensic Tool Catalog // The National Institute of Standards and Technology (NIST) is an agency of the U.S. Commerce Department [Электронный ресурс]. URL: https://toolcatalog.nist.gov (дата обращения: 27.09.2018).

6. Червяков Н.И., Коляда А.А., Ляхов П.А. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях. М.: ФИЗМАТЛИТ, 2017. 400 с.

7. Omondi A., Premkumar B. Residue Number Systems: Theory and Implementation // Imperial College Press. UK 2007. 296 p.

8. Жигалов К.Ю., Иванов В.А. Преодоление низкой частоты дискретизации аналого-цифрового преобразователя для задач синтеза речевого сигнала // Прикладные исследования и технологии ART2015: сборник трудов Второй международной конференции, 2015. С. 148–150.

9. Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности: учеб. пособие для вузов. М.: Горячая линия Телеком, 2007. 320 с.

10. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. М.: Академия, 2009. 272 с.

11. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Издательство ТРИУМФ, 2003. 816 с.