УДК 343.983

П. А. Олейникова

Московский государственный технический университет им. Н.Э. Баумана, Москва, e-mail: polina4456616@yandex.ru

А. В. Караваева

Московский государственный технический университет им. Н.Э. Баумана, Москва, e-mail: karlova_av@bmstu.ru

ПОИСК СЛЕДОВ ПРИМЕНЕНИЯ ВИРТУАЛЬНОЙ МАШИНЫ ORACLE VM VIRTUALBOX НА ПРЕДМЕТ НАЛИЧИЯ КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ

Ключевые слова: виртуальная машина, программное обеспечение, реестр, файлы, системные каталоги.

В работе рассматривается – какие следы оставляет виртуальная машина Oracle VM VirtualBox на компьютере. Oracle VM VirtualBox – это программа, которая позволяет на одном компьютере запускать одновременно несколько операционных систем, например: Windows, Linux и другие. Исследование данного программного обеспечения направлено на обнаружение следов установки, настройки и запуска программы, а также на изучение содержимого файлов, создаваемых виртуальной машиной. Для выявления следов загрузки и запуска Oracle VM VirtualBox были проанализированы файлы реестра и системные каталоги с использованием программного обеспечения «Windows Registry Recovery» и «WinPrefetchView». Содержимое файлов виртуальной машины, таких как *.vbox и *.vdi, анализировалось на поиск криминалистически значимой информации при помощи программ «WinHex» и «7-File File Manager». Изучение этих файлов показало, что они хранят информацию об операционной системе, дате и времени создания виртуальной машины, MAC-адресе, а также системные и пользовательские файлы, такие как документы, изображения, видео и другие. Проведенное исследование позволило прийти к выводу о том, что анализ виртуальных машин способствует расследованию и раскрытию преступлений.

P. A. Oleinikova

Bauman Moscow State Technical University, Moscow, e-mail: polina4456616@yandex.ru

A. V. Karavaeva

Bauman Moscow State Technical University, Moscow, e-mail: karlova_av@bmstu.ru

SEARCH FOR TRACES OF THE USE OF THE ORACLE VM VIRTUALBOX VIRTUAL MACHINE FOR THE PRESENCE OF FORENSICALLY SIGNIFICANT INFORMATION

Keywords: virtual machine, software, registry, files, system directories.

The paper considers what traces the Oracle VM VirtualBox virtual machine leaves on the computer.. Oracle VM VirtualBox is a program that allows you to run several operating systems on one computer at the same time, for example: Windows, Linux and others. The study led to come to the conclusion that the analysis of virtual machines contributes of the program, as well as studying the contents of files created by the virtual machine. Registry files and system directories were analyzed using “Windows Registry Recovery” and “WinPrefetchView” software to identify traces of loading and starting Oracle VM VirtualBox. The contents of the virtual machine files, such as *.vbox and *.vdi, were analyzed to search for forensically significant information using the WinHex and 7-File File Manager programs. The study of these files showed that they store information about the operating system, the date and time the virtual machine was created, the MAC address, as well as system and user files such as documents, images, videos, and others. The study led to the conclusion that the analysis of virtual machines contributes to the investigation and detection of crimes.

По статистике МВД РФ существенным фактором, оказывающим негативное влияние на криминогенную ситуацию в стране, является рост IT-преступности. В январе – феврале 2022 года зарегистрировано 79,7 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфе-

ре компьютерной информации. Так, одним из средств совершения данных преступлений является использование виртуальных машин.

Актуальность работы заключается в том, что информация, полученная посредством изучения виртуальных машин, может помочь следствию при расследовании дел в сфере компьютерной информации. Временные файлы, расположение графических или текстовых файлов, журналы активности в Интернете, создание вредоносного программного обеспечения – вот некоторые примеры доказательств, которые можно собрать при исследовании образа виртуальной машины, если их тщательно проанализировать. Ценные данные, связанные с виртуальной машиной, могут иметь важное значение для расследования, следовательно, компьютерно-технический эксперт должен полностью исследовать образ виртуальной машины.

При изучении представленной темы были проанализированы зарубежные статьи следующих авторов: Бретта Шейверса, Хуана Карлоса Флореса Круса и Трэвиса Аткисона. Специалисты в своих работах освещают, по каким файлам можно обнаружить следы установки и запуска виртуальных машин. Так, Бретт Швейверс повествует о том, что данные следы могут находиться в системных файлах, например, в DLL-файле, в lnk-файлах. Еще один из важных помощников в обнаружении следов виртуальных машин, Бретт Швейверс выделяет реестр: «Реестр почти всегда будет содержать следы установки / удаления программ, а также другие связанные с ними данные, относящиеся к приложениям виртуальной машины» [4].

Авторы Хуан Карлос Флорес Крус и Трэвис Аткисон в своей статье советуют изучать системные файлы, записи в реестре, журналы операционной системы (далее – ОС), системные события. Собирая и анализируя эти данные, эксперт может сказать существовала ли виртуальная машина на компьютере или нет [5].

Новизна данной статьи заключается в разработанной методике по обнаружению следов установки и запуска виртуальной машины Oracle VM VirtualBox в ОС Windows 10. Также в работе освещается какая криминалистически значимая информация может содержаться в файлах *.vbox и *.vdi, и с помощью какого программного обеспечения можно изучить их содержимое.

Цель работы заключается в обнаружении криминалистически значимой информации, оставляемой виртуальными машинами для обеспечения производства судебных компьютерно-технических экспертиз. Отсюда, изначально нужно рассмотреть понятие средств виртуализации и изучить какие следы оставляется виртуальная машина при инсталляции программы и какая криминалистически значимая информация может содержаться в образе.

Виртуализация – это концепция установки операционной системы (далее – ОС) не на физическую аппаратуру, а на виртуальную, которая, в свою очередь, работает на физической платформе [2, стр.15].

Основная *идея* виртуализации – использование одной физической машины для выполнения нескольких виртуальных. Это немного напоминает разбиение одного физического жесткого диска на несколько логических. Виртуализация использует физические устройства машины и предоставляет вместо них виртуальные средства. Например, жесткий диск виртуальной машины – это просто файл в файловой системе физической машины [2, стр.20].

Согласно ГОСТ Р 57429-2017 «Судебная компьютерно-техническая экспертиза. Термины и определения» *виртуальная машина* – это программная среда, которая внутри одной программной и/или аппаратной системы эмулирует работу другой программной и/или аппаратной системы [1].

Для использования виртуальных машин (далее-ВМ) применяются различные программные обеспечения (далее – ПО), наиболее популярные VMware, Microsoft Hyper-V, Oracle VM VirtualBox.

В работе будет рассматриваться ПО Oracle VM VirtualBox. VirtualBox – это программа, которая позволяет на одном компьютере запускать одновременно несколько ОС. Среди этих операционных систем могут быть Linux, Windows, Mac и другие. Сама VirtualBox работает также на различных системах. Основным преимуществом данной ВМ является то, что она является бесплатной программой.

Так как Oracle VM VirtualBox это программа, то она, как и любое программное обеспечение, оставляет следы установки в ОС.

Следы установки программ можно обнаружить в:

– Файлах реестра.

– Каталогах создаваемых VirtualBox.
– Системных каталогах и файлах

Рассмотрим какие следы остаются в файлах реестра.

С использованием файла software, который находится по пути: C:\Windows\System32\config, и ПО MiTeC Windows Registy Recovery возможен анализ данного файла.

Загрузив файл Software, в графе Windows Installation и пункте Installed Software просматриваем список установленных программ на компьютер.

Также одним из важных файлов является NTUSER.DAT – это файл реестра, он содержит в себе информацию о персональных и системных данных пользователя. Данный файл можно обнаружить по пути: C\Users\имя пользователя. Использую программу «Windows Registry Recovery» изучим содержимое файла.

В ходе анализа NTUSER.DAT обнаружена запись об установки ПО VirtualBox в ветви: SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall. Стоит отметить, что данный путь будет размещен только в том случае, если программа установлена на компьютере.

Если же программа удалена, то по пути: Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU можно обнаружить файлы ассоциации. Так как у ВМ есть свои особенности касаемо файлов, которые она создает, именно по этим файлом можно узнать было ли установлено данное ПО или нет. Так, ассоциация файлов – задание соответствия между конкретным типом данных с определённым расширением и программой, которая открывает его по умолчанию.

Oracle VM VirtualBox создает файлы форматом .vdi и .vbox. Если данные файлы присутствуют по указанному пути, то можно предположить, что ВМ устанавливалась на исследуемый компьютер и использовалась пользователем (рис. 1).

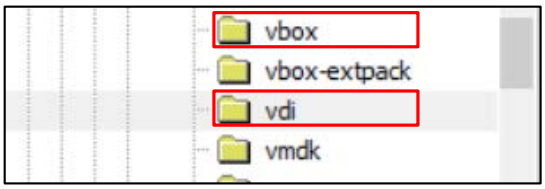

Рис. 1. Фрагмент окна MiTeC Windows Registy Recovery с информацией об ассоциации файлов ВМ VirtualBox

Если же программа удалена, то следы ее использования останутся в реестре по следующим путям:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Classes\AppID

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Classes\ TypeLib

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class – данный путь остается в том случае, если к ВМ подключалось USB-устройство.

Также по умолчанию вышеописанная программа устанавливается в каталог Program Files\Oracle\VirtualBox. Еще ВМ можно обнаружить в каталоге ProgramData. Данный каталог является системной папкой Windows, предназначенной для хранения установочных файлов, данных, файлов параметров программ и приложений, которые есть на компьютере.

Каталоги .VirtualBox и VirtualBox VMs, создающиеся по умолчанию в домашнем каталоге текущего пользователя системы, также могут свидетельствовать об установки ВМ VirtualBox. Зачастую расположение данных каталогов по адресу: C:\Users\username.

Одним из системных каталогов, хранящий временные файлы, в том числе и сведения о запущенных программах, является Prefetch. Каталог Prefetch также содержит данные о программном обеспечение, которое уже удалено на компьютере. С использованием бесплатной утилиты WinPrefetchView, возможно просмотреть этот каталог. Представленная программа показывает какие приложения запускались, а также дату и время их запуска (рис. 2).

После обнаружения того, что ВМ была установлена на исследуемый компьютер или ноутбук, необходимо найти файлы:

• *.vbox – файл настроек, описывающий ВМ и её настройки;
• *.vdi– файл образа диска ВМ.

Под * понимается префикс имени файла как .vdi, так и .vbox, т.е. имя виртуальной машины, заданное пользователем при создании.

В данной работе файлы *.vbox и *.vdi будут рассматриваться с использованием программ:

– WinHex;
– 7-File File Manager версия – 07.21.

Изначально рассмотрим файл .vbox на содержание криминалистически значимой информации. Исследование будет производиться на примере файлов ВМ ОС Windows 10.

Рис. 2. Фрагмент программы WinPrefetchView с информацией о запущенном программном обеспечении

Рис. 3. Окно программы 7-Zip File Manager с информацией о содержимом 1.ntfs

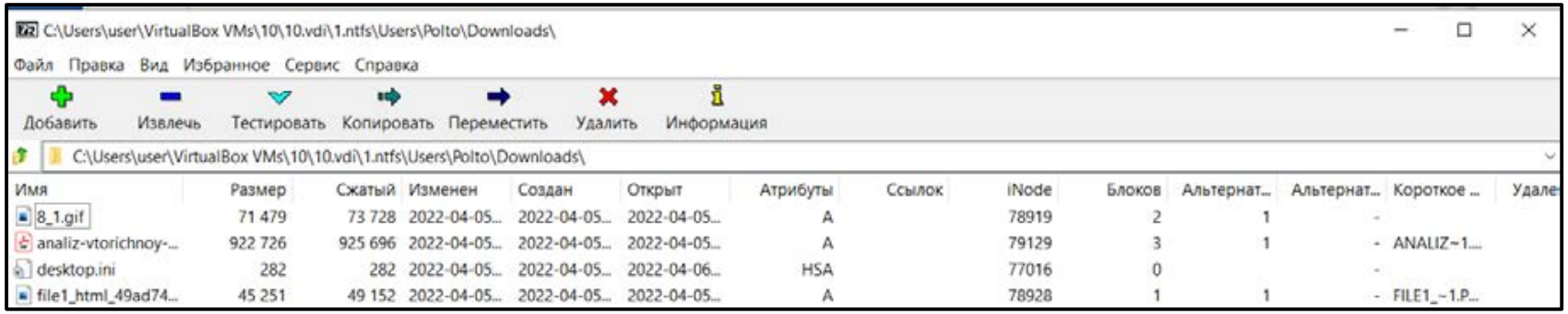

Рис. 4. Окно программы 7-Zip File Manager с информацией о содержимом папки Download

9	9	https://yandex.ru/search/?...	кейлоггер — Яндекс: нашлось ...	2
10	10	https://yandex.ru/search/?...	кейлоггер — Яндекс: нашлось ...	1
11	11	https://www.kaspersky.ru/blog/chto-...	Что такое Кейлоггер? | Блог ...	1
12	12	https://yandex.ru/search/?...	скачать keylogger — Яндекс: нашло...	2
13	13	https://yandex.ru/search/?...	скачать keylogger — Яндекс: нашло...	1
14	14	https://yandex.ru/search/?...	скачать actual keylogger — Яндекс: ...	2
15	15	https://yandex.ru/search/?...	скачать actual keylogger — Яндекс: ...	1

Рис. 5. Окно программы DB Browser for SQLife с информацией о запросах пользователя ВМ

В ходе изучения файла 10.vbox были обнаружены следующие данные:

− Версия ОС и название ВМ;

− Дата и время установки ВМ;

− Размер оперативной памяти;

− Mac-адрес сети. MAC-адрес является уникальным "именем" устройства в сети, однозначно идентифицирующим и отличающим его от остальных адаптеров и узлов. Этот адрес прописывается для каждого сетевого устройства на физическом уровне в памяти самого интерфейса.

С помощью WinHex изучим файл 10.vdi с целью обнаружения интересующей эксперта информации. Так, при анализе содержимого образа найдено установленное вредоносное программное обеспечение – кейлоггер, а именно приложение Actual Keylogger. В образе также содержится ссылка, откуда возможно скачать данное приложение.

Кроме того, стоит отметить, что vdi-файл позволяет запускать образ ВМ. Для реализации запуска необходимо установить ПО VirtualBox, выставить параметры, которые были обнаружены в vbox-файле, подключить vdi – образ и ISO – файл с необходимой ОС. После выполнения всех операций ВМ запустится. Но из-за возможной установки пароля на учётную запись пользователем изучить содержимое ВМ не получится.

Решением данной проблемы служит программа 7-Zip File Manager. С ее помощью можно изучить содержание образа ВМ не запуская. Программа позволяет просматривать содержимое файлов vdi, vhd, vmdk и извлекать их разделы независимо от того, какая файловая система используется [3].

Запустив данную программы, переходим по пути, где у нас расположен образ данных ВМ. Обнаружив файл образа ВМ, его можно разархивировать или открыть в данной программе для дальнейшего изучения. Открывая 10.vdi, видим список разделов с указанием файловой системы:

− 0.ntfs – зарезервированная область (дисковое пространство, предназначенное для хранения обновлений, временных файлов и кэша);

− 1.ntfs – раздел с ОС и пользовательской информацией;

− 2.ntfs – среда восстановления (Windows RE) средство операционной системы Windows для устранения проблем с загрузкой операционной системы, устранения серьезных неполадок в работе ОС;

− 3 – образ Windows 10.

Наиболее интересующий раздел диска – 1.ntfs, так как он содержит пользовательскую информацию (рис. 3).

Изучаем содержимое образа ВМ. В папке загрузки обнаружено два графических изображения и pdf-документ (рис. 4). Данные файлы можно открыть для просмотра.

Также можно просмотреть историю Yandex-браузера с использованием программы DB Browser for SQLife (рис. 5). Для этого в программе 7-Zip File Manager переходим по пути расположения файла с историей браузера, т.е. C:\Users\user\AppData\Local\Yandex\YandexBrowser\UserData\Default, и загружаем History в программе для просмотра баз данных.

Таким образом, при изучении файлов, создаваемых ВМ, было выявлено, что они содержат криминалистически значимую информацию.

Так, файл *.vbox хранит в себе информацию об ОС, дате и времени создания ВМ, MAC-адресе.

А файл *.vdi содержит полностью образ ВМ, включая в себя все программы, установленные на ВМ, пользовательские файлы (документы, изображения, видео и т.д), системные файлы и другое. При этом образ можно запустить с использованием ПО 7-Zip File Manager и полностью изучить его содержимое. Именно поэтому виртуальные машины необходимо исследовать на наличие интересующей следствие информации. Отсюда, следователи могут назначать компьютерно-технической экспертизу с вопросами, касающихся виртуальных машин.

Библиографический список

1. ГОСТ Р 57429-2017 «Судебная компьютерно-техническая экспертиза. Термины и определения». [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200144960 (дата обращения: 26.04.2022).

2. Роджер Диттнер Виртуализация и Microsoft Virtual Server 2005. Полное и исчерпывающее руководство по Virtual Server 2005 / Перевод с английского под редакцией А.П. Караваева. М.: ООО «Бином-Пресс», 2008. 432 с.

3. Открытие файлов с использованием 7-Zip File Manager [Электронный ресурс]. URL: https://goo.su/E1brg7 (дата обращения: 26.04.2022).

4. A discussion of Virtual Machines Related to Forensics Analysis [Электронный ресурс]. URL: https://www.forensicfocus.com/articles/a-discussion-of-virtual-machines-related-to-forensics-analysis/ (дата обращения: 26.04.2022).

5. Digital Forensics on a Virtual Machine. [Электронный ресурс]. URL: http://atkison.cs.ua.edu/papers/ACMSE11_JF.pdf (дата обращения: 26.04.2022).