УДК 343.98

Я. Ю. Коліса
головний судовий експерт

Полтавський науково-дослідний експертно-криміналістичний центр Міністерства внутрішніх справ України

ВІРТУАЛІЗАЦІЯ В КОМП'ЮТЕРНІЙ КРИМІНАЛІСТИЦІ

У статті на основі комп'ютерної віртуалізації розглянуто алгоритми та послідовність дій для проведення «живого» дослідження цифрової інформації в ході судової комп'ютерно-технічної експертизи. В результаті пропонується метод створення віртуальних копій досліджуваних фізичних дисків.

***Ключові слова**: віртуалізація, віртуальна машина, віртуальна копія, фізичний диск.*

Об'єктом судової комп'ютерно-технічної експертизи (далі – СКТЕ) є цифрова техніка (далі – комп'ютер), яка була задіяна в інциденті чи злочині. Пристрій який міг бути використаний при вчиненні фізичного злочину так і стати його метою [1]. Тому при дослідженні комп'ютера доказову цінність несе саме накопичувач інформації (тобто «жорсткий» диск або твердотільний накопичувач, або інший носій цифрової інформації), який міститься в ньому. Саме тому при проведенні СКТЕ демонтується накопичувач (далі – фізичний диск), який підключається до робочої станції експерта (за допомогою пристрою для блокування запису інформації) та створюється повна його копія.

Після виконаних операцій експерт переходить до аналізу цифрової інформації. Але зважаючи на різноманітність завдань та питань, які може ставити ініціатор СКТЕ, не існує єдиного підходу до проведення дослідження накопичувача [1].

Можливий, як «мертвий», так і «живий» аналіз. Перший розуміє дослідження повної копії за допомогою спеціалізованих комп'ютерних програм. Але особливістю даного аналізу є те, що спеціалізовані комп'ютерні програми експерта дозволяють переглядати і аналізувати цифрове наповнення фізичного диску у вигляді деревоподібної структури. Тобто вивчаючи його вміст експерт спостерігає безліч ієрархічно розміщених файлів і каталогів. При живому ж аналізі відбувається пошук інформації з використанням операційної системи (далі – ОС) або інших ресурсів досліджуваного комп'ютера. Але значним недоліком даного підходу є внесення змін в досліджуваний фізичний диск, на якому міститься цифрова інформація.

Вирішенням цього недоліку є використання методу віртуалізації (з англ. virtualization) – створення віртуального, тобто штучного, об'єкта чи середовища [2].

Тобто метою статті є обґрунтування можливості застосування технології віртуалізації при проведенні СКТЕ.

Метод віртуалізації дозволяє використати копію фізичного диску без внесення змін до оригіналу. Тобто за допомогою нього будь-яку систему Windows можна перенести на віртуальну машину [3]. Де віртуальна машина – програмна реалізація комп'ютера (машини), яка виконує програми подібно до справжньої машини [2].

Засобів і прийомів виконання даного методу декілька. В даній статті ми розглянемо один із них, а саме із застосуванням комп'ютерних програм: Paragon GoVirtual 2015 та Oracle VM VirtualBox. Особливістю даних програм є їх безкоштовність.

Далі більш детально розглянемо програму Paragon GoVirtual 2015. Особливістю даної програми є її направленість на ОС Windows. Тобто з будь якими іншими ОС, такими наприклад як Linux або MacOS програма не працює. Для встановлення Paragon GoVirtual 2015 потрібно вказати адрес електронної пошти на яку прийде лист із посиланням на завантаження [4; 5]. Також в листі вказується ключ продукту та серійний номер, які потрібно ввести при встановленні програми.

Основною функцією програми Paragon GoVirtual 2015, яка необхідна для даного методу є копіювання (P2V Copy) цілого фізичного диску або окремого логічного диску (volumes) на нову віртуальну машину [6].

Після того, як фізичний диск був підключений до робочої станції експерта, за допомогою пристрою для копіювання запису, потрібно запустити програму. В меню програми потрібно вибрати «P2V Copy», який активує майстер створення віртуальної копії (далі – майстер).

Далі слідуємо наведеного алгоритму:

1. Вибрати фізичний диск або логічний диск, який потрібно скопіювати.

2. Програма самостійно визначає, яка ОС міститься на вибраному фізичному диску. Експерту ж потрібно вибрати віртуальне програмне забезпечення на яке буде орієнтована майбутня віртуальна копія. Вибір між Oracle VirtualBox і VMware Workstation. Вибираємо першу програму.

3. Визначаємо назву віртуальної машини (Virtual machine name), версію віртуальної машини (Virtual machine version), кількість пам'яті (Memory amount). Всі ці пункти можливо залишити без змін. Змінити можна назву машини та додати або зменшити кількість оперативної пам'яті.

4. Властивості віртуального диску залишаємо без змін.

5. Вибрати каталог в який буде скопійована віртуальна копія. При цьому програма підказує яка ємність диску в гігабайтах потрібна

та чи достатньо її на диску C:\ (за замовчуванням саме на нього програма зберігатиме майбутній диск). Проте є можливість вибрати інший каталог та логічний диск.

6. Відбувається створення віртуальної машини. Цей процес проходить декілька етапів, а саме: підключення віртуального диску (Connect virtual drive), селективне копіювання диску (Selective copy disk), налаштування ОС для завантаження на віртуальне обладнання (Adjust OS to boot on virtual hardware), створення конфігурації віртуальної машини (Create virtual machine configuration), відключення віртуального диску (Disconnect virtual drive).

Далі майстер повідомляє про успішне завершення. Після натиснення кнопки Finish, здійснюється перехід в початкове меню програми.

Інколи бувають випадки невдалого виконання копіювання. Про це майстер повідомляє в процесі та пропонує проігнорувати помилку або припинити процес. Якщо її проігнорувати, то є ймовірність, що потім віртуальна машина все ж таки запуститься. Під помилками ж програма ідентифікує проблеми із завантажувачем ОС, або ж можливе пошкодження файлової системи. В будь-якому випадку дані помилки виникають, наприклад при несподіваному вимкненні живлення, або неправильному вимкненні ОС, коли вона ще не встигла завершити всі процеси. Дана ситуація є достатньо частим явищем для фізичних дисків, які надаються на дослідження СКТЕ.

В результаті процесу в заданій теці створюється два файли наступних типів і розширень: VirtualBox Machine Definition (.vbox) і Virtual Disk Image (.vdi).

Файл vbox – це файл налаштувань (використовується Oracle VM VirtualBox), які зберігаються у форматі XML та містить такі параметри, як ім'я віртуальної машини, тип ОС, оперативна пам'ять. Файли VBOX використовуються для запуску віртуальних машин [7].

Файл vdi є віртуальною копією (образом) скопійованого фізичного диску.

Таким чином копіювання та створення віртуальної копії досліджуваного диску є простим процесом. Майже ніяких змін в налаштуваннях програми, які пропонує майстер не потрібно.

Так як Paragon GoVirtual 2015 вже створив файл налаштувань для Oracle VM VirtualBox [8], то відразу переходимо в теку створення віртуальної копії. За допомогою файлу *.vbox (назва якого відповідає імені віртуальної машини, яка була вказана раніше) запускаємо його на виконання. В результаті віртуальна машина вноситься в список програми Oracle VM VirtualBox.

Далі переходимо в налаштування віртуальної машини та слідуємо наступного алгоритму:

1. У вкладці «Загальне» вказуємо правильну версію ОС, адже при інтеграції віртуальної машини у VirtualBox вона не відповідає дійсній. Якщо це не зробити, при запуску буде отримана помилка.

2. У вкладці «Мережа», прибираємо галочку – Ввімкнути мережевий адаптер. Дана дія потрібна, щоб від'єднати досліджувану систему від мережі Інтернет. Це робиться для ізоляції досліджуваної системи [1].

3. Запускаємо віртуальну машину.

У випадку, коли віртуальна машина не запускається, а видає синій екран або помилку, або ж починає циклічно перезавантажуватися, то потрібно її вимкнути та знову перейти до її налаштувань. Спробувати вимкнути звукову карту, або зі списку «Порядок завантаження» (вкладка «Система») прибрати дисководи для гнучких магнітних дисків (дискет) та оптичних дисків, або ж увімкнути підтримку EFI.

Де EFI – інтерфейс між ОС і мікропрограмами керування складовими частинами комп'ютера, який призначений замінити базову систему введення/виведення (BIOS) [9].

Можуть бути і інші варіанти вирішення даної проблеми, але все це залежить від ситуації.

У випадку відсутності файлу *.vbox його в теці із файлом *.vdi, після створення віртуальної копії програмою Paragon GoVirtual 2015 відразу запускаємо Oracle VM VirtualBox та слідуємо наступному альтернативному алгоритму:

1. Створюємо нову віртуальну машину.

2. Вказуємо назву віртуальної машини, тип та версію ОС, які стали відомі за допомогою Paragon GoVirtual 2015.

3. Задаємо розмір оперативної пам'яті.

4. Далі серед 3-ох пунктів: не додавати віртуальний жорсткий диск, створити віртуальний жорсткий диск та використовувати існуючий файл віртуального жорсткого диску, вибираємо останній. Після цього вказуємо шлях до файлу Virtual Disk Image (.vdi) та натискаємо «Створити».

5. Вибираємо налаштування створеної віртуальної машини та у вкладці Мережа, прибираємо – «Ввімкнути мережевий адаптер».

6. Запускаємо віртуальну машину.

В результаті отримуємо працюючу копію досліджуваного фізичного диску та встановленої на нього ОС. Тепер експерт СКТЕ має можливість провести дослідження не лише методом аналізу «мертвої» системи, але і «живої» ОС.

Таким чином переваги даного методу полягають в наступному:

1. Повторюваність, так як оригінальний фізичний диск не використовується в ході досліджень, а у випадку внесення змін в копію, можливо створити нову віртуальну копію.

2. Візуальність, адже в експерта СКТЕ з'являється можливість наочно побачити внутрішнє цифрове наповнення зі сторони користувача ОС.

3. Не значні затрати часу на створення копії.

До недоліку даного методу можна віднести орієнтованість програми Paragon GoVirtual 2015 тільки на ОС Windows. При дослідженні ж фізичних дисків із інстальованими ОС Linux або MacOS, або ОС на їх базі, необхідне застосування інших методів.

Отже, застосування віртуалізації при проведенні СКТЕ дозволяє розширити можливості дослідження комп'ютерної техніки та аналізу цифрової інформації.

Перелік посилань

1. *Кэрриэ Б.* Криминалистический анализ файловых систем. Санкт-Петербург, 2007. 480 с.: ил.

2. *Віртуалізація* – Вікіпедія [Електронний ресурс]: [Веб-сайт]. Електронні дані. Режим доступу: https://uk.wikipedia.org/wiki/Віртуалізація (дата звернення 21.04.2018). Назва з екрана.

3. *Paragon Go Virtual* 2015 – бесплатная лицензия – Новости и Обзоры [Електронний ресурс]: [Веб-сайт]. Електронні дані. Режим доступу: http://www.comss.info/page.php?al=paragon_go_virtual_2015 (дата звернення 21.04.2018). Назва з екрана.

4. *Download* Paragon Go Virtual 2015 With Free License [Електронний ресурс]: [Веб-сайт]. – Електронні дані. – Режим доступу: https://www.itechtics.com/download-paragon-go-virtual-2015-with-free-license/ (дата звернення 21.04.2018). Назва з екрана.

5. *PARAGON* Software Group [Електронний ресурс]: [Веб-сайт]. Електронні дані. Режим доступу: https://www.paragon-software.com/landing-pages/2015/virtualization-manager-win10/index.html (дата звернення 21.04.2018). Назва з екрана.

6. *Paragon Go Virtual* – Описание продукта [Електронний ресурс]: [Веб-сайт]. Електронні дані. Режим доступу: http://www.paragon.ru/home/go-virtual/ (дата звернення 21.04.2018). Назва з екрана.

7. *VBOX File Extension* – What is a .vbox file and how do I open it? [Електронний ресурс]: [Веб-сайт]. Електронні дані. Режим доступу: https://fileinfo.com/extension/vbox (дата звернення 23.04.2018). Назва з екрана.

8. *VirtualBox* [Електронний ресурс]: [Веб-сайт]. Електронні дані. Режим доступу: http://www.oracle.com/technetwork/ru/servers-storage/virtualbox/overview/index.html (дата звернення 21.04.2018). Назва з екрана.

9. *Установка дистрибутива* на компьютер с EFI | Русскоязычная документация по Ubuntu [Електронний ресурс]: [Веб-сайт]. Електронні дані. Режим доступу: http://help.ubuntu.ru/wiki/установка_дистрибутива_на_ компьютер_с_efi (дата звернення 27.04.2018). Назва з екрана.

ВИРТУАЛИЗАЦИЯ В КОМПЬЮТЕРНОЙ КРИМИНАЛИСТИКЕ

Я. Ю. Колиса

В статье отмечается, что при проведении судебной компьютерно-технической экспертизы важным аспектом является исследование накопителя информации не только как структуры файлов и каталогов. Так как восприятие цифровой информации экспертом и пользователем компьютера отличаются. Пользователь взаимодействует с аппаратной составляющей с помощью буфера, которым является операционная система. Поэтому хоть и исследование файловой структуры с помощью специализированных программных средств более актуально, но взгляд со стороны пользователя не стоит недооценивать. Так как, если поставить себя на место преступника, можно увидеть события его глазами. То же самое происходит в случае с компьютером и установленной на него операционной системой.

То есть в статье предлагается метод исследования накопителя информации «вживую». При этом подвергается изменениям его виртуальная копия. Этот подход позволяет не нарушать главный принцип компьютерной криминалистики, а именно сохранение цифровых следов. И этому же принципу подчиняется вся криминалистика.

Кроме того метод виртуализации позволяет изучить психологию пользователя компьютера. К этому относится, то какие и как расположены ярлыки приложений на рабочем столе, названия папок на логических дисках, логины и пароли которые сохраняют веб-браузеры и т.д. Все это и многое другое говорит о человеке, который пользовался компьютером. И таким образом мы приходим к тому, что компьютерная криминалистика это намного большее, чем просто запустить приложение, отметить нужные галочки или выполнить, какой то алгоритм.

Как итог в статье приводиться метод, который намного расширит компьютерное исследование и, самое главное, позволит затронуть те аспекты, о которых даже не задумывались ранее.

VIRTUALIZATION IN COMPUTER FORENSICS

Y. Kolisa

In the article it is considered that when carrying out the computer-technical expertise an important aspect is the study of the information store not only as a structure of files and catalogs. Since the perception of digital information by an expert and a computer user is different. The user interacts with the hardware component using the buffer, which is the operating system. Therefore, although the study of file structure with the help of specialized software is more relevant, but the view from the user's side should not be underestimated. Since, if you put yourself in the place of a criminal, you can see the events with his eyes. The same happens with the computer and the operating system installed on it.

That is, the article proposes a method for studying the information store «live». At the same time, the virtual copy is being changed. This approach allows not to violate the main principle of computer forensics, namely the preservation of digital tracks. And this same principle is subject to all forensic science.

In addition, the virtualization method allows you to study the psychology of the user of the computer. This applies, then what and how are the shortcuts of applications on the desktop, the names of the folders on the logical disks, the logins and passwords that web browsers store, etc. All this and much more speaks about the person who used the computer. And so we come to the fact that computer forensics is much more than just running the application, ticking the checkboxes or doing something, which is the algorithm.

As a result, the article cites a method that will greatly expand computer research and, most importantly, will allow to touch on aspects that were not even thought of earlier.