Дослідження інформаційного вмісту віртуальних машин, створених за допомогою програмного забезпечення *VMware Workstation*

Іван Старенький,
Одеський НДЕКЦ МВС України, ORCID: https://orcid.org/0009-0004-2271-8512,
e-mail: ivan_starenkii@ukr.net

Розглянуто послідовність дій експерта в дослідженні віртуальної машини, створеної за допомогою програмного забезпечення VMware Workstation, у випадку розподілу віртуального носія інформації на декілька файлів із метою отримання одного суцільного файлу, який надалі може бути досліджений за допомогою спеціалізованого криміналістичного програмного забезпечення.

Ключові слова: VMware Workstation; цифровий носій інформації; образ; копія; монтування; файлова система; операційна система; віртуальна машина.

Information content investigation of virtual machines created using VMware Workstation software

Ivan Starenkiy

The paper outlines the sequence of expert actions while examining a virtual machine which was created with the help of the VMware Workstation software, in case of dividing the virtual storage medium into several files, in order to obtain one complete file, which can be further examined with the help of specialized forensic software.

Keywords: VMware Workstation; digital media storage; image; copy; montage; file system; operating system; virtual machine.

Віртуальна машина (далі — *ВМ*) — це програмне забезпечення (далі — *ПЗ*) або апаратна система, яка емулює апаратне забезпечення персонального комп'ютера (далі — *ПК*) *guest*-платформи за рахунок апаратних можливостей *host*-платформи. До найвідоміших програмних продуктів з організації віртуальних машин належать *VirtualBox* [2], *VMware Workstation* [3], *QEMU* [4], *Hyper-V* [5] та *Proxmox Virtual Environment* [6].

Можливості, які надано користувачам ВМ, дають змогу злочинцям використовувати їх для здійснення протизаконних дій, залишаючись непомітними для органів правопорядку, за умови використання на *host*- та *guest*-платформах відповідного ПЗ із маскування своєї діяльності. Отже, ВМ може бути інструментом у плануванні та здійсненні протизаконних дій.

Саме тому, досліджуючи інформаційне наповнення на накопичувачах інформації під час комп'ютерно-технічних експертиз, у випадку виявлення в пам'яті накопичувача файлів віртуальних машин дослідження цих файлів є необхідним, адже протизаконна діяльність могла вестися у середовищі операційної системи (далі — *ОС*), розгорнутої на базі файлів виявленої віртуальної машини. Далі розглянуто випадок дослідження файлів віртуальної машини, створеної за допомогою ПЗ *VMware Workstation*.

ПЗ *VMware Workstation* під час створення віртуального жорсткого диску нової віртуальної машини дає можливість користувачеві обрати, як його буде створено: одним суцільним файлом або він буде розділений на декілька файлів (див. рис. 1).

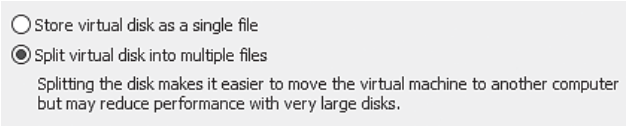

Рис. 1. Меню створення носія інформації в середовищі ПЗ *VMware Workstation*

Послідовність дій експерта в дослідженні файлів ВМ напряму залежить від того, який саме тип віртуального носія інформації буде обрано під час створення ВМ (один файл чи декілька). Якщо під час дослідження інформації в пам'яті об'єкта дослідження буде виявлено один суцільний файл віртуального носія інформації певної ВМ, то дослідження інформації, що містить пам'ять цього файлу, можна проводити відповідно до методик, затверджених Міністерством юстиції України [1].

Якщо віртуальний носій інформації ВМ було створено з розподілом на декілька файлів (див. рис. 2), то експерт має декілька способів для отримання одного суцільного файлу.

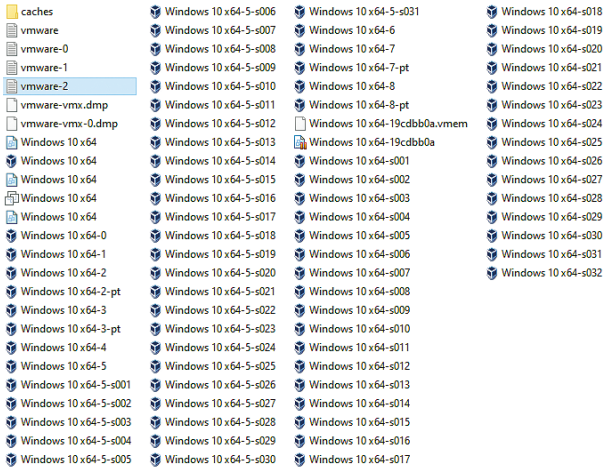

Рис. 2. Конфігураційні файли віртуального носія інформації, створеного за допомогою ПЗ *VMware Workstation*

Перший спосіб конвертації кількох файлів віртуального носія інформації передбачає наявність інстальованого на тестовому ПК експерта (або в середовищі ВМ, яку експерт може використовувати як *guest*-платформу на своєму тестовому ПК) ПЗ *VMware Workstation* та використання терміналу ОС сімейства *Windows* для введення команди:

```
“C:\Program Files(x86)\VMware\VMware
Workstation\vmware-vdiskmanager.exe” -r
“назва_.vmdk” -t 0 “нова_назва_ВМ.vmdk”.
```

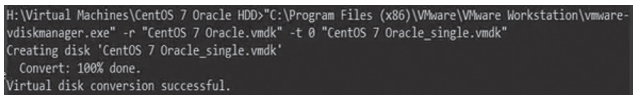

Рис. 3. Приклад успішного виконання команди в середовищі терміналу ОС *Windows*

Другий спосіб передбачає запуск віртуальної машини зі змонтованим *Live*-образом одного з криміналістичних дистрибутивів ОС сімейства *Linux* (наприклад, *Deft* або *Kali*) із подальшим завантаженням в середовищі ВМ криміналістичного дистрибутиву ОС *Linux*. Тоді, використовуючи команду терміналу «*sudo fdisk -l*» або використовуючи ПЗ *GParted* [7], можна визначити перелік носіїв інформації, доступних користувачеві. На рис. 4 наведено, як у середовищі ОС *Linux* інтерпретується носій інформації ВМ, конфігураційні файли якої наведено на рис. 2.

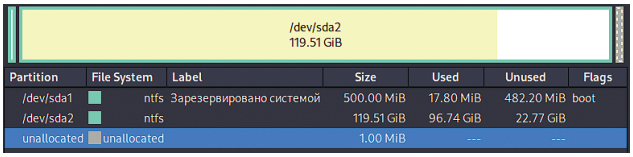

Рис. 4. Інтерпретація файлів віртуального носія інформації в середовищі ОС *Linux*

Інтерпретація в середовищі ОС *Linux* віртуального диску як блочного приладу (*Block Device*) дає можливість створити його побітові копії на підключений до тестового ПК експерта зовнішній носій інформації, який також можна підключити до запущеної ВМ у середовищі ОС Linux, використовуючи команду терміналу «*sudo dd if=/dev/sda of=/місце_збереження/назва_файлу.dd bs=64k conv=noerror,sync*» або скориставшись ПЗ Guymager [8], яке також виконує цю команду із застосуванням графічного інтерфейсу.

Отриманий файл із розширенням «**.dd*», який бути побітовою копією носія інформації ВМ, у подальшому можна дослідити відповідно до методик, затверджених Мін’юстом України.

Кожний із розглянутих методів дає змогу отримати один файл як вихідний, що фактично є побітовою копією інформаційного вмісту віртуального носія інформації, який містить кілька конфігураційних файлів.

Перелік джерел посилання

1. Методика дослідження інформації на жорстких дисках [10.9.01].
2. Oracle VM VirtualBox. URL: https://www.virtualbox.org/ (дата звернення: 09.03.2023).
3. VMware Workstation. URL: https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html/ (дата звернення: 09.03.2023).
4. QEMU. URL: https://www.qemu.org/ (дата звернення: 09.03.2023).
5. Hyper-V. URL: http://www.microsoft.com/hyper-v/ (дата звернення: 09.03.2023).
6. Proxmox Virtual Environment. URL: https://www.proxmox.com/en/proxmox-ve/ (дата звернення: 09.03.2023).
7. GParted. URL: https://gparted.org/ (дата звернення: 09.03.2023).
8. Guymager. URL: https://guymager.sourceforge.io/ (дата звернення: 09.03.2023).