УДК 343.98

Старенький Іван Володимирович, судовий експерт сектору досліджень телекомунікаційних систем та засобів лабораторії досліджень об’єктів інформаційних технологій Одеського науково-дослідного інституту судових експертиз Міністерства юстиції України
e-mail: ivan_starenkii@ukr.net

Донченко Олександра Ігорівна, судовий експерт лабораторії досліджень об’єктів інформаційних технологій Одеського науково-дослідного інституту судових експертиз Міністерства
e-mail: donchenko2707@gmail.com

ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОГО НАПОВНЕННЯ ПОБІТОВОЇ КОПІЇ НОСІЯ ЦИФРОВОЇ ІНФОРМАЦІЇ ШЛЯХОМ УТВОРЕННЯ ЙОГО VMDK-КОПІЇ

STUDY OF INFORMATION CONTENT OF A BIT-BY-BIT COPY OF A DIGITAL MEDIA BY CREATING ITS VMDK COPY

Анотація. У роботі описано послідовність дій задля створення VMDK-посилання на примонтований образ побітової копії цифрового носія інформації з метою подальшого віртуалізування утвореного VMDK-файлу в середовищі програмного забезпечення “Oracle VirtualBox”.

Ключові слова: цифровий носій інформації, образ, копія, монтування, файлова система, операційна система, віртуальна машина.

Abstract. The paper describes the sequence of actions to create a VMDK-link to the mounted image of the winning copy of the digital media, in order to further virtualize the resulting VMDK-file in the software environment “Oracle VirtualBox”.

Key words: digital media storage, image, copy, mount, file system, operating system, virtual machine.

Алгоритм дослідження інформаційного наповнення цифрових носіїв інформації, таких як жорсткі диски, SSD-накопичувачі, USB-накопичувачі, проводиться відповідно до методик, затверджених Міністерством юстиції України.

Дослідження цифрових носіїв інформації проводиться в такий спосіб, щоб запобігти внесенню будь-яких змін у файлову структуру носія інформації. Із цією метою під час дослідження носіїв інформації можуть використовуватися декілька методів, що запобігають внесенню змін в інформаційне наповнення цифрового носія інформації, а саме: апаратні блокіратори запису, блокування запису на рівні ядра операційної системи.

Одним з етапів комп’ютерно-технічного дослідження є створення побітової копії цифрового носія інформації, або образу (наприклад, з розширенням «*.dd»), який зазвичай можна створити в середовищі операційної системи Linux.

Значним плюсом у подальшому дослідженні побітової копії є можливість віртуалізації операційної системи, що міститься в пам’яті цифрового носія інформації. Для віртуалізації побітової “dd” копії цифрового носія інформації гарним інструментом є безкоштовне програмне забезпечення (далі – ПЗ) “Oracle VirtualBox” [2], у середовищі якого можна провести різноманітні налаштування, які будуть відповідати налаштуванням досліджуваного об’єкта та його носія (або носіїв) інформації.

Однак програмне забезпечення “Oracle VirtualBox” не призначене для роботи з образом “dd” та вимагає повного доступу (читання й запису) інформації. Виходом із цієї ситуації є використання додаткового програмного забезпечення для монтування “dd”-образу, наприклад “AccessData FTK Imager” [3]. “AccessData FTK Imager” дає змогу монтувати “dd” у режимі повного доступу (читання й запису), при цьому для забезпечення незмінності вихідного образу створюється спеціальний файл для збереження змін. З використанням внутрішніх команд “Oracle VirtualBox” зі змонтованого образу можна створити VMDK [4] файл-посилання. Для зручності рекомендується оформити команду створення VMDK-файлу у вигляді batch-файлу [5].

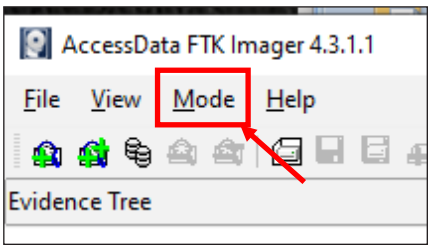


Рис. 1. Меню монтування образу в ПЗ “AccessData FTK Imager”

Опишемо більш детально алгоритм дій, що наведені в попередньому абзаці. Після створення “dd” образу носія інформації в ПЗ “AccessData FTK Imager” виконується послідовність дій із монтування створеної “dd” копії цифрового носія інформації, яка продемонстрована на рисунках 1–4.

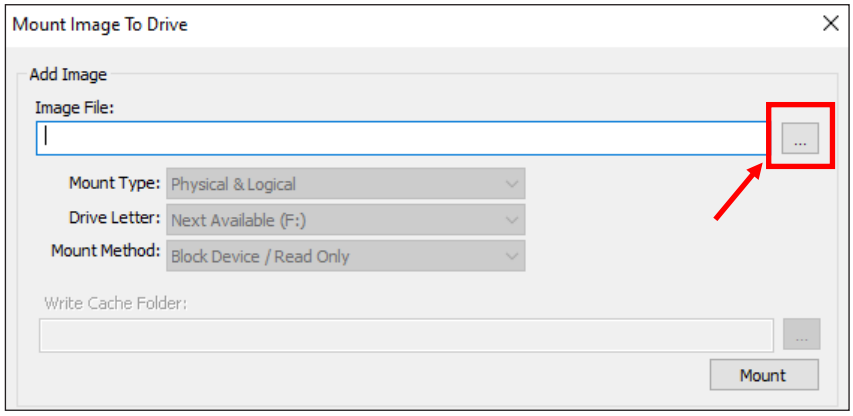


Рис. 2. Фрагмент вікна вибору образу для монтування в ПЗ “AccessData FTK Imager”

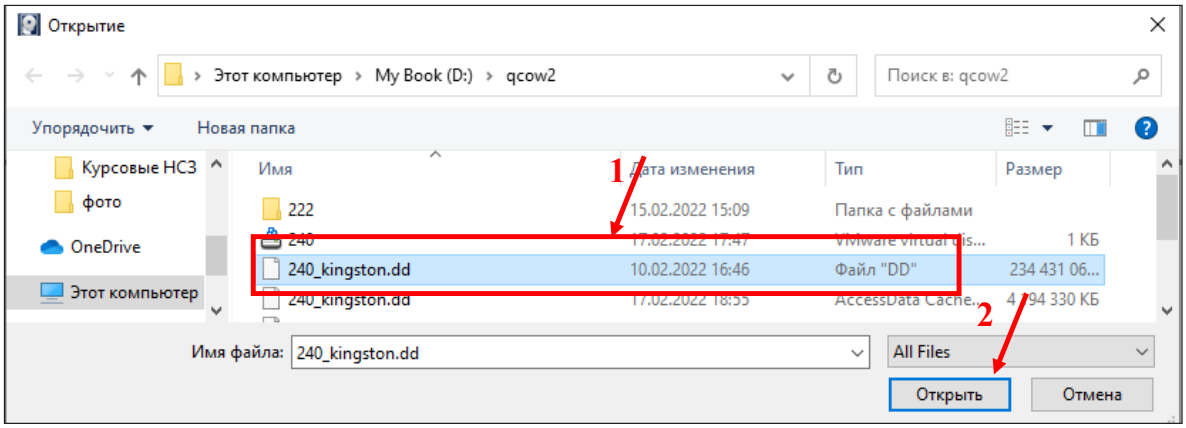


Рис. 3. Вибір конкретного образу для монтування в ПЗ “AccessData FTK Imager”

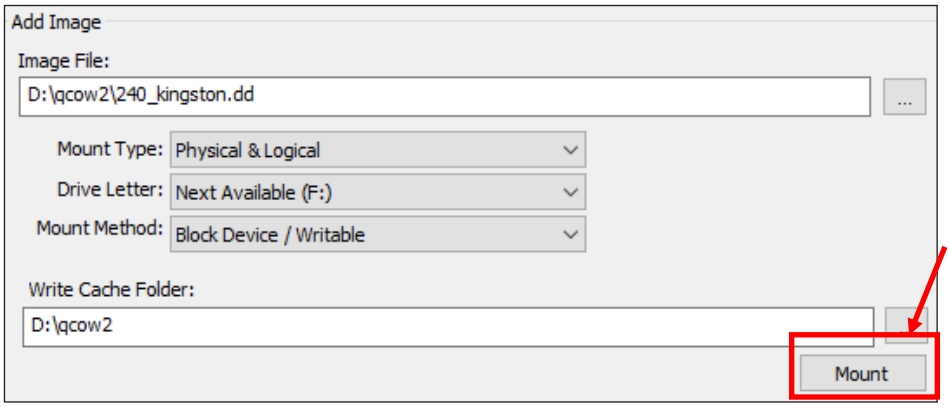


Рис. 4. Налаштування монтування вибраного образу в ПЗ “AccessData FTK Imager”

Так, після виконання послідовності дій, продемонстрованих на рисунках 1–4, змонтований образ “dd” копії носія інформації в ПЗ “AccessData FTK Imager” отримує певний ідентифікатор носія інформації в операційній системі (PhysicalDrive3) та логічну літеру розділу в операційній системі користувача (G) (див. рис. 5, 6).

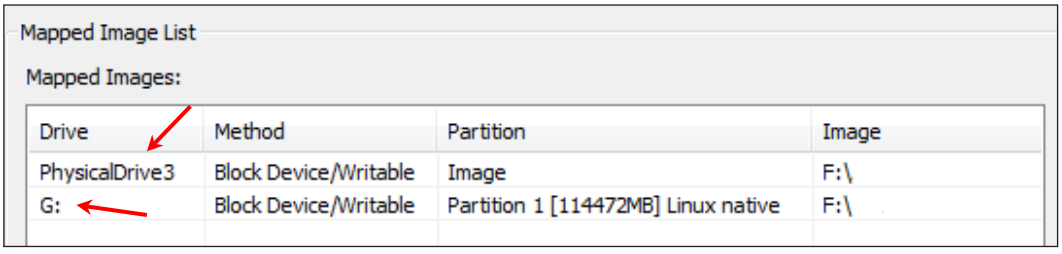


Рис. 5. Фрагмент вікна ПЗ “AccessData FTK Imager”

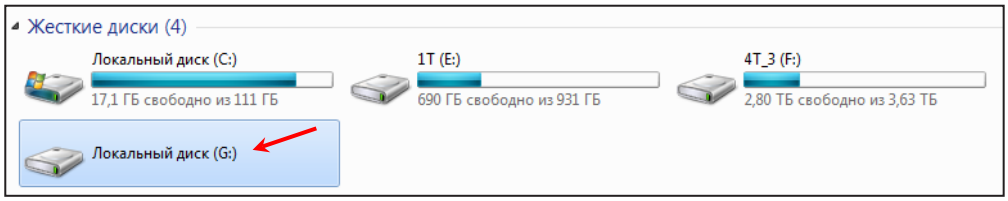


Рис. 6. Вікно доступних носіїв інформації

Значення ідентифікатора носія інформації в операційній системі та логічна літера розділу можуть змінюватися залежно від наступних вільних у черзі ідентифікаторів носія інформації та логічної літери розділу операційної системи в момент монтування образу “dd” копії цифрового носія інформації.

Наступним кроком є генерування batch-файлу для створення VMDK файлу-посилання на примонтований розділ файлової структури “dd” побітової копії цифрового носія інформації.

Приклад вмісту такого batch-файлу наведено нижче:

```
«C:\Program Files\Oracle\VirtualBox\VBoxManage.exe» internalcommands createrawvmdk -filename F:\120.vmdk -rawdisk \\.\PhysicalDrive3
pause
```

Такий batch-файл у майбутньому потребує певних налаштувань, зокрема: замість “PhysicalDrive3” варто вказувати саме той фізичний пристрій, до якого змонтовано образ, а замість “F:\120.vmdk” – шлях та ім’я файлу, які бажаєте отримати.

На рисунках 7, 8 зображено властивості утвореного VMDK файлу-посилання та його вибір у середовищі ПЗ “Oracle VirtualBox”.

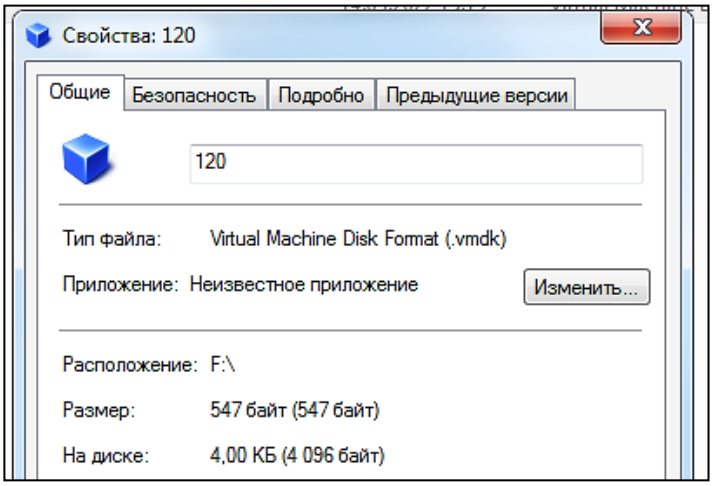


Рис. 7. Фрагмент вікна властивостей VMDK файлу-посилання

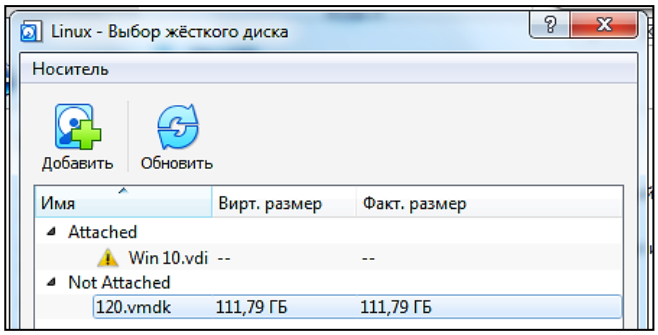


Рис. 8. Фрагмент вікна ПЗ “Oracle VirtualBox”

Таким чином, з використанням ПЗ “AccessData FTK Imager” та VMDK файлу-посилання на примонтований в “AccessData FTK Imager” розділ файлової структури за допомогою ПЗ “Oracle VirtualBox” можна запустити віртуальну машину на основі операційної системи з файлової структури побітової “dd” копії цифрового носія інформації.

Однак реалізація вищезазначеного методу можлива лише за безпосереднього використання ПЗ “AccessData FTK Imager” або його аналогів. Тому доцільно розглянути ще один метод створення VMDK-файлу на основі побітової “dd” копії цифрового носія інформації, і в цьому випадку новоутворений VMDK-файл уже не буде посиланням на примонтований розділ файлової структури.

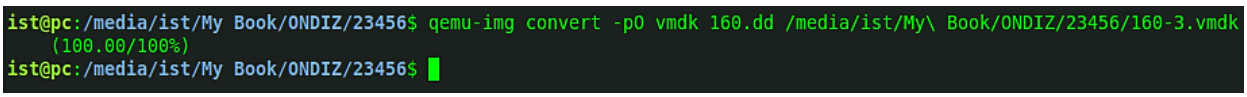
Так, у середовищі операційної системи сімейства “Linux” за допомогою термінальної команди можна конвертувати “dd” образ побітової копії цифрового носія інформації в будь-який образ QEMU-формату [6] (у тому числі VMDK), наприклад:

```
qemu-img convert -pO vmdk /path/disk.dd /path/disk.vmdk
```

У цьому рядку термінальної команди:

- “-p” відображує прогрес конвертації, що дуже зручно дає можливість для відстеження процесу конвертації;
- “O vmdk” вказує на вихідний формат сконвертованого файлу;
- “/path/disk.dd” позначає шлях до “dd” файлу образу побітової копії цифрового носія інформації;
- “/path/disk.vmdk” позначає шлях розміщення сконвертованого VMDK-файлу.

Так, на рисунку 9 наведено результат роботи цієї термінальної команди з конвертації побітової “dd” копії цифрового носія інформації, результатом якої є файл “160-3.vmdk”.



а)

б)

Рис. 9. Результат роботи термінальної команди з конвертації побітової “dd” копії цифрового носія інформації

Мінусами такого методу є витрата часу на конвертацію “dd”-образу у VMDK-файл та розмір вихідного сконвертованого файлу. Проте безпосереднім плюсом цього методу є те, що він дає можливість сконвертувати “dd”-образ побітової копії цифрового носія інформації в один із підтримуваних QEMU-образів (raw,

cloop, cow, qcow, qcow2, vmdk, vdi, vhdx, vpc) на робочій станції, що не потребує великих робочих потужностей, і продовжити дослідження новоутвореного сконвертованого файлу вже на більш потужній робочій станції без попереднього монтування “dd”-образу побітової копії цифрового носія інформації, що дає змогу паралельно задіяти “dd”-образ для інших досліджень у межах виконання експертного дослідження.

Перелік використаних джерел:

1. Методика дослідження інформації на жорстких дисках (№ 10.9.01), внесена до Реєстру методик проведення судових експертиз 5 червня 2009 р. / Харківський науково-дослідний інститут судових експертиз Міністерства юстиції України. URL: https://rmpse.minjust.gov.ua/page/9 (дата звернення: 18.04.2022).

2. VirtualBox. URL: https://www.virtualbox.org/ (date of access: 18.04.2022).

3. FTK Imager. AccessData. URL: https://accessdata.com/product-download/ftk-imager version-4-5 (date of access: 18.04.2022).

4. VMDK. *Вікіпедія: вільна енциклопедія*. URL: https://ru.wikipedia.org/wiki/ VMDK (дата звернення: 18.04.2022).

5. Пакетний файл. *Вікіпедія: вільна енциклопедія*. URL: https://uk.wikipedia.org/wiki/Пакетний_файл (дата звернення: 18.04.2022).

6. QEMU / Images. *Wikibooks*. URL: https://en.wikibooks.org/wiki/QEMU/Images (date of access: 18.04.2022).

References:

1. Kharkiv Research Institute of Forensic Expertise of the Ministry of Justice of Ukraine (2009). Metodyka doslidzhennia informatsii na zhorstkykh dyskakh (№ 10.9.01), vnesena do Reiestru metodyk provedennia sudovykh ekspertyz 5 chervnia 2009 r. [Methodology for the study of information on hard drives (№ 10.9.01), entered into the Register of Forensic Examination Methods on June 5, 2009]. Retrieved from: https://rmpse.minjust.gov.ua/page/9 [in Ukrainian].

2. N. a. (n. d.). VirtualBox. Retrieved from: https://www.virtualbox.org/ [in English].

3. N. a. (n. d.). FTK Imager. *AccessData*. Retrieved from: https://accessdata.com/product-download/ftk-imager-version-4-5 [in English].

4. N. a. (n. d.). VMDK. *Wikipedia: the free encyclopedia*. Retrieved from: https://ru.wikipedia.org/wiki/VMDK [in Ukrainian].

5. N. a. (n. d.). Paketnyi fail [Batch file]. *Wikipedia: the free encyclopedia*. Retrieved from: https://uk.wikipedia.org/wiki/Пакетний_файл [in Ukrainian].

6. N. a. (n. d.). QEMU / Images. *Wikibooks*. Retrieved from: https://en.wikibooks.org/wiki/QEMU/Images [in English].