УДК 004.42

[0000-0002-4937-747X] **В. В. Павлов,** *судовий експерт*
*відділу комп'ютерно-технічних та телекомунікаційних досліджень Черкаського НДЕКЦ МВС*
Черкаський науково-дослідний експертно-криміналістичний центр МВС України
вул. Пастерівська, 104, м. Черкаси, 18001, Україна

# ПРАКТИКА ЗАВАНТАЖЕННЯ ОПЕРАЦІЙНОЇ СИСТЕМИ, ЩО МІСТИТЬСЯ НА ЦИФРОВОМУ НОСІЇ ІНФОРМАЦІЇ В СЕРЕДОВИЩІ ВІРТУАЛЬНОЇ МАШИНИ

*Правильність висновку проведеного дослідження найкраще перевіряється повторним дослідженням та порівнянням отриманих результатів. У криміналістичних видах експертиз дуже великий відсоток видів досліджень, в яких застосування руйнуючих методів є необхідним. Комп'ютерно-технічна експертиза відрізняється від багатьох інших видів досліджень наявністю мінімальної кількості методів, що призводять до руйнування або зміни інформаційного вмісту речового доказу після проведеного дослідження. При дослідженні носіїв інформації виконавцю (експерту) надається унікальна можливість скопіювати увесь інформаційний вміст накопичувача інформації на свою робочу станцію для подальшого дослідження. Тим самим відкривається можливість проведення самоконтролю – копіювання інформаційного вмісту та застосування до нього програмних засобів можна провести декілька разів, чим можливо підтвердити правильність зробленого висновку.*

*Судові експерти в практиці виконання комп'ютерно-технічної експертизи фізично не стикаються з власником наданого на дослідження носія, але в ході дослідження інформаційного вмісту мимоволі складається деяке уявлення про людину (психологічний портрет), що займалася наповненням цього інформаційного вмісту, особливо, коли на носії інформації міститься операційна система. В операційній системі та в прикладному програмному забезпеченні, що може в ній міститися, зберігається дуже багато інформації про свого користувача. Прикладне програмне забезпечення може зберігати в собі особисті налаштування користувача, і при його дослідженні «ззовні», тобто з іншої операційної системи, ці особисті налаштування найчастіше не видно або досліджуване програмне забезпечення взагалі не зможе завантажитись в середовищі іншої операційної системи.*

***Ключові слова**: віртуальна машина, Virtual Box, накопичувач інформації, операційна система, комп'ютерно-технічна експертиза.*

**Вступ.** З практики виконання комп'ютерно-технічних експертиз варто зауважити, що сам по собі цифровий носій інформації – доволі крихка річ, а особливо, якщо він є речовим доказом. На цифровий носій, що був вилучений як речовий доказ [1], ще до проведення безпосередніх процесуальних процедур можуть вплинути різні фактори руйнівного характеру. Тому при проведенні процесуальної дії (огляді або комп'ютерно-технічній експертизі) цифровий носій інформації як речовий доказ буде підключено до робочої станції експерта, виконавцю слід дотримуватись обережності при проводженні всіх маніпуляцій та процедур.

Сучасні цифрові носії інформації хоча фізично й невеликі за розмірами, але можуть містити дуже цінну інформацію для подальшого розслідування [2], яка може невиправно вплинути на долю людини, будь то обвинувачений чи потерпілий.

Зазвичай програмні засоби, що використовуються в комп'ютерно-технічній експертизі, передбачають проведення дослідження без завантаження самої операційної системи, тобто ззовні. Для розуміння причин цього процесу треба знати, що на професійному рівні дослідження в комп'ютерній криміналістиці використовуються пристрої апаратного блокування запису (пристрої, що забезпечують читання, у той же час перешкоджають внесенню жодних змін в інформаційний вміст носія інформації). В експертних установах МВС України в розпорядженні експерта є набір пристроїв апаратного блокування запису (рисунок 1).


DOI:10.24025/2306-4412.1.2020.193369


**Рисунок 1 – Експертна валіза з набором пристроїв апаратного блокування запису**

Необхідність використання пристроїв апаратного блокування запису обумовлена тим, що після підключення до робочої станції експерта носія інформації, який підлягає дослідженню, операційна система робочої станції при першій ініціалізації нового пристрою автоматично вносить деякі зміни (статистичного характеру) в інформаційний вміст підключеного носія інформації [3].

Повертаючись до питання крихкості носіїв інформації, для забезпечення повного та всебічного дослідження, на яке витрачається чимало годин, а також з метою збереження об'єкта і забезпечення можливості, за необхідності, повторного дослідження використовується не безпосередньо пристрій накопичувача інформації, а його виготовлена цифрова побітова копія (Raw (dd) (далі –файл-образ). RAW (англ. raw – сирий, необроблений) – вид даних, який містить необроблені (або оброблені мінімальною мірою) дані, що дає змогу уникнути втрат інформації, і не має чіткої специфікації. У таких файлах міститься інформація, що не інтерпретована під жодний формат, тобто у «первозданному» вигляді. У випадку з носіями інформації створений Raw образ – це повна побітова копія його інформаційного вмісту. Поширеними в комп'ютерній криміналістиці програмними засобами для створення файл-образу накопичувача інформації та його подальшого дослідження є Access Data FTK Imager [4], X-Ways Forensic. В операційних системах сімейства Linux для побітного копіювання використовується утиліта «dd» [5]. У процесі дослідження виготовлений файл-образ носія інформації зберігається на дисковому просторі робочої станції експерта.

**Аналіз останніх досліджень та публікацій.** Науково-теоретичним підґрунтям написання статті стали праці науковців: Н. Н. Федотова, О. К. Гультяєва, Андре Лейбовича, Роберта Коллінса, Тоні Робертсона та інших, які в своїх працях торкались проблем віртуалізації з подальшим дослідженням носіїв інформації та операційних систем.

**Метою статті** є вирішення питання підготовки та завантаження операційної системи, що міститься на носії інформації, за допомогою програмного забезпечення Virtual Box.

**Наукова новизна** роботи полягає в розширенні області використання віртуальної машини при проведенні криміналістичних досліджень.

На практиці проведення криміналістичного дослідження комп'ютерної техніки експерту для наочності та розуміння напряму, в якому проводити подальше дослідження, які програмні засоби використовувати, якими методами користуватися, необхідно побачити, як операційна система досліджуваного носія інформації виглядає «зсередини», тобто виникає необхідність у завантаженні її у віртуальному середовищі – віртуальній машині.

**Виклад основного матеріалу.** Віртуальна машина – модель обчислювальної машини, створеної шляхом віртуалізації обчислювальних ресурсів: процесора, оперативної пам'яті, пристроїв зберігання та вводу і виводу інформації [6].

Віртуальні машини використовуються, насамперед, для тестування операційних систем та інших програмних продуктів. В криміналістиці запуск операційної системи досліджуваного носія інформації в середовищі операційної системи дає можливість детальніше дослідити операційну систему і дати якісний висновок з поставлених питань. На практиці найпопулярніші програмні засоби – віртуальні машини: Oracle Virtual Box; VMware Workstation; Microsoft Virtual PC тощо.


DOI:10.24025/2306-4412.1.2020.193369

У статті мова піде саме про Oracle Virtual Box (далі – Virtual Box).

Virtual Box – це програма віртуалізації для операційних систем, розроблена німецькою фірмою Innotek, нині належить Oracle Corporation. Virtual Box встановлюється на наявну операційну систему, яка називається «хостовою», всередину цієї програми встановлюється інша операційна система, яку називають «гостьовою» операційною системою.

Перевагою програмного забезпечення Virtual Box є кросплатформеність, підтримка різних форматів образів і вільне використання, тобто це програмне забезпечення є безкоштовним [7].

Базові налаштування та інсталяція нової операційної системи у віртуальне середовище VirtualBox не вимагають від користувача спеціальної підготовки та спеціальних знань (рисунок 2).

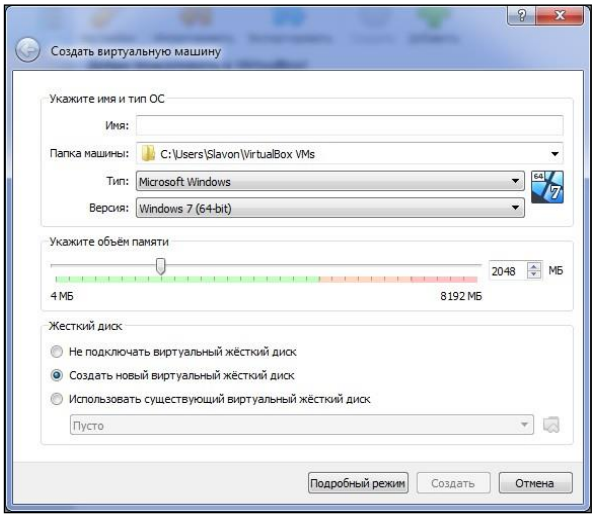


**Рисунок 2 – Вікно створення нової віртуальної машини у Virtual Box**

Проблеми виникають саме з процедурою запуску вже існуючої операційної системи, що інстальована на носій інформації. Все більше ускладнень виникає з завантаженням операційних систем останніх релізів. Основною причиною тому є деяка особливість сучасних операційних систем, особливо операційних систем сімейства Windows. У процесі завантаження сучасні операційні системи обов'язково потребують можливості внесення статистичних змін в інформаційний вміст накопичувача інформації, з якого відбувається завантаження, що є неприйнятним у криміналістичному дослідженні. За відсутності цієї можливості операційна система виведе повідомлення про помилку, процес завантаження операційної системи буде перервано.

Як вже було зазначено, для подальшого дослідження оптимальним форматом для зберігання файлів-образів носіїв інформації є Raw [8]. За замовчуванням, віртуальні машини не розпізнають файлів-образів Raw, у тому числі й Virtual Box.

Програмне забезпечення Virtual Box розпізнає такі формати:

- **VMDK (*.vmdk)** Virtual Machine Disk – формат, спочатку розроблений для файлів-образів програмного забезпечення VMware. Специфікація була закритим вихідним кодом, але нині стала відкритим форматом, який повністю підтримується VirtualBox. VMDK дає можливість розбивати себе на кілька файлів по 2 Гб. Ця функція особливо корисна, коли необхідно зберегти віртуальну машину на комп'ютерах, які не підтримують дуже великі файли;
- **VDI (*.vdi)** Virtual Disk Image – формат, який є власним стандартом VirtualBox. Нові віртуальні машини, що створюються в програмному забезпечені VirtualBox, зберігаються у форматі .vdi;
- **VHD (*.vhd)** Virtual Hard Disk – формат для файлів-образів програмного забезпечення Virtual PC;
- **Parallels (*.hdd)** Hard Disk File – формат для файлів-образів програмного забезпечення Parallels Desktop;
- **QED (*.qed)** QEMU enhanced disk – формат для файлів-образів програмного забезпечення QEMU;
- **QCOW (*.qcow *.qcow2)** QEMU Copy-On-Write – формат для файлів-образів програмного забезпечення QEMU;
- **VHDX (*.vhdx)** Virtual Hard Drive File – спеціально розроблений формат файлів-образів для операційних систем Windows [9].

Для прикладу, візьмемо файл-образ, який було створено з накопичувача інформації на жорстких магнітних дисках (Seagate ST380815AS) (рисунок 3).


DOI:10.24025/2306-4412.1.2020.193369


**Рисунок 3 – Вигляд накопичувача інформації на жорстких магнітних дисках**

Для створення файлу-образу було застосовано програмне забезпечення Access Data FTK Imager. Аналогічно до інформаційного вмісту накопичувача інформації, отриманий файл-образ має розмір 74,5 Гб (рисунок 4).

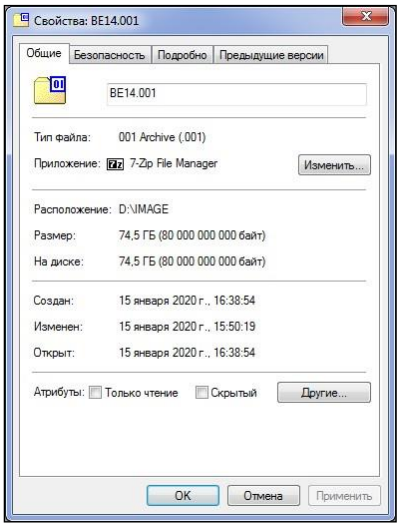


**Рисунок 4 – Властивості створеного файлу-образу накопичувача інформації**

Як показує власний досвід, конвертувати формат Raw у формат, що підходить VirtualBox, відомими засобами часто не видається можливим та й імовірність отримання непрацездатного образу є надзвичайно великою.

Ця проблема вирішується за допомогою утиліти V Box Manage, що входить у програмний пакет Virtual Box. За допомогою V Box Manage можна створити додатковий файл конфігурації до образу носія Raw у форматах vdi або vmdk. Таким чином, Virtual Box через створений файл конфігурації може звертатися та читати необхідний файл-образ носія інформації. В графічному інтерфейсі програмного забезпечення Virtual Box викликати утиліту V Box Manage для створення цього файлу конфігурації неможливо. Звернутися до V Box Manage можливо лише через командний рядок операційної системи [10].

Першочергово в процесі створення файлу конфігурації потрібно в командному рядку за допомогою команди «cd» здійснити перехід до кореневого каталогу, в якому інстальований VirtualBox (за замовчуванням – cd c:\Program Files\Oracle\VirtualBox).

У кореневому каталозі звертаємось до файлу «VBoxManage.exe» командою для створення файлу формату vmdk та зазначенням місця знаходження файлу-образу носія (VBoxManage.exe internalcommands creat-?rawvmdk -filename "шлях розташування\назва файлу.vmdk" -rawdisk "шлях розташування\назва файлу.001").

Відмінність цієї команди для виконання її в різних сімействах операційних систем (Windows, Linux, Mac OS X) полягає в принципі зазначення розташування шляхів до потрібних файлів.

Повідомлення про вдале виконання команди виглядає наступним чином: «RAW host disk access VMDK file шлях розташування\назва файлу .vmdk created successfully» (рисунок 5).

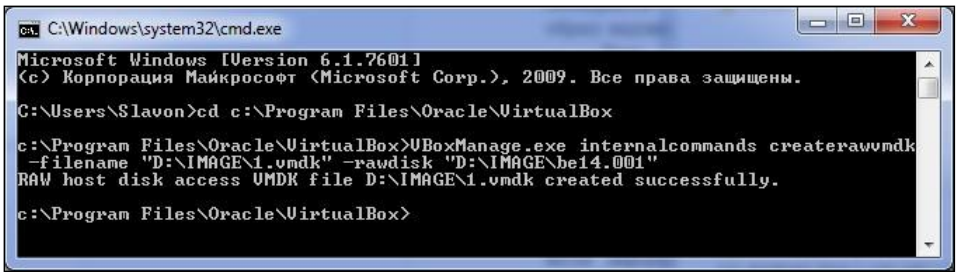


**Рисунок 5 – Вигляд командного рядка після вдалого виконання команди**


DOI:10.24025/2306-4412.1.2020.193369

Після вдалого виконання команди за вказаним у команді шляхом буде створено файл конфігурації з розширенням vmdk (рисунки 6, 7).

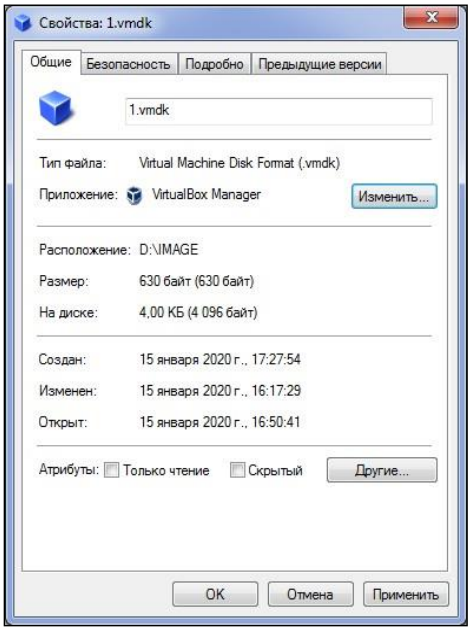


**Рисунок 6 – Властивості файлу конфігурації 1.vmdk**

```
# Disk DescriptorFile
version=1
CID=cdca3e2d
parentCID=ffffffff
createType="fullDevice"

# Extent description
RW 156250000 FLAT "BE14.001" 0

# The disk Data Base
#DDB

ddb.virtualHWVersion = "4"
ddb.adapterType="ide"
ddb.geometry.cylinders="16383"
ddb.geometry.heads="16"
ddb.geometry.sectors="63"
ddb.uuid.image="5993a01f-f7da-490a-a7b7-a4413a55d711"
ddb.uuid.parent="00000000-0000-0000-0000-000000000000"
ddb.uuid.modification="c1bb8ae1-33b8-44b6-92f2-4c7a553de5df"
ddb.uuid.parentmodification="00000000-0000-0000-0000-000000000000"
ddb.geometry.biosCylinders="1024"
ddb.geometry.biosHeads="255"
ddb.geometry.biosSectors="63"
```

**Рисунок 7 – Інформаційний вміст файлу 1.vmdk**

Вказавши цей файл у VirtualBox як файл-образ носія інформації, отримуємо можливість підключати зроблений раніше файл-образ та завантажувати наявну на ньому операційну систему.

Звертаємо увагу, що сам файл конфігурації має розмір до 1 Кб, але після підключення його у Virtual Box фактичний розмір вказується файлу-образу (74,51 Гб) (рисунок 8).

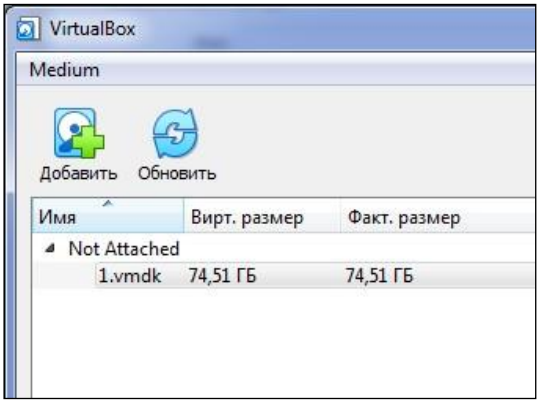


**Рисунок 8 – Вигляд підключеного файлу-образу через файл конфігурації**

**Висновки.** Розглянуто метод завантаження операційної системи, що міститься на цифровому носії інформації в середовищі віртуальної машини за допомогою програмного забезпечення Oracle VirtualBox.

Запропонований метод має такі переваги: по-перше, економія часу; після створення файлу-образу повторне створення файлу-образу безпосередньо під ту чи іншу віртуальну машину може займати кілька годин, тоді як процес створення файлу конфігурації vmdk займає лічені хвилини. По-друге, економія дискового простору, файл-конфігурації vmdk займає лише кілька Кб дискового простору, тоді як створення додаткового файлу-образу накопичувача інформації займає досить багато місця. По третє, файл-образ можна створити майже стосовно кожного носія інформації, а відповідно вже до нього можна створити файл конфігурації та провести завантаження у віртуальному середовищі.

### Список використаних джерел

[1] Кримінально-процесуальний кодекс України. Речові докази, ст. 98. Редакція від 16.01.2020. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/ show/4651-17

[2] Б. Б. Теплицький та ін., "Загальний аналіз та кримінально-правова характеристика складів злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж електрозв'язку" – розділ 2, у *Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів),*


DOI:10.24025/2306-4412.1.2020.193369

*систем та комп'ютерних мереж і мереж електрозв'язку*. Київ, 2019, с. 26-28.
[3] Б. Кэрриэ, "Снятие данных с жесткого диска" – глава 3, в *Криминалистический анализ файловых систем*. Санкт-Петербург, 2007, с. 68-71.
[4] С. С. Бартащук, Р. Н. Дерій, та М. О. Герасименко, "Програмне забезпечення для дослідження носіїв інформації" – розділ 4, у *Проведення комп'ютерно-технічних досліджень носіїв цифрової інформації*. Київ, 2010, с. 21-22.
[5] dd (програма). Матеріал з Вікіпедії – вільної енциклопедії. [Електронний ресурс]. Режим доступу: https://ru.wikipedia.org/wiki/Dd
[6] Віртуальна машина. Матеріал з Вікіпедії – вільної енциклопедії. [Електронний ресурс]. Режим доступу: https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D1%80%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%BC%D0%B0%D1%88%D0%B8%D0%BD%D0%B0
[7] VirtualBox. Матеріал з Вікіпедії – вільної енциклопедії. [Електронний ресурс]. Режим доступу: https://ru.wikipedia.org/wiki/VirtualBox
[8] AccessData Academic Program Instructor Handbook. [Online]. Available: https://ru.scribd.com/document/77940243/AccessData-Academic-Program-Instructor-Handbook. Линдон, США, 2008.
[9] ArchLinux. VirtualBox. [Online]. Available: https://wiki.archlinux.org/index.php/VirtualBox_(%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9)#%D0%A4%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D1%8B,_%D0%BF%D0%BE%D0%B4%D0%B4%D0%B5%D1%80%D0%B6%D0%B8%D0%B2%D0%B0%D0%B5%D0%BC%D1%8B%D0%B5_VirtualBox
[10] Oracle Vm Virtualbox User Manual for Release 6.0. VBoxManage. [Online]. Available: https://docs.oracle.com/cd/E97728_01/E97727/html/vboxmanage-intro.html

**References**

[1] Code of Criminal Procedure of Ukraine. Evidence, Art. 98. Ed, on 16.01.2020 [Online]. Available: https://zakon.rada.gov.ua/laws/show/4651-17
[2] B. B. Teplicky et al., "General analysis and criminal characteristics of crimes in the use of electronic computers (computers), systems and computer telecommunication networks" – Section 2, in *Crimes in the use of electronic computers (computers), systems and computer networks and telecommunication networks*. Kyiv, 2019, pp. 26-28 [in Ukrainian].
[3] B. Carrie, "Removing data from the hard drive" – Chapter 3, in *Forensic analysis of file systems*. St. Petersburg, 2007, pp. 68-71 [in Russian].
[4] S. S. Bartashuk, R. N. Deriy, and M. O. Gerasimenko, "Software for researching media" – Section 4, in *Conducting computer studies of digital media*. Kyiv, 2010, pp. 21-22 [in Ukrainian].
[5] dd (program). Material from Wikipedia – the free encyclopedia. [Online]. Available: https://ru.wikipedia.org/wiki/Dd
[6] Virtual machine. Material from Wikipedia – the free encyclopedia. [Online]. Available: https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D1%80%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%BC%D0%B0%D1%88%D0%B8%D0%BD%D0%B0
[7] VirtualBox. Material from Wikipedia – the free encyclopedia. [Online]. Available: https://ru.wikipedia.org/wiki/VirtualBox
[8] AccessData Academic Program Instructor Handbook. [Online]. Available: https://ru.scribd.com/document/77940243/AccessData-Academic-Program-Instructor-Handbook. Lyndon, USA, 2008.
[9] ArchLinux. VirtualBox. [Online]. Available: https://wiki.archlinux.org/index.php/VirtualBox_(%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9)#%D0%A4%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D1%8B,_%D0%BF%D0%BE%D0%B4%D0%B4%D0%B5%D1%80%D0%B6%D0%B8%D0%B2%D0%B0%D0%B5%D0%BC%D1%8B%D0%B5_VirtualBox
[10] Oracle Vm Virtualbox User Manual for Release 6.0. VBoxManage. [Online]. Available: https://docs.oracle.com/cd/E97728_01/E97727/html/vboxmanage-intro.html


DOI:10.24025/2306-4412.1.2020.193369

**V. V. Pavlov**, *forensic expert*
*of the department of computer-technical and telecommunication researches*
*of Cherkasy scientific-expert forensic center of the Ministry of Internal Affairs of Ukraine*
Cherkasy scientific-expert forensic center of the Ministry of Internal Affairs of Ukraine
Pasterivska str., 104, Cherkasy, 18001, Ukraine

# PRACTICE OF DOWNLOADING THE OPERATING SYSTEM ON DIGITAL MEDIA IN VIRTUAL MACHINE ENVIRONMENT

*The correctness of the conclusion of the conducted research is best verified by repeated research and comparison of the obtained results. In forensic research, there is a very large percentage of research types in which the use of destructive research methods is necessary. Computer-based expertise differs from many other types of research by having a minimal number of methods that lead to the destruction or alteration of the information content of the material evidence after the study. When researching information carriers, the performer (expert) is given a unique opportunity to copy all information content of the information storage to his workstation for further research. This opens up the possibility of self-control – copying information content and applying software to it can be done several times, which can confirm the correctness of the conclusion.*

*Forensic experts do not physically encounter the owner of the media provided for the research in the practice of computer-technical expertise, but in the course of the research of the information content, unintentionally they get some idea about the person (psychological portrait) who has been engaged in filling this information content, especially when a storage medium contains an operating system. A lot of information about its user is stored in the operating system and in the application software that may be contained therein. The application software can store the personal settings of the user, and when examined from the outside, that is, from another operating system, these personal settings are often not visible or the software under study will not be able to download at all in another operating system environment.*

***Keywords:*** *virtual machine, VirtualBox, information storage, operating system, computer technical expertise.*

*Стаття надійшла 17.01.2020*
*Прийнято 03.02.2020*


DOI:10.24025/2306-4412.1.2020.193369