УДК 004.056

ОСОБЛИВОСТІ ВИКОРИСТАННЯ СЛУЖБИ ТІНЬОВОГО КОПІЮВАННЯ ОПЕРАЦІЙНОЇ СИСТЕМИ WINDOWS В ІНТЕРЕСАХ ЦИФРОВОЇ КРИМІНАЛІСТИКИ

Павленко В.С., Агасов С.М.
e-mail: vladyslav.pavlenko3@nure.ua, salman.agasov@nure.ua
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В. В. Поповського
м. Харків, Україна

The study analyzes the possibilities of using information from the shadow copy service for digital forensics tasks. The purpose of the shadow copy service, its functioning when creating copies of disks and files, and the processes by which such copies are created are analyzed. The study presents the possibilities for conducting forensic analysis of shadow copies, and presents the tools with which a digital forensics expert can analyze shadow copies.

Служба тіньового копіювання (Volume Shadow Copy Service, VSS) - це системна служба в операційній системі (ОС) Windows, яка дозволяє створювати моментальні копії (снапшоти, snapshot) файлів або цілих томів диска, навіть якщо ці файли в цей момент використовуються системою або програмами. Снапшот є точною копією даних на певний момент часу, яка створюється практично миттєво без зупинки працюючих додатків. На відміну від традиційного резервного копіювання, моментальний знімок не потребує тривалого копіювання всіх даних. Натомість він використовує спеціальні алгоритми, такі як copy-on-write (копіювання при записуванні) або redirect-on-write (перенаправлення при записуванні), які відстежують лише зміни даних після створення снапшота. Снапшот-копія (тіньова копія) створюється Службою тіньового копіювання в такі моменти часу:

- під час створення точки відновлення системи (System Restore), при якому VSS робить копію системного диска щоб зафіксувати стан системних файлів і налаштувань на цей момент;
- під час резервного копіювання, якщо програма резервного копіювання використовує VSS. Снапшот-копія створюється на початку резервного копіювання щоб отримати узгоджену копію файлів, якщо вони відкриті;
- під час системних оновлень, встановлення програм і драйверів, за розкладом служби захисту ОС Windows;
- вручну адміністратором системи.

Важливість для цифрової криміналістики служби тіньового копіювання полягає в наступних можливостях:

- відновленні видалених файлів. Тіньові копії можуть містити старі версії файлів, навіть якщо вони видалені з файлової системи;

- провести аналіз попередніх версій файлів, оскільки VSS може зберігати кілька версій одного ж самого файлу. Експерти-криміналісти можуть виявити які були зміни в файлі і в які моменти часу;

- провести аналіз попереднього стану системних файлів, реєстру ОС, конфігурації системи;

- провести аналіз шкідливих програм, якщо в тіньових копіях залишилися старі копії таких програм;

- проаналізувати часові мітки файлів в тіньових копіях, провести аналіз часових міток зміни в системі;

- отримати попередні версії реєстру ОС, журналу подій, системних конфігурацій, журналів браузера та провести аналіз змін порівнюючи з діючими версіями даних артефактів.

Цифровий криміналіст може аналізувати інформацію служби тіньового копіювання за допомогою спеціалізованих інструментів:

- Autopsy, який є спеціалізованим криміналістичним інструментом і дозволяє автоматично знаходити тіньові копії, переглядати старі версії файлів, будувати часову лінію подій;

- FTK (Forensic Toolkit) – спеціалізоване професійне криміналістичне програмне забезпечення, яке дозволяє, відновлювати старі версії файлів, порівнювати різні версії файлів один з одним;

- EnCase – професійний криміналістичний інструмент, який дозволяє аналізувати попередні версії файлової системи, відновлювати дані;

- X-Ways Forensic – професійний криміналістичний інструмент для аналізу дисків, який дозволяє відновлювати старі версії файлів та аналізувати зміни в файлових системах;

- Vssadmin, яка є вбудованою утилітою ОС Windows, яка дозволяє переглядати список тіньових копій, перевіряти їх стан та отримувати інформацію про томи VSS.

Також можна відмітити можливість застосування такої програми, як ShadowExplorer, яка дозволяє переглядати тіньові копії. Окремим напрямком дослідження VSS є використання інструменту Volatility, який призначений для аналізу дампу оперативної пам’яті комп’ютера. Цей інструмент дозволяє знайти інформацію про використання VSS під час інциденту.

Необхідно відмітити, що в цифровій криміналістиці напрямок використання інформації зі служби тіньового копіювання не є достатньо розвиненим, тому авторами розробляється методика роботи цифрового криміналіста з тіньовими копіями VSS.

Список використаних джерел:

1. Volume Shadow Copy Service, VSS. Microsoft Build 2026. URL: https://learn.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service. (дата звернення: 12.03.2026).