УДК 004.056:[343.98:004.9]

СУЧАСНІ АСПЕКТИ ПОШУКУ ПРИХОВАНИХ РОЗДІЛІВ НА ДИСКУ В КОНТЕКСТІ ЦИФРОВОЇ КРИМІНАЛІСТИКИ

Алфьоров С.П.
e-mail: serhii.alforov@nure.ua
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського
м. Харків, Україна

The study of hidden partitions within digital storage systems represents a pivotal aspect of contemporary digital forensics. This work critically examines the methodologies employed in concealing storage partitions, including Host Protected Area (HPA), Device Configuration Overlay (DCO), and advanced NTFS-based hiding mechanisms. A comparative analysis of forensic techniques used to detect and interpret these covert partitions is conducted, with an emphasis on their implications for cybersecurity and forensic investigations. Furthermore, this study explores emerging trends in anti-forensic techniques and discusses their potential countermeasures.

З розвитком методів цифрової криміналістики зростає необхідність у розширеному аналізі прихованих розділів, які є складним викликом у контексті методів антикриміналістики. Приховані розділи можуть застосовуватись як для легітимних цілей, включаючи резервне копіювання даних, так і для зловмисних намірів, так і для несанкціонованого використання, зокрема ухилення від виявлення зловмисного програмного забезпечення або прихованого зберігання даних. Виявлення прихованих розділів на диску стає дедалі складнішим завданням, оскільки методи приховування стають більш досконалими та інтегруються безпосередньо в апаратне забезпечення. Глибоке розуміння їхньої структури, принципів функціонування та можливостей детекції є критично важливим для експертів із цифрової криміналістики.

Приховування інформації у файлових системах передбачає маніпуляцію логічними структурами та низькорівневими параметрами жорстких дисків. Одними з найбільш складних для виявлення методів є Host Protected Area (HPA) та Device Configuration Overlay (DCO), які дозволяють приховувати певні області диска без внесення змін у файлову систему.

Також широко використовуються NTFS Alternate Data Streams (ADS), Slack Space і класифікація секторів як пошкоджених із метою їхнього виключення з процесів індексації операційною системою. Останні дослідження демонструють, що методи приховування даних у файлових системах значно ускладнилися завдяки можливості динамічного створення невидимих контейнерів і використанню шифрування для унеможливлення прямого аналізу вмісту.

Крім того, одним із перспективних напрямків є використання технік стеганографії у файлових системах, які дозволяють приховувати інформацію всередині легітимних файлів без зміни їхнього зовнішнього вигляду. Зловмисники активно застосовують комбінації методів для створення багаторівневих механізмів приховування, що потребує розробки комплексних підходів до їх виявлення.

Аналіз методів, запропонованих у дослідженні [1], дозволяє глибше зрозуміти два основні підходи до виявлення прихованих розділів. Апаратні методи аналізу базуються на використанні низькорівневого доступу до диска для перевірки прихованих секторів. Найбільш ефективними серед них є спеціалізовані утиліти, такі як HDAT2 та MHDD, які використовують команди ATA для отримання точних відомостей про фізичну геометрію диска. Завдяки цим інструментам можна виявити приховані розділи, навіть якщо файлові системи були змінені для маскування даних. Однак цей метод вимагає значних технічних знань, специфічного обладнання та часу на проведення аналізу, що робить його менш доступним для загального застосування.

Програмні методи детекції орієнтовані на аналіз файлових систем і пошук аномальних структур у розподілі даних. У цьому контексті такі утиліти, як EnCase, надають потужні інструменти для ідентифікації прихованих файлових потоків, аномальних розділів і підозрілих модифікацій у таблицях розділів. Ці методи є більш гнучкими та доступними для широкого кола криміналістів, проте їх ефективність значною мірою залежить від характеру приховування даних і рівня їхньої інтеграції у файлову систему.

Ключова відмінність між апаратними та програмними методами полягає в рівні деталізації аналізу. Апаратні методи дозволяють отримати безпосередній доступ до фізичних секторів диска, що унеможливлює обхідні маневри за рахунок маніпуляцій з файловою системою. Натомість програмні методи часто стикаються з обмеженнями файлових систем та необхідністю обходити стандартні засоби шифрування та маскування. У перспективі ефективне виявлення прихованих розділів має поєднувати обидва підходи, щоб забезпечити максимальну точність і швидкість аналізу.

З огляду на зростаючу складність методів антикриміналістики, майбутні дослідження у сфері цифрової криміналістики мають бути зосереджені на розробці інтелектуальних систем підтримки експертів. Використання штучного інтелекту та глибокого аналізу даних дозволить не лише автоматизувати процес виявлення прихованих розділів, а й підвищити точність класифікації виявлених аномалій. Такі системи зможуть аналізувати великі масиви даних, ідентифікуючи невідповідності у файлових структурах та їхній поведінці на рівні апаратного забезпечення.

Застосування алгоритмів машинного навчання та гібридних підходів дозволить створювати адаптивні моделі аналізу, що враховують змінність

методів приховування та антикриміналістичних технік. Це дасть можливість криміналістам не лише ефективно ідентифікувати приховані розділи, а й прогнозувати можливі шляхи їх модифікації, мінімізуючи ризики неповного або спотвореного аналізу. Подальша інтеграція таких інтелектуальних систем у криміналістичні програмні комплекси сприятиме більшій автоматизації та прискоренню судово-експертних процесів.

Методи приховування розділів диска продовжують еволюціонувати, створюючи нові виклики для цифрової криміналістики. Використання антикриміналістичних технологій ускладнює роботу експертів, що потребує розробки нових інструментів аналізу, здатних ідентифікувати аномальні структури у файлових системах та дискових масивах. Подальші дослідження в цьому напрямку мають зосередитися на автоматизації криміналістичних процесів, інтеграції штучного інтелекту та розробці методів аналізу, що забезпечують виявлення прихованих даних незалежно від використовуваних методів їхнього маскування.

Список використаних джерел:

1. Leng J., Li T. Research on Computer System Information Hiding Anti-Forensic Technology // Advances in Computer Science Research. 2018. Vol. 83. P. 55–60.

2. Rogers M. Hidden Disk Areas: HPA and DCO // International Journal of Digital Evidence. 2006. Vol. 5, no. 1.

3. Kai-Wee C. Analysis of hidden data in NTFS file system. 2006. URL: https://www.forensicfocus.com/articles/analysis-of-hidden-data-in-the-ntfs-file-system/ (дата звернення: 21.02.2025).