Переваги та недоліки застосування декількох програмних засобів під час експертного дослідження одного об'єкта

Богдан Глущенко

технік, Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України, м. Київ, Україна, e-mail: scale.were@gmail.com

Програмне забезпечення для комп'ютерної криміналістики представлене на ринку багатьма виробниками, і більшість програмних продуктів має аналоги. Коли постає необхідність залучення двох та більше різних програмних засобів одночасно, треба розуміти, які переваги й недоліки можуть існувати.

Ключові слова: *переваги; програмне забезпечення; експертне дослідження; докази; валідація; системні ресурси; конфлікт програмного забезпечення.*

Benefits and Disadvantages While Using Several Software Tools During Expert Resseach of a Single Object

Bohdan Hlushchenko

Forensics software is represented on the market by many manufacturers, many software products have alternatives. When need rises to use two or more different software, understanding benefits and disadvantages of this approach is the key.

Keywords*: benefits; software tools; expert research; forensics; evidence; validation; system resources; software conflict.*

У 2025 році на ринку комп'ютерної криміналістики представлено багато різноманітних засобів, що поставляються на платній, безоплатній та умовно-безкоштовній основі, починаючи від простих утиліт, наборів макрокоманд та скриптів, спеціалізованих операційних систем і закінчуючи спеціальними програмно-апаратними комплексами. Продукти світових лідерів індустрії комп'ютерної криміналістики відомі майже кожному: *Cellebrite, Magnet Axiom, EnCase, X-Ways Forensics, FTK, Autopsy*. Рано чи пізно постає питання не тільки «який продукт кращий для певних завдань?», але й щодо можливості застосування різних засобів проведення дослідження на одному об'єкті [1, 2].

Тож розглянемо особливості застосування двох чи більше засобів проведення дослідження одного об'єкта, переваги, а також можливі недоліки, на які слід звернути увагу.

Зазвичай мета експертного дослідження — це отримання певних відомостей, що можуть бути використані як доказ у суді. Для цього треба бути впевненим у правильності застосування програмних засобів на всіх етапах дослідження, починаючи зі збереження об'єкта дослідження без

змін, аналізу інформації, яка на ньому міститься, оброблення та фільтрації інформації і закінчуючи поданням зібраної інформації у формі, яка може бути використана як доказ. Одними з головних принципів є:

- повторюваність результатів дослідження — збереження об'єкта дослідження у незмінному стані, застосування чітких критеріїв аналізу, методик та методичних рекомендацій для багаторазового отримання ідентичних результатів;
- перевірка результатів на сценаріях реальних подій — тестування програмного забезпечення на сценаріях, які є реальними випадками, простими та комплексними, що виникали раніше й були досліджені;
- залучення широкого кола осіб та організацій — проведення міжлабораторних досліджень, проведення експертних досліджень фахівцями з різнем рівнем досвіду та навичок.

Загалом валідація результатів декількома програмними засобами дає змогу надавати зворотній зв'язок для виробників програмних засобів, підтримувати впевненість у правильності застосування вибраних програмних засобів, зменшувати ризики, розробляти та застосовувати галузеві стандарти, підвищувати ефективність роботи та успішно захищати результати дослідження під час судових процесів. До того ж недоліком є збільшення витрат часу кваліфікованих фахівців, збільшення фінансового навантаження, необхідність залучення фахівців, що мають навички не тільки дослідження, але й проведення та документування тестування [3].

Кожен програмний засіб має свою специфіку застосування, певні засоби є універсальними, інші виявляють себе краще в окремих сферах. Також існують програмні засоби, спеціалізовані лише для виконання певного виду досліджень: мобільних пристроїв, відеореєстраторів, проведення зняття та дослідження дампу (образу) оперативної пам'яті тощо [4].

Швидкість проведення дослідження буде залежати від обсягу досліджуваної інформації (як наявної, так і раніше видаленої) та технічних характеристик комп'ютера (робочої станції). Для прискорення дослідження робоча станція, крім застосування *SSD*-накопичувачів (для зберігання образів, копіювання результатів, виділення простору для робочих та тимчасових файлів) повинна мати потужний процесор та достатній обсяг оперативної пам'яті. Сучасне програмне забезпечення для комп'ютерної криміналістики працює з одночасним застосуванням великої кількості потоків (віртуальних ядер) процесора. Золоте правило для задач з великим залученням ресурсів — це мати два гігабайти оперативної пам'яті на кожен потік. Отже, лише на потреби одного програмного засобу може знадобитися робоча станція, що має тридцять два віртуальні ядра і шістдесят чотири гігабайти оперативної пам'яті. Звичайно кількість залучених потоків та оперативної пам'яті може бути обмежена за рахунок збільшення часу,

потрібного на дослідження об'єкта [5].

Кваліфікованим спеціалістам доволі легко помітити та виправити стандартний випадок «війни за ресурси» між операційною системою, запущеними на ній процесами, програмним забезпеченням та антивірусними програмами проти кількох ресурсомістких криміналістичних програмних засобів, запущених одночасно [6].

Наведемо приклад простого випадку, коли може виникнути конфлікт програмного забезпечення, що може призвести до значних утрат часу. Звичайний робочий день експерта з комп'ютерної криміналістики, раптово виникає необхідність залишити свою комфортну лабораторію (установу, організацію тощо) і провести збирання інформації та її попереднє дослідження в польових умовах. У короткі строки збирається портативна робоча станція (ноутбук), на яку встановлюється необхідне (відповідно до фабули задачі) програмне забезпечення. Оскільки експерт має відповідну кваліфікацію і навички, він тестує програмне забезпечення після встановлення, звичайно, це не повне тестування, а просто коротка перевірка. Установлюється «Програмний засіб № 1», тестується, установлюється «Програмний засіб № 2», теж тестується. Усе працює, експерт задоволено бере свою робочу станцію та їде в польові умови. І тільки згодом виявляється, що запуск «Програмного засобу № 1» більше неможливий через те, що під час встановлення «Програмний засіб № 2» перезаписав під свої потреби частину гілок реєстру операційної системи та замінив один з драйверів, які були потрібні «Програмному засобу № 1» для підключення до досліджуваних мобільних пристроїв. І виправити проблему можливо лише повним переустановленням операційної системи, а також застосуванням лише одного з двох програмних засобів хоча б на час виконання завдання в польових умовах.

Комп'ютерна криміналістика — це галузь, яка постійно рухається вперед, постійно розвивається. Застосування кількох програмних засобів дає змогу покращувати кваліфікацію персоналу, легше підтверджувати придатність знайдених інформаційних відомостей як доказу в суді, більш докладно проводити дослідження об'єктів. А правильний розподіл ресурсів робочих станцій та уважність до можливих конфліктів програмного забезпечення допоможе уникнути негативних наслідків, компенсуючи збільшення часу та витрат.

Перелік джерел посилання

1. Top Cyber Forensics Software in 2025: A Comprehensive Guide. *Connection Cafe*. URL: https://www.connectioncafe.com/top-cyber-forensics-software-in-2025/ (дата звернення: 05.04.2025).
2. 10 Best Digital Forensic Investigation Tools — 2025. *Cybersecurity News*. URL: https://cybersecuritynews.com/free-forensic-investigation-tools/ (дата звернення: 05.04.2025).
3. Validating and Testing Forensics Software. *Geeks for Geeks*. URL: https://www.geeksforgeeks.org/validating-and-testing-forensics-software/ (дата звернення: 08.03.2025).

4. Digital Forensics Tools: The Ultimate Guide (2024). *Magnet Forensics.* URL: https://www.magnetforensics.com/blog/digital-forensics-tools-the-ultimate-guide-2024/ (дата звернення: 08.03.2025).
5. A Guide to Peak Hardware Performance for Magnet AXIOM. Magnet Forensics. URL: https://www.magnetforensics.com/blog/a-guide-to-peak-hardware-performance-for-magnet-axiom/ (дата звернення: 08.03.2025).
6. Common Computer Issues: Issues arising from conflicts between different security software installed on the laptop. *Safemode Computer Service*. URL: https://safemode.com.au/common-computer-issues-conflicts-between-different-security-software/ (дата звернення: 02.04.2025).