

КОМПЛЕКСНИЙ АНАЛІЗ ЦИФРОВИХ АРТЕФАКТІВ ДЛЯ РЕКОНСТРУКЦІЇ WINDOWS-ІНЦИДЕНТУ

А. Г. Худоба^{1,а}, М. В. Коломицев¹

¹ Навчально-науковий Фізико-технічний інститут

Анотація

У роботі розглянуто підхід до реконструкції кіберінциденту у Windows-середовищі засобами цифрової криміналістики та реагування на інциденти. Запропоновано DFIR-методику, що поєднує аналіз мережевого трафіку, журналів Windows і Sysmon, дискового образу, оперативної пам'яті та реєстрових артефактів. Для перевірки змодельовано лабораторний інцидент, у межах якого Windows 11-система завантажує підозрілий виконуваний файл із HTTP-ресурсу та встановлює зворотне підключення до вузла Kali Linux. Дані досліджено за допомогою Wireshark, Autopsy, Volatility 3, FTK Imager, Magnet RAM Capture та засобів журналювання Windows. Для оцінювання використано індикатори *DEI* та *EQI*. Результати показали, що кореляція різних груп доказів дає змогу відновити послідовність подій, підтвердити запуск файла та оцінити придатність доказового набору для криміналістичного звіту.

Ключові слова: цифрова криміналістика, DFIR, Windows, цифрові докази, цифрові артефакти.

Вступ

Сучасні кіберінциденти у корпоративних Windows-середовищах залишають різноманітні цифрові сліди у файловій системі, журналах подій, оперативній пам'яті, мережевому трафіку та реєстрі. Окремий артефакт рідко дає повну картину: трафік фіксує факт з'єднання, але не завжди пояснює, який процес його створив; журнали подій потребують зіставлення з файловими та пам'яттєвими даними [1].

У DFIR-процесі важливо забезпечити виявлення слідів інциденту, цілісність доказів, відтворюваність аналізу та документування результатів. Ці вимоги відповідають підходам до інтеграції цифрової криміналістики у реагування на інциденти та принципам збирання цифрових доказів [2, 3]. Тому реконструкція потребує методики, що визначає джерела доказів, порядок їх збору, перевірку цілісності та критерії оцінювання.

Метою роботи є перевірка комплексної DFIR-методики для реконструкції подій Windows-інциденту на основі кореляції мережевих, журнальних, дискових, пам'яттєвих і реєстрових артефактів.

Об'єктом дослідження є процес цифрового розслідування кіберінциденту у Windows-середовищі, а предметом — методи збору, аналізу та оцінювання доказів для відновлення послідовності подій.

1. Методика дослідження

Для перевірки підходу було сформовано ізольоване лабораторне середовище з двох віртуальних машин: Windows 11 як досліджуваної системи та Kali Linux як вузла атакуючої сторони. Сценарій передбачав завантаження файла *Invoice_04_2026.pdf.exe* з HTTP-ресурсу, його запуск у Windows та встановлення зворотного мережевого підключення.

Сценарій було побудовано так, щоб одна дія залишала сліди в кількох незалежних джерелах: мережевому трафіку, журналах Windows і Sysmon, PowerShell Operational, дисковому образі, Prefetch, реєстрі та дампі оперативної пам'яті. Це дає змогу перевірити не лише наявність артефактів, а й можливість їх взаємного підтвердження.

Збір доказів виконувався з урахуванням пріоритету легких даних: спочатку фіксувалися оперативна пам'ять, активні процеси, мережеві з'єднання та поточний стан системи, після цього — журнали подій, дисковий образ, файли, реєстрові дані та журнал дій дослідника. Така послідовність зменшує ризик втрати інформації після перезавантаження або завершення процесів.

Для збору та аналізу даних використовувалися Magnet RAM Capture, FTK Imager, Autopsy, Volatility 3, Wireshark, Windows Event Viewer і Sysmon. Перед аналізом для основних файлів доказового набору було обчислено контрольні суми SHA-256, що зафіксувало незмінність дампу пам'яті, мережевого трафіку, журналів Windows, дискового образу та реєстрових експортів. Така логіка відповідає підходам до дослідження Windows-інцидентів у

^аarsenhudob-ipt27@lill.kpi.ua

корпоративному середовищі [4, 5].

Для кількісного узагальнення результатів використано два допоміжні індикатори: індекс повноти доказового набору *DEI* та індекс якості доказового набору *EQI*. Вони застосовуються для формалізації результатів лабораторного DFIR-дослідження.

Для кожної групи доказів оцінка Q_j визначалася за критеріями цілісності, релевантності, часової визначеності, відтворюваності, зрозумілого походження та підтвердження іншими джерелами. Узагальнене значення *EQI* обчислювалося за формулою (1):

$$EQI = \frac{1}{n} \sum_{j=1}^n Q_j, \quad (1)$$

де Q_j — якість окремої групи цифрових доказів, n — кількість груп доказів.

DEI характеризує внесок груп доказів у реконструкцію інциденту та обчислюється за формулою (2):

$$DEI = \sum_{j=1}^n w_j Q_j, \quad (2)$$

де w_j — вага групи доказів у реконструкції подій інциденту, $\sum w_j = 1$. У змодельованому сценарії ваги задано відповідно до ролі джерела: мережеві артефакти — ,20; журнали Windows і Sysmon — ,25; дискові артефакти — ,225; оперативна пам'ять — ,25; реєстрові артефакти — ,075. Оцінки задавалися в діапазоні від 0 до 1, після чого результат переводився у відсотки.

Такий підхід не замінює експертний аналіз, але дає змогу прозоро показати значущість кожного джерела, що узгоджується з процесною логікою цифрового розслідування [6].

2. Результати дослідження

У PCAPNG-файлі зафіксовано HTTP GET-запит до ресурсу, з якого завантажувався файл `Invoice_04_2026.pdf.exe`, відповідь сервера 200 OK і подальшу TCP-взаємодію між Windows 11 та Kali Linux. Мережеві дані дали змогу визначити канал доставки файла і напрям подальшої взаємодії.

Журнали Windows і Sysmon відобразили запуск підозрілого виконаного файла, створення процесу `cmd.exe` та виконання команд PowerShell. Ці дані дозволяють відрізнити просте завантаження файла від його фактичного виконання.

Дисковий аналіз у Autopsy показав наявність файла у каталозі завантажень користувача, Prefetch-запис, файловий маркер та інші сліди активності після виконання підозрілого файла. Завдяки цим артефактам мережеву подію завантаження було пов'язано з локальними змінами у файловій системі.

Аналіз оперативної пам'яті за допомогою Volatility 3 доповнив картину інциденту даними про процесні об'єкти, фрагменти командних рядків, файлові об'єкти та RAM-рядки, пов'язані з URL-адресою завантаження. Такі артефакти корисні для фіксації активної фази інциденту.

Реєстрові артефакти використано як додаткове джерело для перевірки змін у системі; їхня інтерпретація потребує зіставлення з журналами Windows, файловими артефактами та даними оперативної пам'яті.

Подальше зіставлення виконувалося не через повторний перелік знайдених об'єктів, а через перевірку трьох питань реконструкції: звідки файл потрапив у систему, чи був він виконаний і які сліди залишив після запуску. Такий підхід дозволив перейти від опису окремих артефактів до часової послідовності подій, у якій кожний висновок підтверджувався щонайменше двома незалежними джерелами.

На основі зібраних артефактів було оцінено якість кожної групи доказів та її внесок у реконструкцію інциденту. Результати оцінювання наведено на рис. 1.

Середнє значення якості п'яти груп доказів становить 96,7 %, що відповідає *EQI*. Сума зважених внесків груп доказів становить 97,4 %, що відповідає *DEI*. Найбільший внесок мали журнальні, дискові та пам'яттєві артефакти, оскільки саме вони підтверджували запуск файла, процесну активність і локальні зміни в системі. Реєстрові артефакти виконували допоміжну роль і потребували зіставлення з іншими джерелами.

Отримані результати показують, що один PCAP-файл фіксує мережеву взаємодію, але не доводить запуск підозрілого файла. Так само Prefetch або журнал Sysmon підтверджують локальну активність, але не завжди пояснюють канал доставки. Тому реконструкція виконувалася через зіставлення мережевих, журнальних, дискових, пам'яттєвих і реєстрових даних. У підсумку сформовано узгоджену картину: файл був завантажений із мережевого ресурсу, запущений у Windows, створив процесну активність, спричинив мережеву взаємодію та залишив сліди у файловій системі, журналах, пам'яті й реєстрі.

Окремо враховано, що доказова сила кожного артефакту залежить не тільки від його наявності, а й від можливості перевірити його походження. Наприклад, мережевий запис набуває більшої ваги тоді, коли він узгоджується з часовими мітками журналів Windows, а Prefetch-запис є переконливішим у поєднанні з даними Sysmon і файловою системою. Саме тому під час оцінювання перевага надавалася не ізольованим знахідкам, а групам артефактів, які взаємно підтверджують одну подію.

Практичне застосування запропонованої схеми полягає в тому, що вона задає послідовність дій для первинного аналізу Windows-інциденту: спочатку фіксуються леткі дані, далі перевіряються журнали та файлові сліди, після чого результати зіставляються з мережевими й реєстровими даними. Такий порядок зменшує ризик помилкової інтерпретації, оскільки кожен висновок спирається на кілька незалежних джерел, а не на один окремий інструмент. У підсумковому звіті це дозволяє окремо показати канал доставки, факт виконання файла та підтверджені наслідки запуску без змішування різних типів артефактів.

Якість і внесок груп цифрових доказів DEI = 97.4 %

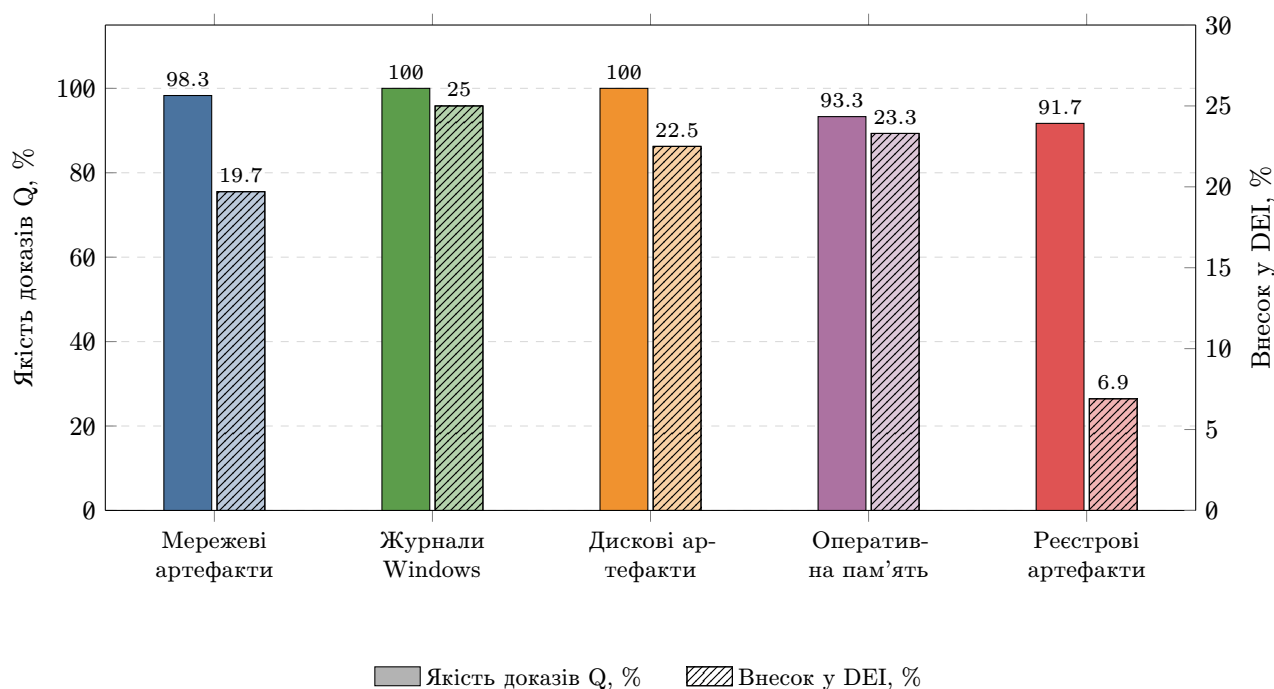


Рис. 1. Якість і внесок груп цифрових доказів.

Висновки

У роботі запропоновано та практично перевірено комплексний DFIR-підхід до дослідження Windows-інциденту. Методика охоплює лабораторний сценарій, збір летких і сталих даних, перевірку цілісності, аналіз цифрових артефактів і оцінювання доказового набору.

Практичний сценарій показав, що поєднання Wireshark, Autopsy, Volatility 3, FTK Imager, Magnet RAM Capture, Windows Event Logs і Sysmon дає змогу відновити основну послідовність подій: завантаження підозрілого файлу, його запуск, створення дочірніх процесів, виконання команд і подальші зміни у системі. Значення $DEI = 97,4\%$ та $EQI = 96,7\%$ вказують на достатню повноту й якість доказів для реконструкції інциденту.

Водночас результати потрібно розглядати як оцінку конкретного лабораторного сценарію. У реальному розслідуванні частина джерел може бути неповною, пошкодженою або навмисно очищеною, тому запропоновані індикатори доцільно використовувати разом з експертною перевіркою часової лінії, цілісності носіїв та узгодженості подій між різними журналами.

Практичне значення роботи полягає у можливості використання підходу в навчальних DFIR-лабораторіях, підготовці фахівців із кібербезпеки та розробці внутрішніх процедур розслідування

Windows-інцидентів. Подальші дослідження доцільно спрямувати на складніші сценарії з persistence, lateral movement, кількома вузлами мережі, SIEM/EDR-телеметрією та частковим видаленням артефактів.

Перелік використаних джерел

1. Kävrestad J., Birath M., Clarke N. Fundamentals of Digital Forensics: A Guide to Theory, Research and Applications. — 3rd ed. — Springer, 2024.
2. Guide to Integrating Forensic Techniques into Incident Response : NIST Special Publication / K. Kent, S. Chevalier, T. Grance, H. Dang ; National Institute of Standards ; Technology. — 2006. — No. 800-86.
3. ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence / International Organization for Standardization. — 2012.
4. Tykushin A., Ostrovskaya S. Incident Response for Windows. — Packt Publishing, 2024.
5. Guha A. Digital Forensics for Enterprises: Beyond Kali Linux. — BPB Publications, 2025.
6. ISO/IEC 27043:2015. Information technology — Security techniques — Incident investigation principles and processes / International Organization for Standardization. — 2015.