КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.24.221228
УДК 004.77

**Богданов Олександр Михайлович**
д.т.н., професор, професор кафедри інформаційної та
кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0009-0005-2605-6189
*a.m.bohdanov@gmail.com*

**Чернігівський Іван Андрійович**
аспірант
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0009-0003-4568-3212
*i.chernihivskiy@gmail.com*

# ТИПИ ЦИФРОВИХ КРИМІНАЛІСТИЧНИХ АРТЕФАКТІВ В КОМП'ЮТЕРАХ ПІД УПРАВЛІННЯМ ОС WINDOWS

**Анотація.** Останнім часом все більшої актуальності набуває питання вирішення різних завдань в умовах, коли вихідних даних для вирішення не вистачає. Пов'язано це з різними проблемами, частина яких виникла і продовжує виникати внаслідок постійного ослаблення економіки України в ході її війни з Російською Федерацією. Зараз обидві країни увійшли до фази «війни на виснаження». Тому виникає об'єктивна необхідність вивчення цього процесу та вироблення стратегії, методів та алгоритмів адаптації до нових умов, коли база вихідних даних для вирішення завдань стає недостатньою. Можна привести множину прикладів, коли життєво потрібно вирішувати завдання в умовах нестачі ресурсів. Це, наприклад, розподіл 10 бронежилетів серед 100 бійців у роті; лікування ранених в умовах нестачі медикаментів; рішення інформаційних задач при відсутності всіх необхідних даних. Ми розглядатимемо інформаційні завдання, пов'язані з комп'ютерною криміналістикою (форензікою). При дослідженні комп'ютера, що зазнав злому, необхідно вирішити питання виявлення факту несанкціонованого проникнення у програмне забезпечення (ПЗ), а також детального аналізу причин та наслідків цього. Ці завдання вже багато в чому вирішені та опубліковані. Але в досліджених публікаціях розглядаються випадки, коли для аналізу доступний сам комп'ютер і достатньо часу на аналіз. Також вважається, що кваліфікація дослідника перебуває на відповідному високому рівні. А от якщо не вистачає часу, кваліфікації, обсягу отриманих вихідних даних? Що і як робити? Стаття і присвячена цій ситуації. Вона починає цикл статей, які об'єднані напрямком «Вирішення задач комп'ютерної криміналістики в умовах неповних вихідних даних».

**Ключові слова:** кібербезпека; форензіка; артефакти; неповні вихідні дані; Windows; Forensic Triage.

## ВСТУП

У сучасному світі, де кількість і складність кібератак на підприємства постійно зростає, потрібно підвищувати кібербезпеку підприємства в умовах недостатніх ресурсів. Один з методів — це ефективно розподілити час та ресурси спеціаліста інформаційної безпеки (ІБ-спеціаліста) для своєчасного виявлення та запобігання загрозам.

**Постановка проблеми.** Зазвичай, для проведення повноцінного forensic-аналізу необхідно мати повний віртуальний образ диску та оперативної пам'яті досліджуваного комп'ютера, фізичний доступ до нього, а також мати достатню кваліфікацію та час на аналіз, що не завжди є можливим у корпоративному середовищі. Додатково до цього, корпоративні ПК мають невизначений термін підключення до мережі, а до аналітика

зазвичай ставиться конкретний перелік питань, які не завжди потребують збору усіх наявних артефактів. У цьому випадку функціонал програм Forensic Triage (частковий збір артефактів з активного ПК) не є оптимальним для вирішення завдань аналітика.

Тож необхідно пришвидшити збір необхідних артефактів з ОС Windows ІБ-спеціалістами та ІТ-адміністраторами в умовах, де неможливо отримати повний віртуальний образ диску та оперативної пам'яті досліджуваного комп'ютера або фізичний доступ до нього (та провести Forensic Triage), на відміну від ситуацій, де у аналітика є вичерпний час на підключення до досліджуваного ПК.

**Аналіз останніх досліджень і публікацій.** У працях науковців Diana Hintea, Robert Bird, Michael Green [1] Marcus K. Rogers, James Goldman, Rick Mislan, Timothy Wedge, Steve Debrota [2] та Jusas V., Birvinskas D., Gahramanov E. [3] пропонується перелік артефактів Windows 10 у цифровій криміналістиці, загальні місця їх розташування, та огляд моделі Cyber Forensic Field Triage Process Model (CFFTPM). Проте відсутня інформація про конкретні місця розташування артефактів у ОС Windows, ранжування від більш важливих до менш важливих артефактів, а також не враховуються ситуації, у яких не можливий збір повного спектру артефактів.

**Метою статті** є визначення основних місць розташування артефактів у ОС Windows, яких буде достатньо для вирішення більшості forensic-кейсів у корпоративному середовищі.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Основні терміни:

**NTFS** — (від англ. New Technology File System — «файлова система нової технології») — стандартна файлова система для сімейства операційних систем Microsoft Windows NT.

**MFT** — (англ. Master File Table — «Головна файлова таблиця») — база даних, в якій зберігається інформація про вміст тома з файловою системою NTFS, що представляє собою таблицю, де рядки відповідають файлам тома, а стовпці — атрибутам файлів.

***Артефакт*** — фрагмент інформації, який може бути використаний для аналізу інцидентів та збирання доказів у судових справах. Це можуть бути окремі файли на комп'ютері, журнали подій, історія браузера, метадані відео\зображень та ін.

***Форензіка*** — комп'ютерна криміналістика (computer forensics) — це галузь цифрової криміналістики, яка стосується доказів, знайдених у комп'ютерах і цифрових носіях інформації. Метою комп'ютерної криміналістики є дослідження цифрових носіїв криміналістично обґрунтованим способом з метою виявлення, збереження, відновлення, аналізу та представлення фактів і думок щодо наявної цифрової інформації.

***Типи артефактів*** — те, що може згрупувати артефакти без урахування того, в якій формі вони представлені. Наприклад, тип «Журнал подій», представлений у вигляді файлів журналів ОС спеціального формату .evtx, окремих журналів програм у текстовому форматі.

***Дамп пам'яті*** — (англ. dump) вміст робочої пам'яті процесу, ядра чи всієї операційної системи в певний момент часу. Зазвичай зберігається у файлах спеціального формату .dmp, .raw.

***Корінь диску\Кореневий каталог*** — (англ. root directory) — каталог файлів, що знаходиться на вершині ієрархії всіх інших каталогів (якщо це диск, на якому встановлена ОС Windows, зазвичай кореневим каталогом диску буде C:\). Процес пошуку місця зберігання будь-якого іншого файла або каталога починається з кореневого каталога.

Зважаючи на те, що на сьогоднішній день найбільш популярною ОС є Windows 10 x64 з файловою системою NTFS [4], ця стаття буде базуватись саме та такій конфігурації ОС (рис. 1).

| ОБЪЕКТ | САМЫЙ ПОПУЛЯРНЫЙ | ДОЛЯ | ДИНАМИКА |
|---|---|---|---|
| Версия ОС | Windows 10 64 bit | 53.45% | -0.08% |
| System RAM | 16 GB | 48.53% | -1.35% |
| Intel CPU Speeds | 2.3 Ghz to 2.69 Ghz | 21.02% | -0.13% |
| Physical CPUs | 6 cpus | 32.11% | +0.23% |
| Video Card Description | NVIDIA GeForce RTX 3060 | 5.13% | +0.24% |
| VRAM | 8 GB | 31.67% | +0.44% |
| Primary Display Resolution | 1920 x 1080 | 59.58% | -0.51% |
| Multi-Monitor Desktop Resolution | 3840 x 1080 | 59.02% | -1.00% |
| Language | English | 36.92% | +0.90% |
| Free Hard Drive Space | 100 GB to 249 GB | 22.76% | -0.70% |
| Total Hard Drive Space | Above 1 TB | 52.75% | +0.76% |
| VR Headsets | Oculus Quest 2 | 37.87% | -2.58% |
| Other Settings | LAHF / SAHF | 100.00% | 0.00% |

*Рис. 1. Перелік популярних конфігурацій комп'ютерів*

Криміналістичні артефакти в операційній системі Windows загалом можна розділити на чотири основні типи (категорії):

– Реєстр (Windows Registry);
– Файлова система (Filesystem NTFS);
– Журнал подій (Event Log\Event viewer);
– Пам'ять (RAM\ROM Memory).

*Артефакти реєстру* знаходяться в реєстрі Windows, який завантажується в пам'ять під час роботи системи та записується на диск під час завершення роботи. Реєстр зберігає параметри конфігурації низького рівня для операційної системи та містить велику кількість криміналістичних артефактів [5].

Оскільки дані реєстру з ключів HKEY_LOCAL_MACHINE та HKEY_USERS містять у собі всі наявні значення (інші ж являються лише посиланнями на них), вони більше всього цікавлять ІБ-аналітика (рис. 2).

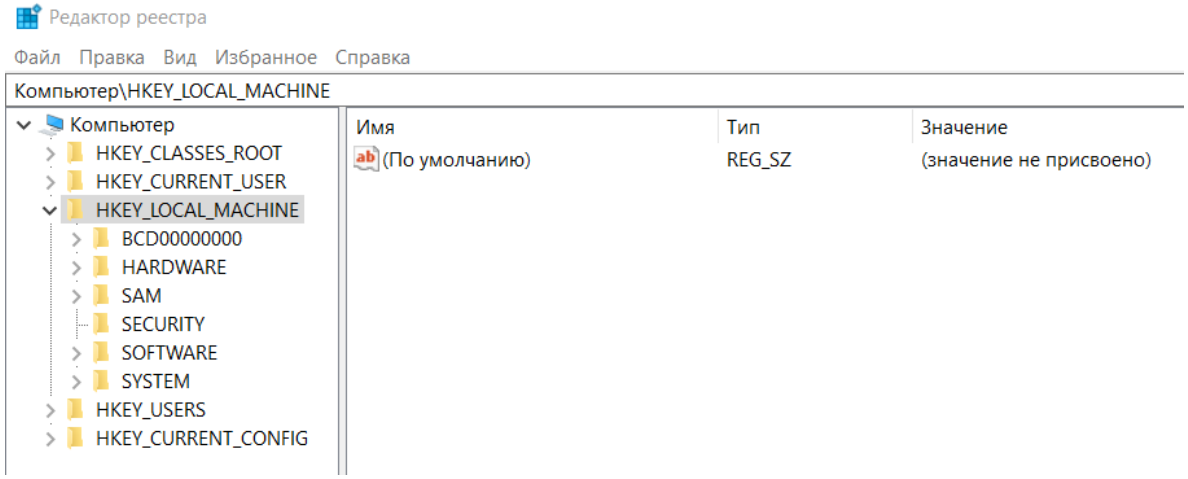


*Рис. 2. Реєстр Windows у вікні «Редактора Реєстру»*

Реєстр знаходиться за шляхом C:\Windows\System32\config у наступних файлах: SAM, SECURITY, SOFTWARE, SYSTEM [6].

З них ми зможемо отримати дані HKEY_LOCAL_MACHINE, проте з включеної системи ми не зможемо скопіювати ці файли, тому треба скористатися командою «reg save» та вивантажити реєстр у вигляді файлу до іншого місця.

Одного файлу, котрий містив би дані HKEY_USERS, не існує, тому треба збирати дані реєстру окремо про кожного користувача за шляхом C:\Users\%username%\NTUSER.DAT та C:\Users\%username%\NTUSER.DAT.LOG*, оскільки не всі системи для аналізу даних реєстру (наприклад, Eric Zimmerman's Registry Explorer) коректно його відображають без .LOG файлів.

Registry Explorer — це інструмент на основі графічного інтерфейсу користувача, який використовується для перегляду вмісту автономних кущів реєстру. Має можливість завантаження кілька кущів одночасно, пошук у всіх завантажених кущах за допомогою рядків або регулярних виразів, має вбудовані шаблони, експорт даних і багато іншого [7].

*Артефакти файлової системи* — це артефакти, які виникають через роботу файлової системи Windows — NTFS (New Technology File System) [5]. Основним файлом, що містить необхідні нам артефакти, буде Master File Table — файл $MFT, оскільки він містить інформацію про всі файли з timestamp, що є на диску. Дані з нього можна витягти за допомогою ntfswalk або скриптів Powershell [8]. Також, для більш глибокого аналізу можуть знадобитися самі файли .exe (наприклад, з папки Автозапуску), але місця їх розташування можна дізнатися лише після попереднього аналізу.

*Артефакти журналу подій* містяться в журналі подій Windows і складаються переважно з журналів аудиту операційної системи, її програм та служб [5] (рис. 3).

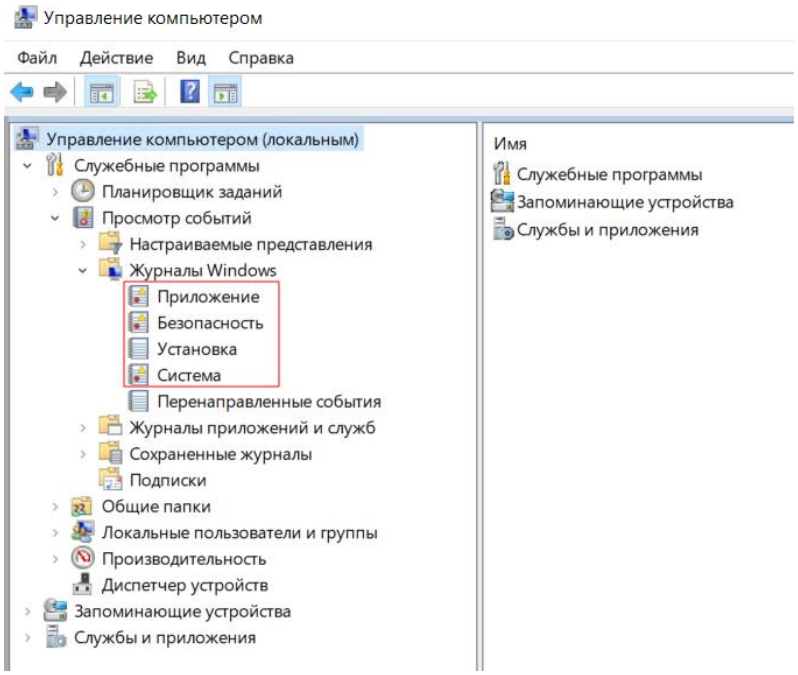


*Рис. 3. Перелік журналів подій у оснастці «Управління комп'ютером»*

Їх можна знайти за шляхом %SystemDrive%\Windows\System32\winevt\Logs, де найважливішим з них є файл Security.evtx, оскільки він містить дані про вхід\вихід користувачів з системи (EventID 4624,4625,4688) та програм, які запускались на комп'ютері (їх повний шлях та час запуску).

*Артефакти пам'яті* — це ті артефакти, які виявляються в пам'яті комп'ютера під час роботи. Ці артефакти мають бути зібрані з живої системи, і вони, як правило, не застосовуються до експертизи виключених дисків, за певними винятками, такими як файли сторінок і файли сплячого режиму, які містять пам'ять, записану на диск [5].

Їх можна отримати за допомогою програм, які знімають інформацію з живої системи, наприклад, можна використати Magnet RAM Capture, створивши повний дамп оперативної пам'яті [9].

Також вони можуть міститися у файлах:

Windows minidump: %SystemDrive%\Windows\Minidump,

Windows Crush Dump: файли .dmp;

за такими шляхами — C:\WINDOWS\ або C:\WINDOWS\Minidump\ .

Файли Pagefile.sys (файл сторінок\підвантаження), Hiberfil.sys (файл гібернації), Swapfile.sys (файл віртуальної пам'яті) — в корні системного диску (%SystemDrive%) [10] (рис. 4).


*Рис. 4. Файли (з атрибутами «Системний» та «Скритий») у корні диска C:*

Проте, їх завантаження займає багато часу і зазвичай не дає корисної інформації для ІБ-аналітика. Більш корисним буде вивантаження активних процесів з повними шляхами до виконуваних файлів.

Також, усі артефакти можна збирати та аналізувати окремо на розсуд аналітика або об'єднувати в «суперчасові шкали» за допомогою спеціального програмного забезпечення, такого як log2timeline [5].

Як ми можемо побачити, існує кілька можливих місць розташування артефактів, і для більш ефективного аналізу нам потрібно викачати їх якомога більше. Проте в умовах, де ми не можемо отримати повний образ диску, а час на викачку артефактів невідомий, нам потрібно визначити черговість викачування файлів з досліджуваного ПК, тобто зробити ранжування інформації в умовах обмежених ресурсів. Тому треба знайти додаткові параметри для визначення необхідної інформації. В майбутньому це дозволить нам викачувати тільки необхідні артефакти для кожного конкретного дослідження.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, повний криміналістичний аналіз кінцевої точки Windows складатиметься з аналізу всіх перелічених вище артефактів. Якість кінцевого аналізу буде залежить від їх повноти та достовірності.

У рамках дослідження визначено типи артефактів в ОС Windows, визначено, що якість аналізу буде досягатися при отримані повного образу диска і оперативної пам'яті комп'ютера, проте, для деяких задач буде достатньо лише невеликої кількості артефактів, які можна швидко зібрати для аналізу.

Пріоритетними напрямками подальших досліджень вважається визначення питань, які зазвичай ставляться до аналітика ІБ у корпоративному середовищі, та ранжування артефактів Windows в залежності від поставленої задачі з урахуванням ситуацій, де у аналітика є обмежений час на підключення до досліджуваного комп'ютера.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Hintea, D., Bird, R., & Green, M. (2017). An investigation into the forensic implications of the Windows 10 operating system: recoverable artefacts and significant changes from Windows 8.1. *International Journal of Electronic Security and Digital Forensics, 9(4).* https://doi.org/10.1504/ijesdf.2017.10008013
2. Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer Forensics Field Triage Process Model. *Journal of Digital Forensics, Security and Law, 1(2).* https://doi.org/10.15394/jdfsl.2006.1004
3. Jusas, V., Birvinskas, D., & Gahramanov, E. (2017). Methods and Tools of Digital Triage in Forensic Context: Survey and Future Directions. *Symmetry, 9(4).* https://doi.org/10.3390/sym9040049
4. *Steam Hardware & Software Survey*. (n.d.). Welcome to Steam. https://store.steampowered.com/hwsurvey/Steam-Hardware-Software-Survey-Welcome-to-Steam
5. *GitHub - Psmths/windows-forensic-artifacts: Handbook of windows forensic artifacts across multiple Windows version with interpretation tips with some examples.* (n.d.). GitHub. https://github.com/Psmths/windows-forensic-artifacts
6. *Windows registry for advanced users - Windows Server*. (n.d.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users
7. Zimmerman, E. R. (2017). *Registry Explorer User manual*. https://www.oit.va.gov/Services/TRM/files/RegistryExplorerManual.pdf
8. *Windows $MFT and NTFS Metadata Extractor Tool*. (n.d.). TZWorks LLC (www.tzworks.com) Homepage. https://tzworks.com/prototype_page.php?proto_id=12
9. *Acquiring Memory with Magnet RAM Capture - Magnet Forensics*. (n.d.). Magnet Forensics. https://www.magnetforensics.com/blog/acquiring-memory-with-magnet-ram-capture/
10. Korkmaz, F. (2021). *Windows artifacts*. Medium. https://r4bb1t.medium.com/windows-artifacts-8fae778aa8c7

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023

**Oleksandr Bohdanov**
Doctor of Technical Sciences, Professor, Professor of the
Volodymyr Buriachok Department of Information and Cyber Security
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0009-0005-2605-6189
*a.m.bohdanov@gmail.com*

**Ivan Chernihivskyi**
graduate student
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0009-0003-4568-3212
*i.chernihivskiy@gmail.com*

# TYPES OF DIGITAL FORENSIC ARTIFACTS IN WINDOWS COMPUTERS

**Abstract.** Recently, the issue of solving various tasks in conditions of initial data shortage becomes more relevant. It is related to various problems, but some of them have arisen and continue to arise as a result of the constant Ukraine's economy cripple during the war with Russian Federation. Currently both countries have entered the "war of attrition" phase. Therefore, there is an objective need to investigate this process and develop strategies, methods and algorithms for adaptation to new conditions, when the initial data base becomes insufficient for tasks solving. Many examples can be given when it is vital to solve tasks under the lack of resources. For example, the distribution of 10 body armor vests among 100 soldiers in a company; treatment the wounded under the medicine's shortage conditions; solving information tasks when there is a lack of the necessary data. We will investigate information tasks related to computer forensics. When a hacked computer is examined, it is necessary to detect the fact of unauthorized access to the software, as well as analyze in detail its causes and consequences. These tasks have already been largely solved and published. But the researched publications consider cases when the computer is available and there is enough time for analysis. It is also considered that the researcher qualification is at a correspondingly high level. But what if there is not enough time, qualifications, and the volume of received initial data? What and how should we do? The article is devoted to the above-mentioned situation. It starts in and does series of articles, arranged in the direction of "Solving the computer forensics issues in the conditions of incomplete initial data".

**Keywords:** cybersecurity; computer forensics; computer digital artifacts; incomplete initial data; Windows; Forensic Triage.

## REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Hintea, D., Bird, R., & Green, M. (2017). An investigation into the forensic implications of the Windows 10 operating system: recoverable artefacts and significant changes from Windows 8.1. *International Journal of Electronic Security and Digital Forensics, 9(4).* https://doi.org/10.1504/ijesdf.2017.10008013
2. Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer Forensics Field Triage Process Model. *Journal of Digital Forensics, Security and Law, 1(2).* https://doi.org/10.15394/jdfsl.2006.1004
3. Jusas, V., Birvinskas, D., & Gahramanov, E. (2017). Methods and Tools of Digital Triage in Forensic Context: Survey and Future Directions. *Symmetry, 9(4).* https://doi.org/10.3390/sym9040049
4. *Steam Hardware & Software Survey.* (n.d.). Welcome to Steam. https://store.steampowered.com/hwsurvey/Steam-Hardware-Software-Survey-Welcome-to-Steam
5. *GitHub - Psmths/windows-forensic-artifacts: Handbook of windows forensic artifacts across multiple Windows version with interpretation tips with some examples.* (n.d.). GitHub. https://github.com/Psmths/windows-forensic-artifacts
6. *Windows registry for advanced users - Windows Server.* (n.d.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users

7. Zimmerman, E. R. (2017). *Registry Explorer User manual*. https://www.oit.va.gov/Services/TRM/files/RegistryExplorerManual.pdf
8. *Windows $MFT and NTFS Metadata Extractor Tool*. (n.d.). TZWorks LLC (www.tzworks.com) Homepage. https://tzworks.com/prototype_page.php?proto_id=12
9. *Acquiring Memory with Magnet RAM Capture - Magnet Forensics*. (n.d.). Magnet Forensics. https://www.magnetforensics.com/blog/acquiring-memory-with-magnet-ram-capture/
10. Korkmaz, F. (2021). *Windows artifacts*. Medium. https://r4bb1t.medium.com/windows-artifacts-8fae778aa8c7