ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ЦИФРОВА КРИМІНАЛІСТИКА

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ

Олександр ПІРОГ



Житомир
2026

ЗАТВЕРДЖЕНО

Науково-методичною радою
Державного університету
«Житомирська політехніка»
протокол від
19 листопада 2026 р. № 7

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
для проведення лабораторних робіт
з навчальної дисципліни
«ЦИФРОВА КРИМІНАЛІСТИКА»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності F5 «Кібербезпека та захист інформації»
освітньо-професійна програма «Кібербезпека»
факультет інформаційно-комп'ютерних технологій
кафедра кібербезпеки та захисту інформації

Рекомендовано на засіданні
кафедри кібербезпеки
та захисту інформації
17 вересні 2026 р.,
протокол № 5

Розробник: к.т.н., доцент кафедри кібербезпеки та захисту інформації,
Олександр ПІРОГ

Житомир
2026

ЗМІСТ

Лабораторна робота 1 ХЕШУВАННЯ 3
Лабораторна робота 2 ДАМП ОЗП ТА ПОБІТОВА КОПІЯ ЦИФРОВОГО НОСІЯ .. 13
Лабораторна робота 3 ВІДНОВЛЕННЯ ФАЙЛІВ 24
Лабораторна робота 4 АНАЛІЗ ОСНОВНИХ АРТЕФАКТІВ WINDOWS 10 38
Лабораторна робота 5 АНАЛІЗ КОШИКУ 46
Лабораторна робота 6 АНАЛІЗ ПОСИЛАНЬ НА НЕДАВНО ВІДКРИТІ ФАЙЛИ (RECENT) ТА ФАЙЛІВ ПОПЕРЕДНЬОГО ЗАВАНТАЖЕННЯ (PREFETCH) 51
Лабораторна робота 7 АНАЛІЗ СИГНАТУР ФАЙЛІВ 57
Лабораторна робота 8 АНАЛІЗ МЕТАДАНИХ ФАЙЛІВ 61
Лабораторна робота 9 АНАЛІЗ ЖУРНАЛУ ПОДІЙ 70
Лабораторна робота 10 АНАЛІЗ РЕЄСТРУ 76
Лабораторна робота 11 АНАЛІЗ ОПЕРАТИВНОЇ ПАМ'ЯТІ 90
Лабораторна робота 12 АНАЛІЗ МОБІЛЬНИХ ПРИСТРОЇВ 98
Лабораторна робота 13 АНАЛІЗ ІНТЕРНЕТ-АКТИВНОСТІ 110
Список рекомендованої літератури 128

Лабораторна робота 1
ХЕШУВАННЯ

Мета заняття: ознайомитися з основними принципами забезпечення цілісності цифрових доказів та роллю криптографічних хеш-функцій у цифровій криміналістиці; дослідити особливості використання алгоритмів хешування для підтвердження автентичності та незмінності цифрових об’єктів; ознайомитися з поняттями ланцюжка зберігання доказів, колізії хеш-функцій та стеганографії; дослідити вплив змін вмісту файлу на його хеш-значення; отримати практичні навички роботи з криміналістичними інструментами FTK Imager, HashMyFiles та HxD; дослідити можливості виявлення дублікатів файлів, модифікацій цифрових об’єктів та прихованих даних у графічних файлах; сформувати практичні навички аналізу цифрових доказів і контролю їх цілісності під час проведення криміналістичних досліджень.

Теоретичні відомості

Одним із ключових принципів цифрової криміналістики є забезпечення цілісності цифрових доказів. Під час вилучення, зберігання, передачі та дослідження цифрових носіїв необхідно гарантувати, що дані не були змінені. Для вирішення цього завдання використовуються криптографічні хеш-функції.

Важливою складовою забезпечення цілісності доказів є ланцюжок зберігання (Chain of Custody).

Ланцюжок зберігання – це документ або серія взаємопов’язаних документів, що відображають історію цифрового доказу від моменту його виявлення та вилучення до завершення дослідження або судового розгляду. Запис ланцюжка зберігання дозволяє встановити, хто, коли, де та з якою метою взаємодіяв із цифровим доказом.

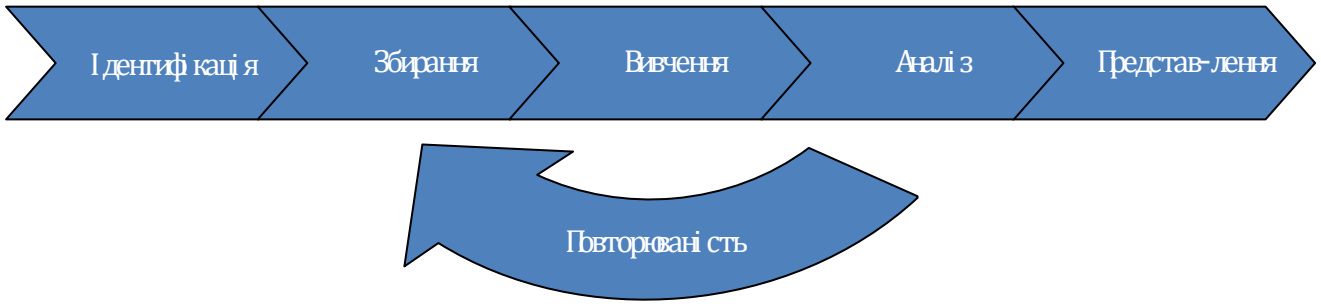


Рис. 1. Ланцюжок зберігання та цілісність доказів

Запис ланцюжка зберігання повинен містити щонайменше:

– унікальний ідентифікатор доказу;

- інформацію про осіб, які мали доступ до доказу;
- дату, час та місце передачі або отримання доказу;
- інформацію про особу, яка перевіряла доказ;
- причину проведення перевірки або дослідження;
- інформацію про будь-які неминучі зміни цифрових доказів;
- поточний статус та місцезнаходження доказу.

Для підтвердження незмінності цифрових доказів використовуються криптографічні хеш-функції.

Хешування – це процес обчислення унікального цифрового відбитка (хеш-значення) для довільного набору даних. Результатом роботи хеш-функції є рядок фіксованої довжини, який однозначно характеризує вміст файлу або іншого цифрового об'єкта.



Рис. 2. Криптографічний хеш

Навіть незначна зміна вихідних даних призводить до суттєвої зміни хеш-значення. Завдяки цьому хешування використовується для контролю цілісності цифрових доказів та виявлення модифікацій даних.

У цифровій криміналістиці хешування застосовується для:

- підтвердження цілісності та незмінності цифрових доказів;
- перевірки коректності створення побітових копій носіїв інформації;
- виявлення змін у файлах;
- пошуку відомих файлів за базами хеш-значень;
- виявлення дублікатів файлів;
- документування результатів криміналістичного дослідження;
- ідентифікації об’єктів інтелектуальної власності;

- виявлення відомого шкідливого програмного забезпечення;
- ідентифікації забороненого контенту без необхідності його зберігання або перегляду.

Наприклад, правоохоронні органи можуть використовувати бази хешів для виявлення незаконного контенту. У такому випадку порівнюються лише хеш-значення файлів без необхідності перегляду їх вмісту.

Криптографічна хеш-функція повинна задовольняти низці вимог:

- Односторонність. За відомим хеш-значенням практично неможливо відновити вихідні дані.
- Детермінованість. Для однакових вхідних даних завжди буде отримано однаковий результат.
- Швидкість обчислення. Хеш-функція повинна швидко обчислюватися навіть для великих обсягів даних.
- Стійкість до колізій. Повинно бути практично неможливо знайти два різні набори даних, які мають однакове хеш-значення.

Колізія виникає тоді, коли два різні цифрові об’єкти мають однакове хеш-значення. Для сучасних криптографічних алгоритмів ймовірність випадкової колізії надзвичайно мала, однак для деяких алгоритмів, зокрема MD5 та SHA-1, були розроблені практичні методи створення колізій.

У цифровій криміналістиці використовуються різні алгоритми хешування.

MD5 був розроблений Рональдом Рівестом у 1991 році та формує 128-бітне хеш-значення. Його перевагами є висока швидкість обчислення та широка підтримка програмним забезпеченням. Недоліком є наявність відомих атак на колізії, тому MD5 більше не рекомендується для криптографічного захисту інформації. Водночас він продовжує використовуватися в криміналістичних інструментах для перевірки цілісності файлів.

SHA-1 формує 160-бітне хеш-значення та також вважається криптографічно застарілим через наявність практичних атак на колізії.

SHA-256 належить до сімейства алгоритмів SHA-2 та формує 256-бітне хеш-значення. На сьогодні він є одним із найбільш поширених алгоритмів для підтвердження цілісності цифрових доказів.

Під час вилучення цифрового носія створюється його криміналістична копія (образ). Після завершення копіювання для оригінального носія та його копії обчислюються хеш-значення. Якщо отримані значення збігаються, вважається, що копія є точною побітовою реплікою оригіналу.

У протоколах огляду та експертних висновках хеш-значення використовуються як цифрові ідентифікатори доказів. У разі зміни хоча б одного біта даних хеш-значення зміниться.

Якщо два файли мають однаковий вміст, їхні хеш-значення також будуть однаковими. Ця властивість використовується для пошуку дублікатів файлів, скорочення обсягу даних під час аналізу, виявлення відомих файлів операційної системи та пошуку відомого шкідливого програмного забезпечення. Водночас збіг хешів не означає, що файли мають однакові назви або розташування – важливим є саме збіг вмісту.

Імовірність колізій безпосередньо пов’язана з довжиною хешу та ентропією даних.

Ентропія – це міра невизначеності або випадковості інформації. У цифровій криміналістиці аналіз ентропії використовується для виявлення зашифрованих даних, стиснених архівів, прихованих контейнерів та інших підозрілих об’єктів.

Таблиця 1

Показники алгоритми хешування та ДНК

	Ймовірність колізії	Ентропія (біт)	Приклад
CRC	1 на 4,294,967,296	32	3A1D2F9C
MD5	1 на 3.4×10^{38}	128	5d41402abc4b2a76b9719d911017c592
SHA1	1 на 1.5×10^{48}	160	a9993e364706816aba3e25717850c26c9cd0d89d
ДНК	1 на $\sim10^{75}$	~250	AGTCGATCG... (послідовність ДНК)

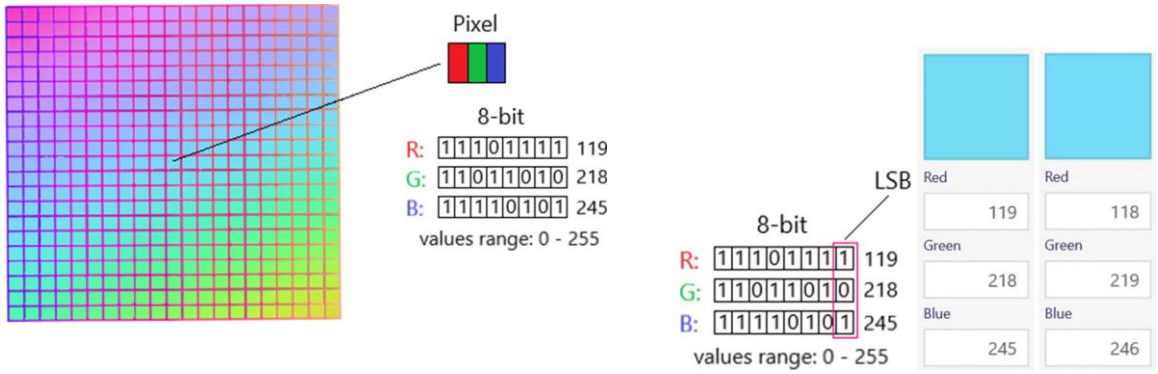
Стеганографія – це метод приховування інформації всередині іншого файлу (наприклад, зображення, аудіофайлу або відеофайлу) таким чином, щоб приховати сам факт існування цієї інформації.

На відміну від шифрування, яке приховує зміст повідомлення, стеганографія приховує сам факт його передавання.

Найпоширенішими методами стеганографії є:

- LSB (Least Significant Bit) – приховування даних у молодших бітах пікселів зображення;
- Metadata Injection – приховування інформації в метаданих файлу;
- Whitespace Hiding – приховування даних за допомогою пробілів та символів форматування;
- Noise Injection – приховування інформації у випадковому шумі цифрового об’єкта.

LSB



Whitespace Hiding

This is an example of white space manipulation.

Hidden code:10010110

Рис. 3. Методи стеганографії

Для створення та аналізу стеганографічних контейнерів використовуються такі інструменти, як OpenStego, Steghide, SilentEye, DeepSound, ExifTool, Binwalk та інші.

Формат JPEG дозволяє розміщувати додаткові дані після завершального маркера зображення. Такі дані можуть не відображатися стандартними засобами перегляду зображень, але залишатися всередині файлу. Зловмисники можуть використовувати цю особливість для приховування повідомлень, архівів або інших файлів.

У цифровій криміналістиці для виявлення подібних артефактів використовуються шістнадцяткові редактори, зокрема HxD. Аналіз структури файлу дозволяє виявити приховані дані, невідповідність сигнатур та інші ознаки модифікації файлу.

Завдання на лабораторну роботу

Налаштуйте Файловий провідник таким чином щоб відображалися розширення імен файлів та приховані файли через меню Вигляд.

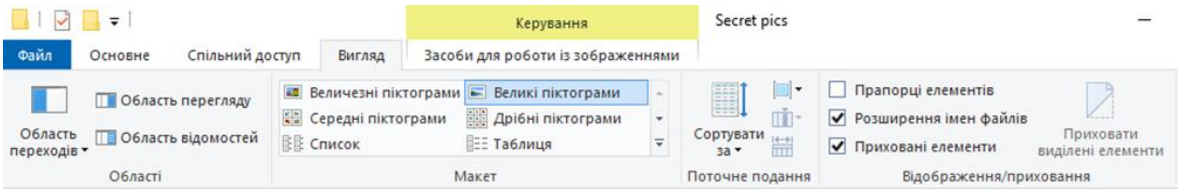


Рис. 4. Налаштування Файлового провідника

Завантажте архів побітової копії підозрілого цифрового носія Vader_Home_Computer.zip (https://drive.google.com/file/d/1ptqbPdTLPGvQ6WzT22AJtobVGkECqdO9)

Дуже великий файл – 10ГБт. Плануйте його завантаження завчасно!

Разархівуйте його. Vader_Home_Computer.001, Vader_Home_Computer.002 … Vader_Home_Computer.005.

Встановіть та відкрийте FTK Imager (https://www.exterro.com/digital-forensics-software/ftk-imager)

Виберіть File > Add Evidence Item > Image File > Browse > Vader_Home_Computer.001 > Finish.

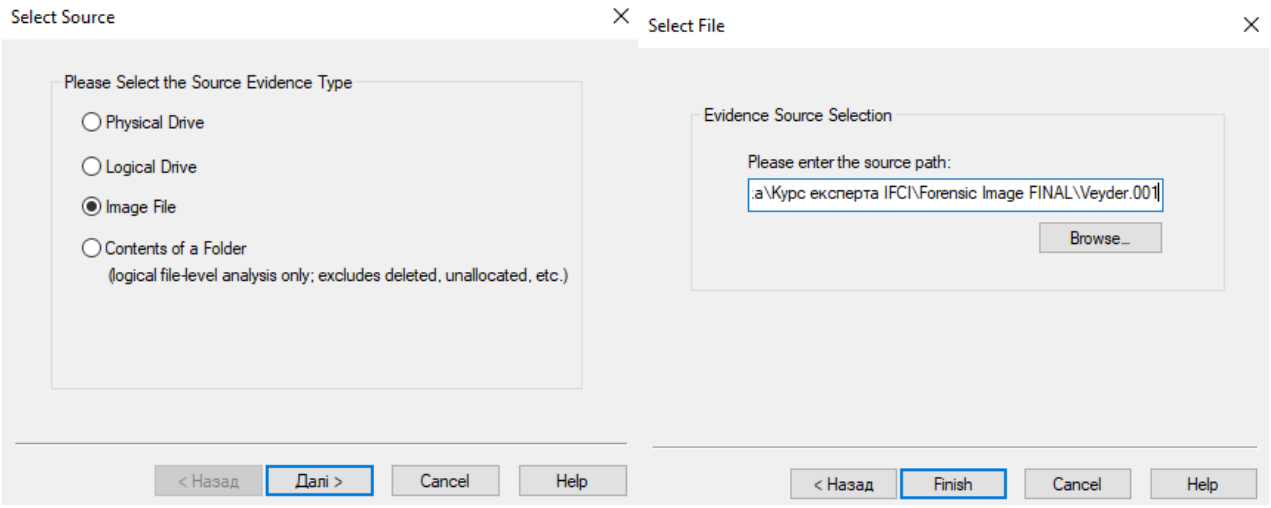


Рис. 5. Відкриття архіву цифрового носія у FTK Imager

Перейдіть до папки C:\Users\Owner\Documents\Secret pics.

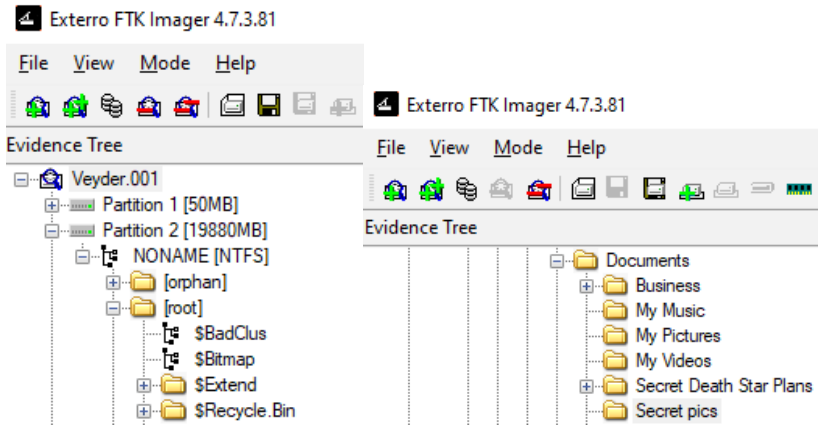


Рис. 6. Робота з образом в FTK Imager

Експортуйте папку «Secret Pics» на локальний жорсткий диск за допомогою контекстного пункту Export Files контекстного меню (натисніть правою кнопкою миші на ній).

Перегляньте на комп'ютері три зображення в папці Secret pics використовуючи Windows, натисніть правою кнопкою миші три надані зображення відкрийте Властивості та запишіть розмір кожного файлу.

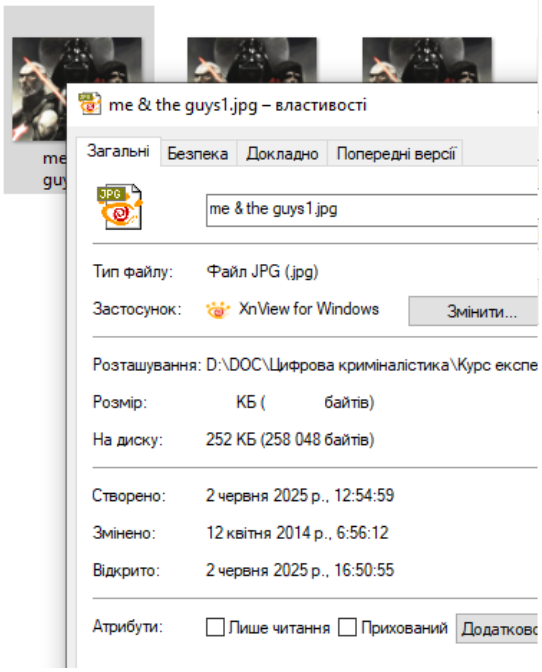


Рис. 7. Властивості файлу

me & the guys1.jpg розмір: _____
me & the guys2.jpg розмір: _____
me & the guys3.jpg розмір: _____

Відкрийте кожне зображення та опишіть вміст.

me & the guys1.jpg Опис: _____

me & the guys2.jpg Опис: _____

me & the guys3.jpg Опис: _____

Чи всі малюнки однакові?

Встановіть HashMyFiles (https://www.nirsoft.net/utils/hash_my_files.html).

Використовуйте HashMyFiles, щоб обчислити хеші всіх 3 файлів.

Файл > Додати файли. Додайте всі три файли.

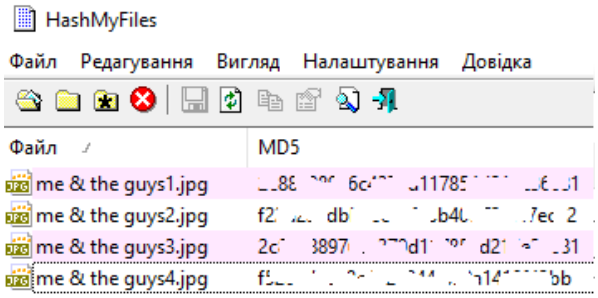


Рис. 8. HashMyFiles

Запишіть хеш-значення MD5 для кожного файлу.

me & the guys1.jpg Хеш MD5: _____

me & the guys2.jpg Хеш MD5: _____

me & the guys3.jpg Хеш MD5: _____

Встановіть HxD Hex Editor (https://mh-nexus.de/en/hxd/) на свій комп'ютер і відкрийте його.

У HxD виберіть Файл > Відкрити. Відкрийте один із 2 дублікатів файлів. Ви знаєте, що вони є дублювати, оскільки вони мають ідентичний хеш.

Перейдіть у нижню частину файлу та змініть останні декілька символів.

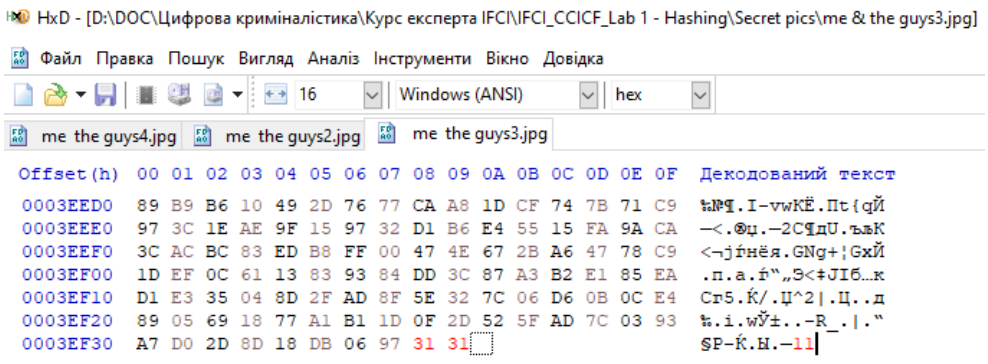


Рис. 9. HxD

Виберіть Файл > Зберегти як і збережіть це зображення під іншою назвою.

Використовуйте Windows, щоб записати розмір файлу та хеш-розрахунок для хешу MD5 нового файлу.

Новий файл:

Опис: _____

Розмір: _____

Хеш MD5: _____

Виходячи з результатів цього тесту, що ви думаєте про надійність MD5 як «цифрового відбитку»?

Використовуйте HxD, щоб перевірити останні декілька байтів кожного з наданих файлів і запишіть все, що може викликати підозру.

Виходячи з вашої відповіді на попереднє запитання, чи вважаєте ви, що злочинці можуть приховати інформацію у файлі jpg?

_____

Контрольні питання

1. Для чого використовується ланцюжок зберігання доказів (Chain of Custody)?
2. Яку інформацію повинен містити запис ланцюжка зберігання доказів?
3. Чому важливо документувати всі операції з цифровими доказами?
4. Що таке хешування?
5. Які властивості повинна мати криптографічна хеш-функція?
6. Що таке односторонність хеш-функції?
7. Що означає детермінованість хеш-функції?
8. Що таке стійкість до колізій?
9. Що таке колізія хеш-функції?
10. Чим відрізняються алгоритми MD5, SHA-1 та SHA-256?
11. Що означає збіг хешів оригінального носія та його копії?
12. Як вплине зміна одного байта файлу на його хеш-значення?
13. Чому хеш-функції використовуються для контролю цілісності цифрових доказів?
14. Чи можуть два файли однакового розміру мати різні хеш-значення?
15. Як хешування використовується для виявлення шкідливого програмного забезпечення?
16. Що таке ентропія даних?
17. Що таке стеганографія?
18. Що таке метод LSB (Least Significant Bit)?

19. У чому полягає метод Metadata Injection?
20. Як працює метод Whitespace Hiding?
21. Що таке Noise Injection?
22. Чому графічні файли часто використовуються для приховування інформації?

Лабораторна робота 2
ДАМП ОЗП ТА ПОБІТОВА КОПІЯ ЦИФРОВОГО НОСІЯ

Мета заняття: ознайомитися з основними принципами вилучення цифрових доказів та особливостями роботи з енергозалежними й енергонезалежними даними; дослідити порядок дій під час вилучення доказів із увімкнених і вимкнених комп'ютерних систем; ознайомитися з принципами створення дампів оперативної пам'яті та побітових копій цифрових носіїв; дослідити особливості використання блокіраторів запису, технологій шифрування BitLocker, RAID-масивів та віртуальних машин під час проведення криміналістичних досліджень; отримати практичні навички створення дампу оперативної пам'яті та побітової копії цифрового носія за допомогою програмних засобів DumpIt і FTK Imager.

Теоретичні відомості

Вилучення цифрових доказів є одним із найважливіших етапів цифрового криміналістичного дослідження. Помилки, допущені під час вилучення доказів, можуть призвести до втрати інформації або поставити під сумнів достовірність результатів дослідження.

Основною метою вилучення цифрових доказів є отримання максимально повної копії інформації із збереженням її цілісності та можливістю подальшого підтвердження автентичності.

Під час роботи з цифровими доказами необхідно дотримуватися таких принципів:

- мінімізувати зміни досліджуваних даних;
- документувати всі виконані дії;
- використовувати спеціалізовані криміналістичні інструменти;
- забезпечувати можливість перевірки результатів іншими фахівцями;
- працювати з копіями доказів, а не з оригіналами.

Вилучення доказів залежить від того, чи перебуває система у ввімкненому стані.

Якщо система вимкнена, першочерговим завданням є збереження стану носіїв інформації. Типовий порядок дій:

- Вилучити носій інформації із системи.
- Підключити його через блокіратор запису.
- Створити побітову копію (образ) носія.
- Обчислити контрольні хеш-значення.
- Задокументувати всі виконані дії.

У такому випадку відсутній ризик втрати енергозалежних даних, оскільки

вони вже були втрачені в момент вимкнення системи.

Якщо система працює, частина важливих доказів може міститися лише в оперативній пам’яті. Типовий порядок дій:

- Підключити зовнішній накопичувач.
- Створити дамп оперативної пам'яті.
- За необхідності ізолювати систему від мережі.
- Зібрати інформацію про активні мережеві з'єднання, процеси та користувачів.
- Створити образи носіїв інформації.
- Задокументувати всі виконані дії.

Під час роботи з активною системою необхідно пам’ятати, що будь-яка виконана дія змінює її стан. Тому слід дотримуватися принципу мінімального впливу на досліджувану систему.

Блокіратор запису (Write Blocker) – це апаратний або програмний засіб, який запобігає внесенню змін до цифрового носія під час його дослідження.



Рис. 10. Блокіратор запису (Write Blocker)

Блокіратор дозволяє виконувати читання даних із носія, але блокує будь-які операції запису.

Використання блокіраторів є стандартною практикою цифрової криміналістики та дозволяє гарантувати незмінність цифрових доказів під час створення криміналістичних копій.

Побітова копія (образ, Forensic Image) – це точна копія цифрового носія, яка містить усі сектори носія без винятку. На відміну від звичайного копіювання файлів, побітова копія включає:

- активні файли;
- видалені файли;
- нерозподілений простір;
- службові структури файлової системи;

– приховані області носія.

Після створення образу для нього обчислюються хеш-значення. Збіг хешів оригінального носія та його копії підтверджує правильність копіювання.

Під час подальшого дослідження використовується саме побітова копія, а не оригінальний носій.

Оперативна пам’ять (Random Access Memory, RAM) – це енергозалежне сховище даних, яке використовується для зберігання інформації, необхідної системі під час роботи.

У пам’яті можуть міститися:

– запущені процеси;
– мережеві з'єднання;
– паролі та токени доступу;
– ключі шифрування;
– буфер обміну;
– відкриті документи;
– дані месенджерів;
– сліди шкідливого програмного забезпечення.

Вміст оперативної пам’яті втрачається після вимкнення живлення. Саме тому створення дампу ОЗП часто є першим кроком під час дослідження працюючої системи.

Дамп оперативної пам’яті – це файл, який містить копію вмісту оперативної пам’яті на певний момент часу.

Для створення дампів використовуються спеціалізовані інструменти, наприклад DumpIt.

Отриманий дамп може бути використаний для:

– пошуку шкідливого програмного забезпечення;
– аналізу мережевих з'єднань;
– вилучення ключів шифрування;
– дослідження активності користувача;
– відновлення інформації, відсутньої на диску.

Вимкнення комп’ютера може призвести до втрати важливих цифрових доказів.

Після вимкнення системи можуть бути втрачені:

– ключі шифрування;
– паролі та токени доступу;
– мережеві сесії;
– VPN-з'єднання;
– інформація про запущені процеси;

- буфер обміну;
- тимчасові файли;
- частина слідів шкідливого програмного забезпечення;
- відкриті документи та незбережені дані.

Тому рішення про вимкнення комп’ютера повинно прийматися лише після оцінки можливих наслідків.

BitLocker – це вбудована система повнодискового шифрування операційних систем Windows.

У зашифрованому стані дані на диску неможливо прочитати без ключа розшифрування або ключа відновлення (Recovery Key).

Якщо комп’ютер вимкнений і диск зашифрований BitLocker, дослідник може отримати лише зашифровані дані.

Якщо система працює, ключі шифрування можуть перебувати в оперативній пам’яті. У такому випадку створення дампу ОЗП дозволяє отримати додаткові можливості для подальшого доступу до даних.

RAID (Redundant Array of Independent Disks) – це технологія зберігання даних, яка об'єднує декілька фізичних дисків в один логічний том.

Залежно від типу RAID інформація може дублюватися або розподілятися між декількома дисками.

Під час криміналістичного дослідження необхідно:

- вилучити всі диски масиву;
- задокументувати порядок їх підключення;
- визначити тип RAID;
- відновити конфігурацію масиву.

Без правильно відновленої конфігурації RAID доступ до даних може бути неможливим.

Віртуальна машина (Virtual Machine, VM) – це програмна емуляція комп’ютера, яка функціонує всередині спеціального програмного забезпечення – гіпервізора.

Найпоширенішими гіпервізорами є: Oracle VirtualBox, VMware Workstation, Microsoft Hyper-V.

Віртуальна машина може містити:

- операційну систему;
- файли користувача;
- журнали подій;
- мережеву активність;
- шкідливе програмне забезпечення.

Під час вилучення цифрових доказів необхідно враховувати наявність

віртуальних машин, оскільки вони можуть містити окремі цифрові артефакти та докази.

Основними принципами збирання цифрових доказів згідно рекомендацій щодо збору цифрових доказів наведені в документі IETF RFC 3227 «Guidelines for Evidence Collection and Archiving» є:

- створення максимально точного знімка системи;
- мінімізація змін у доказах;
- детальне документування всіх дій;
- використання перевірених інструментів;
- швидке збирання найбільш нестійких доказів;
- збирання доказів до початку аналізу;
- фіксація часу та часових поясів;
- забезпечення можливості повторної перевірки результатів.

Згідно з RFC 3227 збір доказів доцільно проводити від найбільш нестійких даних до найбільш стійких:

- Вміст регістрів процесора та кешів.
- Таблиці процесів.
- Мережеві з'єднання.
- Вміст оперативної пам'яті.
- Тимчасові файлові системи.
- Дані на локальних дисках.
- Дані віддалених журналів.
- Конфігурація мережі.
- Архівні копії.

Такий підхід дозволяє мінімізувати втрату важливої інформації.

Деякі сучасні інформаційні системи можуть містити механізми автоматичного знищення даних.

Такі механізми можуть спрацьовувати у випадках:

- втрати мережевого з'єднання;
- спроби несанкціонованого доступу;
- вимкнення живлення;
- зміни конфігурації системи.

Для мінімізації ризиків використовуються:

- програмне ізолювання від мережі;
- блокування трафіку за допомогою фаєрволів;
- відключення мережевих кабелів без вимкнення живлення;
- використання екранувальних контейнерів (Faraday Bags);

– створення резервних копій перед вимкненням пристрою.



Рис. 11. Екранувальні контейнери (Faraday Bags)

Завдання на лабораторну роботу

Помістіть виконуваний файл DumpIt (https://www.magnetforensics.com/resources/magnet-dumpit-for-windows/) у каталог, який слугуватиме місцем зберігання для оперативної пам'яті.

*Примітка: зазвичай це розташування буде зовнішнім пристроєм, оскільки ви ніколи не бажайте писати на диск доказів. Однак для цілей цієї лабораторії не соромтеся для зберігання енергонезалежної пам'яті на ваш диск.

Двічі натисніть DumpIt і дайте відповідь на запитання програми.

```
DumpIt 3.6.20230117 (X64) (Jan 17 2023)
Copyright (C) 2007 - 2021, Matt Suiche (msuiche)
Copyright (C) 2016 - 2021, Comae Technologies DMCC <https://www.comae.com>
Copyright (c) 2022, Magnet Forensics, Inc. <https://www.magnetforensics.com/>
All rights reserved.

Thanks for using DumpIt! Always use Microsoft crash dumps!

  Destination path:          \??\d:\DOC\??????? ????????????\???? ???????? IFCI\
IFCI_CCICF_Lab 2 - Forensic Acquisition\EXPERT1-20250603-085041.dmp

  Computer name:             EXPERT1


  --> Proceed with the acquisition ? [y/n] y

  [+] Information:
  Dump Type:                  Microsoft Crash Dump


  [+] Machine Information:
  Windows version:            10.0.19045
  MachineId:                  03560274-043C-0540-5A06-410700080009
  TimeStamp:                  133934142439966575
  Cr3:                        0x1ad000
  KdCopyDataBlock:            0xfffff80566f11228
  KdDebuggerData:             0xfffff80567600b20
  KdpDataBlockEncoded:        0xfffff80567650b00

  Current date/time:          [2025-06-03 (YYYY-MM-DD) 8:50:44 (UTC)]
  + Processing...
```

Рис. 12. Використання DumpIt

Розмір створеного дампу: _____

Візьміть невеликий USB-накопичувач або MicroSD картку (бажано менше 8 ГБ, чим більше, тим більше триватиме процес) і вставте його в комп’ютер.

Скопіюйте папку з файлами на ваш вибір на зовнішній накопичувач.

Відкрийте FTK Imager.

Виберіть File > Create Disk Image, виберіть Physical Drive і натисніть Далі.

Виберіть фізичний пристрій, який представляє ваш зовнішній накопичувач. (Імовірно \\.\PHYSICALDRIVE1). Натисніть Finish.

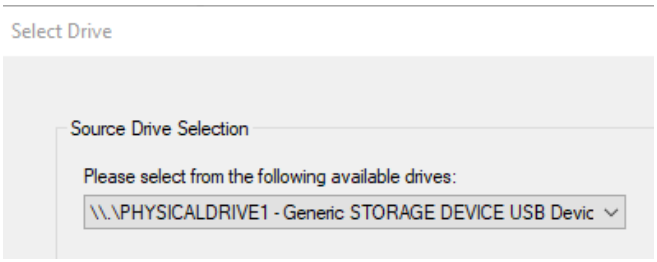


Рис. 13. Процес виготовлення побітової копії носія за допомогою FTK Imager

Під полем призначення образу Image Destination(s) натисніть кнопку Add.

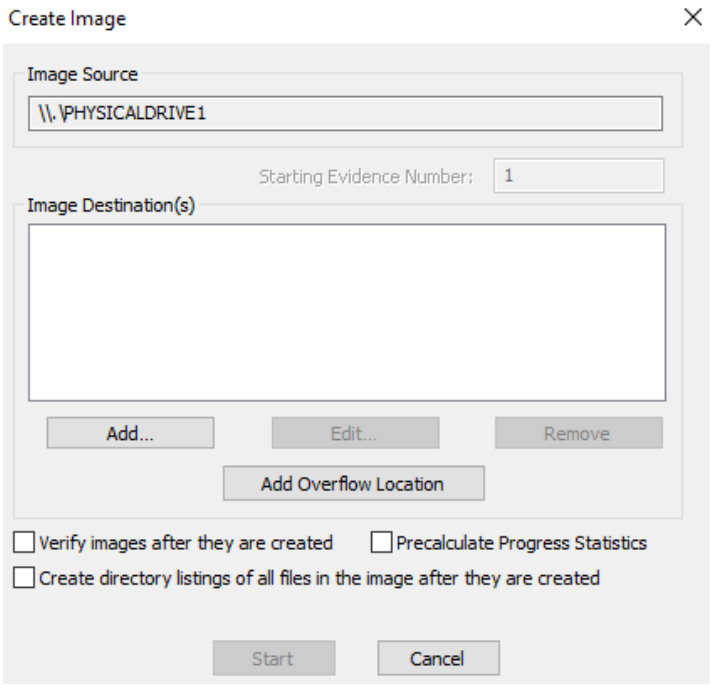


Рис. 14. Процес виготовлення побітової копії носія за допомогою FTK Imager

Виберіть Raw (dd) і натисніть Далі.

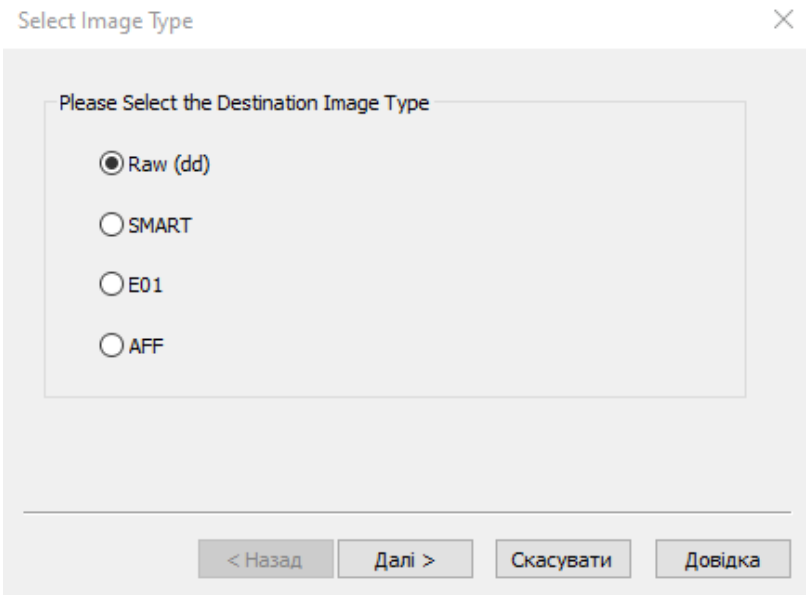


Рис. 15. Процес виготовлення побітової копії носія за допомогою FTK Imager

Додайте інформацію про справу за власним вибором.

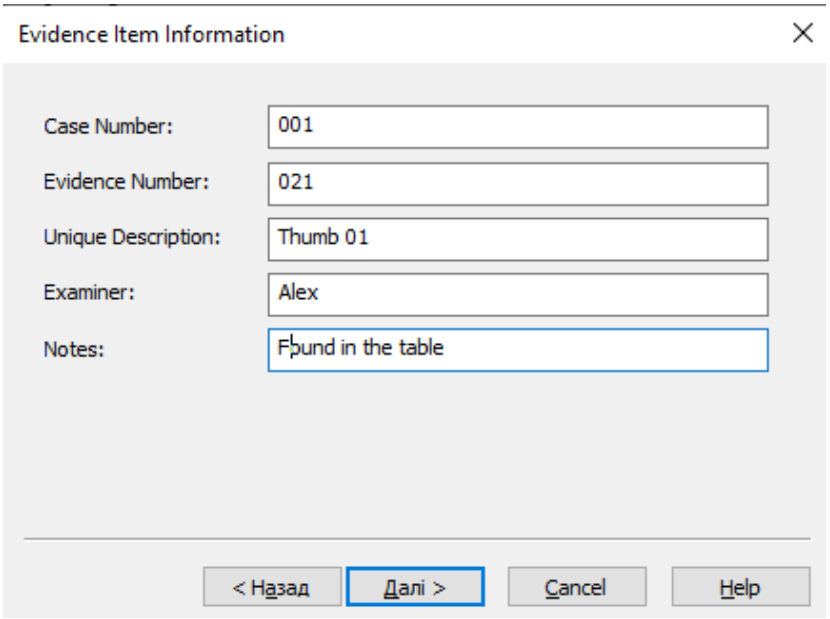


Рис. 16. Процес виготовлення побітової копії носія за допомогою FTK Imager

Виберіть папку призначення для побітової копії цифрового носія та дайте їй назву файлу.

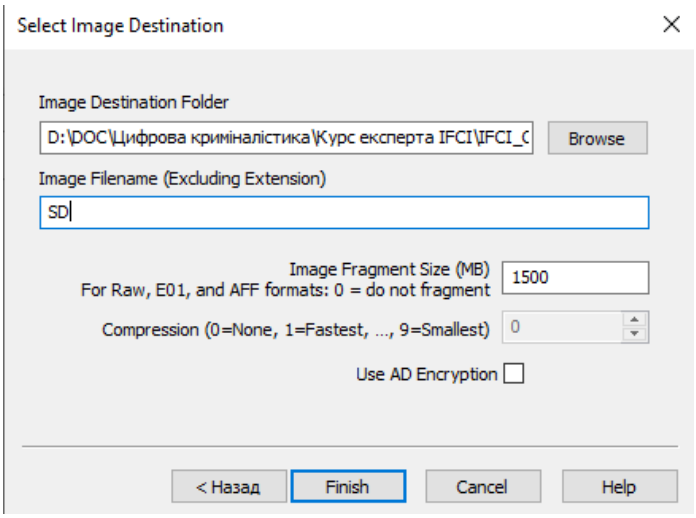


Рис. 17. Процес виготовлення побітової копії носія за допомогою FTK Imager

Натисніть Finish.

Зніміть позначку з пункту Перевіряти зображення після їх створення (Verify images after they are created). У реальній справі це гарна ідея, але це збільшить час, необхідний для виконання цієї лабораторної.

Після завершення криміналістичного образу натисніть Image Summary. Запишіть наступну інформацію:

Хеш MD5: _____

Розмір вихідних даних (Source data size): _____

Кількість секторів (Sector count): _____

Виберіть File > Add Evidence Item > Image File > Далі.

Перейдіть до файлу побітової копії цифрового носія. Якщо він багатосегментний, виберіть лише перший (.001).

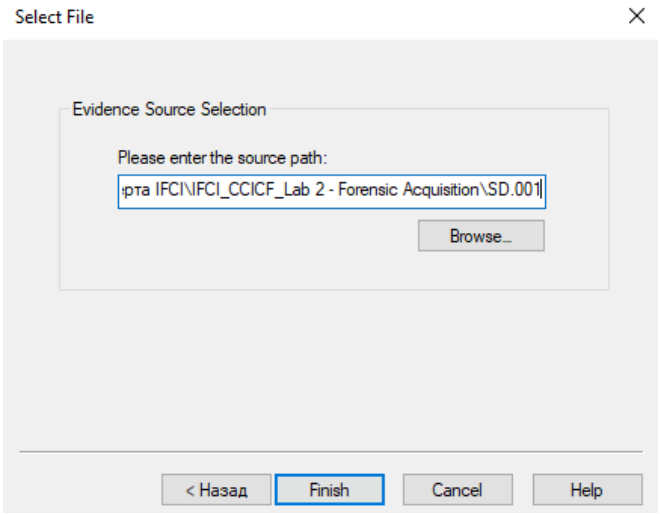


Рис. 18. Відкриття побітової копії носія за допомогою FTK Imager

Перегляньте структуру папок копії носія, зверніть увагу на файли, які ви зберегли туди раніше.

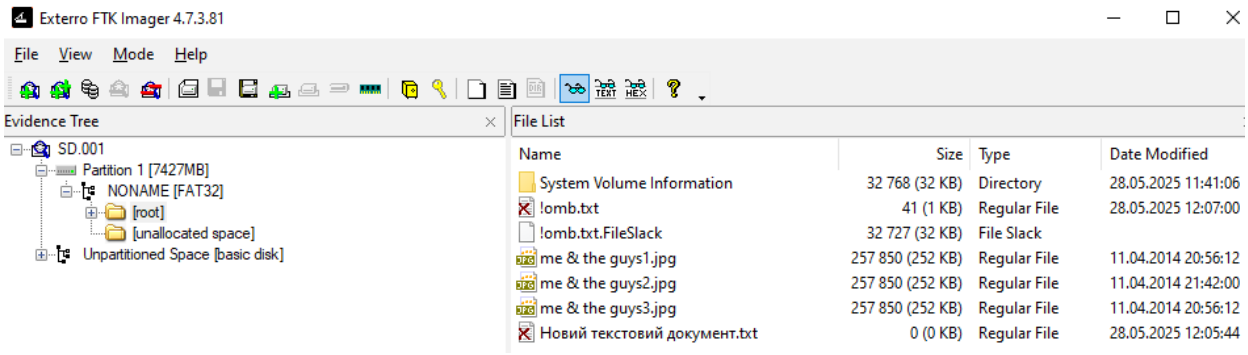


Рис. 19. Відкриття побітової копії носія за допомогою FTK Imager

Контрольні питання

1. Які принципи необхідно дотримуватися під час вилучення цифрових доказів?
2. Чому під час криміналістичного дослідження рекомендується працювати з копіями, а не з оригінальними носіями?
3. Які особливості вилучення цифрових доказів із вимкненої системи?
4. Які особливості вилучення цифрових доказів із увімкненої системи?
5. Чому під час дослідження працюючої системи рекомендується спочатку створювати дамп оперативної пам’яті?
6. Які типи даних можуть міститися в оперативній пам’яті?
7. Що таке дамп оперативної пам’яті?
8. Яку інформацію можна отримати з дампу оперативної пам’яті?
9. Які дані можуть бути втрачені після вимкнення комп’ютера?
10. Що таке побітова копія цифрового носія?
11. Чим побітова копія відрізняється від звичайного копіювання файлів?
12. Які дані містить побітова копія носія?
13. Для чого після створення побітової копії обчислюються хеш-значення?
14. Що таке блокіратор запису (Write Blocker)?
15. Для чого використовуються блокіратори запису?
16. Які наслідки може мати підключення носія без блокіратора запису?
17. Що таке BitLocker?
18. Чому наявність BitLocker ускладнює криміналістичне дослідження?
19. Що таке RAID-масив?
20. Які труднощі можуть виникнути під час дослідження RAID-масивів?
21. Що таке віртуальна машина?

22. Які популярні гіпервізори використовуються сьогодні?
23. Які цифрові докази можуть міститися у віртуальній машині?
24. Яке призначення програми DumpIt?
25. Які рекомендації щодо збору доказів наведені в IETF RFC 3227?
26. У якій послідовності рекомендується збирати цифрові докази згідно з RFC 3227?
27. Чому рекомендується використовувати власні криміналістичні інструменти, а не програми досліджуваної системи?
28. Чому не рекомендується вимикати систему до завершення збору доказів?
29. Які події можуть активувати механізм самознищення даних?
30. Для чого використовуються Faraday Bags?
31. Які способи ізоляції системи від мережі можуть застосовуватися під час розслідування?

Лабораторна робота 3
ВІДНОВЛЕННЯ ФАЙЛІВ

Мета заняття: ознайомитися з принципами організації зберігання даних у файлових системах та особливостями розміщення файлів на цифрових носіях; дослідити структуру файлових систем FAT32 та NTFS, механізми адресації даних за допомогою секторів і кластерів, а також особливості використання вільного простору та Slack Space; ознайомитися з принципами видалення файлів у сучасних файлових системах та можливостями їх відновлення; дослідити вплив файлової системи на процес відновлення цифрових доказів; отримати практичні навички пошуку та відновлення видалених файлів, аналізу вільного простору носія інформації та дослідження залишкових даних за допомогою спеціалізованих криміналістичних інструментів.

Теоретичні відомості

Файлова система – це спосіб організації, зберігання та доступу до даних на носіях інформації (жорстких дисках, SSD-накопичувачах, картах пам'яті, флеш-накопичувачах тощо). Вона визначає структуру розміщення файлів і каталогів, правила їх іменування, механізми керування вільним простором та доступом до даних.

Різні операційні системи використовують різні файлові системи.

Таблиця 2

Файлові системи

Операційна система	Windows	Windows, USB	Windows, macOS, Android	Linux, Android	macOS, iOS
Файлова система	NTFS	FAT32	exFAT	ext4	APFS

Під час криміналістичного дослідження знання особливостей файлових систем є необхідним для пошуку, аналізу та відновлення цифрових доказів.

Сектор є найменшою фізичною одиницею зберігання даних на носії інформації. Традиційно розмір сектора становить 512 байт, хоча сучасні накопичувачі можуть використовувати сектори розміром 4096 байт (4 КБ).

Кластер є найменшою логічною одиницею зберігання даних, яку використовує файлова система. Один кластер складається з одного або декількох секторів. Розмір кластера визначається під час форматування носія та може становити 4 КБ, 8 КБ, 16 КБ або більше.

Файлова система працює саме з кластерами. Навіть якщо файл займає лише декілька байтів, для нього виділяється цілий кластер.

Наприклад, якщо розмір кластера становить 4096 байт, а розмір файлу – 3000 байт, то решта 1096 байт залишаться незаповненими.

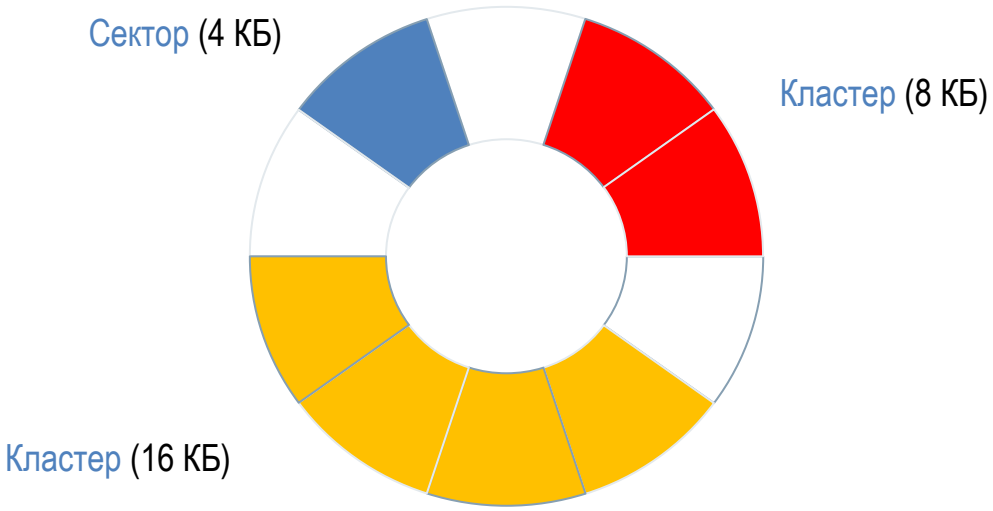


Рис. 20. Сектори та кластери

Slack Space – це незаповнений простір між кінцем файлу та кінцем кластера, виділеного для цього файлу.

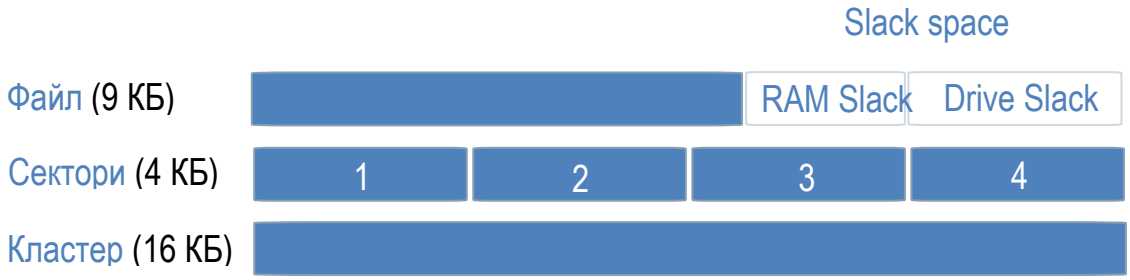


Рис. 21. Slack Space

У цифровій криміналістиці slack space становить особливий інтерес, оскільки може містити залишки раніше записаних даних.

Розрізняють два види slack space:

- RAM Slack – простір між кінцем файлу та кінцем сектора.
- Drive Slack – простір між кінцем сектора та кінцем кластера.

Оскільки операційна система зазвичай не очищує цей простір під час запису нового файлу, у ньому можуть зберігатися фрагменти документів, зображень, електронних листів та інших даних. Дослідження slack space часто дозволяє отримати інформацію навіть після видалення файлів.

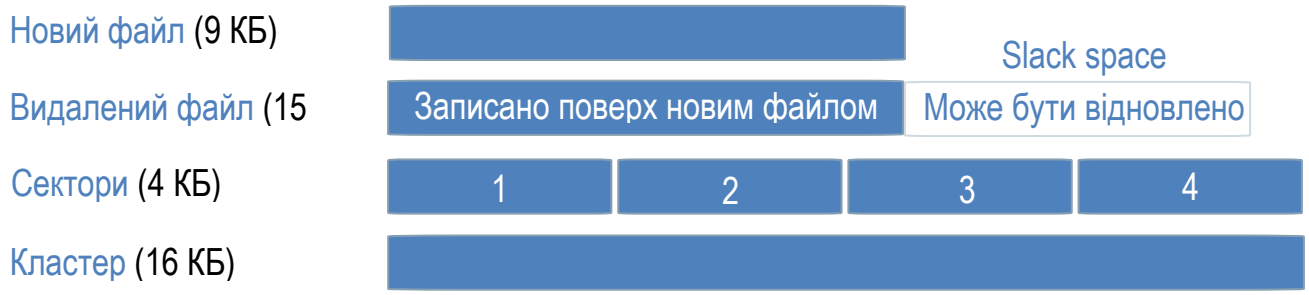


Рис. 22. Slack Space та відновлення файлів

Поширеною помилкою є припущення, що після видалення файл негайно зникає з носія інформації. У більшості файлових систем видаляється не сам файл, а лише інформація про нього у файловій таблиці. Область диска, яку займав файл, позначається як доступна для повторного використання. Фізичні дані залишаються на носії до моменту їх перезапису новими даними. Саме тому видалені файли часто можуть бути відновлені за допомогою криміналістичних інструментів. Відновлення файлів можливе доти, доки відповідні сектори або кластери не були перезаписані.

Вільний простір (Free Space) – це область носія, яку файлова система вважає доступною для запису нових даних. Наявність позначки «вільний простір» не означає відсутність даних. Часто у таких областях зберігаються:

- видалені файли;
- фрагменти раніше існуючих файлів;
- залишки тимчасових файлів;
- службова інформація файлової системи.

Тому аналіз вільного простору є важливим етапом криміналістичного дослідження.

FAT32 є однією з найстаріших файлових систем, яка досі широко використовується на флеш-накопичувачах та картах пам’яті.



Рис. 23. Структура FAT32

Основними компонентами файлової системи FAT32 є:

- Boot Sector – початковий сектор носія, який містить завантажувальний код та параметри файлової системи.
- File Allocation Table (FAT) – таблиця розміщення файлів, яка містить інформацію про використання кластерів та їх належність файлам.

– Root Directory – кореневий каталог файлової системи.
– Data Area – область даних, у якій безпосередньо зберігаються файли та каталоги.

Під час видалення файлу FAT32 не стирає його вміст. Виконуються такі дії:

– перший символ імені файлу замінюється спеціальним маркером E5h;
– запис про файл у таблиці FAT видаляється;
– кластери позначаються як вільні.

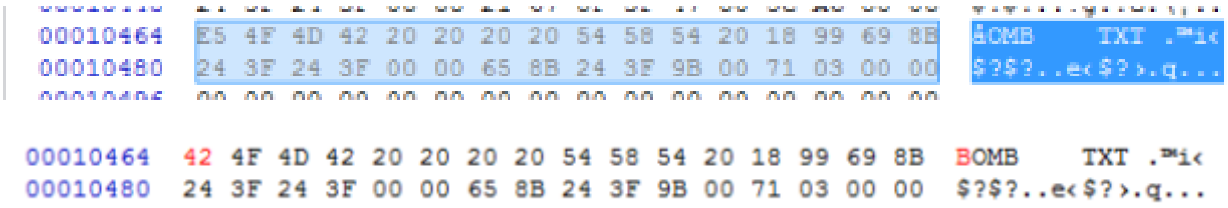


Рис. 24. Видалення файлу у FAT32

До моменту перезапису цих кластерів файл може бути відновлений спеціалізованими програмами.

NTFS є основною файловою системою сучасних операційних систем Windows. Центральним елементом NTFS є головна файлова таблиця – Master File Table (MFT). MFT являє собою спеціальний системний файл, що містить записи про всі файли та каталоги файлової системи.

Для кожного файлу зберігаються:

– ім’я файлу;
– розмір;
– розташування даних;
– часові позначки;
– атрибути безпеки;
– додаткова службова інформація.

Файлова система також створює резервну копію критично важливих структур MFT. Під час видалення файлу його дані зазвичай не знищуються. Файлова система:

– видаляє запис про використання кластерів;
– позначає відповідні області як вільні;
– залишає самі дані на диску.

Тому відновлення файлів часто можливе навіть після очищення кошика.

Кластери файлу можуть розташовуватися на диску непослідовно. Таке явище називається фрагментацією.

Відновлення файлів – це процес пошуку та реконструкції даних, які були видалені або втратили зв’язок із файловою системою.



Рис. 25. Розташування кластерів файлу на диску (фрагментація)

Для відновлення використовуються два основних підходи:

- Відновлення за файловою системою. У цьому випадку аналізуються записи файлових таблиць (FAT, MFT та інші), які можуть містити інформацію про видалені файли.
- Відновлення за сигнатурами файлів (File Carving). У цьому випадку пошук виконується за характерними послідовностями байтів, що визначають початок та кінець файлів певних форматів.

На сучасних SSD-накопичувачах використовується команда TRIM. Після видалення файлу операційна система може повідомити накопичувачу, що відповідні блоки більше не використовуються. Контролер SSD виконує фізичне очищення цих блоків, що суттєво ускладнює або робить неможливим подальше відновлення файлів. Тому відновлення даних із SSD після виконання TRIM значно менш ефективне, ніж відновлення даних із традиційних жорстких дисків.

Для відновлення файлів використовуються спеціалізовані інструменти цифрової криміналістики, зокрема FTK Imager, Autopsy, X-Ways Forensics, EnCase, PhotoRec та інші.

Завдання на лабораторну роботу

Завантажте архів побітової копії підозрілого зовнішнього накопичувача Suspect_MicroSD.zip (https://drive.google.com/file/d/1g2TAl1BecvndsuezcnGhckbQ0kYZ2hdC). Розархівуйте його.

Відкрийте FTK Imager.

Виберіть File > Image Mounting

Додайте файл образу Suspect_MicroSD.001, не змінюйте параметри за замовчуванням і натисніть Mount.

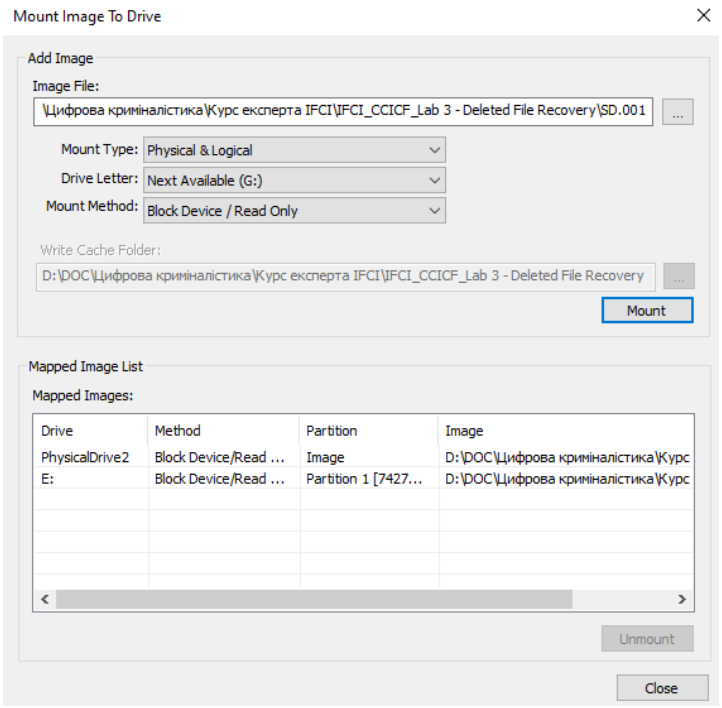


Рис. 26. Додавання файлу образу в FTK Imager

Перейдіть до Провідника Windows і відкрийте диск «E:».

*ПРИМІТКА: Скоріш за все у вас це буде «E:», але може бути й інший диск

Це змонтована версія образу MicroSD картки підозрюваного. Зверніть увагу на файли, які зараз знаходяться у образі.

В FTK Imager виберіть монтовані диски та натисніть Unmount.

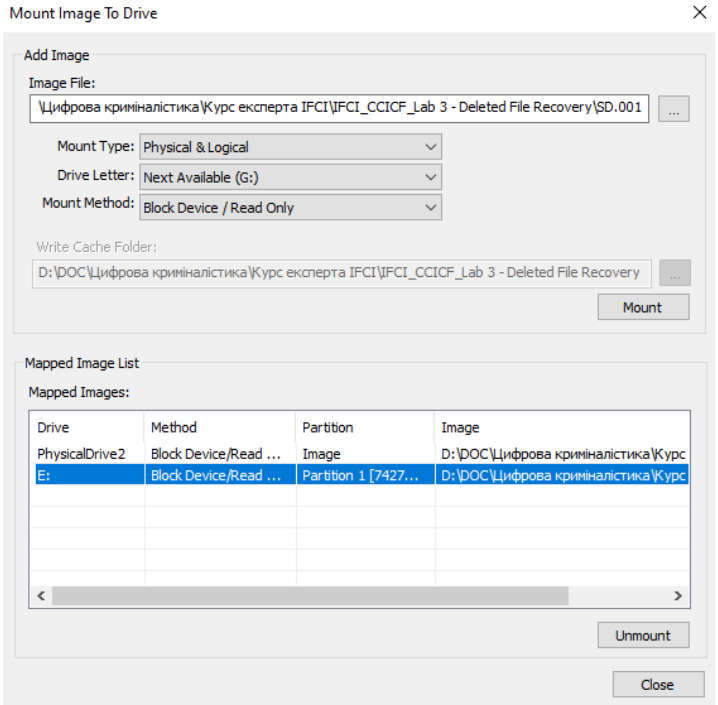


Рис. 27. Додавання файлу образу в FTK Imager

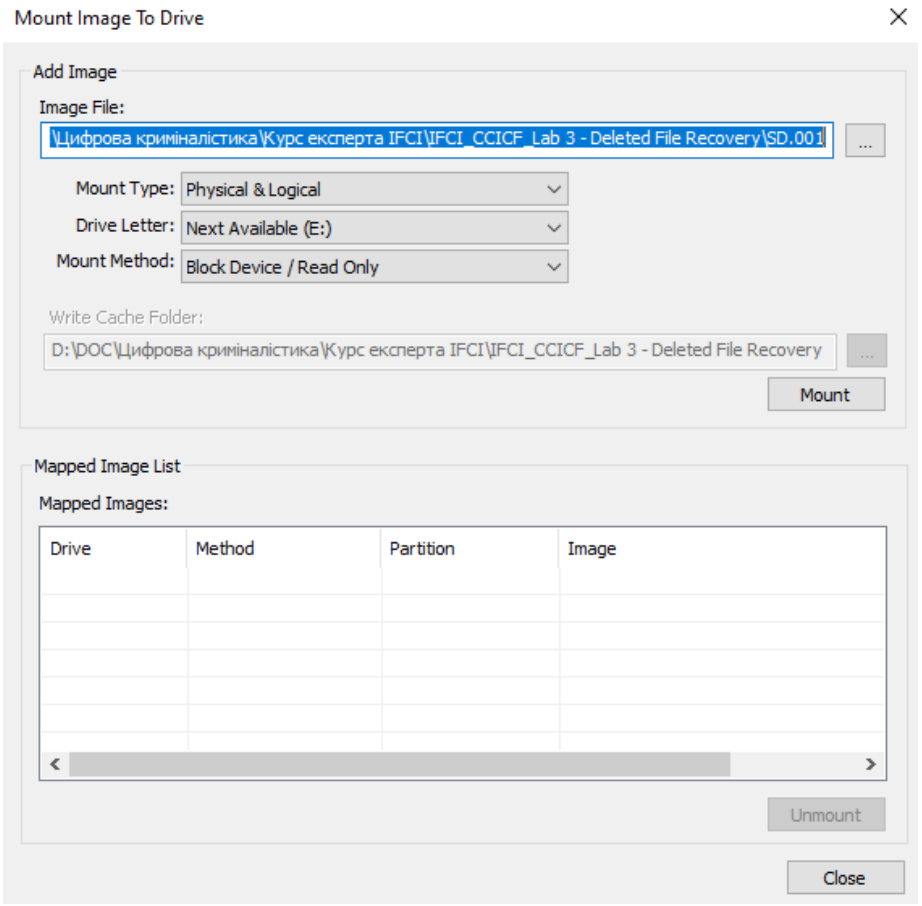


Рис. 28. Додавання файлу образу в FTK Imager

Натисніть Close.

Відкрийте шістнадцятковий редактор «HxD».

Виберіть Інструменти > Відкрити образ диска та Suspect_MicroSD.001.

Здійсніть пошук за запитом txt Пошук > Знайти або Ctrl + F

Пошук вниз – F3, пошук вверх – Shift + F3.

Потім за запитом omb.

Або відразу перейдіть до сектора 16384. Це початок таблиці розміщення файлів (FAT). Вона зберігає метадані файлу, такі як розмір, час створення, час зміни та ім'я файлу, а також фізичне розташування файлу на диску.

В секторі 16384 ви побачите назву файлу, який починається з шістнадцяткового символу E5 (сигма). Це позначає видалений файл. У файловій системі FAT перший символ видаленого файлу замінюється на шістнадцятковий E5 (сигма), а розташування файлу обнуляється, таким чином позначаючи його як доступний.

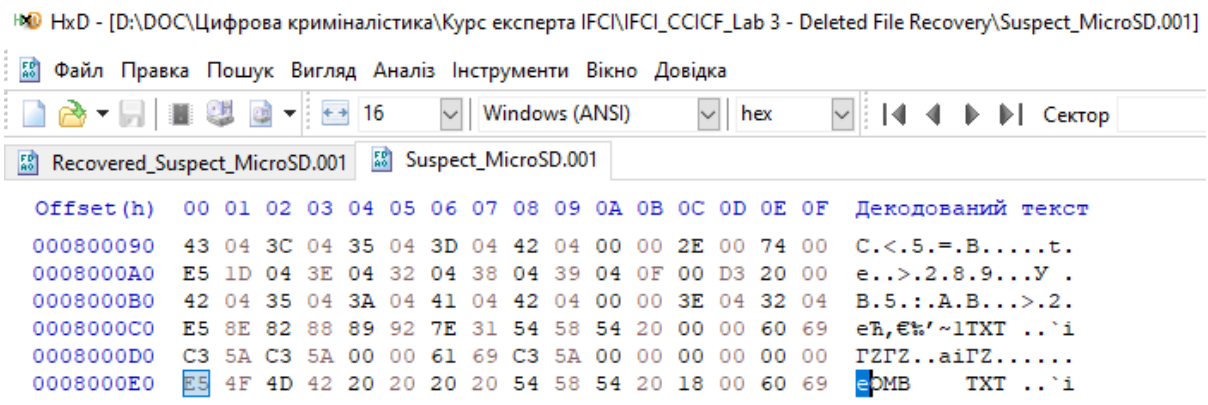


Рис. 29. Пошук видаленого файлу у HxD

Виберіть символ E5 та замініть його на B.

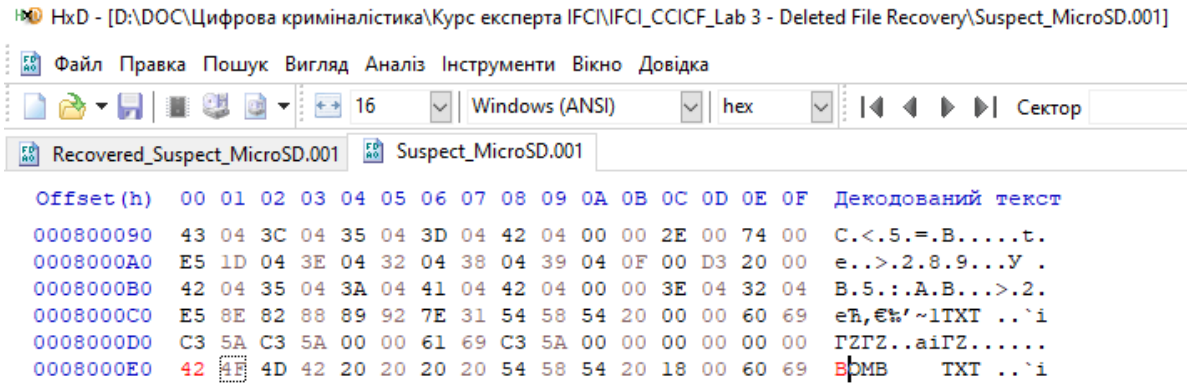


Рис. 30. Відновлення видаленого файлу у HxD

Виберіть Файл > Зберегти як та збережіть цей файл під назвою Recovered_Suspect_MicroSD.001.

Поверніться до FTK Imager, скористайтеся утилітою монтування, щоб змонтувати Recovered_Suspect_MicroSD.001 так само, як ви змонтували оригінальний образ.

Відкрийте змонтований диск у Файловому провіднику Windows. Зверніть увагу на файли, які тепер знаходяться на образі.

*ПРИМІТКА: Новий файл «bomb.txt» тепер видно з усіма його метаданими (відкрийте властивості файлу через контекстне меню). Однак фізичне розташування файлу все ще обнулено в таблиці FAT. Тому ми не зможемо фактично відкрити цей файл.

Поверніться до FTK Imager знову відмонтуйте диск та закрийте монтування побітової копії.

Виберіть File > Add Evidence Item.

Виберіть Image File та перейдіть до файлу Suspect_MicroSD.001 і натисніть Finish.

FTK Imager автоматично відновлює розташування видаленого файлу та відображає його. Знайдіть вміст образу в кореневій папці.

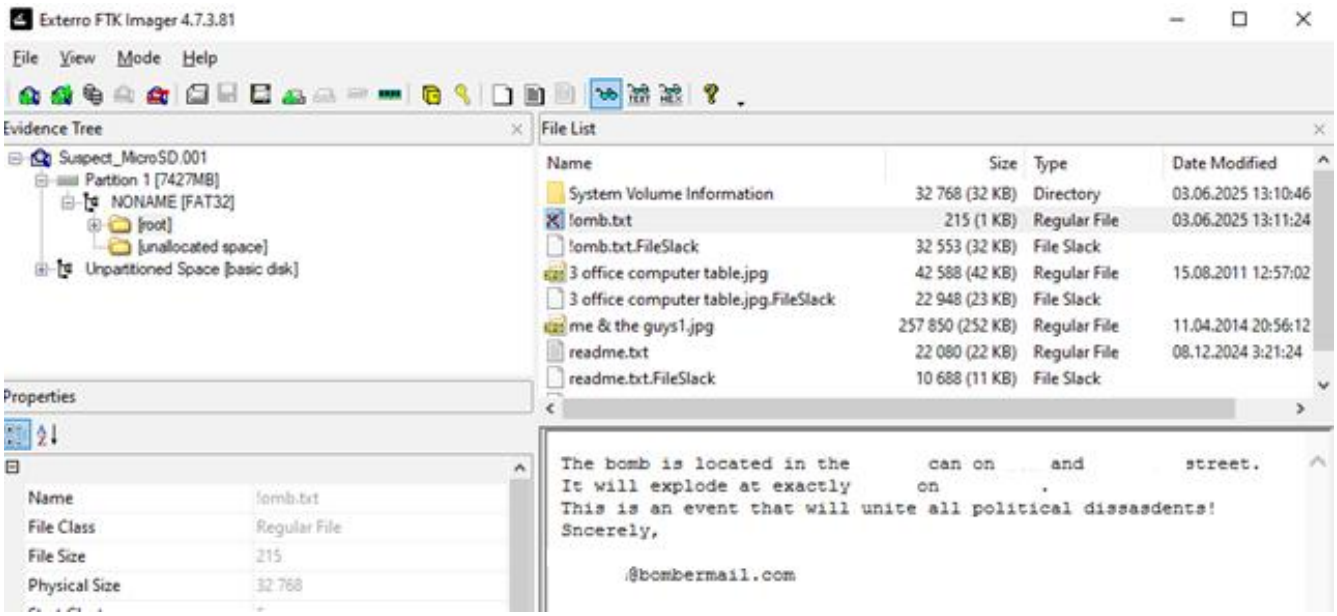


Рис. 31. Пошук видаленого файлу у FTK Imager

Бомба знаходиться:_____
Вибух станеться:_____
Автор листа:_____
Встановіть та відкрийте Autopsy (https://www.autopsy.com/download/)

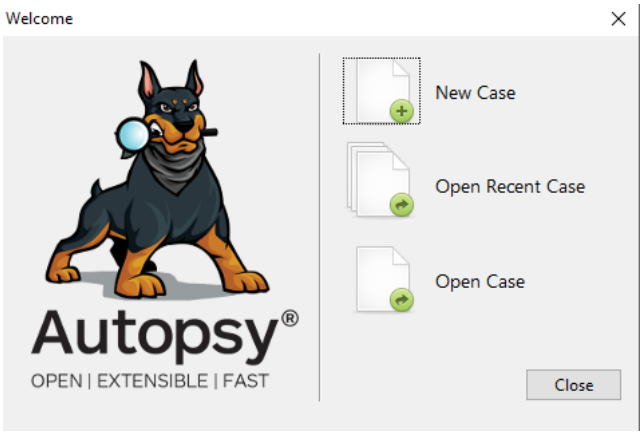


Рис. 32. Додавання файлу образу в Autopsy

Введіть назву справи (Case Name:) та через Brows вкажіть папку, де будуть зберігатися файли справи. Next.

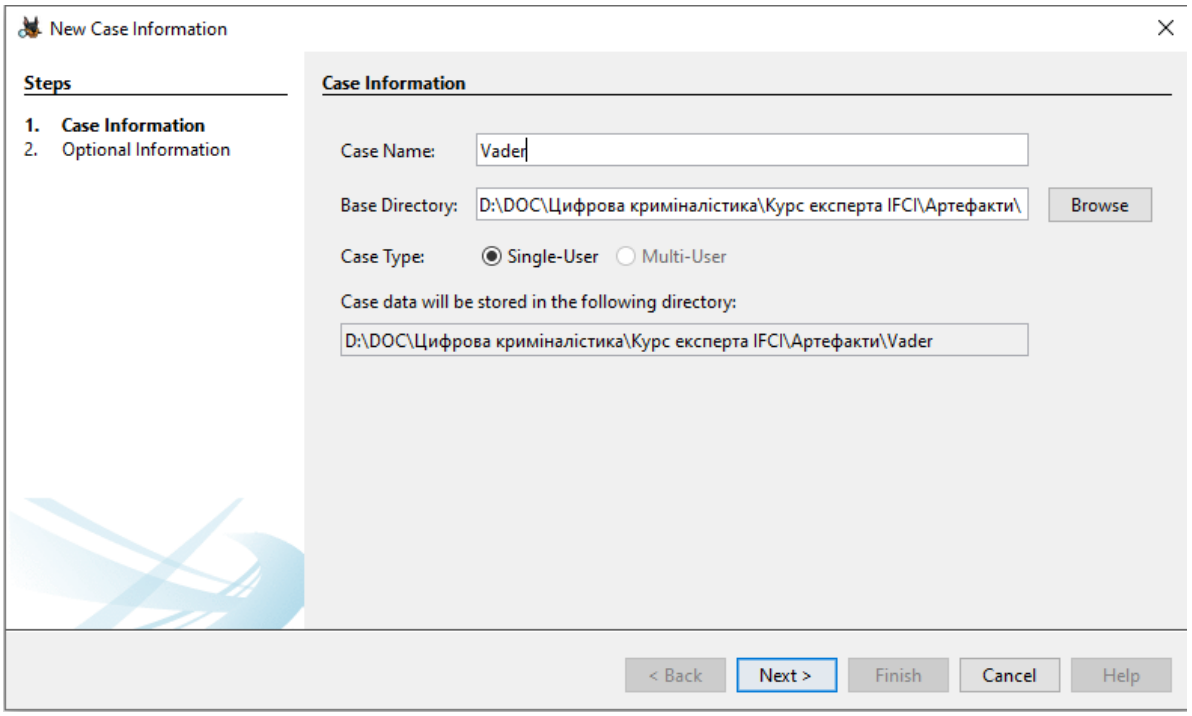


Рис. 33. Додавання файлу образу в Autopsy

Введіть свою інформацію.

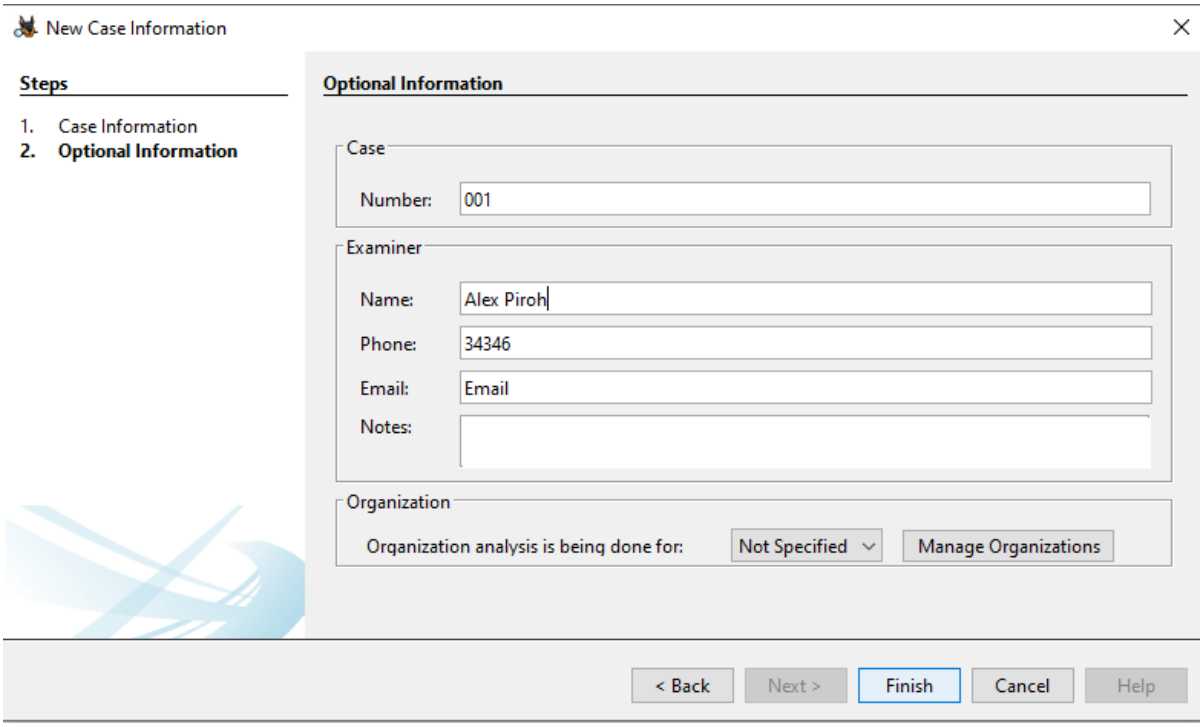


Рис. 34. Додавання файлу образу в Autopsy

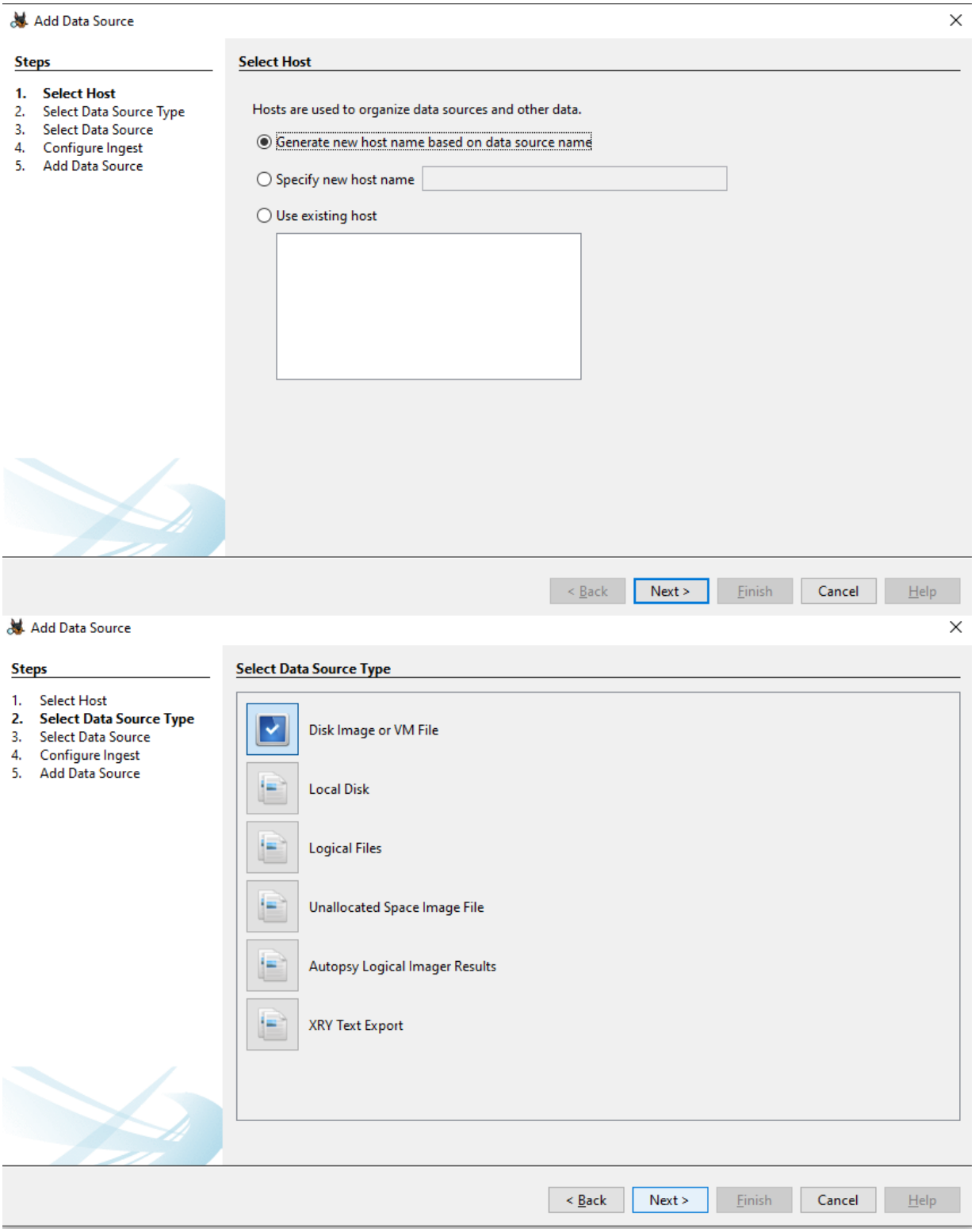


Рис. 35. Додавання файлу образу в Autopsy

Disk Image or VM File.
Browse та вкажіть файл образу Suspect_MicroSD.001.

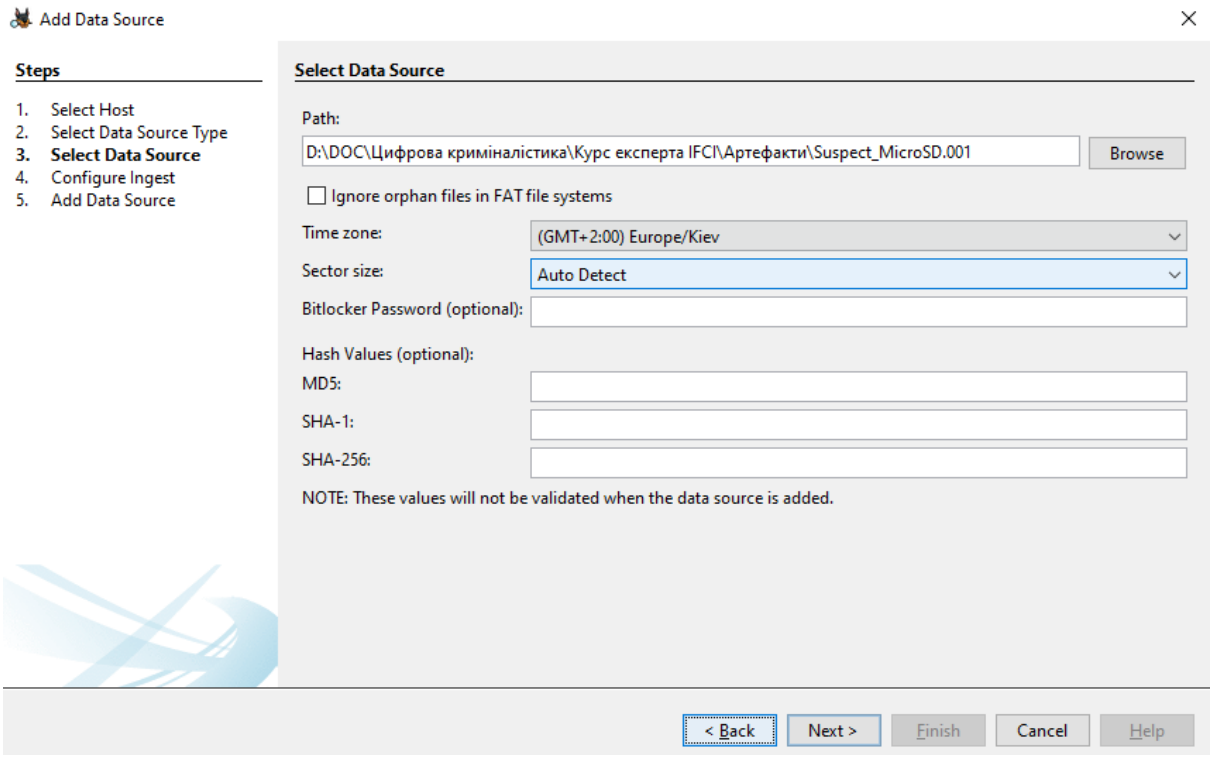


Рис. 36. Додавання файлу образу в Autopsy

Для економії часу аналізу виберіть тільки той модуль, що на малюнку.
Залиште лише: Recent Activity.
Також зверніть увагу, що вибрано All Files and Directories (Not Unallocated Space).

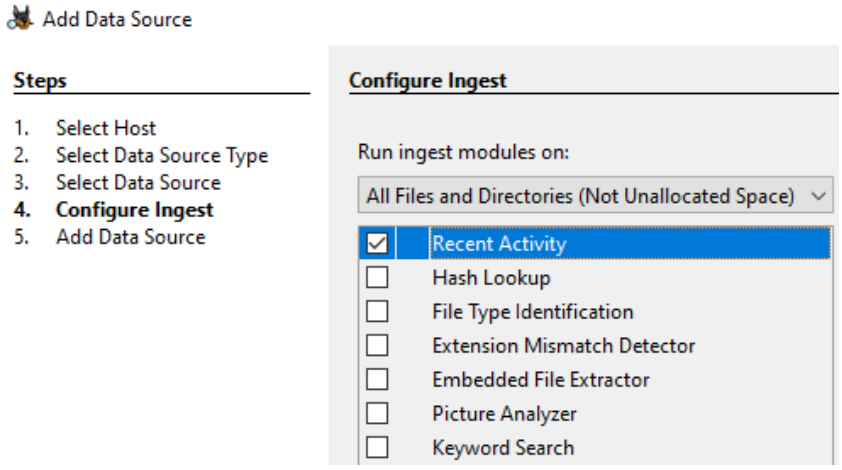


Рис. 37. Додавання файлу образу в Autopsy

Finish.
Подивиться видалені файли.

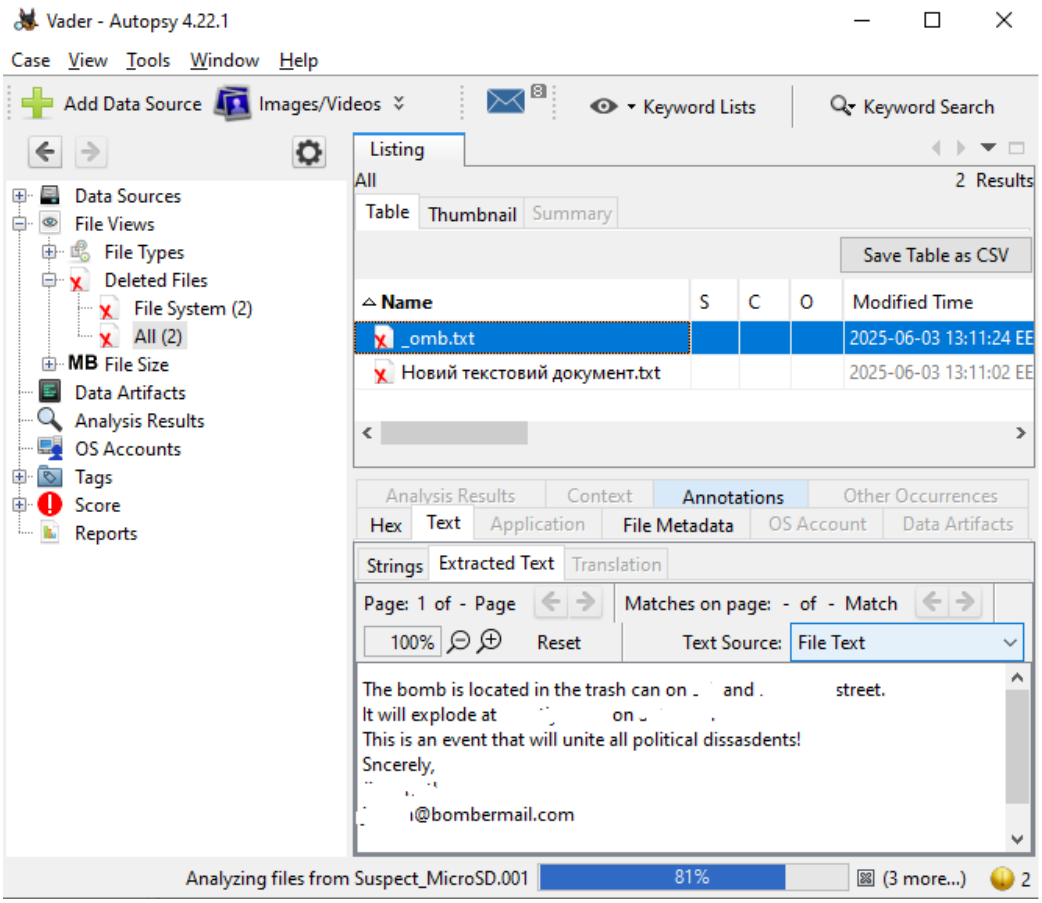


Рис. 38. Пошук видаленого файлу в Autopsy

Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки?

_____

Контрольні питання

1. Що таке файлова система?
2. Які основні функції виконує файлова система?
3. Які файлові системи найчастіше використовуються в операційних системах Windows?
4. Які файлові системи використовуються в Linux?
5. Яка файлова система використовується в сучасних операційних системах macOS?
6. Що таке сектор?
7. Який типовий розмір сектора на сучасних носіях інформації?
8. Що таке кластер?
9. Чим кластер відрізняється від сектора?
10. Що таке Slack Space?
11. Що таке RAM Slack?
12. Що таке Drive Slack?

13. Яка інформація може міститися у Slack Space?
14. Чому Slack Space становить інтерес для цифрової криміналістики?
15. Що відбувається з файлом під час його видалення?
16. Чи зникає файл фізично після його видалення?
17. За якої умови можливе відновлення видаленого файлу?
18. Що таке вільний простір (Free Space)?
19. Які дані можуть міститися у вільному просторі носія?
20. Які основні структурні елементи файлової системи FAT32?
21. Яке призначення таблиці FAT?
22. Що відбувається під час видалення файлу у файловій системі FAT32?
23. Для чого використовується маркер E5 у FAT32?
24. Що таке MFT?
25. Яку інформацію містить запис MFT?
26. Що відбувається з файлом під час його видалення у файловій системі NTFS?
27. Що таке фрагментація файлів?
28. Що таке відновлення файлів?
29. Які основні підходи використовуються для відновлення файлів?
30. У чому полягає відновлення файлів за файловою системою?
31. Що таке File Carving?
32. Що таке команда TRIM?
33. Для чого використовується команда TRIM у SSD-накопичувачах?
34. Як TRIM впливає на можливість відновлення видалених файлів?
35. Чому відновлення даних із SSD часто складніше, ніж із жорстких дисків?
36. Які програмні засоби можуть використовуватися для відновлення видалених файлів?
37. Які можливості надає FTK Imager під час аналізу файлової системи?

Лабораторна робота 4
АНАЛІЗ ОСНОВНИХ АРТЕФАКТІВ WINDOWS 10

Мета заняття: ознайомитися з цифровими артефактами операційної системи Windows 10; дослідити структуру профілю користувача Windows і розташування основних джерел цифрових доказів; ознайомитися з особливостями зберігання користувацьких документів, ярликів, тимчасових файлів та файлів мініатюр зображень; дослідити можливості використання артефактів Windows для відновлення відомостей про діяльність користувача; отримати практичні навички пошуку, аналізу та інтерпретації цифрових артефактів за допомогою криміналістичних інструментів.

Теоретичні відомості

Під час використання комп'ютера операційна система та прикладні програми постійно створюють, змінюють та зберігають різноманітні службові дані. Такі дані називаються цифровими артефактами.

Цифровий артефакт – це будь-який об'єкт або слід, створений у результаті роботи користувача, операційної системи чи програмного забезпечення, який може містити інформацію про події, що відбувалися в системі.

До цифрових артефактів належать:

- файли та каталоги;
- журнали подій;
- реєстр Windows;
- ярлики (LNK-файли);
- файли попереднього перегляду зображень;
- файли історії браузерів;
- кеш програм;
- тимчасові файли;
- службові файли операційної системи.

Аналіз артефактів є одним із найважливіших напрямів цифрової криміналістики, оскільки дозволяє відновити дії користувача та встановити обставини події.

Операційна система Windows є найпоширенішою операційною системою для персональних комп'ютерів. Починаючи з перших версій Windows і до сучасних Windows 10 та Windows 11, система накопичує значну кількість службових даних про діяльність користувача. У криміналістиці особливий інтерес становлять артефакти Windows 10, оскільки ця операційна система тривалий час була домінуючою серед користувачів персональних комп'ютерів.



Рис. 39. Версії ОС Windows

Цифрові докази в Windows можуть міститися як у звичайних файлах користувача, так і в прихованих системних структурах.

Під час аналізу необхідно враховувати особливості профілів користувачів, оскільки більшість артефактів зберігається саме в їхніх каталогах. Для кожного користувача Windows створюється окремий профіль. Типовий шлях до профілю користувача: C:\Users<UserName>. У профілі користувача зберігаються:

- документи;
- налаштування програм;
- тимчасові файли;
- історія використання системи;
- файли робочого столу;
- кеші різних програм.

Саме профіль користувача є одним із найважливіших джерел цифрових доказів.

Робочий стіл Windows є одним із найпоширеніших місць зберігання документів користувача. Файли та ярлики робочого столу розташовуються за адресою: C:\Users<UserName>\Desktop. Під час криміналістичного дослідження аналіз вмісту робочого столу дозволяє встановити:

- документи, з якими працював користувач;
- програми, які запускалися;
- ярлики на зовнішні носії.

Каталог Documents (Мої документи) є стандартним місцем зберігання користувацьких файлів. Типовий шлях: C:\Users<UserName>\Documents. У цьому каталозі можуть зберігатися:

- текстові документи;
- електронні таблиці;
- презентації;
- архіви;
- графічні файли;
- резервні копії даних.

Аналіз цього каталогу дозволяє встановити коло інтересів користувача та характер його діяльності.

Під час роботи програм та операційної системи створюється велика кількість тимчасових файлів. Типовий каталог: C:\Users<UserName>\AppData\Local\Temp. Тимчасові файли можуть містити:

- проміжні результати роботи програм;
- автоматично збережені документи;
- файли встановлення програм;
- фрагменти завантажених файлів;
- службову інформацію прикладного програмного забезпечення.

Часто саме в тимчасових каталогах можуть залишатися цифрові сліди діяльності користувача навіть після видалення основних файлів.

Під час перегляду графічних файлів Windows автоматично створює зменшені копії зображень для швидкого відображення в Провіднику. Ці копії називаються мініатюрами (thumbnails). Файли мініатюр зберігаються у спеціальних базах даних: C:\Users<UserName>\AppData\Local\Microsoft\Windows\Explorer. Типові файли:

- thumbcache_32.db
- thumbcache_96.db
- thumbcache_256.db
- thumbcache_1024.db

Навіть якщо оригінальне зображення було видалено, його мініатюра може залишатися у файлах thumbcache. У цифровій криміналістиці аналіз thumbcache дозволяє:

- встановити факт перегляду зображень;
- відновити ескізи видалених файлів;
- підтвердити наявність файлів у системі в минулому.

Під час відкриття документів та запуску програм Windows автоматично створює ярлики (LNK-файли). Ярлик містить службову інформацію про файл або програму:

- повний шлях до об'єкта;
- дату створення;
- дату останнього доступу;
- дату останньої зміни;
- розмір файлу;
- серійний номер тому;
- інформацію про носій інформації.

Навіть після видалення оригінального файлу ярлик може залишатися в системі. Тому аналіз LNK-файлів дозволяє встановити:

- які файли відкривав користувач;

- коли відбувався доступ до них;
- на яких носіях вони знаходилися.

Під час роботи користувача в системі формуються численні артефакти активності. До них належать:

- відкриті документи;
- запущені програми;
- ярлики;
- тимчасові файли;
- мініатюри зображень;
- історія доступу до файлів;
- файлові шляхи;
- часові позначки подій.

Комплексний аналіз документів користувача, ярликів, тимчасових файлів, файлів мініатюр та інших артефактів дає можливість встановити:

- які файли використовувалися;
- коли відбувався доступ до них;
- які програми запускалися;
- які носії інформації підключалися;
- які дії виконував користувач.

Завдання на лабораторну роботу

Відкрийте програму FTK imager.

Додайте побітову копію підозрілого цифрового носія (Vader_Home_Computer.001) до програми FTK Imager.

File > Add Evidence Item > Image File та Далі > Browse та вибрати файл копії цифрового носія, вибрати Vader_Home_Computer.001 та відкрити > Finish.

Натисніть кнопки + для навігації по копії цифрового носія.

Перейдіть до кореневого каталогу Розділу 2 (root Partition 2).

Перейдіть до папки \Users\Owner\Documents\

Які файли можуть свідчити про злочинну діяльність?

_____

Що це за злочинна діяльність?

_____

Перейдіть до папки \Users\Owner\AppData\Local\Microsoft\Windows\Explorer\

Експортуйте її на ваш комп’ютер.

Завантажте та запустить Thumbcache Viewer (https://thumbcacheviewer.github.io/).

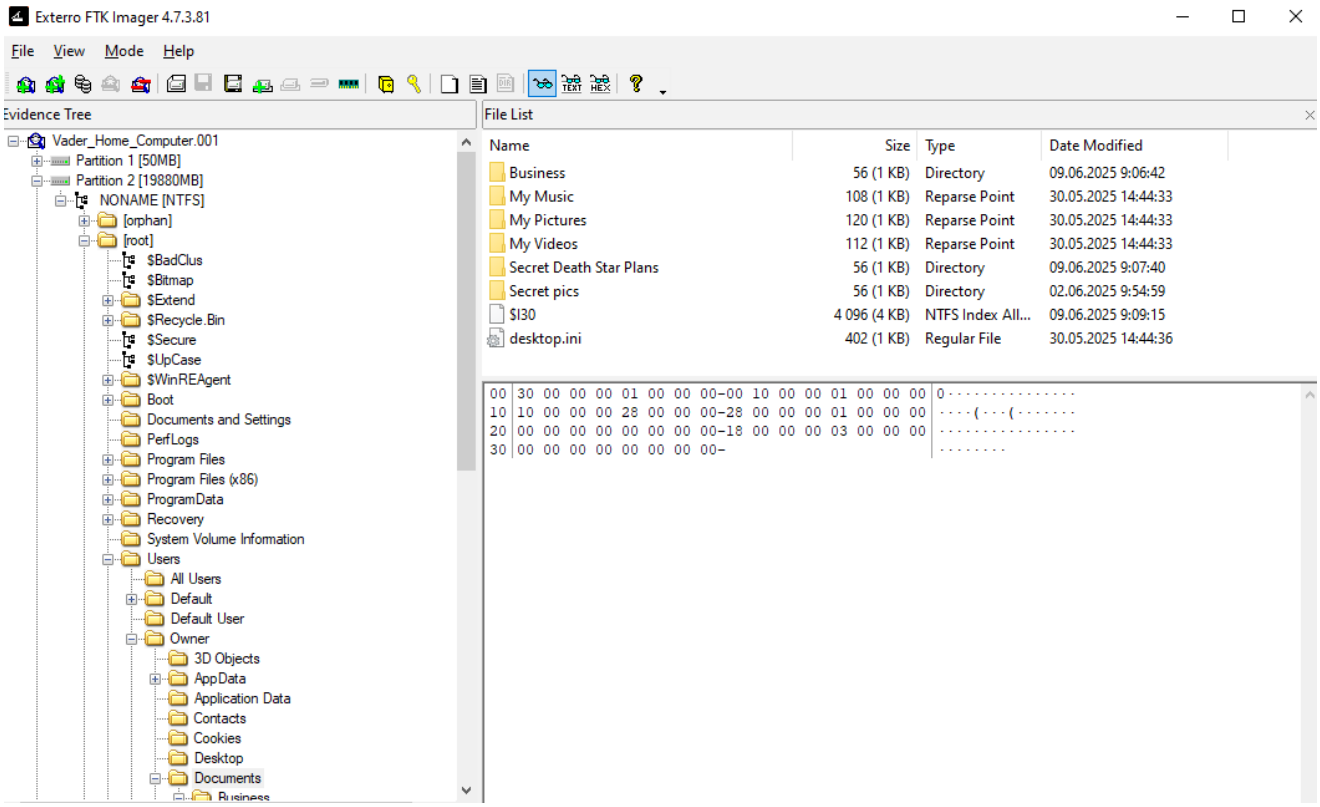


Рис. 40. Перегляд документів у FTK Imager

Відкрийте завантажені файли в Thumbcache Viewer

File > Open > Папка на вашому комп'ютері, де ви зберегли Explorer > thumbcache_768.db .

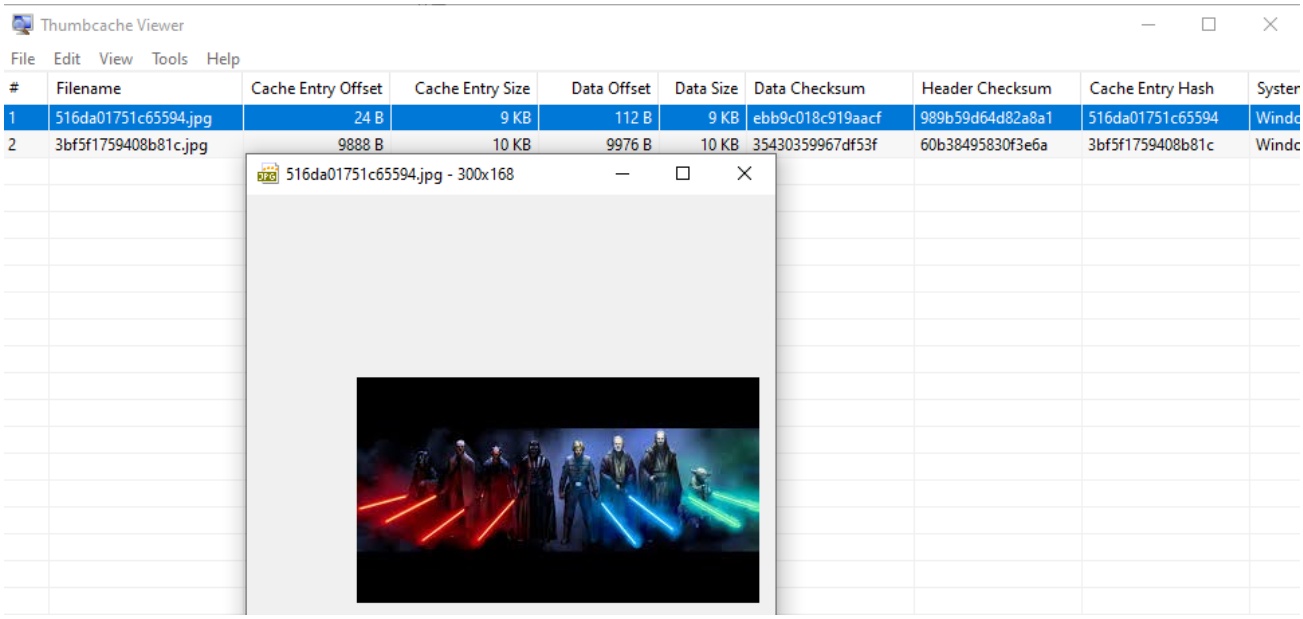


Рис. 41. Файли мініатюр в Thumbcache Viewer

Чим можуть допомогти в розслідуванні файли мініатюр (thumbcache_*.db)? Чому?

_____

Відкрийте Autopsy.

Відкрийте справу, що ви відкрили у попередніх лабораторних – Open Recent Case

Додайте нове джерело – Add Data Source.

Вкажіть шлях до Vader_Home_Computer.001.

Для економії часу аналізу виберіть тільки той модуль, що на малюнку.

Залиште лише: Recent Activity.

Також зверніть увагу, що вибрано All Files and Directories (Not Unallocated Space).

Finish.

Дочекайтеся завершення аналізу!

Це може зайняти значний час.

Tools > Options > View > When displaying times > Use another time zone > (GTM+2:00) Europe/Kyiv

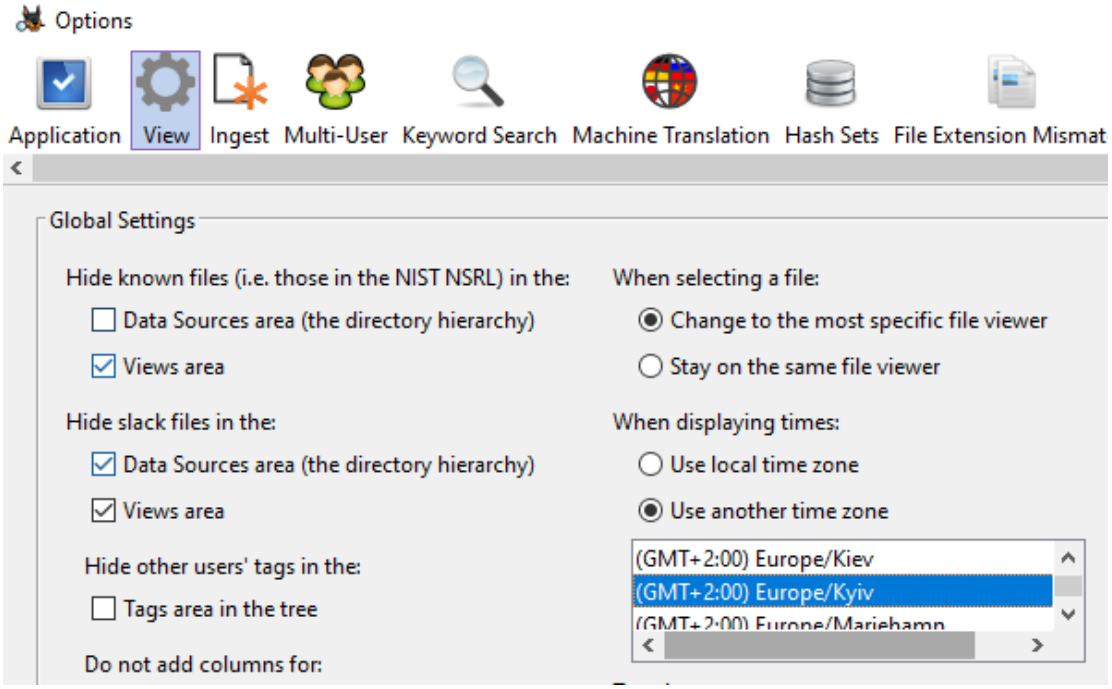


Рис. 42. Встановлення часового поясу в Autopsy

Перейдіть Data Sources > Vader_Home_Computer.001 > vol3 > \Users\Owner\Documents\

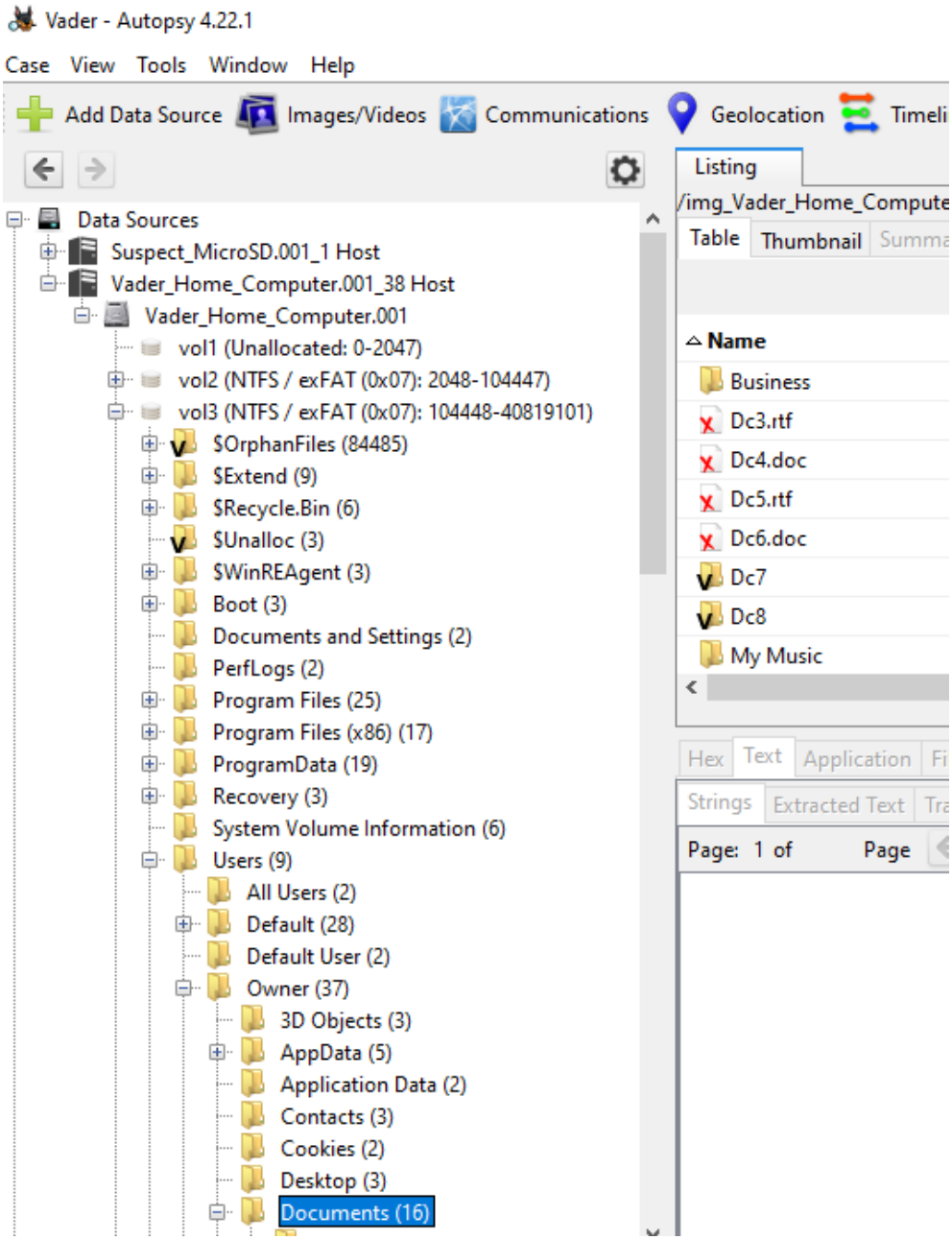


Рис. 43. Перегляд документів в Autopsy

Передивіться документи.
Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки?

Перейдіть \Users\Owner\Documents\Busines\ та перемкніть вкладку на Thumbnail

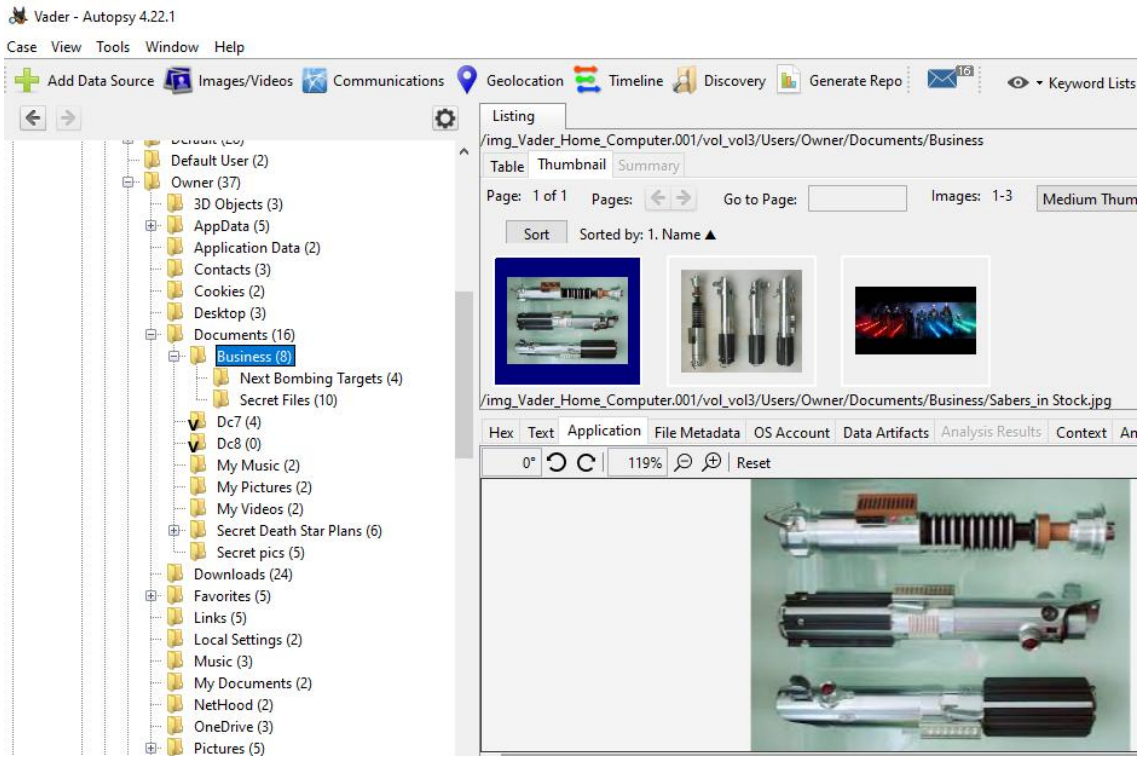


Рис. 44. Перегляд мініатюр в Autopsy

Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки?

_____

Контрольні питання

1. Що таке цифровий артефакт?
2. Які об'єкти можуть вважатися цифровими артефактами в операційній системі Windows?
3. Де зазвичай розташовується профіль користувача Windows?
4. Які дані зберігаються в профілі користувача?
5. Де розташовуються файли робочого столу користувача?
6. Яку інформацію можна отримати під час аналізу каталогу Desktop?
7. Де зазвичай зберігаються документи користувача Windows?
8. Де зазвичай розташований каталог тимчасових файлів користувача?
9. Яка інформація може міститися в каталозі Temp?
10. Що таке файли мініатюр (Thumbcache)?
11. Де розташовуються файли thumbcache у Windows?
12. Яку інформацію дозволяє отримати аналіз файлів Thumbcache?
13. Яку інформацію містить LNK-файл?
14. Які відомості про файл можна отримати з ярлика?
15. Як аналіз ярликів допомагає встановити дії користувача?

Лабораторна робота 5
АНАЛІЗ КОШИКУ

Мета заняття: ознайомитися з принципами видалення файлів в операційній системі Windows та особливостями функціонування Кошика (Recycle Bin) як джерела цифрових доказів; дослідити механізми переміщення файлів до кошика, структуру каталогів $Recycle.Bin та особливості зберігання службової інформації про видалені об'єкти; ознайомитися з призначенням файлів $I та $R, їх структурою та криміналістичним значенням; отримати практичні навички пошуку, аналізу та інтерпретації відомостей про видалені файли; дослідити можливості встановлення початкової назви, шляху розташування, часу видалення та вмісту видалених файлів.

Теоретичні відомості

Під час роботи користувача з файлами операційна система Windows забезпечує можливість їх тимчасового зберігання після видалення. Для цього використовується спеціальний системний компонент – кошик (Recycle Bin). Кошик призначений для запобігання випадковій втраті даних та дозволяє відновити видалені файли без використання спеціалізованих засобів відновлення. У цифровій криміналістиці кошик є важливим джерелом цифрових доказів, оскільки дозволяє встановити:

- факт видалення файлу;
- дату та час видалення;
- початкове розташування файлу;
- початкову назву файлу;
- зміст видаленого файлу;
- обліковий запис користувача, який виконав видалення.

Поведінка операційної системи під час видалення файлів залежить від способу видалення та типу носія інформації. У стандартному випадку після натискання клавіші Delete файл не видаляється остаточно, а переміщується до кошика. При цьому відбуваються такі зміни:

- початковий запис про файл у файловій системі більше не використовується для роботи користувача;
- для об'єкта у кошику створюється новий запис;
- файл переноситься до спеціального системного каталогу кошика;
- створюється службова інформація про видалений файл.

Самі дані файлу при цьому не змінюються.

У сучасних версіях Windows файли кошика розміщуються у прихованому системному каталозі: C:$Recycle.Bin. Для кожного користувача створюється окремий підкаталог, назва якого відповідає його SID (Security Identifier).

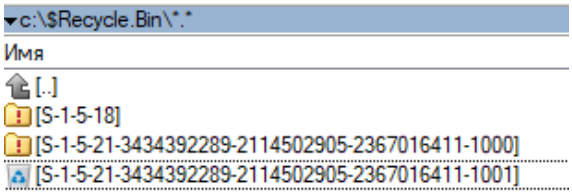


Рис. 45. Підкаталоги кошику для різних SID

SID є унікальним ідентифікатором облікового запису Windows. Завдяки цьому можна встановити, який саме користувач видалив файл.

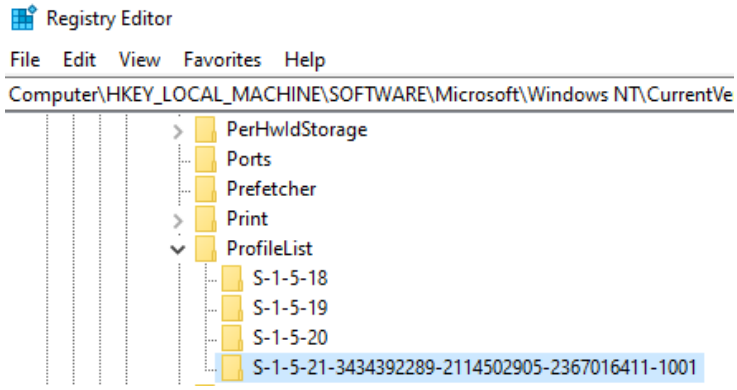


Рис. 46. SID у реєстрі

Після видалення файлу до кошика Windows створює два об'єкти:

1. Файл $R. Файл із префіксом $R містить фактичний вміст видаленого файлу ($R3GQQ8F.txt). Саме цей файл містить дані, які можуть бути відновлені користувачем через кошик.

2. Файл $I. Файл із префіксом $I містить службову інформацію про видалений об'єкт ($I3GQQ8F.txt). Файл $I містить:

- початкову назву файлу;
- початковий шлях до файлу;
- дату та час видалення;
- розмір файлу.

Саме файл $I є одним із найцінніших джерел цифрових доказів під час криміналістичного дослідження. Формат файлів $I документований та дозволяє автоматизовано відновлювати інформацію про видалені об'єкти. Ця інформація часто дозволяє підтвердити або спростувати показання користувача.

Якщо кошик не був очищений, файл можна відновити штатними засобами Windows. У випадку криміналістичного дослідження файл може бути відновлений шляхом аналізу відповідного файлу $R. Навіть після очищення

кошика частина інформації про видалені файли може залишатися у файловій системі та бути доступною для відновлення спеціалізованими інструментами цифрової криміналістики.

Існує декілька способів видалення файлів без їх переміщення до кошика. Найпоширеніші з них:

- використання комбінації клавіш Shift + Delete;
- видалення файлів із командного рядка;
- очищення кошика після видалення;
- видалення файлів зі змінних носіїв;
- використання спеціалізованих програм безповоротного видалення.

У таких випадках файл одразу позначається файловою системою як видалений. Проте фізичні дані файлу зазвичай залишаються на носії до моменту їх перезапису.

Завдання на лабораторну роботу

Відкрийте програму FTK imager.

Додайте побітову копію підозрілого цифрового носія (Vader_Home_Computer.001) до програми FTK imager.

File > Add Evidence Item > Image File та Далі > Browse та вибрати файл копії цифрового носія, вибрати Vader_Home_Computer.001 та відкрити > Finish.

Натисніть кнопки + для навігації по зображенню.

Перейдіть до кореневого каталогу Розділу 2 (root Partition 2).

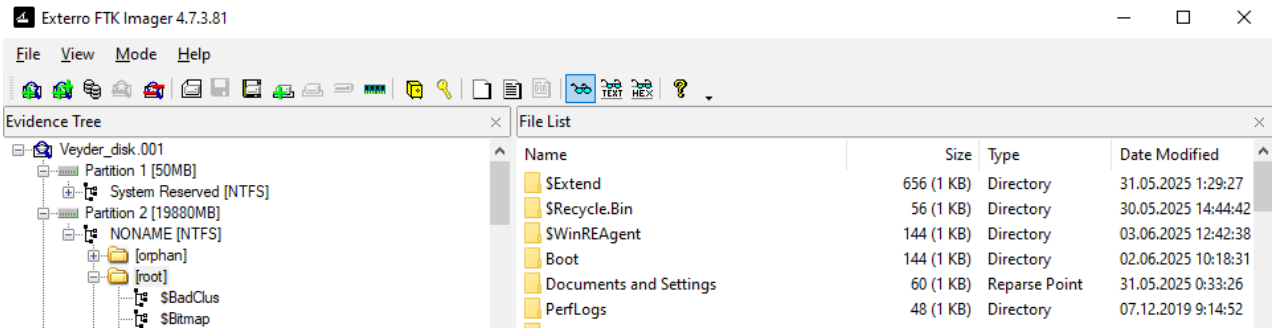


Рис. 47. Перегляд кореневого каталогу у FTK Imager

Яка назва та файлова система цього розділу?

_____

Перейдіть до папки $Recycle.Bin.

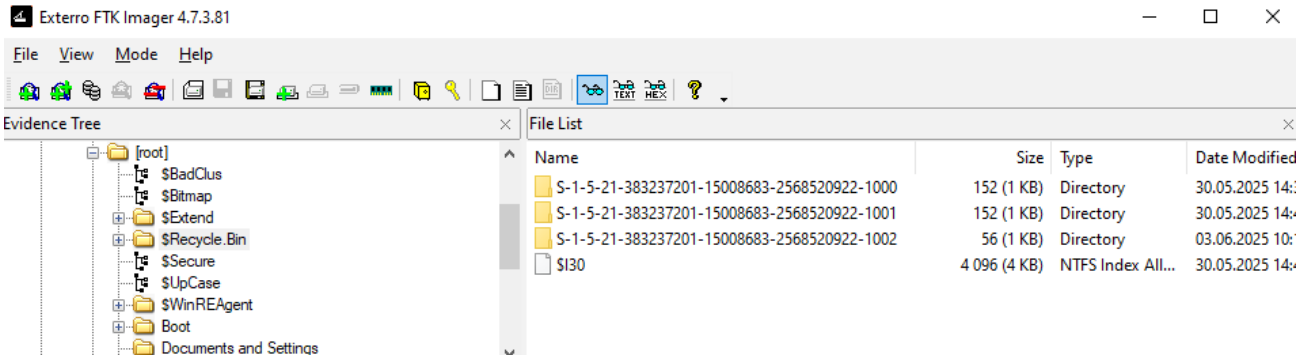


Рис. 48. Перегляд папки $Recycle.Bin у FTK Imager

Його підкаталоги – це довге число.

Що це за число?

_____

Перегляньте всі файли з каталогу S-1-5-21-383237201-15008683-2568520922-1002. Чи є якісь із них ознаки потенційних злочинних планів? Який саме? Які були плани?

_____

Які були шляхи до файлів, ім'я, розмір і дата видалення підозрілих файлів?

_____

Відкрийте Autopsy.

Відкрийте справу, що ви завели у попередніх лабораторних – Open Recent Case.

Перейдіть Data Artifacts > Recycle Bin.

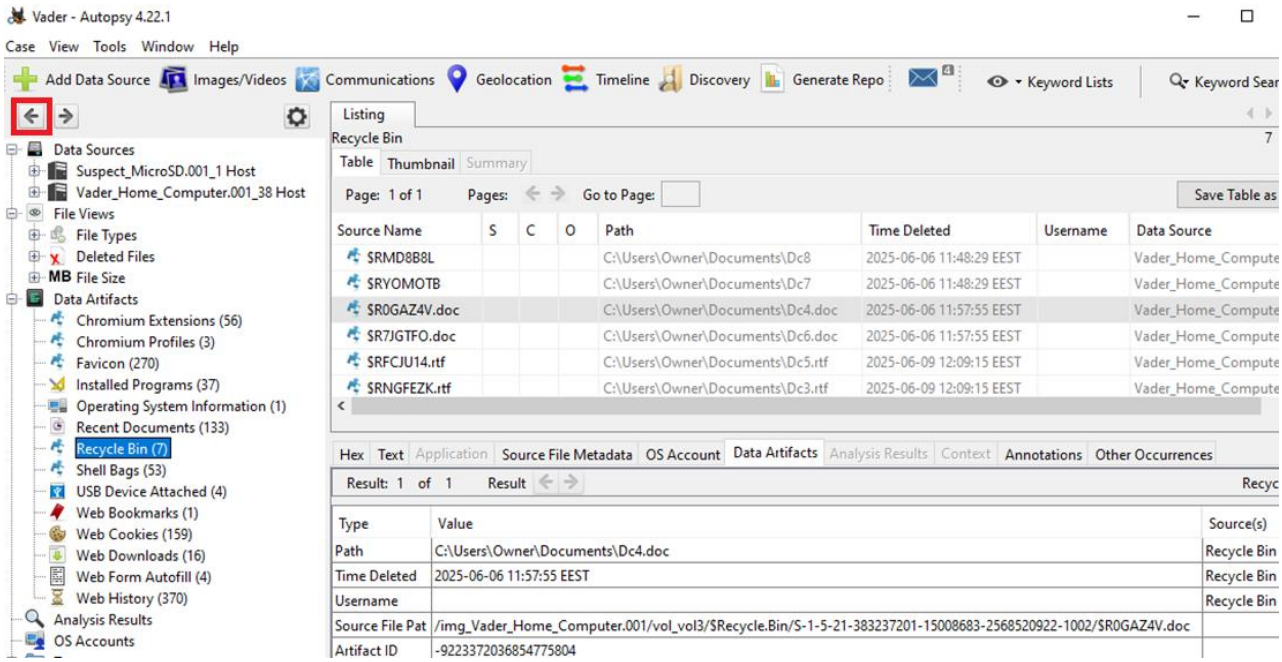


Рис. 49. Перегляд $Recycle.Bin в Autopsy

Через контекстне меню виберіть для знайдених файлів View Downloaded File in Directory, щоб подивитися їх. Повернення назад за допомогою стрілки у лівому верхньому куті.

Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки?

_____

Контрольні питання

1. Що таке Кошик (Recycle Bin) в операційній системі Windows?
2. Яке призначення кошика?
3. Яка інформація може бути отримана під час аналізу Кошика?
4. Що відбувається з файлом після натискання клавіші Delete?
5. Чому після видалення файл зазвичай можна відновити?
6. Де розташовується каталог кошика в сучасних версіях Windows?
7. Що таке SID (Security Identifier)?
8. Для чого використовується SID у структурі кошика?
9. Які типи файлів створюються в кошику після видалення об'єкта?
10. Яка інформація міститься у файлі $I?
11. Яка інформація міститься у файлі $R?
12. Які способи дозволяють видалити файл без переміщення до кошика?

Лабораторна робота 6
АНАЛІЗ ПОСИЛАНЬ НА НЕДАВНО ВІДКРИТІ ФАЙЛИ (RECENT) ТА ФАЙЛІВ ПОПЕРЕДНЬОГО ЗАВАНТАЖЕННЯ (PREFETCH)

Мета заняття: ознайомитися з каталогом нещодавно відкритих файлів (Recent) та файлами попереднього завантаження програм (Prefetch); дослідити принципи формування та зберігання LNK-файлів і Prefetch-файлів, їх структуру та криміналістичне значення; ознайомитися з можливостями використання артефактів Recent і Prefetch для встановлення фактів відкриття файлів, запуску програм; отримати практичні навички пошуку, аналізу та інтерпретації відомостей про діяльність користувача за допомогою спеціалізованих криміналістичних інструментів.

Теоретичні відомості

Під час відкриття документа Windows автоматично створює ярлик на цей файл у спеціальному каталозі Recent. Типовий шлях:

C:\Users<UserName>\AppData\Roaming\Microsoft\Windows\Recent

У цьому каталозі зберігаються файли з розширенням .lnk. Файл ярлика містить службову інформацію про об'єкт, який відкривав користувач. Аналіз каталогу Recent дозволяє встановити:

- які файли відкривалися користувачем;
- де вони розташовувалися;
- коли відбувався доступ до них;
- чи знаходилися вони на локальному диску або зовнішньому носії.

LNK-файл (ярлик Windows) є спеціальним файлом, який містить відомості про інший об'єкт файлової системи. У ярлику можуть міститися:

- повний шлях до файлу;
- назва файлу;
- розмір файлу;
- серійний номер тому;
- дата створення;
- дата останнього доступу;
- дата останньої зміни;
- інформація про носій інформації.

Навіть якщо оригінальний файл був видалений, ярлик часто залишається в системі та може використовуватися як джерело цифрових доказів.

Для прискорення запуску програм Windows використовує механізм попереднього завантаження (Prefetch). Під час першого запуску програми система аналізує процес її завантаження та створює спеціальний файл Prefetch. Типовий шлях:

C:\Windows\Prefetch

Файли Prefetch мають розширення .pf. Для кожної програми зазвичай створюється окремий Prefetch-файл.

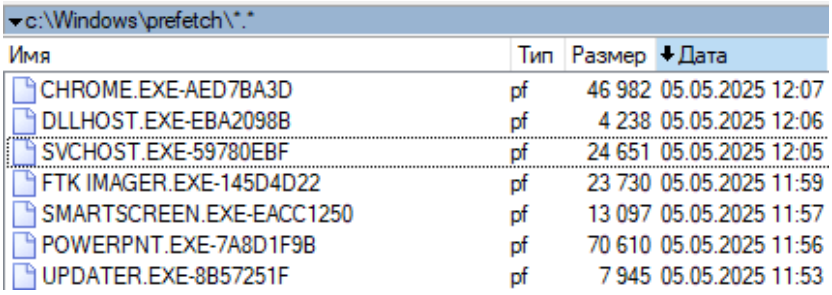


Рис. 50. Файли Prefetch

Основне призначення механізму Prefetch полягає у прискоренні запуску програм шляхом попереднього зчитування необхідних даних із диска. Однак для цифрової криміналістики ці файли є надзвичайно цінними артефактами користувацької активності. Файл Prefetch може містити:

- назву виконуваного файлу;
- повний шлях до програми;
- дату та час останнього запуску;
- кількість запусків програми;
- перелік файлів і бібліотек, які використовувалися під час запуску;
- інформацію про том, з якого запускалася програма.

Завдяки цьому можна встановити факт запуску певного програмного забезпечення навіть після його видалення.

Це особливо важливо під час розслідування випадків використання:

- програм віддаленого доступу;
- програм шифрування;
- утиліт видалення даних;
- шкідливого програмного забезпечення;
- інструментів цифрової криміналістики.

Windows автоматично підтримує обмежену кількість файлів Prefetch. У сучасних версіях Windows зазвичай зберігається до кількох сотень останніх записів. Старі записи можуть автоматично видалятися системою. Крім того,

механізм Prefetch може бути відключений адміністратором або відсутній на деяких серверних версіях Windows.

Наявність Prefetch-файлу свідчить про запуск програми, але не дозволяє однозначно встановити, хто саме її запускав. Для підтвердження дій користувача результати аналізу Prefetch необхідно співставляти з іншими артефактами:

- журналами подій Windows;
- файлами Recent;
- записами реєстру;
- часовими позначками файлової системи.

Найбільш достовірні результати досягаються шляхом кореляції кількох джерел цифрових доказів. Наприклад, якщо файл присутній у каталозі Recent, а відповідна програма згадується у Prefetch, це може підтверджувати факт відкриття документа певною програмою.

Завдання на лабораторну роботу

Відкрийте FTK imager.

Відкрийте побітову копію підозрілого цифрового носія (Vader_Home_Computer.001) у FTK imager.

Перейдіть до Users\Owner\AppData\Roaming\Microsoft\Windows\Recent\

Перегляньте файл Death_star1.lnk у шістнадцятковому вікні перегляду у FTK Imager? Яку інформацію ви можете розшифрувати?

_____

Експортуйте всі файли з папки Recent до нового каталогу на вашому комп’ютері, назвіть папку Recent.

Встановіть або відкрийте RecentFileView від Nirsoft. (https://www.nirsoft.net/utils/recent_files_view.html).

RecentFileView потрібно запускати від імені Адміністратора (в контекстному меню – Запустити з правами адміністратора)!

За замовчуванням RecentFileView аналізує файли на головному комп'ютері.

У Options > Advanced Options у полі Load from виберіть External Source.

У полі Recent Folder вкажіть шлях до каталогу, куди ви експортували файли з папки Recent.

Виходячи з назв файлів, чи може якийсь із цих файлів свідчити про незаконну діяльність? Які їхні назви та коли вони були відкриті востаннє?

_____

Зверніть увагу на різні типи інформації, записаної у файлах посилань. Чи бачите ви аномалію у повідомленому шляху для файлів посилань?

**Це пояснюється тим, що Windows бачить файли посилань, інтегруючи їх у локальну систему.

Якщо ваш підозрюваний стверджує, що він не знав, що компрометуючий файл був у його системі, і він ніколи його не відкривав. Як ви можете відреагувати, виходячи з доказів файлу посилань?

Один з компрометуючих файлів – це zip-файл. Використовуйте FTK Imager, щоб перейти до шляху, де цей zip-файл знаходиться на підозрілому зображенні. Які файли містяться в zip-файлі?

Припустимо, що один з компрометуючих файлів виявився зашифрованим, і вам потрібен був пароль, щоб відкрити його. Чи вказують файли посилань на будь-які файли, які можуть містити пароль?

Де він знаходився і як ви могли б знайти цей файл?

Відкрийте Autopsy.

Відкрийте справу, що ви завели у попередніх лабораторних – Open Recent Case

Перейдіть Data Artifacts > Recent Documents

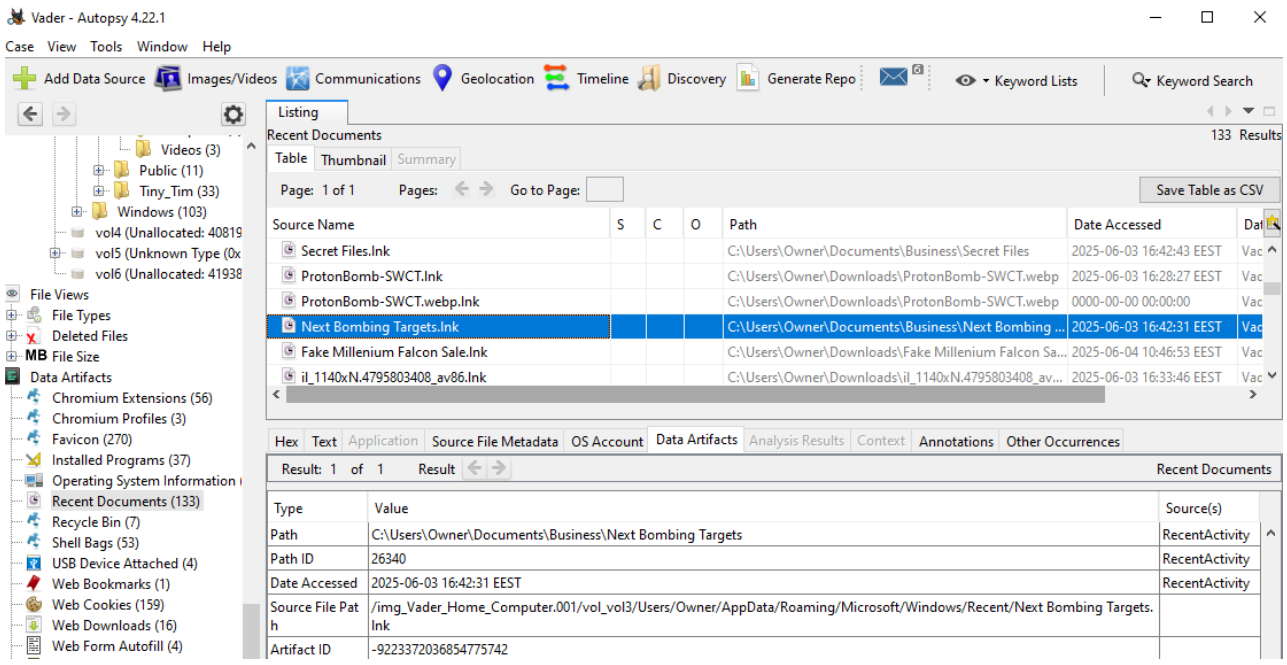


Рис. 51. Відкриття файлів Recent в Autopsy

Через контекстне меню виберіть для знайдених файлів View Downloaded File in Directory, щоб подивитися їх. Повернення назад за допомогою стрілки у лівому верхньому куті.

Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки?

_____

Відкрийте FTK Imager

Змонтуйте підозрілий образ (Vader_Home_Computer.001) до локального диска.

Використовуйте WinPrefetchView (https://www.nirsoft.net/utils/win_prefetch_view.html) для аналізу файлів попередньої вибірки підозрілої системи.

WinPrefetchView потрібно запускати від імені Адміністратора (в контекстному меню – Запустити з правами адміністратора)!

За замовчуванням WinPrefetchView аналізує файли попередньої вибірки на головному комп'ютері.

У Options > Advanced Options виберіть параметри та вкажіть шлях до файлів Prefetch змонтованого образу (F:\Windows\Prefetch).

Які програми найчастіше виконувалися на підозрілому комп'ютері?

(Можна відсортувати по стовпцю Run Counter).

_____

Коли WINRAR.EXE востаннє виконувався на цій системі? Чи є якісь вказівки щодо того, які файли відкривався за допомогою WinRar?

(Подивиться нижнє вікно WinPrefetchView, там вказані файли, з якими взаємодіяв програма, що виділена у верхньому вікні).

_____

Коли Блокнот (Notepad.exe) запускався вперше та востаннє на цій системі?

(Стовпець Last Run Time).

_____

Чи є якісь вказівки щодо того, які файли міг відкриватися за допомогою Блокноту?

_____

Перед закриттям FTK Imager відмонтуйте всі змонтовані диски.

Контрольні питання

1. Що таке каталог Recent?
2. Де розташовується каталог Recent у Windows?
3. Які файли зберігаються в каталозі Recent?
4. За яких умов Windows створює записи в каталозі Recent?
5. Що таке LNK-файл?
6. Яку інформацію містить LNK-файл?
7. Чи може LNK-файл зберегтися після видалення оригінального документа?
8. Для чого використовується механізм Prefetch в операційній системі Windows?

9. Де розташовуються файли Prefetch?
10. Яке розширення мають файли Prefetch?
11. За яких умов створюється файл Prefetch?
12. Яку інформацію містить файл Prefetch?
13. Чому результати аналізу Prefetch необхідно співставляти з іншими артефактами?

Лабораторна робота 7
АНАЛІЗ СИГНАТУР ФАЙЛІВ

Мета заняття: ознайомитися з принципами ідентифікації типів файлів за їх сигнатурами; дослідити поняття сигнатури файлу та її значення під час цифрового криміналістичного дослідження; ознайомитися з основними сигнатурами поширених форматів файлів та методами перевірки відповідності між розширенням файлу і його фактичним вмістом; отримати практичні навички використання шістнадцяткових редакторів для аналізу структури файлів та пошуку сигнатур; дослідити можливості виявлення прихованих, замаскованих і підроблених файлів, а також відновлення файлів за сигнатурами.

Теоретичні відомості

Під час цифрових криміналістичних досліджень часто виникає необхідність встановити справжній тип файлу незалежно від його назви або розширення. Для цього використовуються сигнатури файлів.

Сигнатура файлу (File Signature, Magic Number) – це спеціальна послідовність байтів, яка розташовується на початку або в окремих випадках наприкінці файлу та дозволяє ідентифікувати його формат.

Таблиця 3

Сигнатури файлів

Розширення	Hex	ASCII
.jpg, .jpeg	FF D8 FF	ÿØÿ
.png	89 50 4E 47 0D 0A 1A 0A	‰PNG
.gif	47 49 46 38	GIF
.pdf	25 50 44 46 2D	%PDF-
.zip	50 4B 03 04	PK..
.rar	52 61 72 21 1A 07	Rar!..
.exe	4D 5A	MZ
.docx, .xlsx	50 4B 03 04	PK..
.mp4	00 00 00 18 66 74 79 70	....ftyp

Операційна система зазвичай визначає тип файлу за його розширенням (.jpg,

.pdf, .docx тощо), однак розширення можна легко змінити без зміни вмісту файлу. Сигнатура ж є частиною внутрішньої структури файлу та використовується програмним забезпеченням для правильного розпізнавання формату даних. Файл може мати назву photo.jpg, але фактично бути виконуваним файлом Windows. Аналіз сигнатури дозволяє виявити таку невідповідність. Кожний формат файлу має характерні сигнатури.

Невідповідність між розширенням та сигнатурою може свідчити про:

- навмисне приховування файлу;
- шкідливе програмне забезпечення;
- помилки користувача;
- спробу обходу систем безпеки.

File Carving – це метод пошуку та відновлення файлів на основі їх сигнатур без використання файлової системи. Під час такого відновлення програма виконує пошук характерних сигнатур у секторах носія та намагається визначити межі файлу. Цей метод особливо корисний у випадках:

- пошкодження файлової системи;
- форматування носія;
- видалення записів файлової таблиці;
- аналізу вільного простору.

Одним із найпростіших способів приховування файлів є зміна їх розширення. У таких випадках файл зберігає свою внутрішню структуру та сигнатуру, тому може бути легко виявлений під час криміналістичного аналізу. Цей метод часто використовується:

- для маскування шкідливого програмного забезпечення;
- приховування документів;
- обходу політик безпеки.

Завдання на лабораторну роботу

Відкрийте FTK Imager.

Відкрийте побітову копію підозрілого цифрового носія (Vader_Home_Computer.001) у FTK imager.

Перейдіть до папки C:\Users\Owner\Documents\Business\Secret Files

Експортуйте папку Secret Files на локальний жорсткий диск.

Відкрийте HxD та використовуйте його, щоб відкрити кожен секретний файл у шістнадцятковому вигляді.

Перевірте початкові байти на початку кожного файлу, щоб визначити підписи файлів. Використовуйте Вікіпедію https://uk.wikipedia.org/wiki/Сигнатура_файлу_(перелік) як орієнтир.

В деяких випадках потрібно звернутися до

https://en.wikipedia.org/wiki/List_of_file_signatures

В деяких випадках потрібно аналізувати не перші 4 байти, а менше.

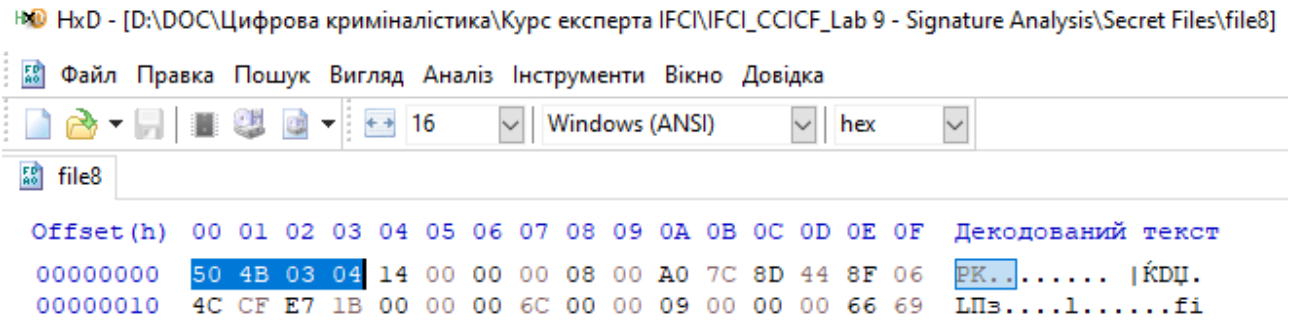


Рис. 52. Відкриття файлів в HxD

Запишіть наступне для кожного файлу.

Ім’я файлу: file1.

Перші 4 байти: ___ ___ ___ ___

Тип/розширення файлу: ____

Перейменуйте файл, додавши правильне розширення, та відкрийте його. Опишіть його._____

Ім'я файлу: file2.

Перші 4 байти: ___ ___ ___ ___

Тип/розширення файлу: ____

Перейменуйте файл з правильним розширенням та відкрийте його. Опишіть його._____

Ім'я файлу: file3.

Перші 4 байти: ___ ___ ___ ___

Тип/розширення файлу: ____

Перейменуйте файл з правильним розширенням та відкрийте його. Опишіть його._____

Ім'я файлу: file4.

Перші 4 байти: ___ ___ ___ ___

Тип/розширення файлу: ____

Перейменуйте файл з правильним розширенням та відкрийте його. Опишіть його._____

Ім'я файлу: file5.

Перші 4 байти: ___ ___ ___ ___

Тип/розширення файлу: ____

Перейменуйте файл з правильним розширенням та відкрийте його. Опишіть його._____

Ім'я файлу: file6.

Перші 4 байти: ___ ___ ___ ___

Тип/розширення файлу: ____

Перейменуйте файл, додавши йому правильне розширення, та відкрийте його. Опишіть його._____

Ім'я файлу: file7.

Перші 4 байти: ___ ___ ___ ___

Тип/розширення файлу: ____

Перейменуйте файл, додавши правильне розширення, та відкрийте його. Опишіть його._____

Ім'я файлу: file8.

Перші 4 байти: ___ ___ ___ ___

Тип/розширення файлу: ____

Перейменуйте файл, додавши правильне розширення, та відкрийте його. Опишіть його._____

Ім'я файлу: file9.

Перші 4 байти: ___ ___ ___ ___

Тип/розширення файлу: ____

Перейменуйте файл, додавши правильне розширення, та відкрийте його. Опишіть його._____

Чи отримали ви якусь інформацію, яка може бути корисною для цього розслідування?

_____

Контрольні питання

1. Що таке сигнатура файлу?
2. Які ще назви використовуються для позначення сигнатури файлу?
3. Для чого використовуються сигнатури файлів у цифровій криміналістиці?
4. Чим сигнатура файлу відрізняється від розширення файлу?
5. Чому розширення файлу не завжди дозволяє правильно визначити його тип?
6. Де зазвичай розташовується сигнатура файлу?
7. Що означає невідповідність між розширенням файлу та його сигнатурою?
8. Які причини можуть призвести до невідповідності сигнатури та розширення?
9. Як зловмисники можуть використовувати зміну розширення файлу?
10. Що таке File Carving?
11. Для чого використовується File Carving у цифровій криміналістиці?
12. У яких випадках застосовується відновлення файлів за сигнатурами?

Лабораторна робота 8
АНАЛІЗ МЕТАДАНИХ ФАЙЛІВ

Мета заняття: ознайомитися з поняттям метаданих файлів та їх значенням під час проведення цифрових криміналістичних досліджень; дослідити основні типи метаданих, що створюються файловими системами, операційними системами, прикладними програмами та цифровими пристроями; ознайомитися з особливостями зберігання часових позначок у файлових системах FAT та NTFS, принципами використання UTC, локального часу та формату Epoch Time; дослідити структуру та вміст метаданих документів, графічних файлів і цифрових фотографій, зокрема EXIF-метаданих; отримати практичні навички пошуку, вилучення та аналізу метаданих; дослідити можливості використання метаданих для встановлення часу створення та модифікації файлів, характеристик пристроїв і місця створення цифрових об'єктів.

Теоретичні відомості

Метадані (Metadata) – це дані про дані, тобто службова інформація, яка описує характеристики файлу, його походження, властивості та історію використання. Метадані створюються операційною системою, прикладними програмами, цифровими пристроями та користувачами під час створення, редагування, копіювання або перегляду файлів. У цифровій криміналістиці аналіз метаданих є одним із найважливіших методів встановлення обставин створення та використання цифрових об'єктів.

Метадані можуть містити відомості, які відсутні у вмісті самого документа або файлу. Аналіз метаданих дозволяє встановити:

- автора документа;
- дату та час створення файлу;
- дату та час останньої модифікації;
- дату та час останнього доступу;
- програму, за допомогою якої створено файл;
- обліковий запис користувача;
- географічні координати місця зйомки;
- модель пристрою;
- параметри цифрової камери;
- історію редагування документа.

Метадані умовно поділяють на декілька категорій.

1. Системні метадані – створюються файловою системою та операційною системою. До них належать:

- назва файлу;
- розмір файлу;

- дата створення;
- дата останньої зміни;
- дата останнього доступу;
- атрибути файлу;
- права доступу.

2. Прикладні метадані – створюються прикладними програмами. Наприклад, документ Microsoft Word може містити:

- ім’я автора;
- організацію;
- дату створення документа;
- дату останнього редагування;
- кількість редагувань;
- використаний шаблон.

3. Технічні метадані – містять технічні характеристики файлу або пристрою. Наприклад:

- модель камери;
- серійний номер пристрою;
- версію програмного забезпечення;
- параметри експозиції;
- роздільну здатність зображення.

4. Метадані файлової системи – будь-яка файлова система зберігає службову інформацію про файли.

У Windows найважливішими є часові позначки. Одним із найважливіших видів метаданих є часові позначки файлів (timestamps). Під час роботи з файлами операційна система автоматично фіксує інформацію про час створення, модифікації та доступу до файлу. Аналіз цих відомостей дозволяє встановлювати послідовність подій, пов'язаних із використанням цифрових доказів. У властивостях файлу Windows зазвичай відображаються такі часові позначки:

- Створено (Created) – Дата та час створення файлу в поточній файловій системі. Не завжди відповідає фактичному часу створення документа, оскільки може змінюватися під час копіювання файлу між носіями або файловими системами.
- Змінено (Modified) – Дата та час останньої зміни вмісту файлу.
- Відкрито (Accessed) – Дата та час останнього доступу до файлу. Слід враховувати, що доступ до файлу може здійснюватися не лише користувачем, а й системними службами або антивірусним програмним забезпеченням, тому ця позначка потребує обережної інтерпретації.

Різні файлові системи використовують різні механізми зберігання часових

позначок.

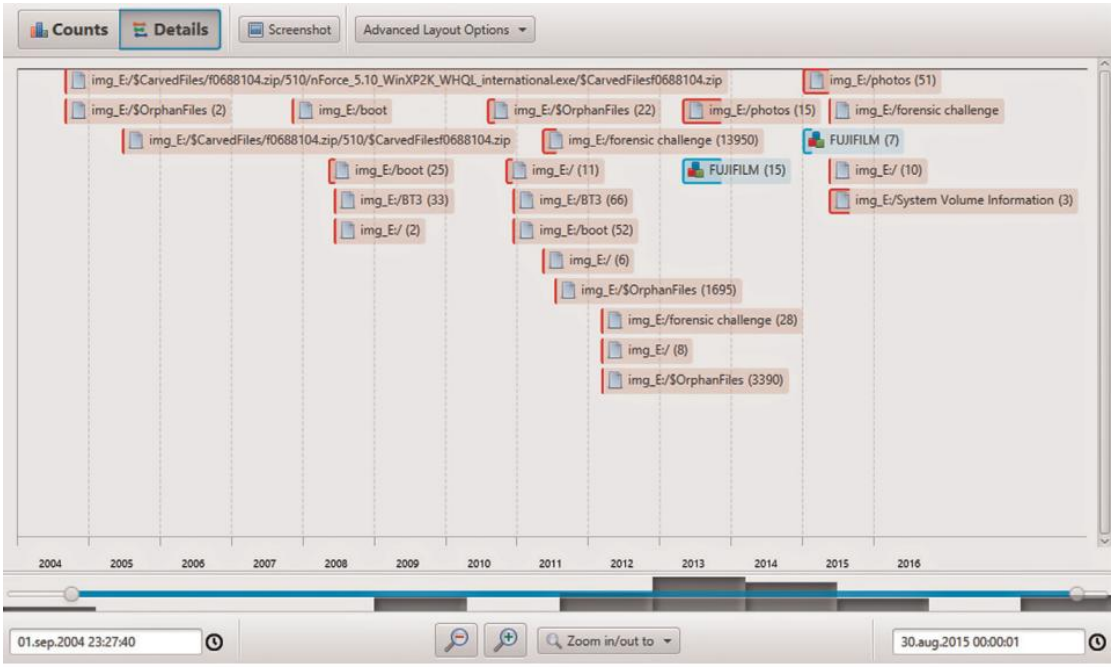


Рис. 53. Часова шкала в Autopsy

Файлова система FAT зберігає часові значення у місцевому часі (Local Time). Це означає, що під час зміни часового поясу або переходу на літній чи зимовий час інтерпретація часових позначок може ускладнюватися.

Файлова система NTFS зберігає часові значення в універсальному координованому часі (UTC). Під час відображення часу Windows автоматично перетворює його відповідно до налаштувань поточної часової зони комп'ютера. Такий підхід дозволяє уникнути неоднозначностей, пов'язаних із переходом між часовими поясами та літнім або зимовим часом.

UTC (Coordinated Universal Time) – це всесвітній координований час, який використовується як міжнародний еталон часу. UTC не залежить від географічного розташування користувача та не змінюється під час переходу на літній або зимовий час. Місцевий час обчислюється шляхом додавання або віднімання зміщення від UTC. Наприклад:

UTC+2 – східноєвропейський час;

UTC+3 – східноєвропейський літній час;

UTC−5 – східний час Північної Америки.

Під час цифрового криміналістичного дослідження необхідно завжди враховувати часовий пояс досліджуваної системи, оскільки неправильне трактування часових позначок може призвести до помилкових висновків щодо послідовності подій.

Інформація про часову зону Windows зберігається в реєстрі. Аналіз цього

ключа дозволяє встановити:

- поточний часовий пояс системи;
- налаштування переходу на літній та зимовий час;
- можливі відомості про географічне розташування користувача.

У багатьох операційних системах, мережевих журналах, базах даних та мобільних пристроях часові позначки зберігаються у форматі Epoch Time (Unix Time).

Epoch Time – це кількість секунд, що минули з початку Unix-епохи (00:00:00 UTC 1 січня 1970 року). Наприклад: 1299691326, відповідає: 9 березня 2011 року 17:22:06 UTC.

Водночас часові позначки не повинні аналізуватися ізольовано. Для отримання обґрунтованих висновків їх необхідно співставляти з іншими цифровими артефактами, журналами подій, метаданими документів та записами файлової системи.

5. Метадані графічних файлів – графічні файли можуть містити значний обсяг додаткової інформації. Найбільш поширеним стандартом є EXIF (Exchangeable Image File Format). EXIF-метадані можуть містити:

- дату та час створення фотографії;
- модель камери;
- виробника пристрою;
- параметри зйомки;
- географічні координати GPS;
- орієнтацію зображення;
- серійний номер пристрою.

Такі відомості можуть бути важливими доказами під час розслідування.

6. GPS-координати в метаданих. Сучасні смартфони часто записують до EXIF-метаданих координати місця зйомки. Це дозволяє встановити:

- місце перебування користувача;
- маршрут переміщення;
- місце створення фотографії.

Проте наявність GPS-даних залежить від налаштувань пристрою.

7. Метадані документів Microsoft Office. Документи Microsoft Word, Excel та PowerPoint можуть містити:

- автора документа;
- організацію;
- дату створення;
- дату останнього редагування;
- кількість редагувань;
- час роботи над документом;
- версію програмного забезпечення.

Навіть після видалення частини вмісту документа метадані можуть залишатися доступними для аналізу.

Користувачі часто не усвідомлюють наявність прихованих метаданих. Під час публікації документів або фотографій можуть ненавмисно розголошуватися:

– особисті дані;
– місце знаходження;
– внутрішні імена користувачів;
– службова інформація організації.

Саме тому перед передаванням документів часто виконується очищення метаданих.

Метадані можуть бути змінені як випадково, так і навмисно. Наприклад:

– змінено системний час комп’ютера;
– використано програми редагування метаданих;
– виконано копіювання файлів між файловими системами;
– застосовано спеціалізовані інструменти приховування інформації.

Тому метадані не повинні розглядатися ізольовано від інших цифрових доказів.

Для дослідження метаданих використовуються спеціалізовані програмні засоби:

– ExifTool;
– FTK Imager;
– Autopsy;
– X-Ways Forensics;
– EnCase;
– Windows Explorer;
– HxD.

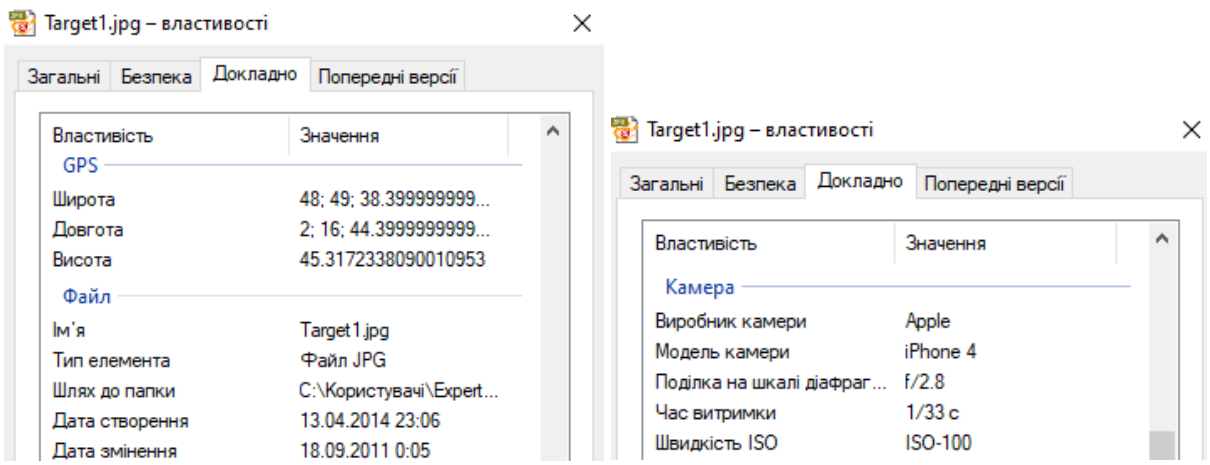


Рис. 54. Метадані у Windows

Найбільш універсальним інструментом аналізу метаданих є ExifTool, який підтримує тисячі форматів файлів.

Завдання на лабораторну роботу

Відкрийте FTK Imager.

Відкрийте побітову копію підозрілого цифрового носія (Vader_Home_Computer.001) у FTK imager.

Перейдіть до папки C:\Users\Owner\Documents\Business\Next Bombing Targets.

Експортуйте папку Next Bombing Targets на свій локальний комп'ютер.

Використайте ExifReader (https://www.exifreader.com/), щоб відкрити target1.jpg.



Рис. 55. ExifReader

Перегляньте метадані, отримані з target1.jpg, та дайте відповіді на наступні питання.

Яка марка та модель камери, якою було зроблено фотографію?

_____

Яка дата та час зйомки фотографії?

_____

Які координати точки (широта та довгота) фотографії?

_____

Перейдіть до Карт Google та введіть точки широти та довготи.

(Пам’ятайте: N = додатна, S = від’ємна, E = додатна, W = від’ємна).

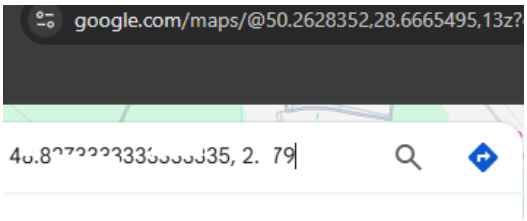


Рис. 56. Карти Google

Де саме знаходиться перша ціль теракту?

_____

Використайте ExifReader, щоб відкрити Target2.jpg.

Перегляньте метадані, отримані з Target2.jpg, і дайте відповідь на наступні питання.

Яка марка та модель камери, якою було зроблено фотографію?

_____

Яка дата та час зйомки фотографії?

_____

Які координати точки (широта та довгота) фотографії?

_____

Перейдіть до Карт Google та введіть точки широти та довготи.

(Пам’ятайте: N = додатна, S = від’ємна, E = додатна, W = від’ємна).

Де саме знаходиться друга ціль теракту?

_____

Відкрийте Autopsy.

Відкрийте справу, що ви завели у попередніх лабораторних – Open Recent Case

Logical Files

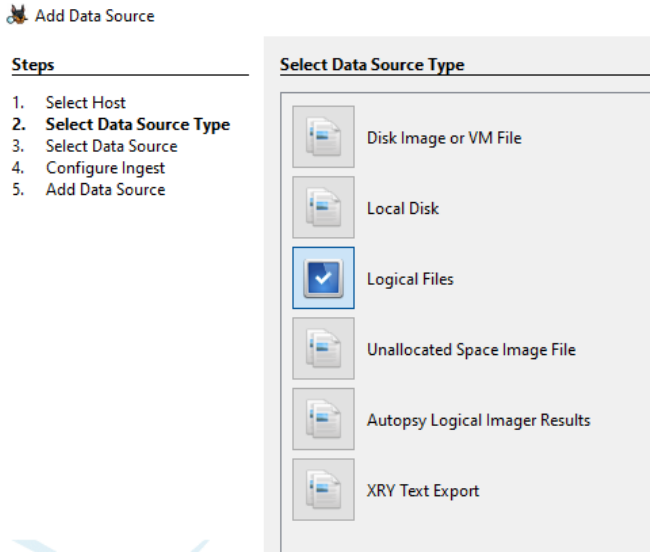


Рис. 57. Відкриття файлу у Autopsy

Add > вкажіть шлях до збереженої папки Next Bombing Targets.

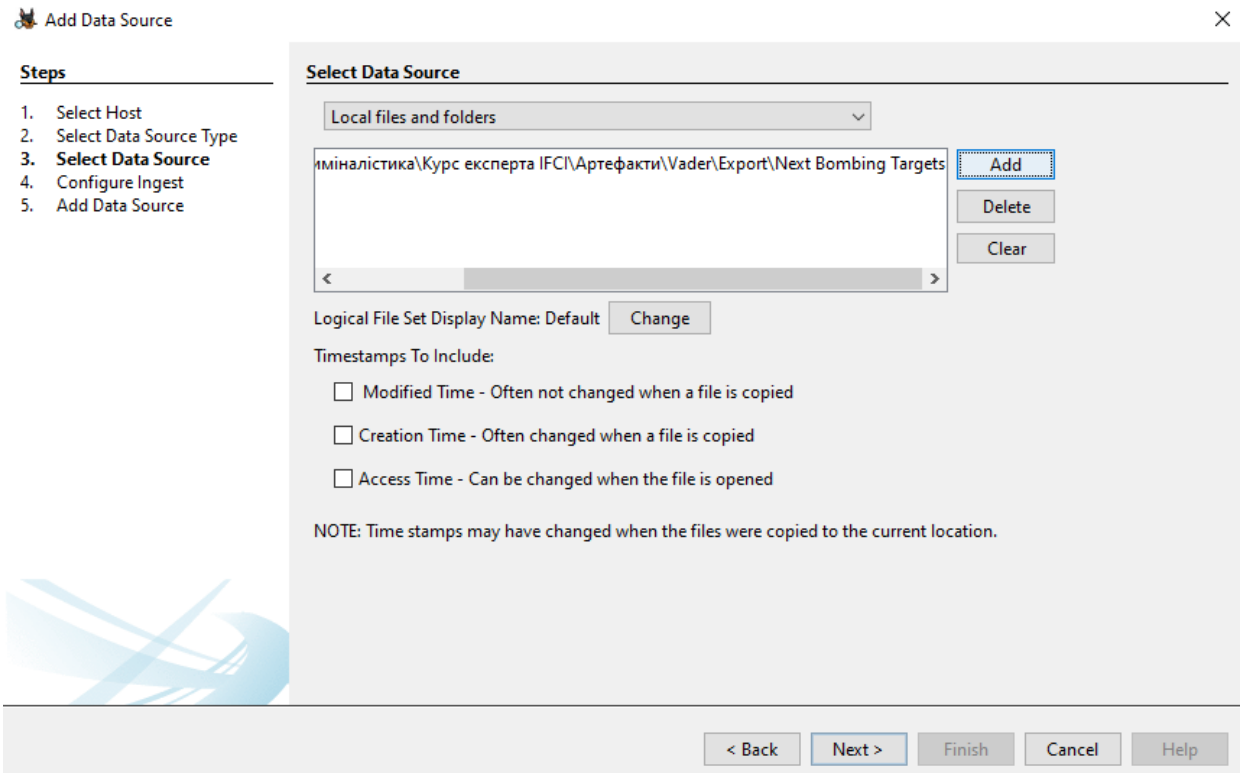


Рис. 58. Відкриття файлу у Autopsy

Виберіть тільки Picture Analyzes.

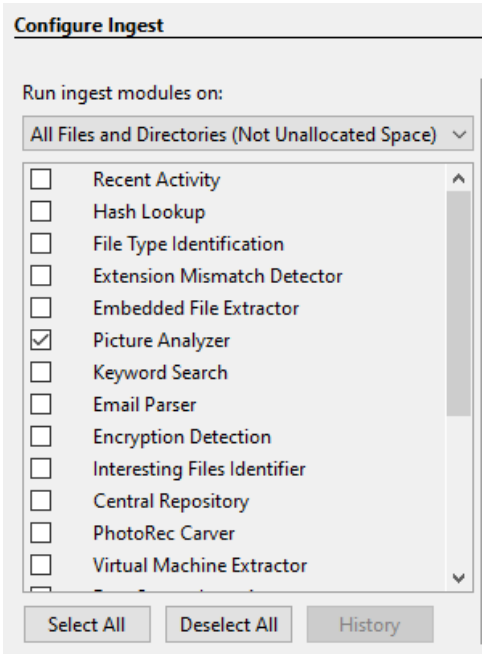


Рис. 59. Аналіз файлу у Autopsy

Analysis Results > EXIF Metadata.

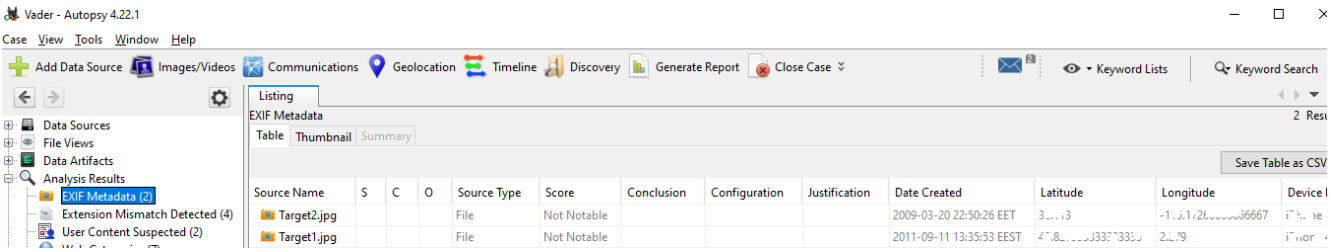


Рис. 60. Аналіз файлу у Autopsy

Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки?

_____

Контрольні питання

1. Що таке метадані?
2. Яке значення мають метадані під час цифрового криміналістичного дослідження?
3. Які відомості можна отримати з метаданих файлу?
4. Які часові позначки відображаються у властивостях файлу Windows?
5. Що означає час створення файлу (Created)?
6. Що означає час зміни файлу (Modified)?
7. Що означає час останнього доступу до файлу (Accessed)?
8. У якому часовому форматі зберігає час файлова система FAT?
9. У якому часовому форматі зберігає час файлова система NTFS?
10. Що таке UTC (Coordinated Universal Time)?
11. Як визначається місцевий час відносно UTC?
12. Чому неправильна інтерпретація часового поясу може призвести до помилкових висновків під час розслідування?
13. Що таке Epoch Time (Unix Time)?
14. Що таке EXIF-метадані?
15. У яких типах файлів найчастіше зустрічаються EXIF-метадані?
16. Яку інформацію можуть містити EXIF-метадані?
17. Що таке GPS-метадані?
18. Які метадані можуть містити документи Microsoft Word?
19. Чому перед публікацією документів іноді виконують очищення метаданих?
20. Чи можуть метадані бути змінені навмисно?
21. Які інструменти використовуються для аналізу метаданих?

Лабораторна робота 9
АНАЛІЗ ЖУРНАЛУ ПОДІЙ

Мета заняття: ознайомитися з принципами ведення журналів подій в операційних системах та їх значенням під час проведення досліджень; дослідити структуру журналів подій Windows, призначення основних журналів (Application, Security, System) та особливості зберігання журналів подій інших інформаційних систем; ознайомитися з поняттями Event ID і Logon Type, їх використанням для аналізу подій автентифікації, доступу до ресурсів, змін конфігурації системи та інших подій безпеки; отримати практичні навички пошуку, фільтрації та аналізу записів журналів подій; дослідити можливості використання журналів подій для виявлення фактів входу до системи, створення та видалення облікових записів, запуску і завершення роботи системи.

Теоретичні відомості

Журнали подій (Event Logs) є одним із найважливіших джерел цифрових доказів під час проведення цифрових криміналістичних досліджень. Вони автоматично створюються операційною системою, службами та прикладними програмами і містять інформацію про події, що відбувалися в інформаційній системі. Аналіз журналів подій дозволяє встановити:

- час виникнення події;
- користувача, який виконав певну дію;
- запуск програм і служб;
- спроби входу до системи;
- підключення до мережевих ресурсів;
- зміни конфігурації системи;
- встановлення програмного забезпечення;
- порушення політик безпеки;
- ознаки несанкціонованого доступу.

Оскільки журнали подій постійно оновлюються під час роботи системи, їх дослідження бажано виконувати одразу після вилучення цифрових доказів або після створення побітової копії носія.

Операційна система Windows використовує технологію Windows Event Log для централізованого ведення журналів подій. Найважливішими журналами є:

1. Application. Містить повідомлення прикладних програм.
2. System. Містить повідомлення операційної системи, драйверів та служб.
3. Security. Містить події аудиту безпеки:
   - входи користувачів;
   - спроби автентифікації;
   - зміни облікових записів;

– доступ до ресурсів;
– зміни політик безпеки.

Для перегляду журналів використовується стандартний інструмент Windows Event Viewer.

Основні можливості Event Viewer:

– перегляд журналів;
– фільтрація подій;
– пошук за Event ID;
– експорт журналів;
– аналіз часової послідовності подій.

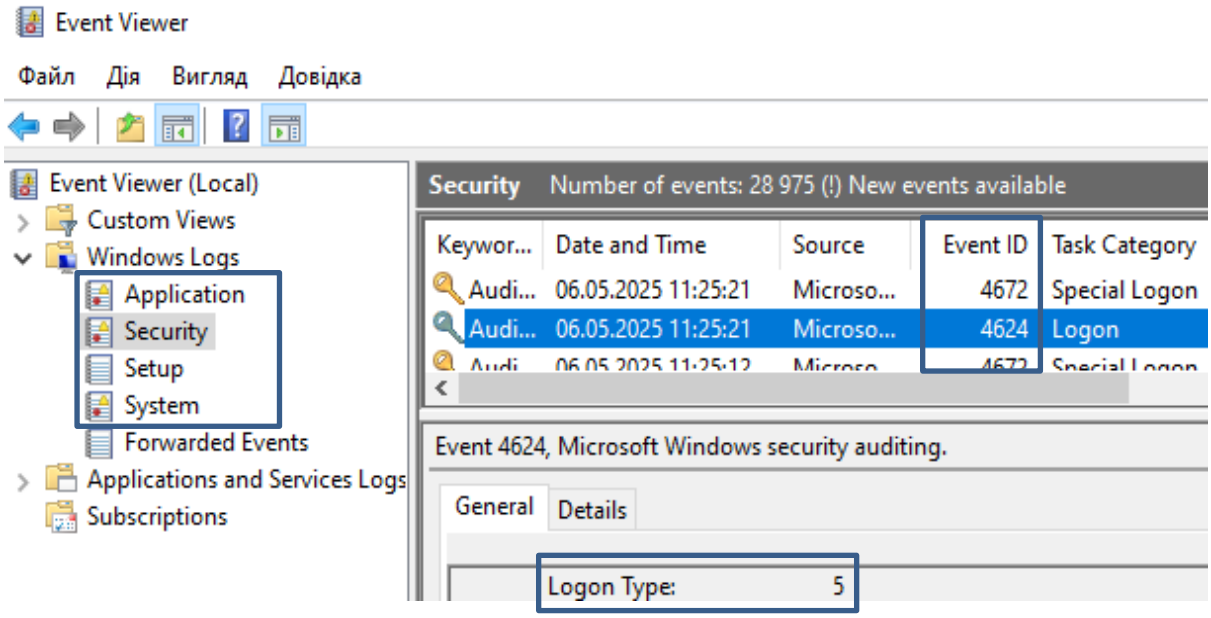


Рис. 61. Журнал подій (Event Viewer)

Саме журнал Security найчастіше використовується під час цифрової криміналістичної експертизи.

Типові місця розташування журналів Windows:

C:\Windows\System32\Winevt\Logs\Application.evtx
C:\Windows\System32\Winevt\Logs\Security.evtx
C:\Windows\System32\Winevt\Logs\System.evtx

Окрім журналів Windows, під час розслідування можуть використовуватися:

1. Журнали вебсерверів, що містять інформацію про HTTP-запити, IP-адреси клієнтів, використані методи, коди відповіді сервера та іншу інформацію про взаємодію користувачів із вебзастосунками.

2. Журнали міжмережевих екранів та IDS.

Firewall Logs та IDS/IPS Logs містять інформацію про:

- мережеві підключення;
- заблоковані з'єднання;
- виявлені мережеві атаки;
- порушення політик безпеки;
- мережеву активність користувачів

Кожна подія Windows має унікальний ідентифікатор – Event ID.

Таблиця 4

Найбільш поширені Event ID

Event ID	Опис
4624	Успішний вхід
4625	Невдалий вхід
4672	Надано привілейований доступ
4656	Спроба доступу (запит прав)
4657	Зміна атрибутів об’єкта
5145	Мережевий доступ до файлів (SMB)
4697	Встановлення служби (Часто при установці бекдорів)
5156	Дозволено з’єднання через Windows Firewall
4720	Створено обліковий запис
4726	Видалено обліковий запис
6005 / 6006	Запуск / вимкнення системи

Під час реєстрації подій входу Windows додатково записує тип входу (Logon Type), який характеризує спосіб автентифікації користувача.

Поєднання Event ID 4624 або 4625 із Logon Type дозволяє визначити спосіб входу користувача до системи.

Таблиця 5

Найважливіші типи входу

Logon Type	Назва	Опис
2	Interactive	Локальний вхід: користувач фізично сидить за ПК
3	Network	Вхід через мережу: доступ до спільної папки, SMB
4	Batch	Запуск через планувальник задач (Task Scheduler)
5	Service	Система входить для запуску служби
7	Unlock	Розблокування комп’ютера
8	NetworkCleartext	Явна аутентифікація по мережі з відкритим паролем
9	NewCredentials	Використання облікових даних через RunAs
10	RemoteInteractive (RDP)	Вхід через Remote Desktop Protocol (RDP)

Журнал PrintService дозволяє встановити факти друку документів. Він доступний у:

Event Viewer → Applications and Services Logs → Microsoft → Windows → PrintService → Admin

Завдання на лабораторну роботу

Відкрийте FTK Imager.

Відкрийте побітову копію підозрілого цифрового носія (Vader_Home_Computer.001) у FTK imager.

Перейдіть до папки \Windows\System32\Winevt\Logs.

Експортуйте три журнали подій (Application.evtx Security.evtx System.evtx) на ваш комп’ютер.

Відкрийте Перегляд подій (Event Viewer) на вашому комп'ютері.

У меню оберіть Дія > Open Saved Log.

Виберіть експортовані файли .evtx.

Перегляньте журнал Security.

Event ID 4720 – це створення облікового запису.

Скористайтеся фільтром Дія > Filter Current Log.

Знайдіть повідомлення журналу, де New Account: Account Name: Owner.

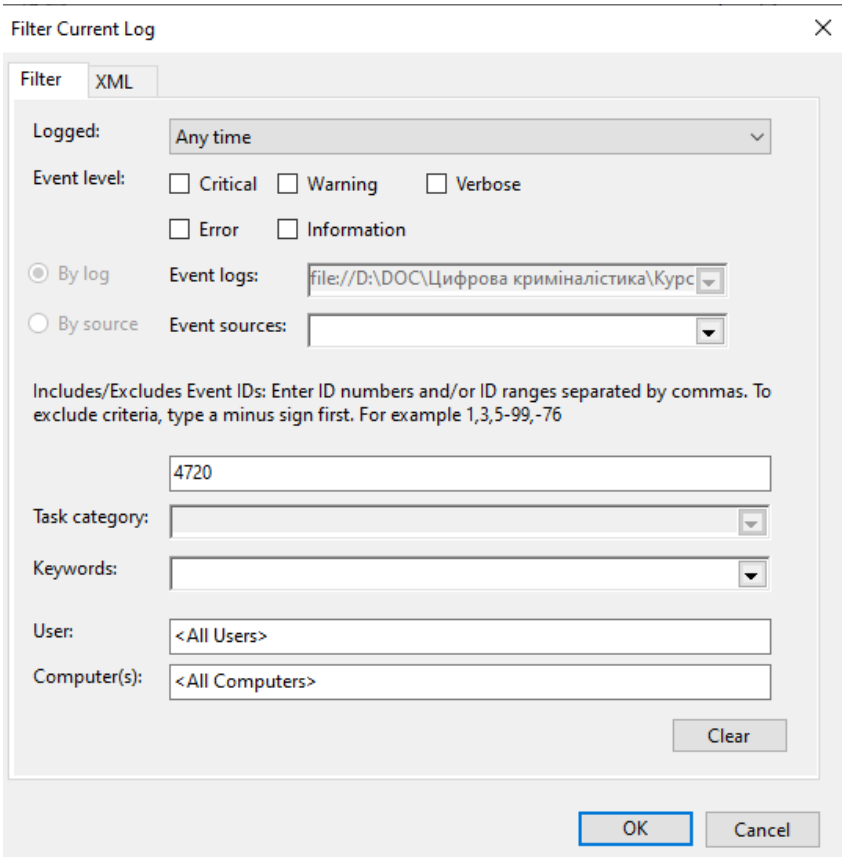


Рис. 62. Фільтр в журналі подій

Коли було створено профіль користувача Owner?

_____

Коли було створено профіль користувача Tiny_Tim?

_____

Для скидання фільтру Дія > Clear Filter.
Event ID 4624 – це вхід до облікового запису.
Скористайтеся фільтром Дія > Filter Current Log.
Потім Скористайтеся пошуком Дія > Find.



Рис. 63. Пошук в журналі подій

Коли Owner входив до свого акаунту востаннє?

_____

Що означає Logon Type: 2?

_____

Коли Tiny_Tim входив до свого акаунту востаннє?

_____

Контрольні питання

1. Що таке журнал подій (Event Log)?
2. Яке призначення журналів подій у сучасних операційних системах?
3. Чому журнали подій є важливим джерелом цифрових доказів?
4. Яку інформацію можна отримати з журналів подій?
5. Які основні журнали подій використовуються в операційній системі Windows?
6. Яке призначення журналу Application?
7. Яке призначення журналу System?
8. Яке призначення журналу Security?
9. Де розташовуються основні журнали подій Windows?
10. Яке розширення мають файли журналів подій Windows?
11. Яку інформацію можуть містити журнали вебсерверів?
12. Яку інформацію можуть містити журнали міжмережевих екранів (Firewall Logs)?
13. Що таке Event ID?
14. Що таке Logon Type?
15. Що означає Logon Type 10?
16. Як за допомогою Event ID та Logon Type визначити факт входу через Remote Desktop Protocol (RDP)?
17. Яке призначення Event Viewer?
18. Як виконати пошук подій?
19. Як виконати фільтрацію подій?
20. Яку інформацію можна отримати з журналу PrintService?
21. Які ознаки несанкціонованого доступу можна виявити за журналами подій?
22. Як за журналами подій встановити факт створення або видалення облікового запису?
23. Як журнали подій допомагають встановити використання мережевих ресурсів?

Лабораторна робота 10
АНАЛІЗ РЕЄСТРУ

Мета заняття: ознайомитися зі структурою та призначенням реєстру Windows; дослідити організацію реєстру, розташування файлів його основних гілок; ознайомитися з найважливішими ключами реєстру, що містять відомості про діяльність користувача, запуск програм, підключення USB-пристроїв, мережеву активність, останні входи до системи та механізми автозапуску; отримати практичні навички пошуку, аналізу та інтерпретації даних реєстру; дослідити артефакти RecentDocs, USBSTOR.

Теоретичні відомості

Реєстр Windows (Windows Registry) – це ієрархічна база даних, у якій операційна система зберігає конфігураційні параметри, інформацію про обладнання, встановлене програмне забезпечення, облікові записи користувачів, налаштування операційної системи та програм.

Під час роботи комп'ютера реєстр постійно оновлюється, накопичуючи значну кількість відомостей про діяльність користувача та стан системи. Завдяки цьому реєстр є одним із найважливіших джерел цифрових доказів у цифровій криміналістиці.

Аналіз реєстру дозволяє встановити:

- відомості про користувачів;
- історію запуску програм;
- перелік відкритих документів;
- історію підключення USB-пристроїв;
- параметри операційної системи;
- налаштування мережі;
- механізми автозапуску;
- встановлене програмне забезпечення;
- відомості про підключені пристрої.

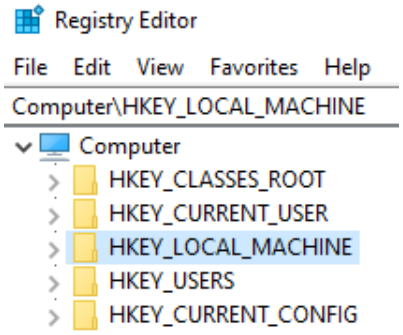


Рис. 64. Реєстр Windows

Реєстр має ієрархічну структуру, подібну до файлової системи. Більшість системних гілок реєстру зберігається у вигляді окремих файлів. Саме ці файли досліджуються криміналістичними програмами після створення побітової копії носія.

Таблиця 6

Найважливіші гілки реєстру

Гілка	Призначення
HKEY_CLASSES_ROOT (HKCR)	Зв’язки типів файлів
HKEY_CURRENT_USER (HKCU)	Налаштування активного користувача
HKEY_LOCAL_MACHINE (HKLM)	Дані всієї системи
HKEY_USERS (HKU)	Дані всіх користувачів
HKEY_CURRENT_CONFIG (HKCC)	Поточна конфігурація обладнання

Таблиця 7

Розташування файлів реєстру

Вміст	Шлях
HKLM\SYSTEM	C:\Windows\System32\config\SYSTEM
HKLM\SOFTWARE	C:\Windows\System32\config\SOFTWARE
HKLM\SECURITY	C:\Windows\System32\config\SECURITY
Облікові записи (логіни / хеші паролів)	C:\Windows\System32\config\SAM
HKCU	C:\Users\<UserName>\NTUSER.DAT
Профіль користувача (HKCU\Software\Classes)	C:\Windows\System32\config\AppData\Local\Microsoft\Windows

Під час відкриття документів Windows автоматично створює записи в реєстрі.

1. RecentDocs – містить інформацію про документи, які нещодавно відкривав користувач.

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

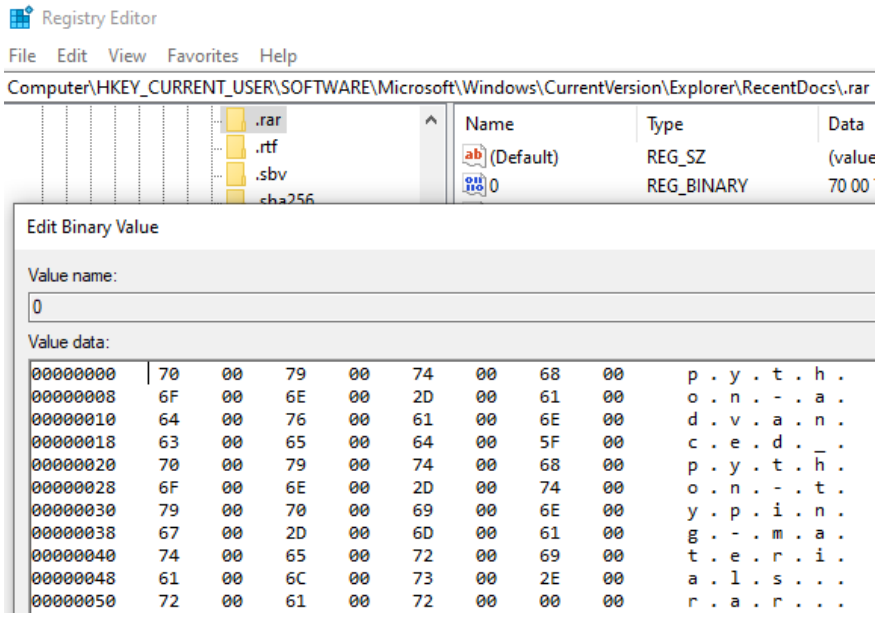


Рис. 65. RecentDocs у реєстрі Windows

2. UserAssist – містить інформацію про програми, які запускалися користувачем.

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

Особливістю UserAssist є те, що назви програм записуються із застосуванням алгоритму ROT13.

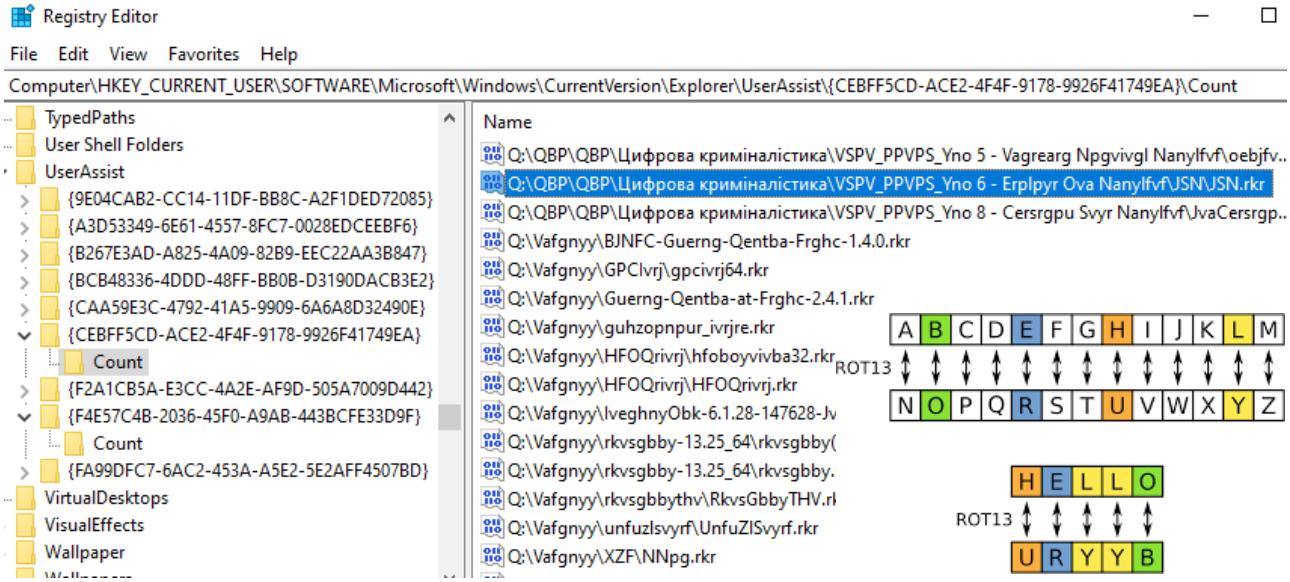


Рис. 66. UserAssist у реєстрі Windows

3. MuiCache – містить назви програм, які запускалися у системі.

HKCR\Local Settings\Software\Microsoft\Windows\Shell\MuiCache

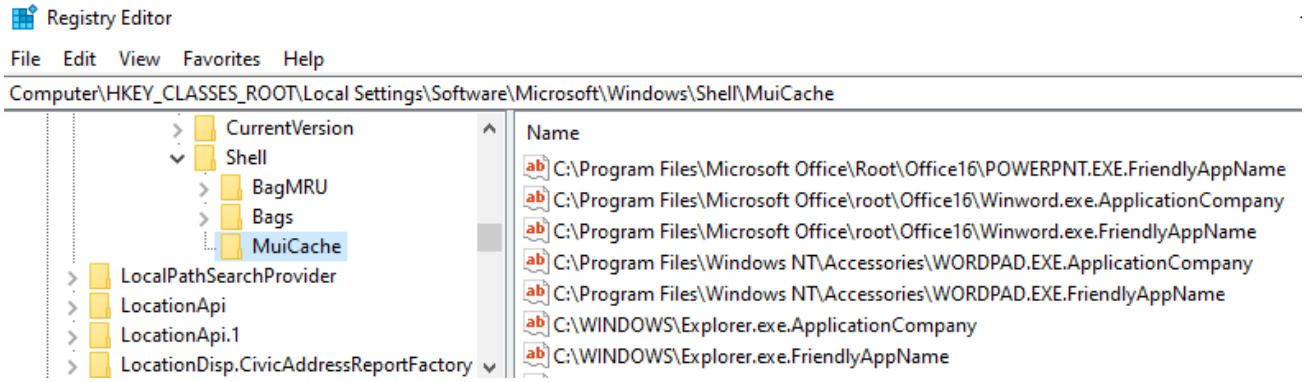


Рис. 67. MuiCache у реєстрі Windows

4. Історія USB-пристроїв (USBSTOR) – містить інформацію про всі USB-накопичувачі, які хоча б один раз підключалися до комп'ютера.

HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR

5. Поточні відеопристрої – містить інформацію про відеоадаптери, встановлені у системі.

HKLM\HARDWARE\DEVICEMAP\VIDEO

6. Відомості про бездротові мережі – містить інформацію про бездротові мережі Wi-Fi, до яких підключався комп'ютер.

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Wireless

Дані про останні входи (LogonUI) – містить інформацію про останніх користувачів, які входили до системи.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI

Одним із найважливіших напрямів аналізу реєстру є дослідження механізмів автоматичного запуску програм.

Таблиця 8

Автозапуск в Реєстрі

Гілка /	Призначення
HKCU\Software\Microsoft\Windows\CurrentVersion\Run C:\Users\<UserName>\AppData\Roaming\ Microsoft\Windows\Start Menu\Programs\Startup	для поточного користувача
HKLM\Software\Microsoft\Windows\CurrentVersion\Run C:\ProgramData\Microsoft\Windows\ Start Menu\Programs\Startup	для всіх користувачів
HKLM\SYSTEM\CurrentControlSet\Services	служби (services.exe)
HKLM\Software\Microsoft\Windows NT\ CurrentVersion\Image File Execution Options	для перехоплення запуску програм (часто – ШПЗ)
HKLM\Software\Microsoft\Windows\ CurrentVersion\Policies\Explorer\Run	з політик
HKCU\Software\Microsoft\Windows NT\ CurrentVersion\Windows\Load	старіший спосіб автозапуску

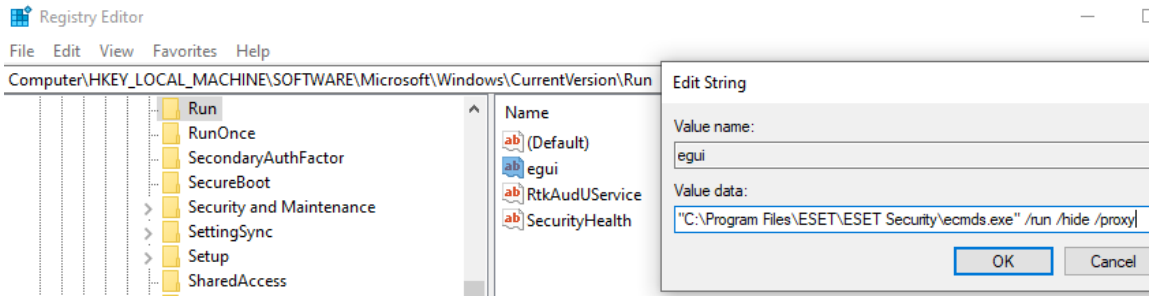


Рис. 68. Автозапуск в реєстрі

Для дослідження реєстру використовуються спеціалізовані програмні засоби:

- Registry Explorer;
- Registry Viewer;
- FTK Imager;
- Autopsy;
- RegRipper;
- RECmd;
- Windows Registry Editor (regedit).

Реєстр Windows є одним із найінформативніших джерел цифрових доказів. Його аналіз дозволяє:

- встановлювати дії користувача;
- визначати історію запуску програм;
- виявляти підключені USB-пристрої;
- досліджувати механізми автозапуску;
- встановлювати факти входу до системи;
- аналізувати підключення до мереж;
- реконструювати послідовність подій.

Завдання на лабораторну роботу

Відкрийте FTK Imager

Змонтуйте побітову копію підозрілого цифрового носія File > Image Mounting > Vader_Home_Computer.001

Встановіть та відкрийте Registry Explorer (https://ericzimmerman.github.io/)

Можливо під час встановлення потрібно буде завантажити та довстановити .NET

Registry Explorer потрібно запускати від імені Адміністратора (в контекстному меню – Запустити з правами адміністратора)!

File > Load hive > F:\Windows\System32\config\SYSTEM

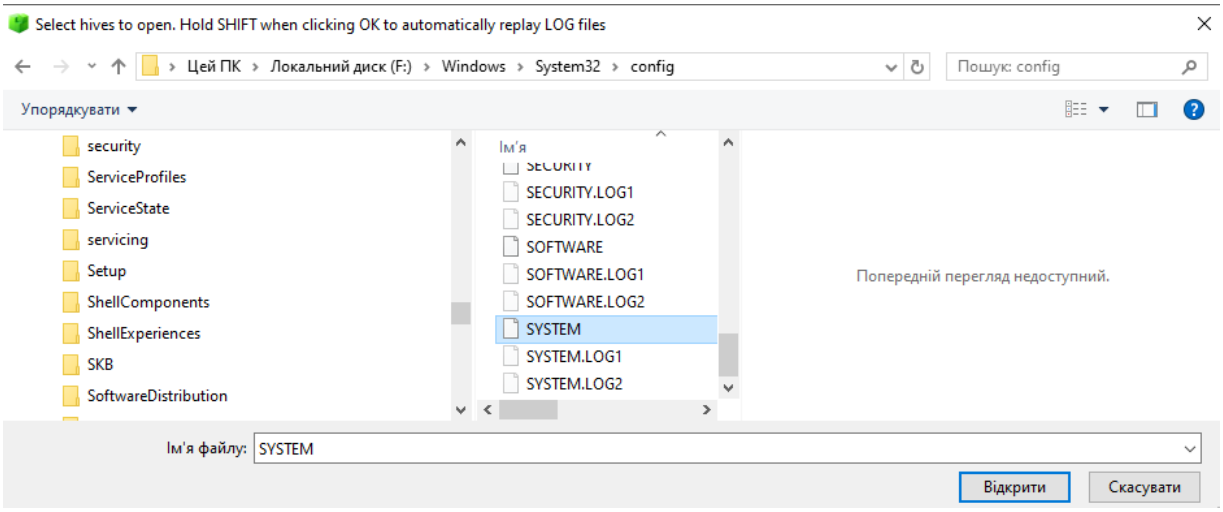


Рис. 69. Вибір hive-файлу для завантаження в Registry Explorer

Відкрити.

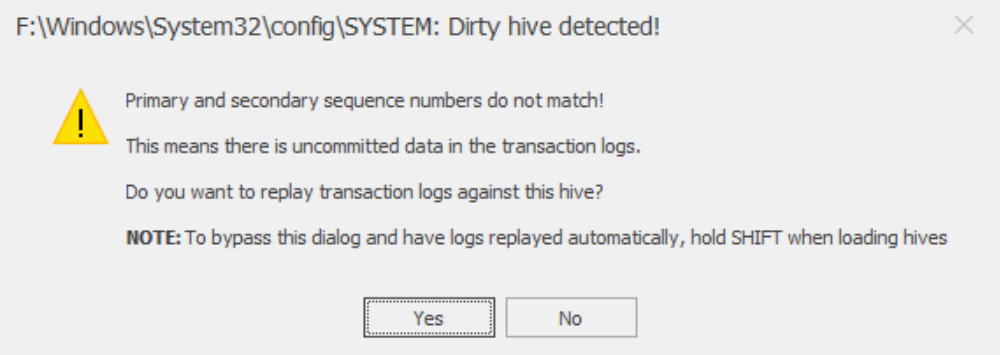


Рис. 70. Повідомлення в Registry Explorer

**Це вікно повідомлення в Registry Explorer означає, що завантажений hive-файл (SYSTEM) є "брудним" (dirty) – тобто, містить незастосовані транзакції, які зберігаються у журнал-файлах (transaction logs). Це вказує на те, що файл реєстру був не повністю записаний перед вимкненням системи — тобто система не завершила роботу коректно. Це питання: чи хочете ви застосувати журнали транзакцій (.LOG1, .LOG2), щоб відновити найактуальніший стан реєстру.

Натискаємо Yes.

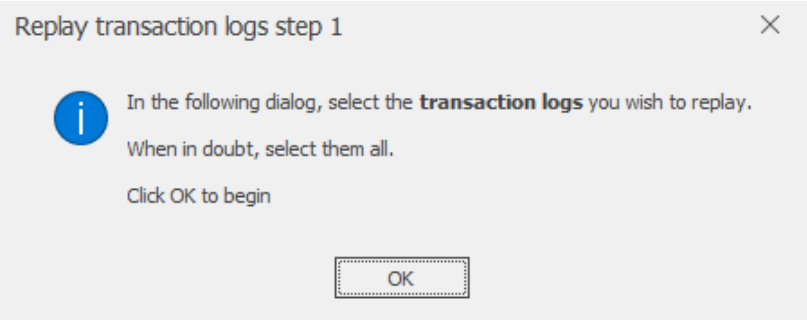


Рис. 71. Завантаження hive-файлу в Registry Explorer

OK

У наступному діалозі позначте всі запропоновані LOG-файли:

SYSTEM.LOG1

SYSTEM.LOG2

(Ctrl + ліва кнопка миші).

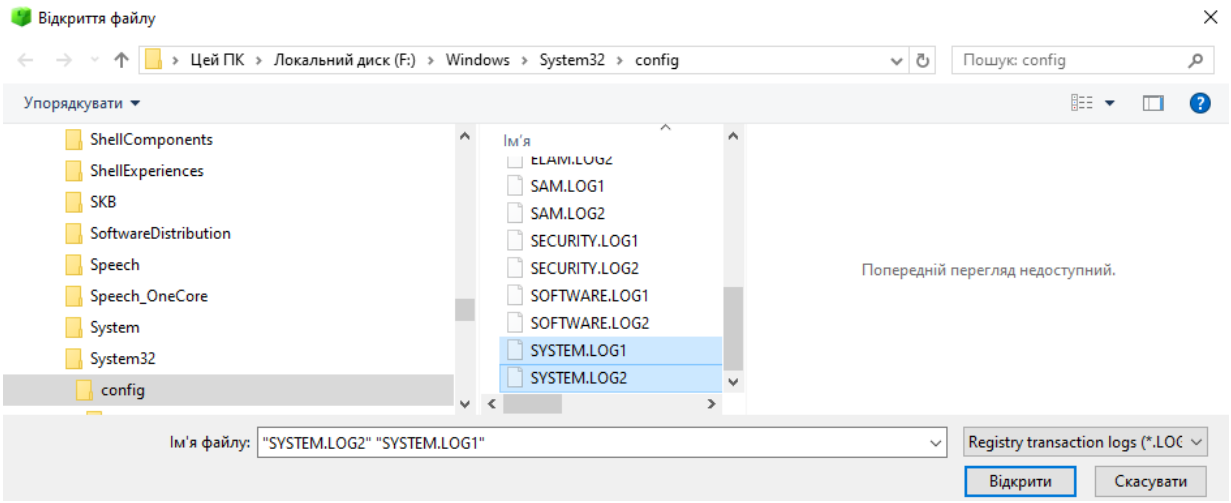


Рис. 72. Вибір hive-файлу для завантаження в Registry Explorer

Відкрити.

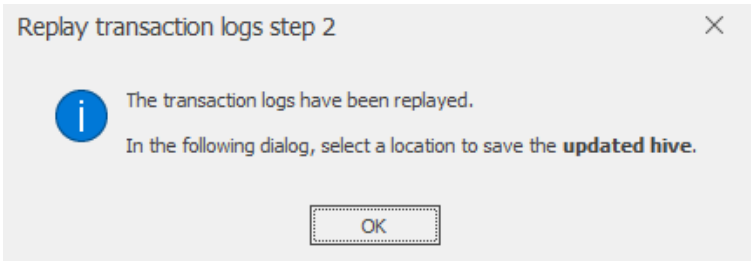


Рис. 73. Завантаження hive-файлу в Registry Explorer

OK.
Зберегти.

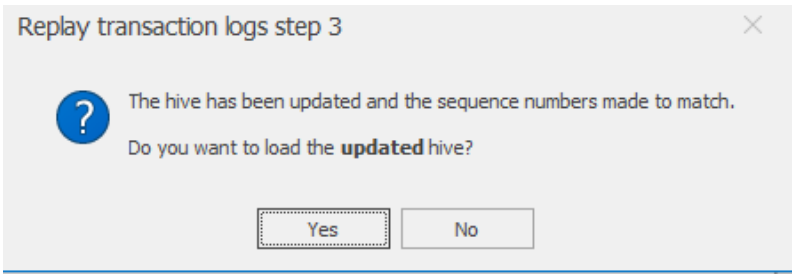


Рис. 74. Завантаження hive-файлу в Registry Explorer

Yes.

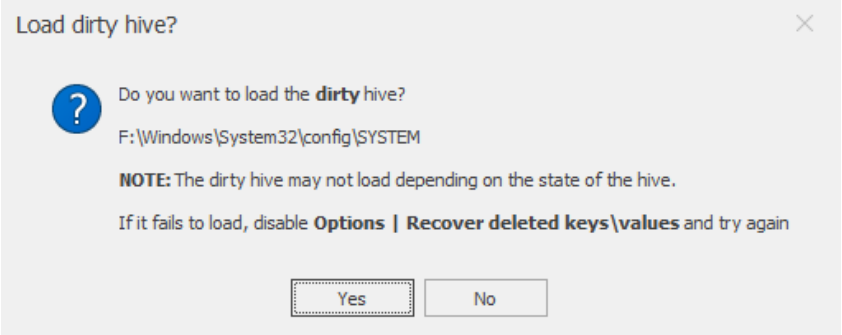


Рис. 75. Завантаження hive-файлу в Registry Explorer

Yes.

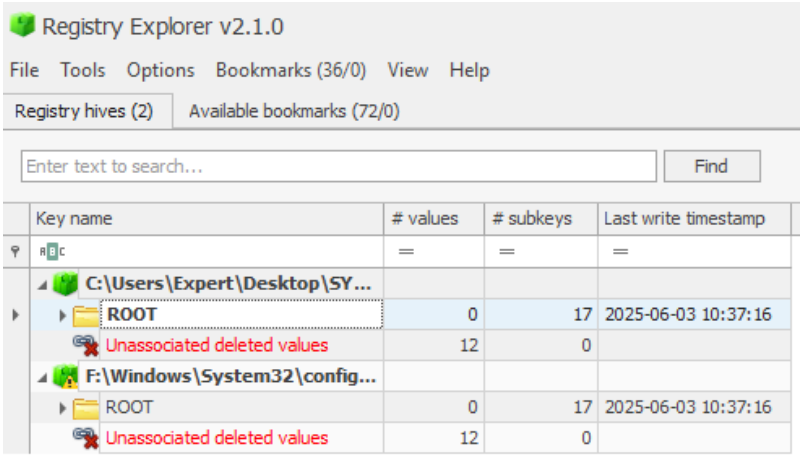


Рис. 76. Registry Explorer після завантаження

Перейдіть у вкладку Available bookmarks.
F:\Windows\System32\config\SYSTEM.

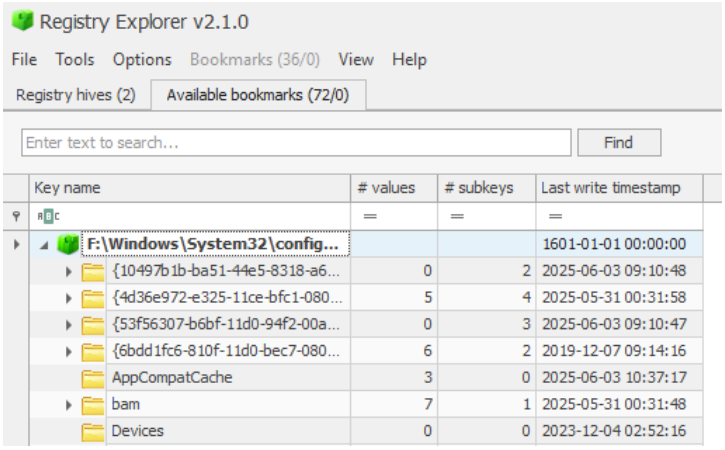


Рис. 77. Available bookmarks в Registry Explorer

USBSTOR.

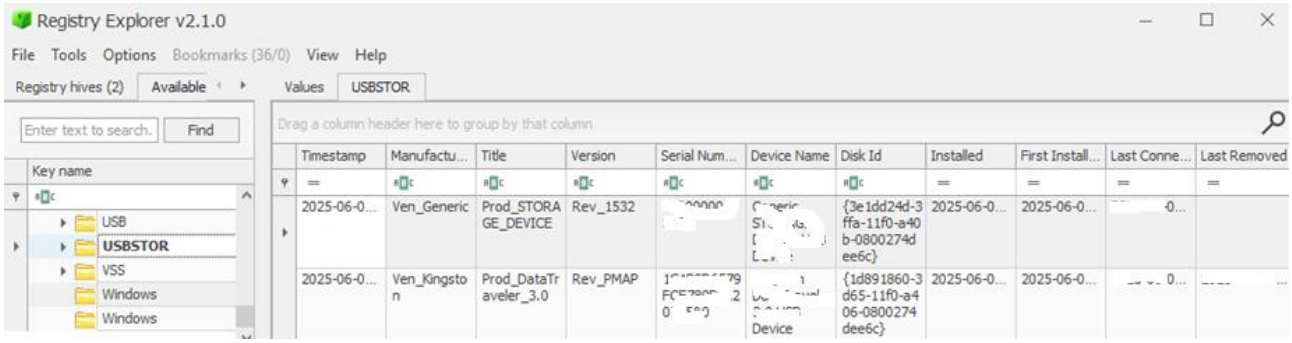


Рис. 78. USBSTOR в Registry Explorer

Які флеш-накопичувачі (Device Name) були підключені до цієї системи?

_____

Які серійні номери пристроїв (Serial Number)?

_____

Коли відбувалося останнє підключення цих накопичувачів до системи?

_____

File > Load hive > F:\Users\Owner\NTUSER.DAT.

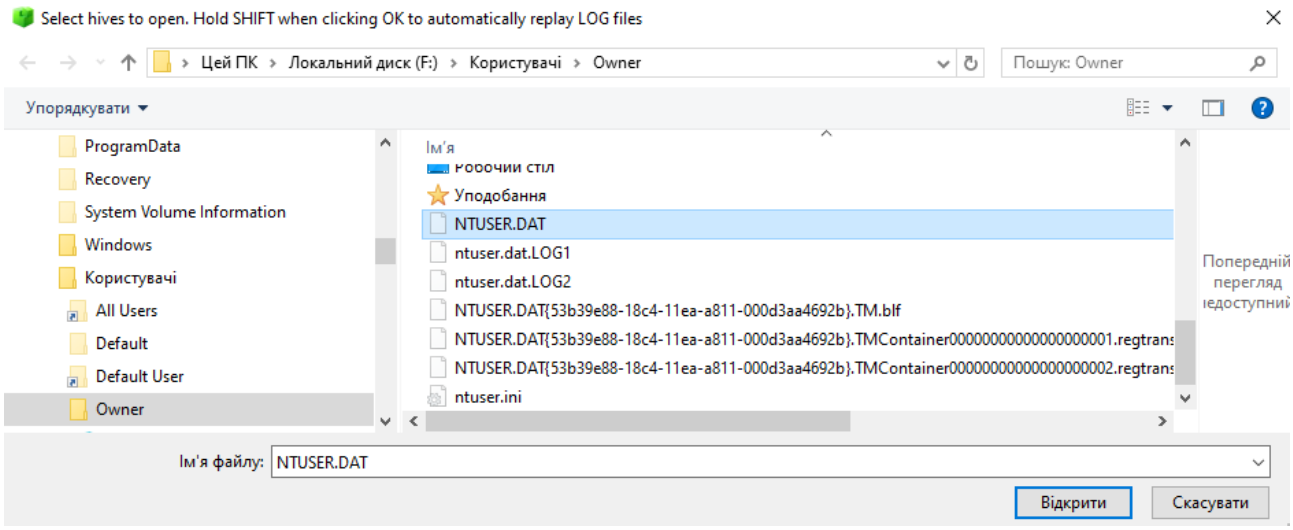


Рис. 79. Вибір hive-файлу для завантаження в Registry Explorer

Далі по аналогії з попереднім процесом.

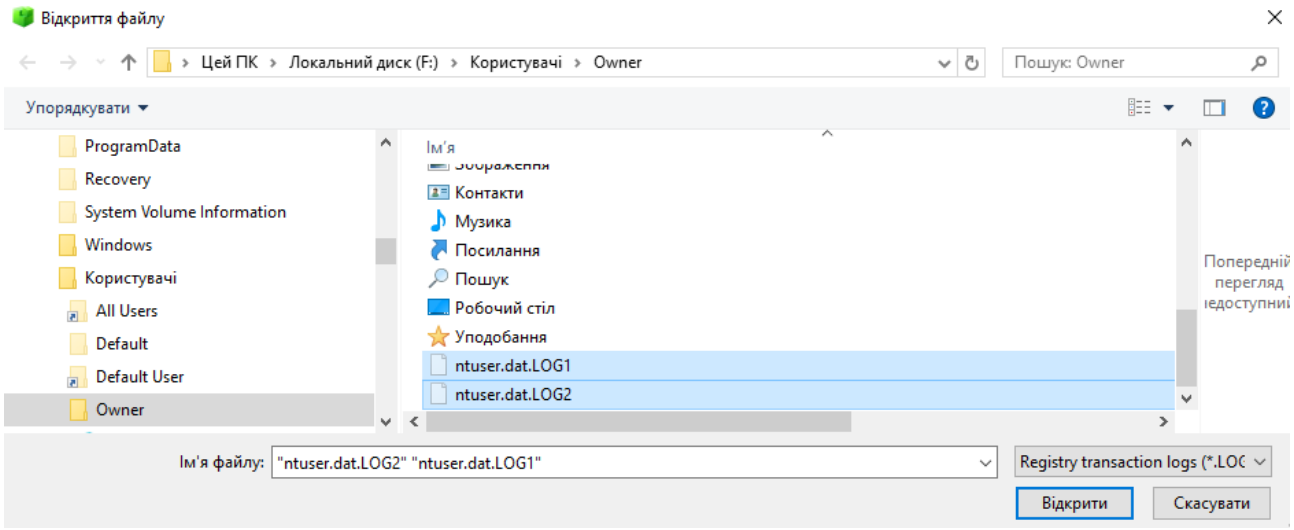


Рис. 80. Вибір hive-файлу для завантаження в Registry Explorer

F:\Users\Owner\NTUSER.DAT.

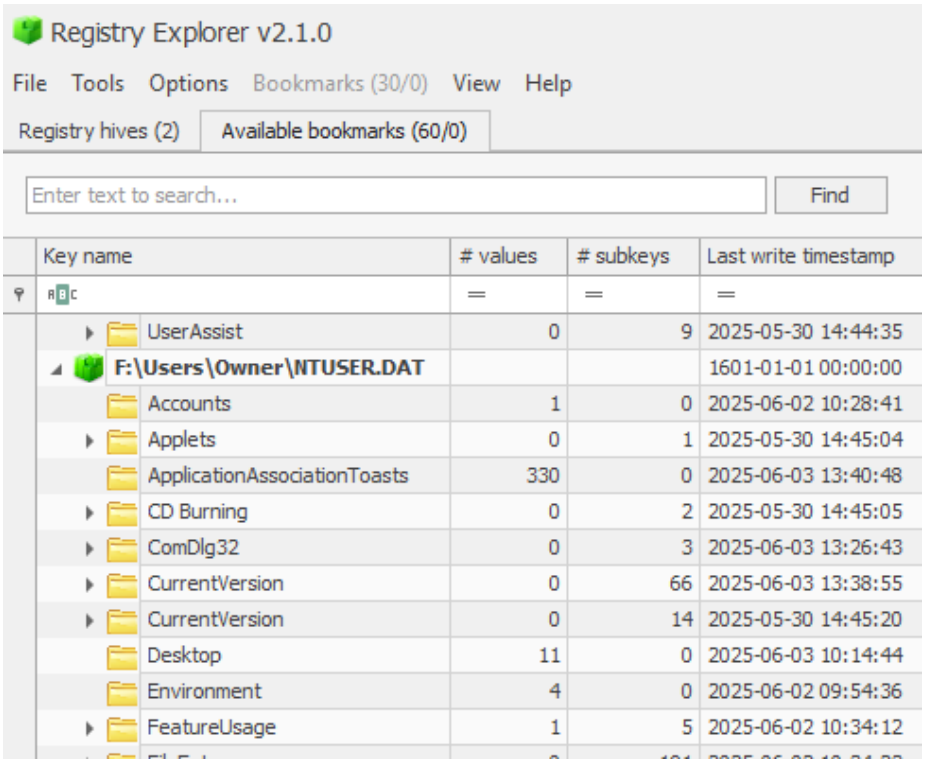


Рис. 81. Available bookmarks в Registry Explorer

RecentDocs.

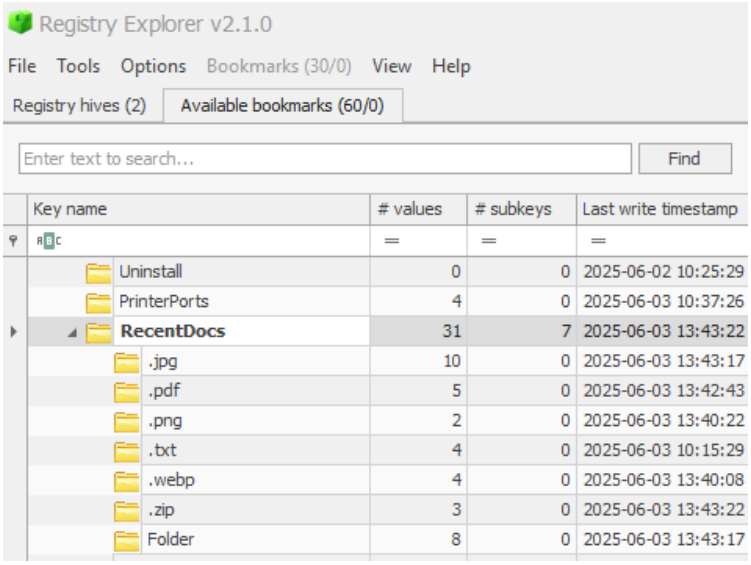


Рис. 82. RecentDocs в Registry Explorer

.txt.

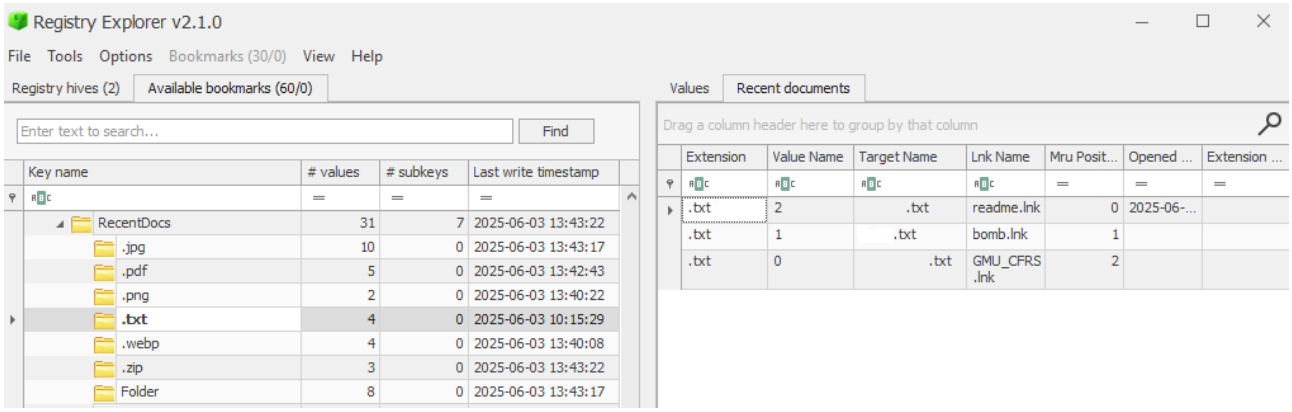


Рис. 83. RecentDocs в Registry Explorer

Які файли .txt відкривалися в цій системі?

_____

Які файли .zip відкривалися в цій системі?

_____

Відкрийте Autopsy.

Відкрийте справу, що ви відкрили у попередніх лабораторних – Open Recent Case

Перейдіть Data Artifacts > USB Device Attaches.

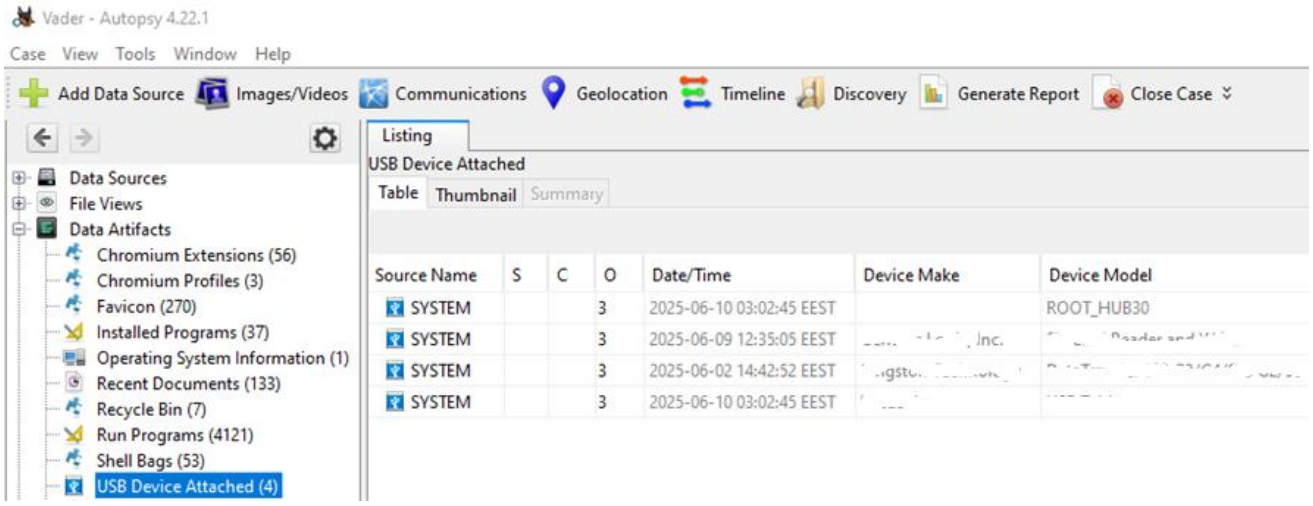


Рис. 84. USB Device Attaches в Autopsy

Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки стосовно флеш-накопичувачів?

_____

Контрольні питання

1. Що таке реєстр Windows?
2. Яке призначення реєстру Windows?
3. Чому реєстр є важливим джерелом цифрових доказів?
4. Яку інформацію можна отримати під час аналізу реєстру?
5. Які основні гілки реєстру Windows ви знаєте?
6. Яке призначення гілки HKLM (HKEY_LOCAL_MACHINE)?
7. Яке призначення гілки HKCU (HKEY_CURRENT_USER)?
8. Яке призначення гілки HKCR (HKEY_CLASSES_ROOT)?
9. Яке призначення гілки HKU (HKEY_USERS)?
10. Яку інформацію містить ключ RecentDocs?
11. Яку інформацію містить UserAssist?
12. Як декодуються записи UserAssist?
13. Яку інформацію містить MuiCache?
14. Яку інформацію можна отримати з ключа USBSTOR?
15. Яку інформацію містить ключ DEVICEMAP\VIDEO?
16. Які відомості можна отримати про мережі Wi-Fi з реєстру?
17. Яке призначення ключа LogonUI?
18. Що таке автозапуск програм?
19. Як шкідливе програмне забезпечення може використовувати механізми автозапуску?

20. Які інструменти використовуються для аналізу реєстру Windows?
21. Які можливості надає Registry Explorer?
22. Які можливості аналізу реєстру має Autopsy?

Лабораторна робота 11
АНАЛІЗ ОПЕРАТИВНОЇ ПАМ'ЯТІ

Мета заняття: ознайомитися з принципами проведення аналізу оперативної пам'яті (Live Forensics) та її значенням як джерела енергозалежних цифрових доказів; дослідити особливості зберігання інформації в оперативній пам'яті, основні формати її збереження; ознайомитися з можливостями аналізу оперативної пам'яті для виявлення активних процесів, драйверів, мережевих з'єднань, відкритих файлів, користувацьких сесій, буфера обміну, ключів шифрування та інших цифрових артефактів; отримати практичні навички використання спеціалізованого криміналістичного інструменту для дослідження дампів оперативної пам'яті – Volatility; дослідити можливості виявлення шкідливого програмного забезпечення, прихованих процесів та інших ознак компрометації інформаційної системи.

Теоретичні відомості

Оперативна пам'ять (Random Access Memory, RAM) є енергозалежною пам'яттю комп'ютера, у якій під час роботи операційної системи тимчасово зберігаються дані активних процесів, програм, драйверів, мережевих з'єднань та іншої службової інформації. На відміну від жорсткого диска або SSD, вміст оперативної пам'яті повністю втрачається після вимкнення живлення. Саме тому аналіз оперативної пам'яті належить до методів живого аналізу (Live Forensics) і є одним із найважливіших напрямів сучасної цифрової криміналістики. У багатьох випадках оперативна пам'ять містить цифрові докази, які відсутні на постійних носіях інформації. Дамп оперативної пам'яті дозволяє дослідити поточний стан комп'ютерної системи в момент її роботи.

Аналіз оперативної пам'яті використовується для:

- виявлення шкідливого програмного забезпечення;
- дослідження активних процесів;
- аналізу мережевих з'єднань;
- вилучення ключів шифрування;
- встановлення користувацьких сесій;
- аналізу відкритих файлів;
- відновлення тимчасових даних;
- дослідження діяльності зловмисника.

Під час вилучення оперативної пам'яті необхідно мінімізувати вплив на досліджувану систему. Рекомендується:

- підключити зовнішній накопичувач;
- виконати дамп оперативної пам'яті спеціалізованим програмним забезпеченням;

– зафіксувати час виконання вилучення;
– задокументувати використані інструменти;
– обчислити криптографічні хеш-значення отриманого дампа;
– зберегти дамп у незмінному вигляді.

Після завершення вилучення аналіз повинен виконуватися лише на копії отриманого файлу.

Оперативна пам'ять може зберігатися у різних форматах залежно від використаного інструмента або операційної системи.

Таблиця 9

Формати запису оперативної пам’яті

Формат	Розширення	Опис
Дамп оперативної пам’яті (RAM dump)	.raw, .bin, .mem	Повна копія вмісту ОЗП, отримана спеціальними інструментами (FTK Imager)
Файл гібернації (Hibernation file)	hiberfil.sys	Створюється при переході в режим гібернації. Містить частину пам’яті.
Файл аварійного завершення (crash dump)	memory.dmp, *.dmp	Створюється при збоях (BSOD). Містить часткову або повну копію ОЗП.
VMware Snapshot VirtualBox (Oracle) Hyper-V (Microsoft)	.vmem, .sav, .vbox-prev, .vdi, .bin + .vsv	Віртуальні машини (VM) можуть зберігати оперативну пам’ять як частину знімку.

Оперативна пам'ять містить значний обсяг інформації, яка відсутня на постійних носіях інформації. Під час аналізу дампа можуть бути виявлені:

1. Активні процеси. Перелік програм, які виконувалися в момент створення дампа. Можна визначити:
– ідентифікатор процесу (PID);
– батьківський процес;
– час запуску;
– використання пам'яті.

2. Завершені процеси. У деяких випадках залишки завершених процесів можуть залишатися в оперативній пам'яті. Це дозволяє встановити програми, які вже завершили роботу.

3. Завантажені драйвери. Дамп містить інформацію про драйвери пристроїв. Аналіз драйверів дозволяє:
– виявляти сторонні драйвери;
– знаходити підозрілі модулі;
– встановлювати драйвери шкідливого програмного забезпечення.

4. Rootkits – це шкідливе програмне забезпечення, яке приховує свою присутність у системі. Оскільки rootkit працює безпосередньо в оперативній пам'яті, його аналіз часто можливий лише за допомогою дампа RAM.

5. Завантажені DLL-бібліотеки. Кожний процес використовує динамічні бібліотеки (DLL). Аналіз DLL дозволяє:

- виявляти ін'єкції бібліотек;
- знаходити сторонні модулі;
- встановлювати використання шкідливого програмного забезпечення.

6. Мережеві з'єднання. Оперативна пам'ять містить інформацію про:

- IP-адреси;
- TCP-з'єднання;
- UDP-з'єднання;
- відкриті порти;
- мережеві сесії.

Ці відомості дозволяють встановити взаємодію комп'ютера з іншими системами.

7. Відкриті файли. У дампі можуть міститися:

- повні шляхи до відкритих файлів;
- дескриптори файлів;
- інформація про процес, який використовував файл.

8. Буфер обміну (Clipboard). Під час створення дампа часто можна отримати вміст буфера обміну Windows. Він може містити:

- текст;
- паролі;
- фрагменти документів;
- URL-адреси.

9. Буфер клавіатури. У деяких випадках можна відновити останні натискання клавіш користувача. Такі дані можуть містити:

- паролі;
- введені команди;
- пошукові запити;
- повідомлення.

10. Облікові дані. Оперативна пам'ять може містити:

- імена користувачів;
- паролі;
- токени автентифікації;
- NTLM-хеші;
- квитки Kerberos.

Такі дані використовуються під час дослідження компрометації облікових

записів.

11. Ключі шифрування. Під час роботи системи ключі шифрування часто знаходяться в оперативній пам'яті. Можуть бути виявлені:

- ключі BitLocker;
- ключі VeraCrypt;
- ключі EFS;
- криптографічні ключі застосунків.

Це дозволяє отримати доступ до зашифрованих носіїв навіть без знання пароля.

12. Користувацькі сесії. У пам'яті можуть залишатися:

- повідомлення месенджерів;
- активні чати;
- фрагменти електронної пошти;
- вебсесії;
- дані браузерів.

Це особливо важливо під час аналізу Telegram, Discord, Signal та інших месенджерів.

13. Розпаковане шкідливе програмне забезпечення. Багато сучасних програм-шкідників зберігаються на диску у зашифрованому або упакованому вигляді. Після запуску вони розпаковуються в оперативній пам'яті. Саме тому аналіз RAM дозволяє отримати повний код шкідливої програми, який неможливо знайти на диску.

Для створення дампа оперативної пам'яті використовуються:

- FTK Imager;
- DumpIt;
- Magnet RAM Capture.

Volatility – один із найпоширеніших відкритих програмних комплексів для аналізу оперативної пам'яті. Програма дозволяє аналізувати дампи оперативної пам'яті операційних систем Windows, Linux та macOS. За допомогою Volatility можна:

- визначати профіль операційної системи;
- отримувати список процесів;
- аналізувати мережеві з'єднання;
- досліджувати драйвери;
- знаходити DLL-бібліотеки;
- виявляти rootkits;
- аналізувати файлові дескриптори;
- відновлювати файли з оперативної пам'яті;
- отримувати ключі шифрування;

– досліджувати користувацькі сесії.

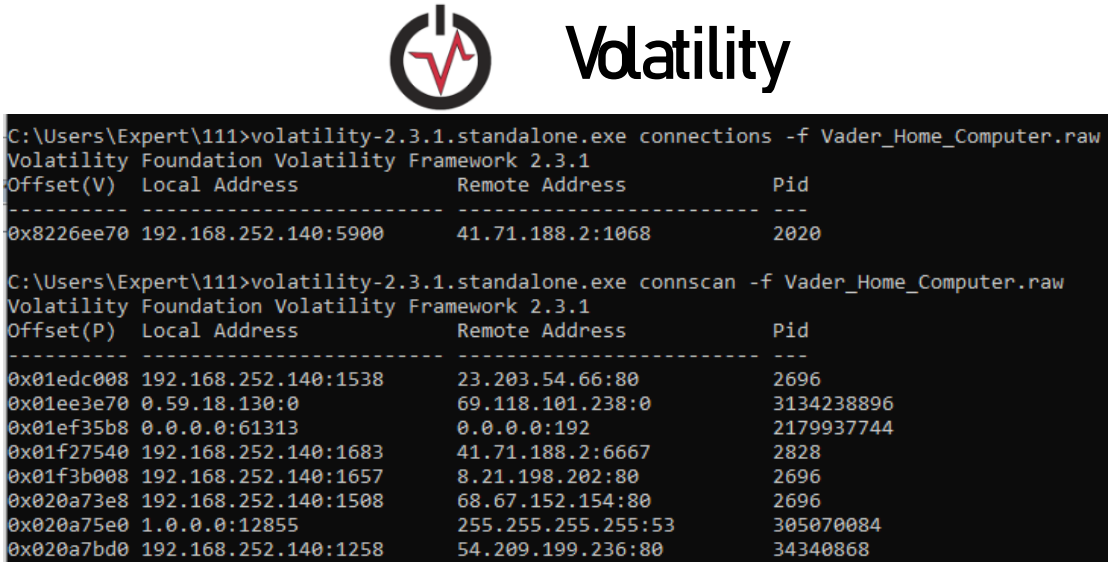


Рис. 85. Дослідження мережевих з'єднань у Volatility

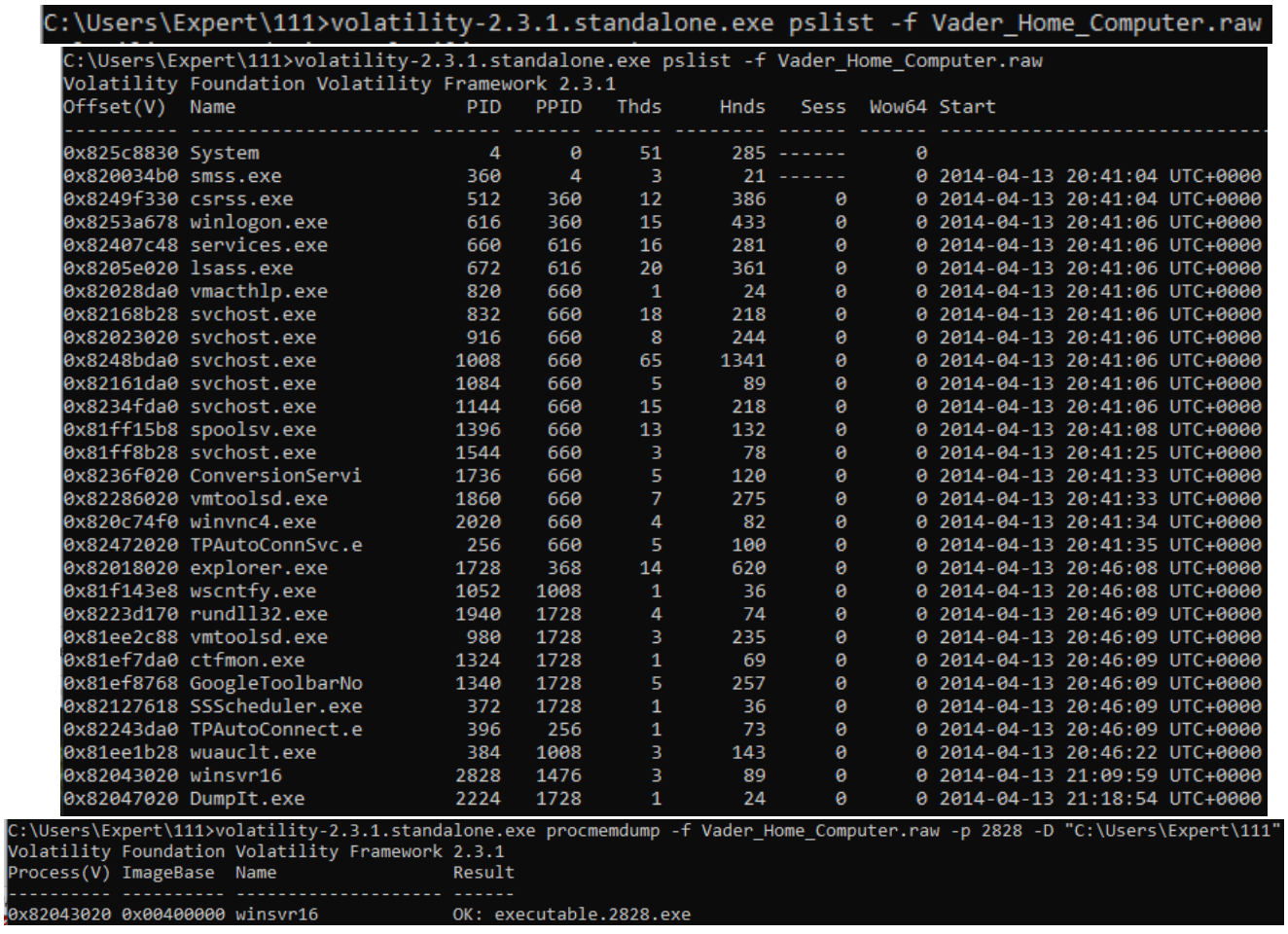


Рис. 86. Дослідження активних процесів та виявлення ШПЗ у Volatility

Volatility підтримує велику кількість модулів (plugins), що дозволяють автоматизувати аналіз різних типів цифрових артефактів.

Завдання на лабораторну роботу

Завантажте архів дампу оперативної пам’яті VaderRAM.zip (https://drive.google.com/file/d/1OJ8G5Majx2AMJ3I80V86-6v_9EI9pbCm). Розархівуйте його.

Завантажте Volatility Workbench V3.0.1012 (16,4 МБ).
(https://www.osforensics.com/tools/volatility-workbench.html).
Запустити VolatilityWorkbench.exe.
Image file: > Browse Image > Вибрати файл дампу VaderRAM.dmp.
Platform: Windows.

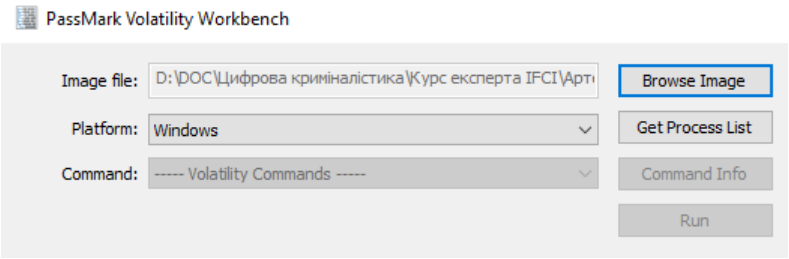


Рис. 87. Volatility Workbench

Кнопка Get Process List.
Який час запису дампу пам’яті?

_____

Command: windows.info.
Яка версія Windows?

_____

Command: windows.pslist.
Чи запущений був під час дампу браузер?

_____

Які PID цього процесу?

_____

Чи підтримувалася під час запису дампу сесія у браузері (SessionId=1)?

_____

Command: windows.netscan.NetScan.
До яких IPv4-адрес зверталася система по порту 80? Що це за процес?

_____

Впишіть усі IP-адреси, до яких було встановлено підключення на момент запису дампу (State=ESTEBLISHED).

_____

Перевірте їх через https://who.is/.

Чи існувало підключення до Google?

_____

Command: windows.hashdump.

Які хеші користувача Owner?

_____

За допомогою HxD Hex Editor відкрийте файл дампу пам’яті VaderRAM.dmp.

За допомогою пошук знайдіть Password.txt.

Яке значення паролю (між Password.txt та PK)?

_____

Відкрийте програму FTK Imager.

Змонтуйте підозріле зображення File > Image Mounting > Vader_Home_Computer.001.

Перейдіть до папки C:\Users\Owner\Documents\.

Знайдіть архів, для розпаковки якого потрібний пароль.

Спробуйте знайдений пароль.

Які серійні номери підроблених світлових мечів?

_____

Контрольні питання

1. Що таке оперативна пам'ять (RAM)?
2. Чому оперативна пам'ять називається енергозалежною?
3. Які цифрові докази з оперативної пам'яті можуть бути втрачені після вимкнення комп'ютера?
4. Які формати файлів використовуються для збереження дампа оперативної пам'яті?
5. Що таке файл hiberfil.sys?
6. Що таке файл memory.dmp?
7. Які формати оперативної пам'яті використовуються у віртуальних машинах?
8. Яку інформацію про процес можна отримати під час аналізу оперативної пам'яті?
9. Що таке rootkit?
10. Чому rootkit часто неможливо виявити лише аналізом файлової системи?
11. Яку інформацію про мережеву активність можна отримати з оперативної пам'яті?
12. Яку інформацію може містити буфер обміну (Clipboard)?
13. Яку інформацію може містити буфер клавіатури?

14. Які облікові дані можуть бути виявлені в оперативній пам'яті?
15. Чому аналіз оперативної пам'яті є важливим для дослідження зашифрованих носіїв BitLocker?
16. Що таке Volatility?
17. Які основні можливості Volatility?
18. Які модулі Volatility використовуються для аналізу мережевих з'єднань?
19. Які модулі Volatility використовуються для пошуку ін'єкцій шкідливого коду?
20. Які інструменти використовуються для створення дампа оперативної пам'яті?

Лабораторна робота 12
АНАЛІЗ МОБІЛЬНИХ ПРИСТРОЇВ

Мета заняття: ознайомитися з основними принципами цифрової криміналістики мобільних пристроїв та особливостями отримання цифрових доказів із сучасних смартфонів і планшетів; дослідити механізми захисту інформації операційних систем Android та iOS, шифрування, автентифікації та ізоляції застосунків; ознайомитися з основними методами криміналістичного дослідження мобільних пристроїв, зокрема ручним, логічним і фізичним вилученням даних, а також методами ISP та Chip-Off; отримати практичні навички виявлення, вилучення та аналізу цифрових доказів, що містяться в мобільних пристроях, зокрема контактів, журналів викликів, повідомлень.

Теоретичні відомості

Мобільні пристрої (смартфони, планшети, смарт-годинники та інші портативні пристрої) є одним із найважливіших джерел цифрових доказів під час розслідування кримінальних правопорушень та інцидентів інформаційної безпеки. Вони містять значний обсяг персональної інформації користувача: контакти, повідомлення, фотографії, документи, геолокаційні дані, журнали викликів, історію використання застосунків та інші відомості. На відміну від персональних комп'ютерів, сучасні мобільні пристрої мають розвинуті механізми захисту інформації, що значно ускладнює отримання цифрових доказів. Саме тому мобільна криміналістика (Mobile Device Forensics) є окремим напрямом цифрової криміналістики.

Під час вилучення мобільних пристроїв необхідно забезпечити збереження цифрових доказів та мінімізувати ризик їх втрати або модифікації. Рекомендується:

- зафіксувати зовнішній вигляд пристрою;
- сфотографувати екран, якщо він увімкнений;
- зафіксувати модель, серійний номер, IMEI та SIM-картки;
- оцінити ризик віддаленого стирання інформації;
- за необхідності ізолювати пристрій від мереж (режим польоту або екранувальний пакет Faraday);
- забезпечити безперервне живлення пристрою;
- задокументувати всі виконані дії;
- підтримувати ланцюг зберігання цифрових доказів (Chain of Custody).

Перед початком дослідження бажано створити логічну або фізичну копію пам'яті пристрою.

Дослідження мобільних пристроїв значно складніше, ніж аналіз персональних комп'ютерів. Основними причинами є:

1. Різноманітність апаратного забезпечення. Існують тисячі моделей мобільних пристроїв, які відрізняються:
   - архітектурою процесора;
   - контролерами пам'яті;
   - способом підключення;
   - типами накопичувачів;
   - версіями завантажувачів.

Це ускладнює створення універсальних криміналістичних інструментів.

2. Різні мобільні операційні системи. Найпоширенішими мобільними платформами є:
   - Android;
   - iOS;
   - BlackBerry OS;
   - Windows Phone.

Кожна система має власні механізми захисту та структуру зберігання даних.

3. Сучасні смартфони використовують:
   - повнодискове або файлове шифрування;
   - апаратні модулі безпеки;
   - біометричну автентифікацію;
   - захищене завантаження;
   - захищені сховища ключів.

4. На відміну від жорстких дисків, для мобільних пристроїв практично не існує аналогів апаратних блокіраторів запису. Будь-яке підключення пристрою потенційно може змінити його вміст.

5. Зловмисники можуть використовувати:
   - приховування інформації;
   - обфускацію;
   - шифрування;
   - автоматичне стирання даних;
   - захищені месенджери.

6. Пристрій може бути захищений:
   - PIN-кодом;
   - графічним ключем;
   - паролем;
   - відбитком пальця;
   - розпізнаванням обличчя.

7. Для дослідження можуть знадобитися:
   - різні USB-кабелі;
   - Lightning-кабелі;

- USB-C;
- спеціальні адаптери;
- зарядні пристрої;
- акумулятори;
- криміналістичні бокси.

8. Неправильні дії можуть призвести до:
   - блокування пристрою;
   - втрати ключів шифрування;
   - скидання налаштувань;
   - видалення інформації.
9. Мобільні пристрої можуть одночасно використовувати:
   - стільникові мережі;
   - Wi-Fi;
   - Bluetooth;
   - NFC;
   - інфрачервоний порт.

Через ці канали можливе віддалене керування або стирання інформації.

10. Шкідливі застосунки можуть:
    - приховувати дані;
    - шифрувати інформацію;
    - стирати цифрові докази;
    - перешкоджати проведенню експертизи.
11. Під час дослідження необхідно враховувати:
    - вимоги законодавства;
    - судові дозволи;
    - юрисдикцію;
    - міжнародні особливості отримання цифрових доказів.

Методи дослідження мобільних пристроїв

1. Ручне вилучення (Manual Extraction). Найпростіший спосіб дослідження. Передбачає перегляд інформації безпосередньо на екрані смартфона.

Переваги:

- працює практично для будь-якого пристрою;
- не потребує спеціального обладнання.

Недоліки:

- висока ймовірність людських помилок;
- неможливість відновлення видалених даних;
- можливість зміни інформації під час перегляду.

Виявлена інформація фотографується або фіксується іншим способом.

Запис може виконуватися через:

– USB;
– Lightning;
– HDMI-адаптер та карту відеозахоплення;
– AirPlay;
– Miracast.

2. Логічне вилучення (Logical Acquisition). Передбачає отримання даних через стандартні інтерфейси:

– USB;
– Bluetooth;
– Wi-Fi;
– інфрачервоний порт.

Отримуються дані, доступні операційній системі.

Переваги:

– швидкість;
– простота;
– підтримується більшістю криміналістичних інструментів.

Недоліки:

– не дозволяє отримати видалені дані;
– під час вилучення можливі зміни інформації.

3. Фізичне вилучення (Physical Acquisition). Передбачає створення побітової копії пам'яті пристрою.

Дозволяє:

– отримувати максимальний обсяг інформації;
– відновлювати видалені дані;
– аналізувати невидимі області пам'яті.

Недоліком є висока технічна складність.

3.1. Chip-Off. Передбачає фізичне демонтування мікросхеми пам'яті. Після цього мікросхема зчитується спеціальним обладнанням. Метод використовується лише тоді, коли інші способи недоступні. Існує високий ризик пошкодження пристрою.

3.2. In-System Programming (ISP). Передбачає зчитування пам'яті без демонтажу мікросхеми шляхом підключення безпосередньо до контактів пам'яті. Метод менш руйнівний, ніж Chip-Off, але також потребує спеціальної підготовки.

3.3. Мікроскопічний аналіз. У виняткових випадках застосовується безпосередній аналіз мікросхем за допомогою спеціалізованого обладнання.

Під час дослідження можуть бути виявлені:

– контакти;
– історія викликів;
– SMS та MMS;

- повідомлення месенджерів;
- фотографії;
- відео;
- аудіозаписи;
- електронна пошта;
- документи;
- історія браузера;
- календар;
- GPS-координати;
- карти;
- дані соціальних мереж;
- резервні копії;
- видалені файли;
- журнали системи.

Особливості дослідження пристроїв iPhone

Пристрої Apple підтримують:

- PIN-код;
- пароль;
- Touch ID;
- Face ID.

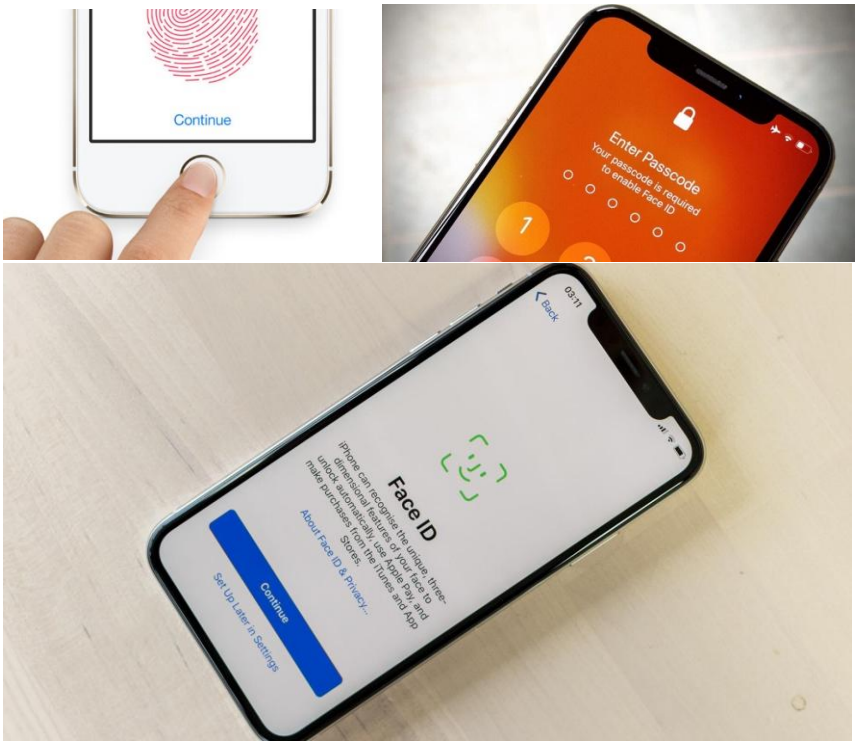


Рис. 88. Доступ до iPhone

Біометрична автентифікація використовується лише для розблокування, а криптографічні ключі зберігаються в Secure Enclave.

iOS використовує:

- Secure Boot Chain;
- Secure Enclave;
- File-Based Encryption;
- Data Protection API;
- App Sandboxing;
- Code Signing;
- Keychain;
- Activation Lock.

У разі вибору користувачем функції «Стерти весь вміст і налаштування» видаляються криптографічні ключі, після чого відновлення даних практично неможливе.

Джерелами цифрових доказів можуть бути резервні копії:

- iTunes Backup;
- iCloud Backup.

Для отримання резервної копії з iCloud зазвичай необхідні:

- Apple ID;
- пароль користувача;
- (за наявності) другий фактор автентифікації.

Jailbreak – це отримання привілейованого доступу (root) до файлової системи iOS. Він відкриває доступ до системних файлів, але одночасно змінює стан пристрою та знижує рівень його захисту.

Особливості дослідження пристроїв Android

Android використовує багаторівневу систему захисту. Основними механізмами є:

- ізоляція застосунків (Sandbox);
- система дозволів;
- цифрове підписування застосунків;
- SELinux;
- Verified Boot;
- File-Based Encryption;
- Google Play Protect.

Найчастіше досліджуються:

- SQLite-бази даних;
- XML-файли Shared Preferences;
- журнали logcat;

– кеш;
– каталоги /data/data/;
– каталоги /sdcard/Android/data/.

ADB (Android Debug Bridge) – це інструмент командного рядка для взаємодії з Android-пристроями через USB. Він дозволяє:

– отримувати журнали;
– копіювати файли;
– запускати команди;
– встановлювати застосунки;
– виконувати налагодження.

Для використання ADB необхідно ввімкнути режим USB debugging, що змінює стан пристрою і повинно бути відображено в протоколі дослідження.

Під час дослідження мобільних пристроїв широко використовуються:

– Cellebrite UFED;
– Oxygen Forensic Detective;
– Magnet AXIOM;
– Autopsy (модулі Android).



Рис. 89. Криміналістичні інструменти для дослідження мобільних пристроїв

Завдання на лабораторну роботу

Завантажте архів пам’яті мобільного телефона Vader_Phone.zip (https://drive.google.com/file/d/19XgxWGRa1Ez9e-gQrAwM7VCONojRSLAH).

Розархівуйте його.

Відкрийте Autopsy.

Відкрийте справу, що ви завели у попередніх лабораторних – Open Recent Case

Logical Files.

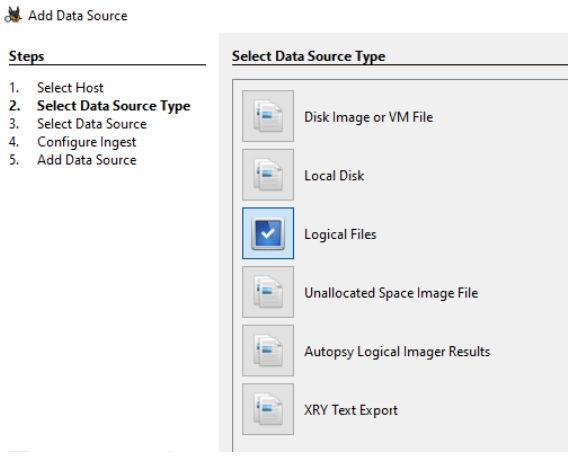


Рис. 90. Відкриття файлів вилучених з мобільного телефона в Autopsy

Add > вкажіть шлях до збереженої папки Vader_Phone.

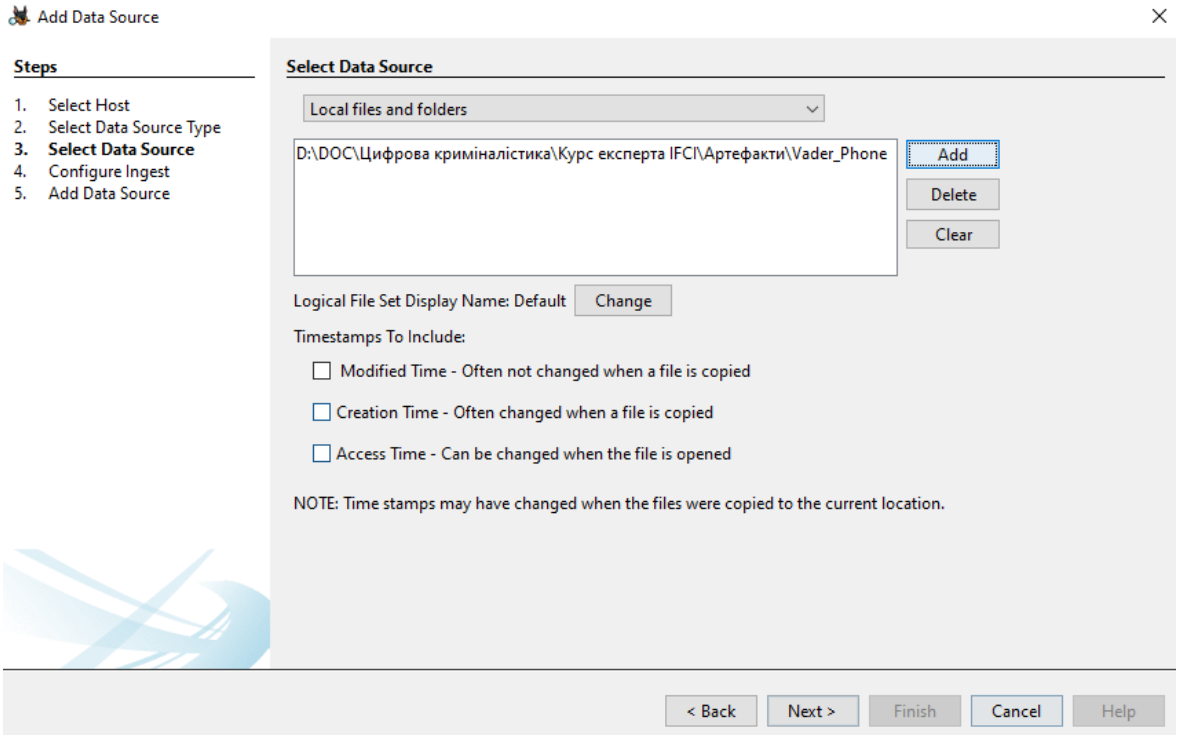


Рис. 91. Відкриття файлів вилучених з мобільного телефона в Autopsy

Виберіть:

- Android Analyzer (aLEAPP),
- Android Analyzer.

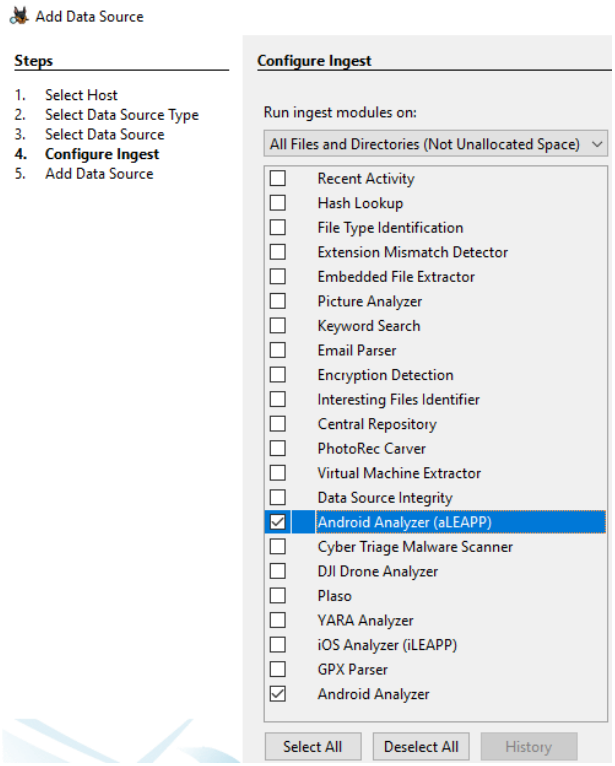


Рис. 92. Вибір модулів аналізу в Autopsy

Data Artifacts > Call Logs.

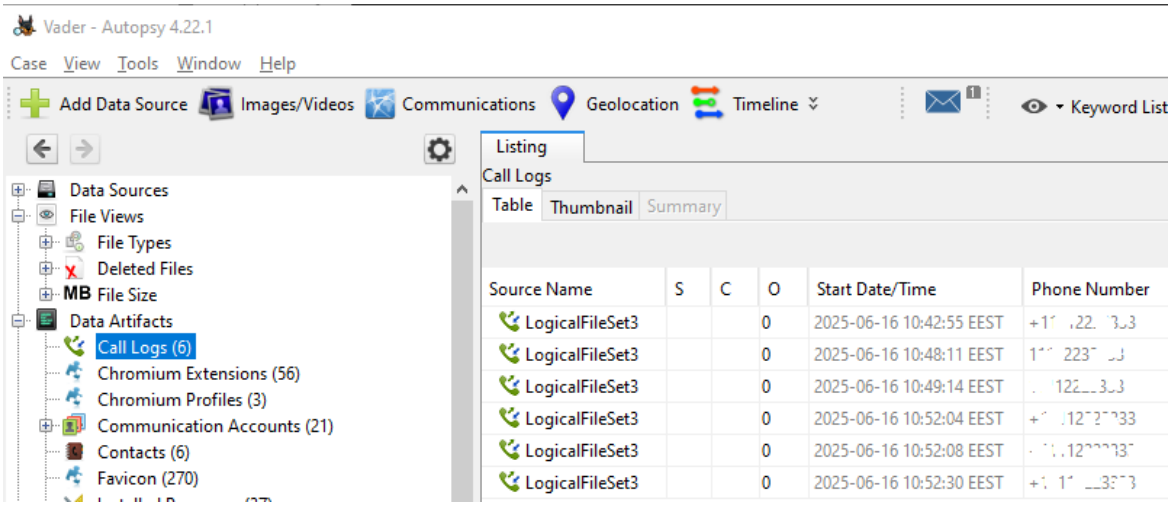


Рис. 93. Аналіз номерів абонентів мобільного телефона в Autopsy

Який номер абонента, з яким велося спілкування?

_____

Data Artifacts > Contacts.

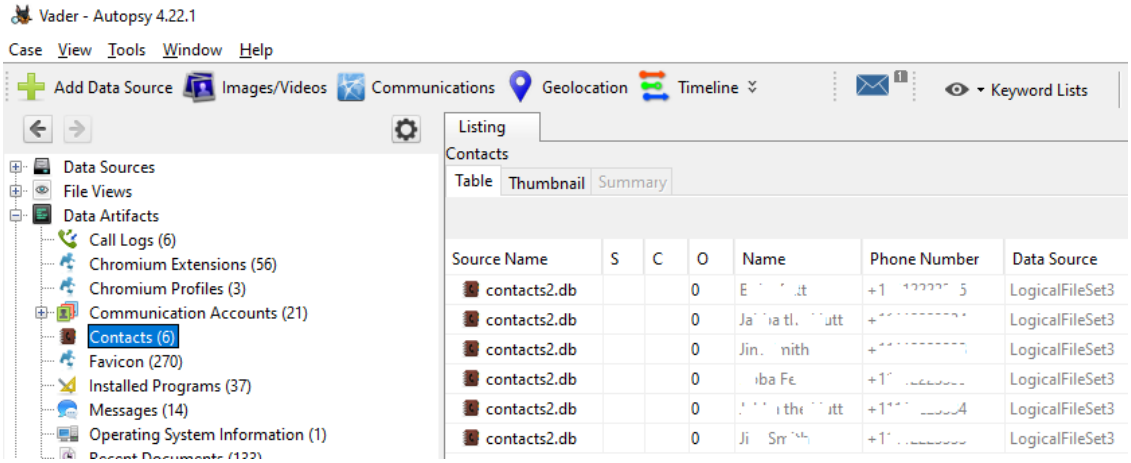


Рис. 94. Аналіз контактів мобільного телефона в Autopsy

Які контакти абонента?

Data Artifacts > Messages.

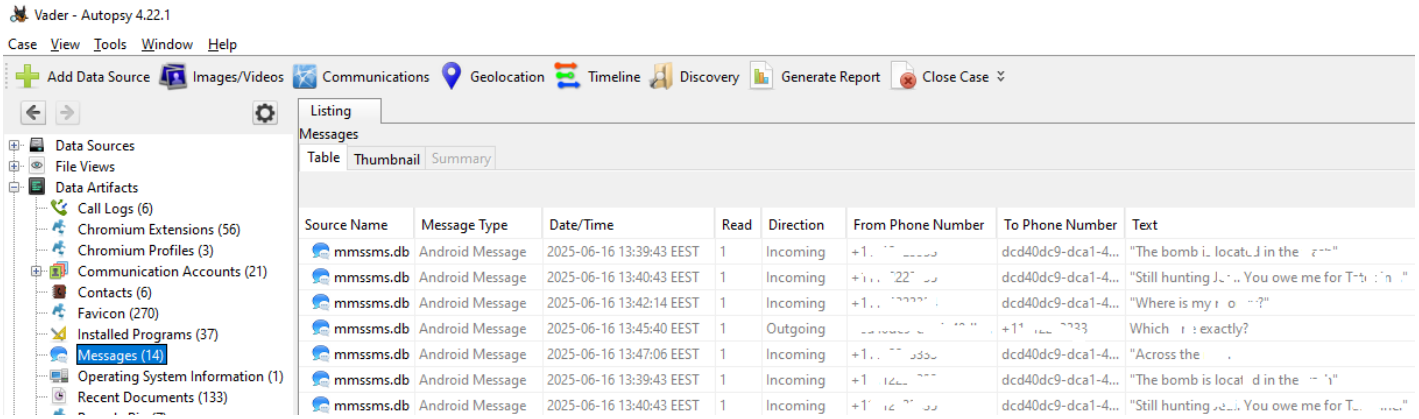


Рис. 95. Аналіз текстових повідомлень мобільного телефона в Autopsy

Відновіть листування абонента?

Data Artifacts > Web Accounts.

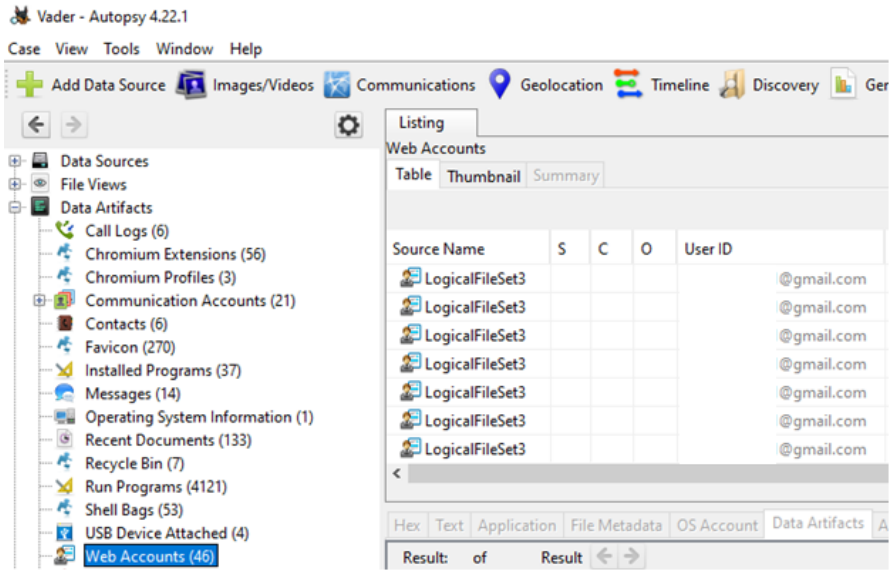


Рис. 96. Аналіз акаунту мобільного телефона в Autopsy

До якого акаунту підключений абонент?

_____

Контрольні питання

1. Які основні труднощі виникають під час дослідження мобільних пристроїв?
2. Які мобільні операційні системи найчастіше зустрічаються під час криміналістичних досліджень?
3. Які механізми захисту даних використовуються в сучасних смартфонах?
4. Чому практично неможливо повністю запобігти зміні даних під час дослідження мобільного пристрою?
5. Які способи протидії криміналістичному дослідженню можуть використовувати зловмисники?
6. Чому необхідно ізолювати мобільний пристрій від мережі після його вилучення?
7. Які правові аспекти необхідно враховувати під час дослідження мобільних пристроїв?
8. Які основні методи криміналістичного дослідження мобільних пристроїв існують?
9. Що таке ручне вилучення даних (Manual Extraction)?
10. Які переваги та недоліки ручного вилучення?
11. Що таке логічне вилучення даних (Logical Acquisition)?
12. Які переваги та недоліки логічного вилучення?
13. Що таке фізичне вилучення даних (Physical Acquisition)?

14. Які переваги фізичного вилучення порівняно з логічним?
15. Що таке метод Chip-Off?
16. Що таке метод ISP (In-System Programming)?
17. Які ризики пов'язані з використанням методів Chip-Off та ISP?
18. Які цифрові докази можуть міститися на мобільному пристрої?
19. Які види автентифікації використовуються в iPhone?
20. Що таке Jailbreak?
21. Які способи резервного копіювання даних використовуються в iOS?
22. Які дані необхідні для отримання резервної копії з iCloud?
23. Які основні механізми захисту використовує Android?
24. Що таке Android Debug Bridge (ADB)?
25. Які криміналістичні інструменти використовуються для дослідження мобільних пристроїв?
26. Що таке захоплення трансльованого зображення екрана смартфона?
27. Які способи захоплення зображення екрана існують?

Лабораторна робота 13
АНАЛІЗ ІНТЕРНЕТ-АКТИВНОСТІ

Мета заняття: ознайомитися з основними принципами цифрової криміналістики під час дослідження інтернет-активності користувачів та джерелами цифрових доказів, що формуються під час роботи в мережі Інтернет; дослідити особливості аналізу історії браузерів, кешу, файлів cookie, журналів завантажень, закладок і пошукових запитів; ознайомитися з методами аналізу мережевої активності за журналами DNS-, DHCP-, VPN-серверів, вебсерверів, файєрволів, мережевого обладнання та мережевого трафіку; ознайомитися з використанням спеціалізованих інструментів для аналізу мережевої активності, зокрема Wireshark, Nmap, Whois та штатних засобів операційної системи; ознайомитися з особливостями аналізу електронної пошти, соціальних мереж, хмарних сервісів, мережі Tor, VPN, проксі-серверів і криптовалют як джерел цифрових доказів; ознайомитися з сучасними методами деанонімізації користувачів, використанням Honeypot та Canarytokens для виявлення шкідливої активності.

Теоретичні відомості

Аналіз інтернет-активності є одним із найважливіших напрямів цифрової криміналістики. Він дозволяє відновити дії користувача в мережі Інтернет, встановити використані вебресурси, час доступу до них, маршрути передавання даних, використані мережеві сервіси та взаємодію між різними інформаційними системами. Джерелами цифрових доказів можуть бути:

- історія браузерів;
- журнали вебсерверів;
- журнали DNS-серверів;
- журнали DHCP;
- журнали VPN;
- журнали файєрволів;
- IDS/IPS;
- мережевий трафік;
- електронна пошта;
- соціальні мережі;
- хмарні сервіси;
- криптовалютні сервіси.

Комплексний аналіз цих джерел дозволяє реконструювати інтернет-активність користувача та встановити обставини кіберінциденту.

Браузери автоматично зберігають значний обсяг інформації про діяльність користувача. Під час криміналістичного аналізу можуть бути досліджені:

– історія перегляду вебсторінок;
– пошукові запити;
– історія завантажень;
– файли cookie;
– кеш браузера;
– закладки;
– збережені паролі;
– дані автозаповнення форм.

За допомогою цих даних можна встановити:

– які вебресурси відвідував користувач;
– коли здійснювався доступ;
– які файли були завантажені;
– які пошукові запити виконувалися;
– використані вебпоштові сервіси;
– використання соціальних мереж.

Основні артефакти браузера Google Chrome розташовані в каталозі профілю користувача.

Історія браузера (SQLite):

C:\Users\<UserName>\AppData\Local\Google\Chrome\User Data\<Profile>\History

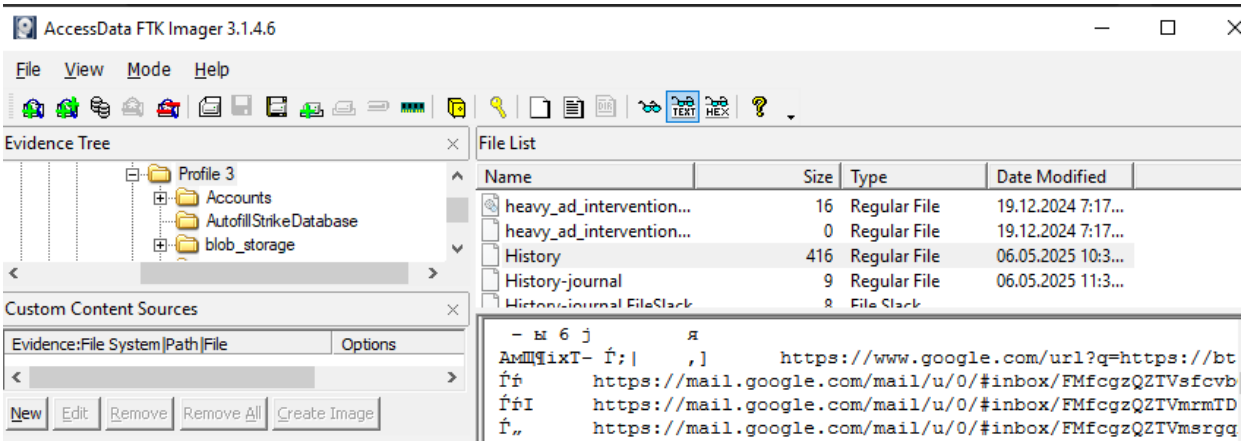


Рис. 97. Історія браузера

Кеш браузера:

C:\Users\<UserName>\AppData\Local\Google\Chrome\User Data\<Profile>\Cache\Cache_Data\

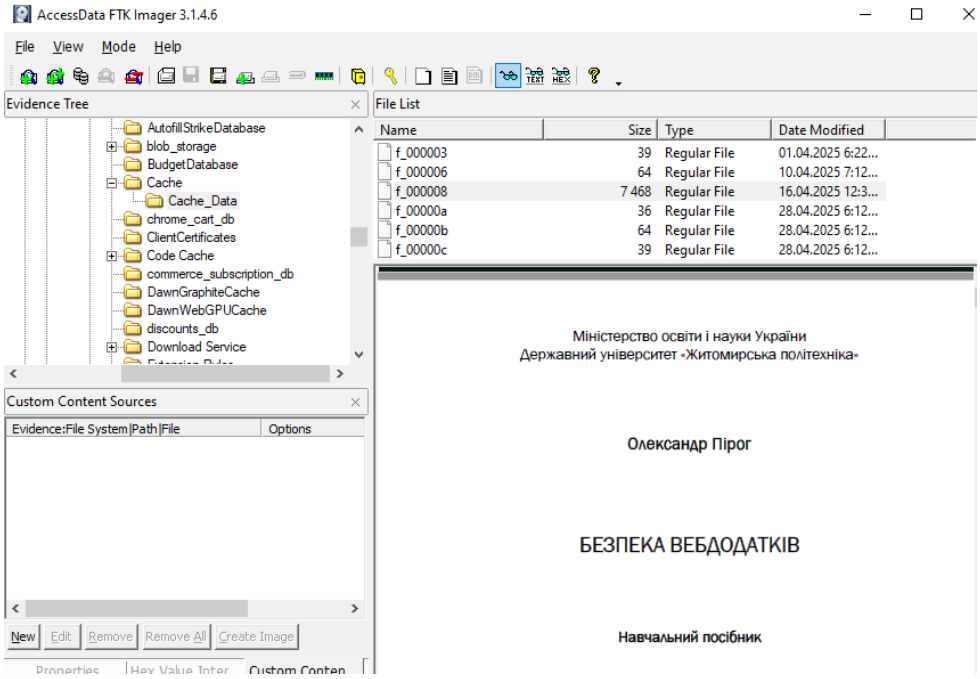


Рис. 98. Кеш браузера

Cookies:

C:\Users\<UserName>\AppData\Local\Google\Chrome\User Data\<Profile>\Network\Cookies

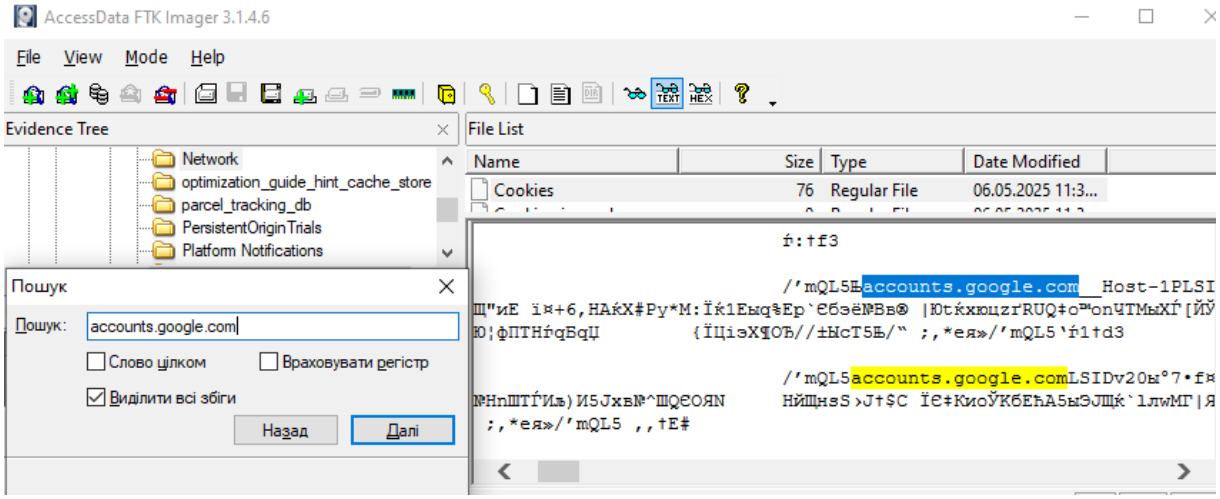


Рис. 99. Cookies

Закладки:

C:\Users\<UserName>\AppData\Local\Google\Chrome\User Data\<Profile>\Bookmarks

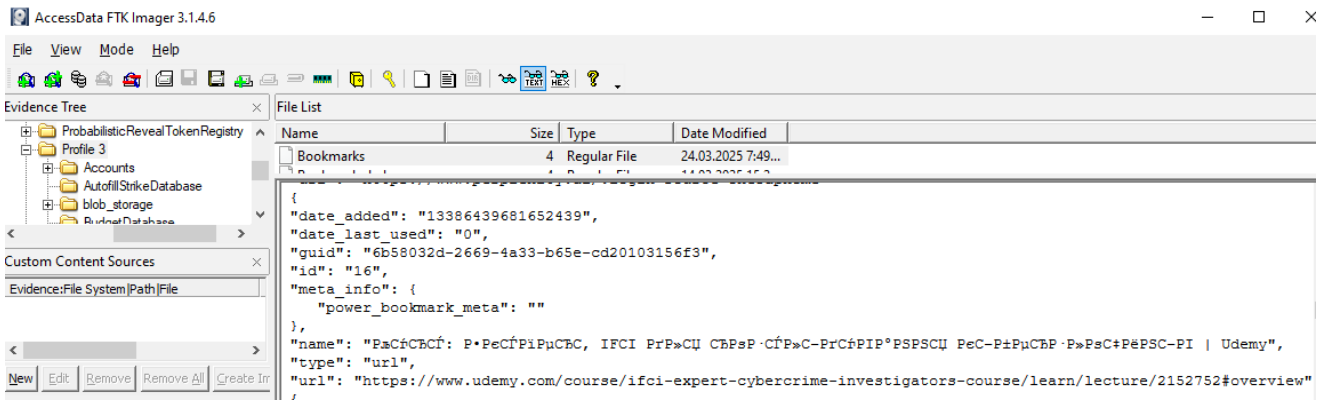


Рис. 100. Закладки

Завантажені файли:

C:\Users\<UserName>\Downloads\

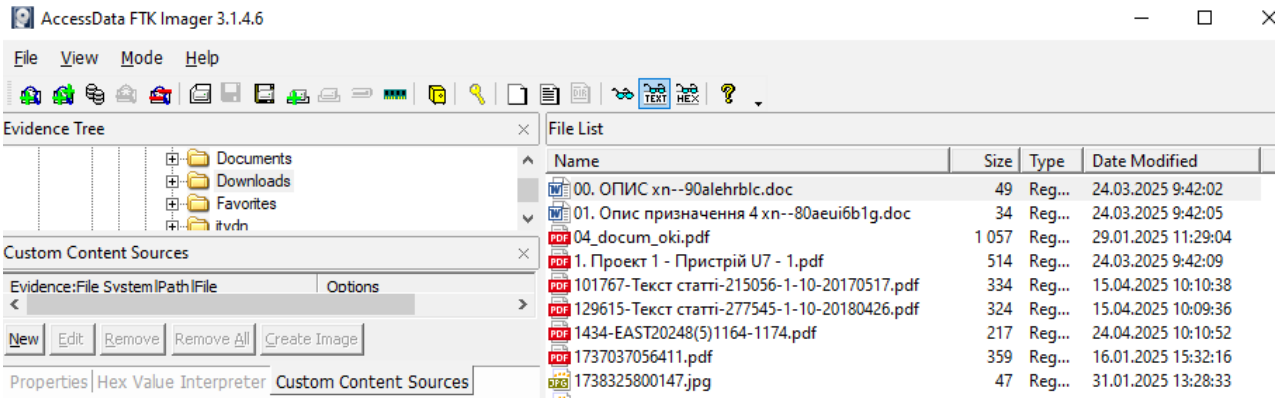


Рис. 101. Завантажені файли

Джерелами інформації про мережеву активність можуть бути:

- DNS-сервер;
- маршрутизатор;
- файєрвол;
- IDS/IPS;
- вебсервер;
- DHCP-сервер;
- VPN-сервер;
- NetFlow.

Поєднання цих журналів дозволяє встановити маршрут проходження мережевого трафіку та взаємодію між пристроями.

Типовий запис вебсервера містить:

- дату та час;
- IP-адресу клієнта;
- HTTP-метод;
- URL;
- код відповіді;
- User-Agent;
- Referrer.

Приклад:

2020-09-09 17:38:25 192.168.1.10 GET /welcome.png - 80 - ::1 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:69.0)+Gecko/20100101+ Firefox/69.0 http://localhost/ 200 0 0 11

Файєрволи фіксують проходження мережевого трафіку. Типовий запис містить:

- джерело (SRC);
- призначення (DST);
- номер порту;
- протокол;
- час;
- напрямок передавання.

Приклад:

Jan 7 14:13:22 quichelorraine kernel: [12167.418837] IN=ens33 OUT= MAC=00:0c:29:bd:3d:3e:f4:5c:89:b7:2c:89:08:00 SRC=192.168.86.21 DST=192.168.86.34 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=44256 DF PROTO=TCP SPT=53542 DPT=80 WINDOW=4096 RES=0x00 ACK URGP=0

DHCP-сервер фіксує:

- видачу IP-адрес;
- MAC-адреси;
- імена комп'ютерів;
- час видачі адрес.

Приклад:

(C:\Windows\System32\dhcp\dhcpserver.log):
10/09/2024 15:32:45 Assign 192.168.1.10 00:1A:2B:3C:4D:5E HostName-PC

DNS (Domain Name System) перетворює доменні імена в IP-адреси. Журнали DNS дозволяють встановити:

- які доменні імена використовувалися;
- час звернення;
- клієнта, який виконав запит.
- DNS-кеш клієнта

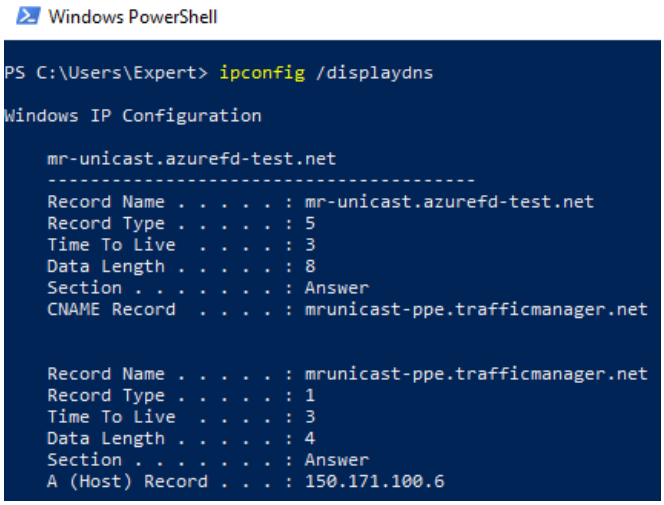


Рис. 102. Журнал DNS

Windows зберігає локальний DNS-кеш. Його аналіз дозволяє встановити нещодавно відвідані ресурси навіть за відсутності історії браузера.

ARP Cache – це таблиця відповідності між IP-адресами та MAC-адресами. Вона використовується для встановлення:

- взаємодії пристроїв у локальній мережі;
- фізичних адрес мережевих адаптерів;
- наявності інших вузлів мережі.

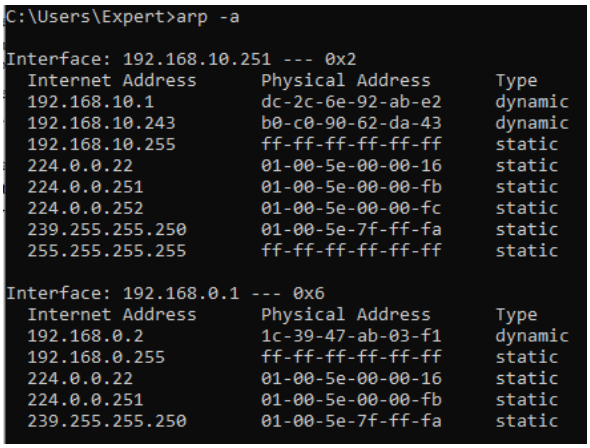


Рис. 103. ARP Cache

Команда netstat відображає:

- активні TCP-з'єднання;
- UDP-з'єднання;
- порти, що прослуховуються;
- стан мережевих з'єднань.

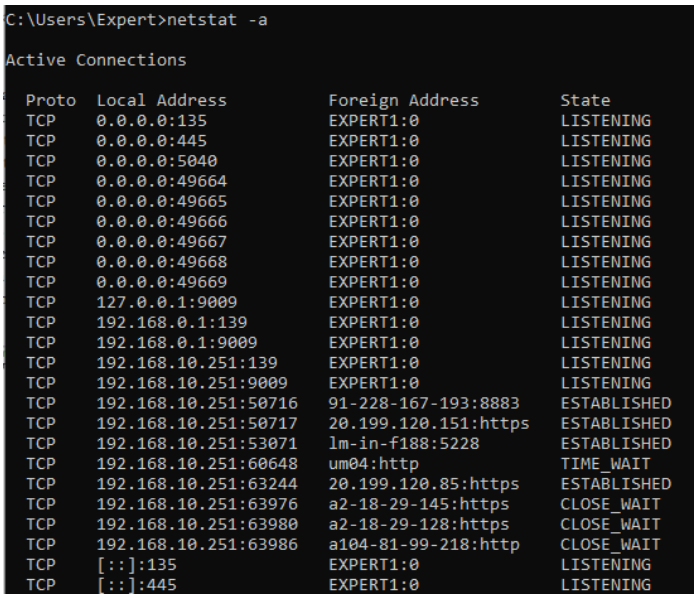


Рис. 104. Команда netstat

Диспетчер завдань Windows дозволяє отримати інформацію про:

- активні процеси;
- використання мережі;
- навантаження процесора;
- використання пам'яті.

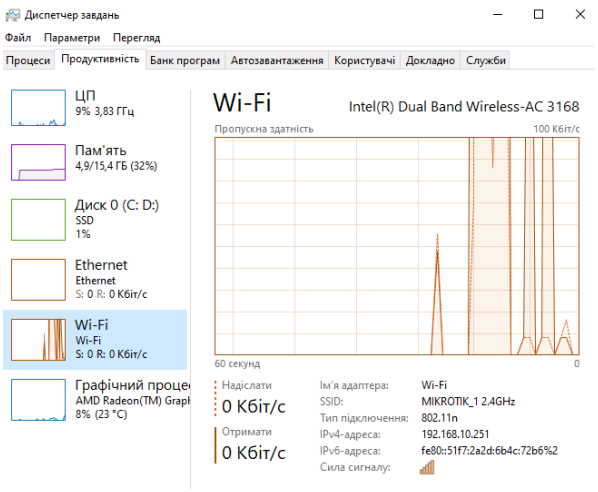


Рис. 105. Диспетчер завдань Windows

Whois – це сервіс отримання інформації про власника доменного імені або IP-адреси. За допомогою Whois можна встановити:

- реєстратора;
- дату реєстрації;
- контактні дані (якщо доступні);
- автономну систему (AS);
- країну реєстрації.

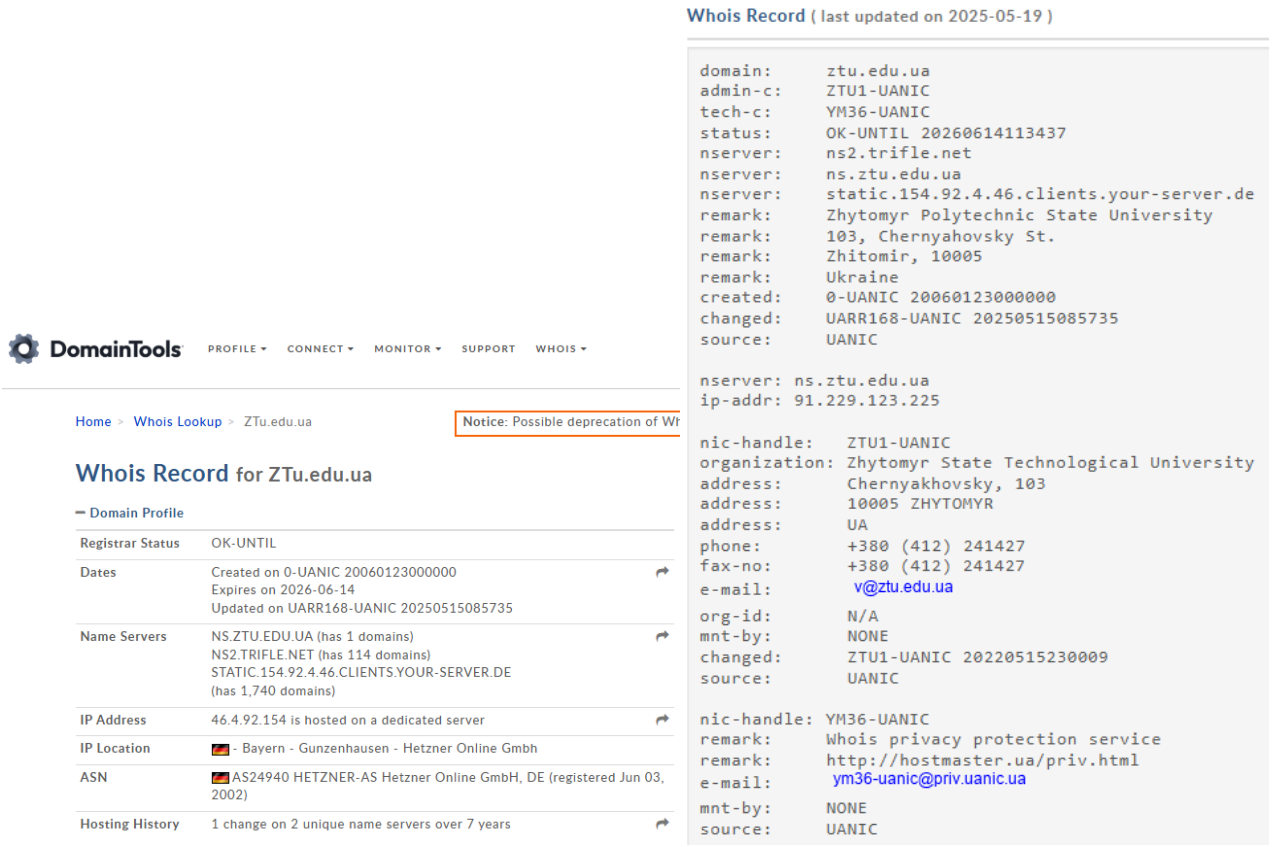


Рис. 106. Whois

Під час огляду місця події необхідно встановити всі активні мережеві пристрої. Для цього використовується сканування мережі. Сканування дозволяє:

- виявити активні вузли;
- визначити відкриті порти;
- встановити сервіси;
- визначити виробника обладнання;
- визначити версії програмного забезпечення.

Nmap (Network Mapper) – один із найпоширеніших мережевих сканерів.

Приклад:

nmap -p 80,554,8000 --open -sV 192.168.1.0/24

де:
-p – перелік портів;
--open – показувати лише відкриті порти;
-sV – визначення версій сервісів;
192.168.1.0/24 – мережа для сканування.

Wireshark – інструментів аналізу мережевого трафіку. Приклади фільтрів:

- http
- rtsp
- ip.addr==192.168.1.10

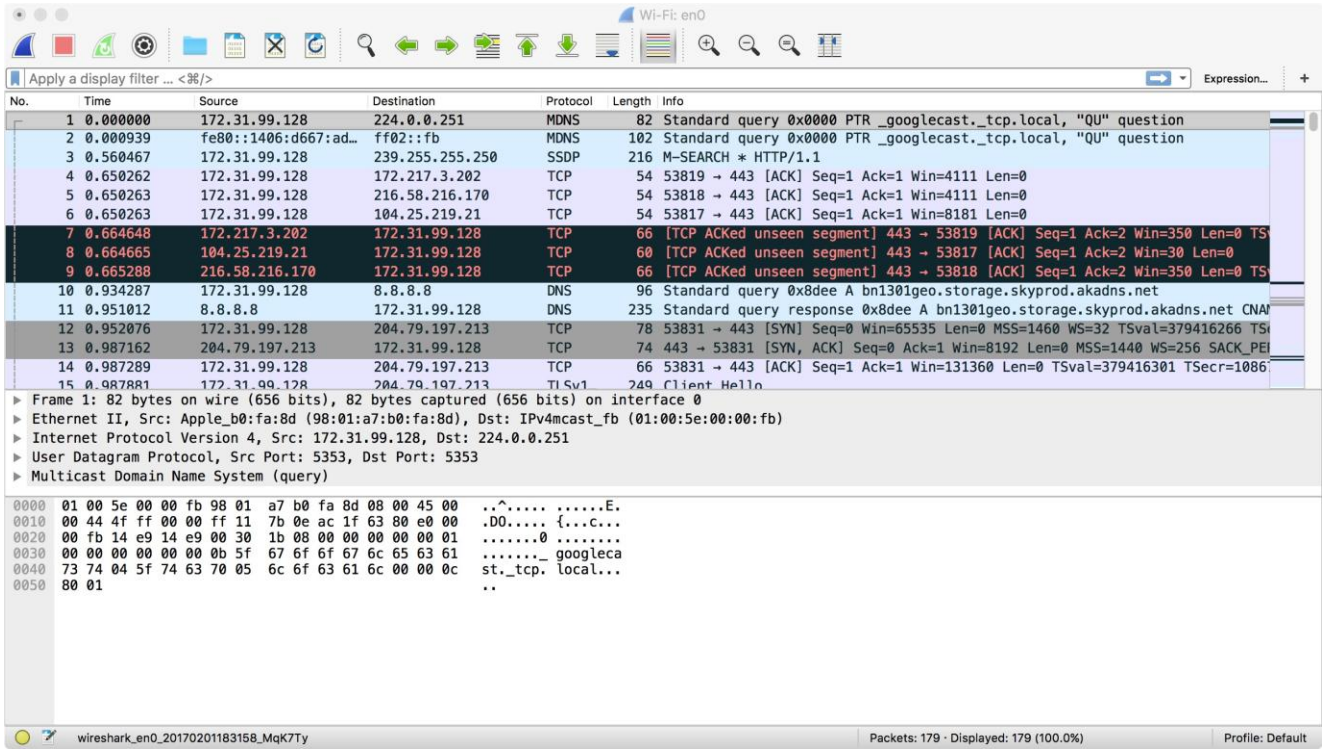


Рис. 107. Wireshark

Honeypot – спеціально налаштована інформаційна система, яка імітує вразливий ресурс. Основні цілі:

- виявлення атак;
- збір цифрових доказів;
- аналіз поведінки зловмисників;
- отримання TTP (Tactics, Techniques and Procedures).

Canarytokens – спеціальні сигнальні об'єкти. Ними можуть бути:

- документи;
- URL;
- DNS-записи;
- електронні листи.

При відкритті або використанні такого об'єкта власник отримує повідомлення про інцидент.

Електронний лист складається з:

- заголовків (Headers);
- тіла повідомлення;
- вкладень.

Заголовки дозволяють встановити:

- маршрут проходження повідомлення;
- IP-адреси серверів;
- час проходження;
- відправника;
- одержувача;
- Message-ID.

Приклад:

```
Return-Path: <attacker@example.com>          // Зворотна адреса відправника
Received: from mail.example.com (mail.example.com. [203.0.113.10])
                                             // Детальний маршрут проходження листа
    by mx.google.com with ESMTPS id u2si5197228qke.208.2024.06.01.10.13.22 // IP-адреси, сервери, дати.
    for <victim@gmail.com>
    (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
    Sat, 01 Jun 2024 10:13:22 -0700 (PDT)
Message-ID: <0e2d1cd2b9f2@example.com>
Date: Sat, 1 Jun 2024 19:13:12 +0200
From: John Smith <attacker@example.com>    // Від кого та кому (може бути підробленим).
To: Victim User <victim@gmail.com>
Subject: Important Update
MIME-Version: 1.0
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable
```

Під час аналізу хмарної активності виникають такі проблеми:

- відсутність фізичного доступу;
- розподілене зберігання даних;
- обмежений строк зберігання журналів;
- різні юрисдикції;

- модель спільної відповідальності.

Для приховування мережевої активності можуть використовуватися:

1. Tor
   - багаторівневе шифрування;
   - приховування IP-адреси;
   - доступ до Dark Web.
2. VPN
   - шифрування всього мережевого трафіку;
   - приховування реальної IP-адреси;
   - зміна географічного розташування.
3. Проксі-сервер
   - працює як посередник;
   - може змінювати IP-адресу;
   - не завжди забезпечує шифрування.

Для встановлення особи користувача (деанонімізації) можуть застосовуватися:

- аналіз метаданих;
- аналіз часової активності;
- аналіз стилю повідомлень;
- Browser Fingerprinting;
- аналіз DNS Leak;
- аналіз WebRTC Leak;
- аналіз акаунтів соціальних мереж.

Dark Web – частина мережі Інтернет, доступ до якої здійснюється через спеціалізовані анонімні мережі (наприклад, Tor). Під час розслідування можуть використовуватися:

- цифрові відбитки (Digital Fingerprinting);
- Honeypots;
- аналіз журналів Tor;
- соціальна інженерія;
- міжнародна співпраця правоохоронних органів.

Завдання на лабораторну роботу

Відкрийте програму FTK imager.

Додайте побітову копію підозрілого цифрового носія (Vader_Home_Computer.001) до програми FTK imager.

File > Add Evidence Item > Image File та Далі > Browse та вибрати файл копії підозрілого цифрового носія, вибрати Vader_Home_Computer.001 та відкрити > Finish.

Натисніть кнопки + для навігації по образу.

Перейдіть до кореневого каталогу Розділу 2 (root Partition 2).

Перейдіть до папки \Users\Owner\Downloads\.

За потреби експортуйте деякі файли на ваш комп’ютер для перегляду.

Які файли можуть свідчити про злочинну діяльність?

_____

Що це за злочинна діяльність?

_____

Перейдіть до файлу \Users\Owner\AppData\Local\Google\Chrome\User Data\Default\Bookmarks.

Проаналізуйте файл закладок.

Який URL закладки?

_____

Перейдіть в вашому браузері за посиланням виявленої закладки.

Які докази ви знайшли?

_____

Перейдіть до папки \Users\Owner\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\

Подивиться файли кешу за 03.06.2025 13:26:33, 03.06.2025 13:30:17, 03.06.2025 13:31:29, 03.06.2025 13:31:33, 03.06.2025 13:31:34, 03.06.2025 13:31:45, 03.06.2025 13:31:53, 03.06.2025 13:32:11, 03.06.2025 13:32:56, 03.06.2025 13:32:57, 03.06.2025 13:33:05, 03.06.2025 13:33:06, 03.06.2025 13:33:07, 06.06.2025 09:07:22, 06.06.2025 09:08:37, 06.06.2025 09:33:14.

Які докази ви знайшли?

_____

Перейдіть до файлу \Users\Owner\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies.

На якому сервісі був аккаунт у підозрюваного?

_____

Змонтуйте підозріле зображення File > Image Mounting > Vader_Home_Computer.001.

Встановіть / відкрийте BrowsingHistoryView від Nirsoft. (https://www.nirsoft.net/utils/browsing_history_view.html).

BrowsingHistoryView потрібно запускати від імені Адміністратора (в контекстному меню – Запустити з правами адміністратора)!

У полі Advanced Options зверніть увагу на поле Filter by visit date/time та виберіть Load History Items from any time.

Залиште позначеними всі веббраузери.

У розділі Load history from.. виберіть: Load history from the specified profile (Forexample: c:\users\admin).

У наступному полі клацніть поле з трьома крапками, щоб відкрити

навігаційний браузер Windows та перейдіть до змонтованого підозрілого зображення та папки \Users\Owner.

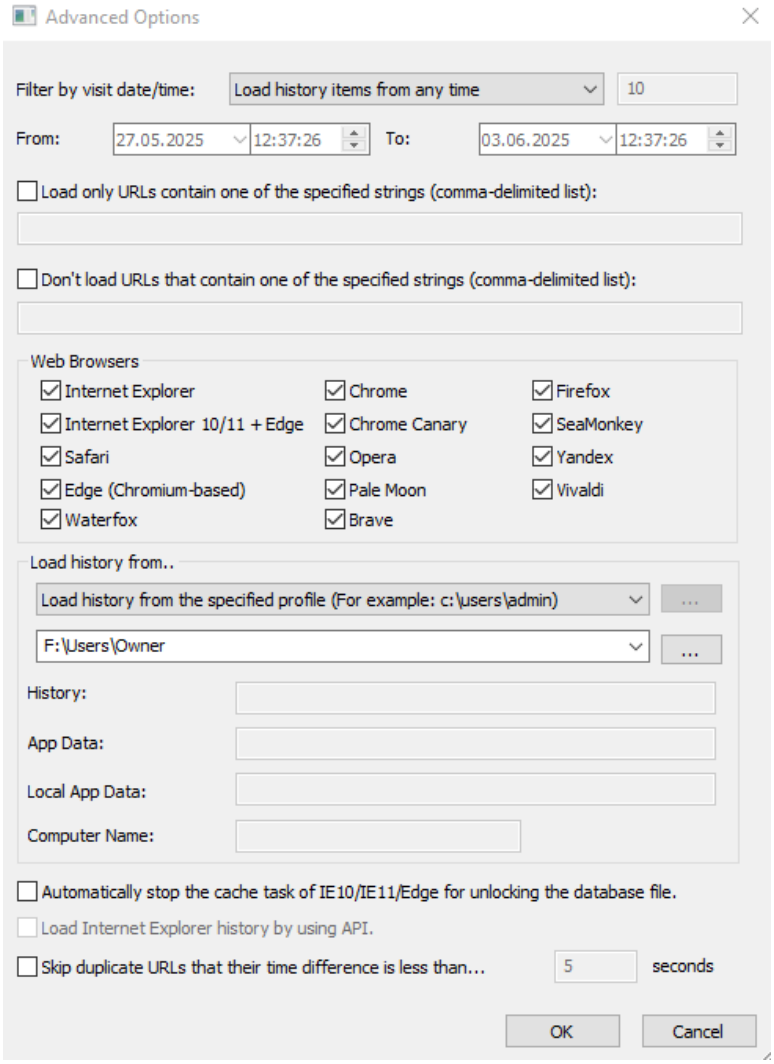


Рис. 108. BrowsingHistoryView

Натисніть OK.

Ви можете сортувати за будь-яким із заголовків. Ви також можете шукати терміни, натиснувши Edit > Find.

Які інтернет-браузери використовувався в цьому профілі?

_____

Знайдіть терміни search, google search, bing. Це дасть вам уявлення про те, які терміни підозрюваний шукав в Інтернеті.

Які пошукові терміни шукав підозрюваний, які можуть бути цікавими для цього розслідування? Яку пошукову систему він використовував? Яка була дата/час?

_____

Пошукайте по слову mail.

Чи мав користувач вебпошту? Яка була його адреса електронної пошти?

_____

Знайдіть термін file:///. Це покаже файли, до яких було отримано доступ у локальній системі, але які були зареєстровані у файлі Index.dat.

**ПРИМІТКА: %20 означає пробіл.

Чи є якісь файли, що стосуються цього розслідування?

_____

Чи знаходилися якісь із вищезгаданих відповідних файлів в іншому місці, ніж диск C:/ комп'ютера? Як вони називалися?

_____

Перед закриттям FTK Imager відмонтуйте всі змонтовані диски.

Відкрийте Autopsy.

Відкрийте справу, що ви завели у попередніх лабораторних – Open Recent Case.

Перейдіть Data Artifacts > Web Downloads.

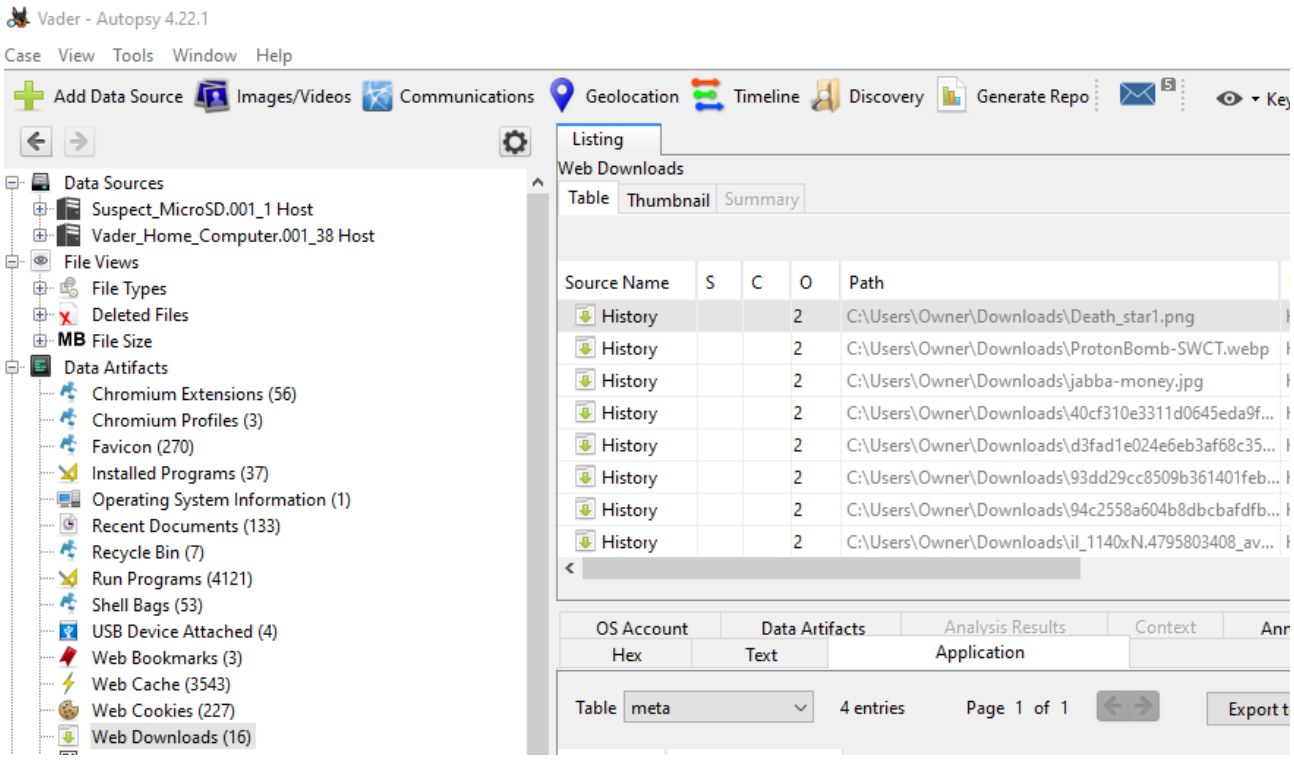


Рис. 109. Web Downloads в Autopsy

Через контекстне меню виберіть для знайдених файлів View Downloaded File in Directory, щоб подивитися їх. Повернення назад за допомогою стрілки у лівому верхньому куті.

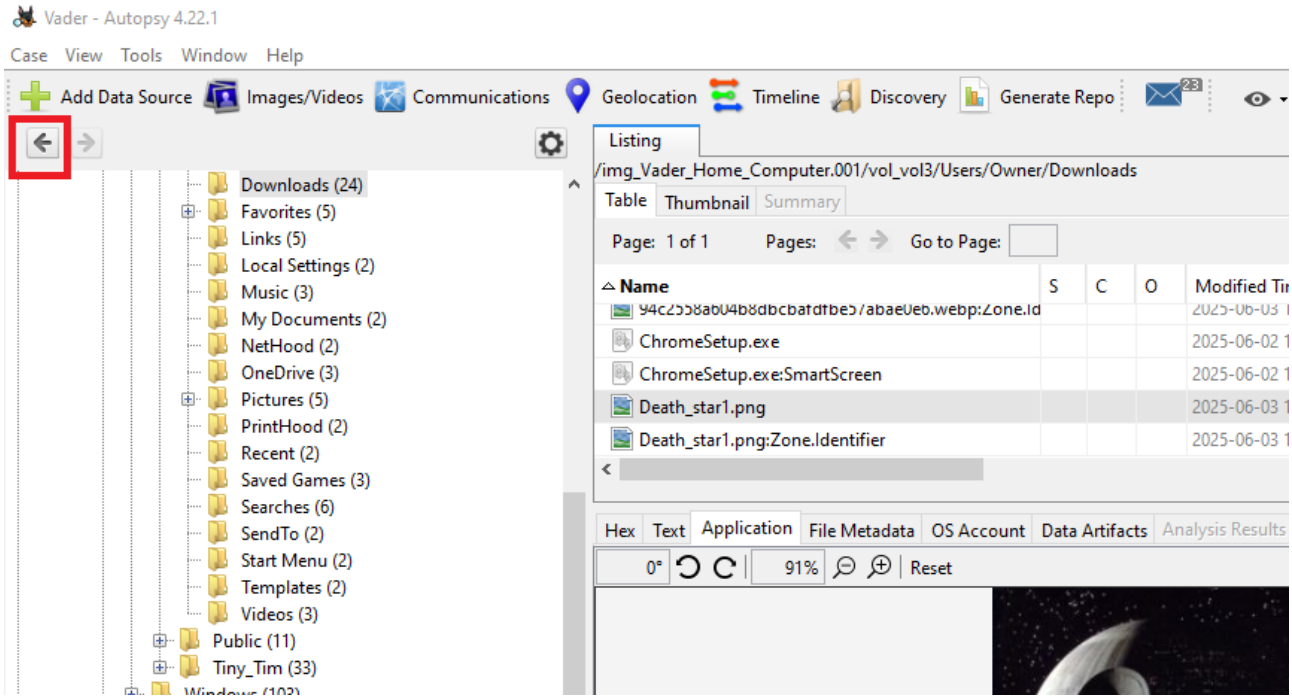


Рис. 110. Перегляд файлів з Web Downloads в Autopsy

Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки?

_____

Перейдіть Data Artifacts > Web Bookmarks.

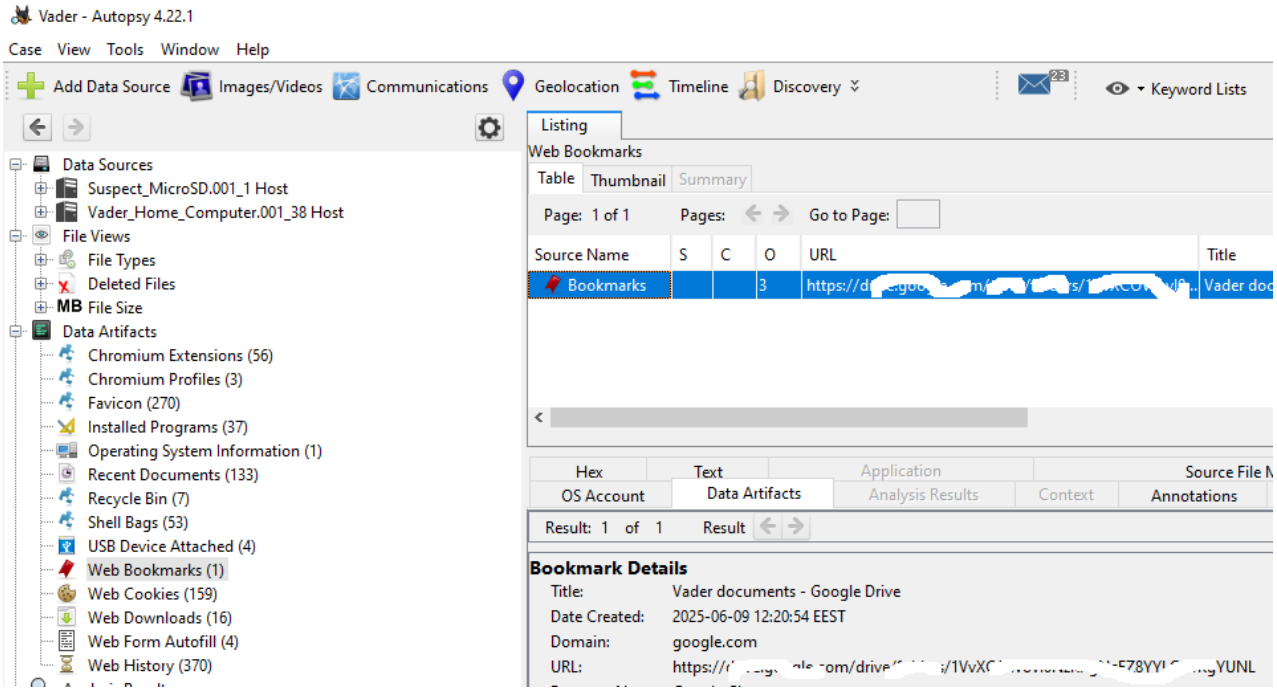


Рис. 111. Web Bookmarks в Autopsy

Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки?

Перейдіть Data Artifacts > Chromium Profiles.

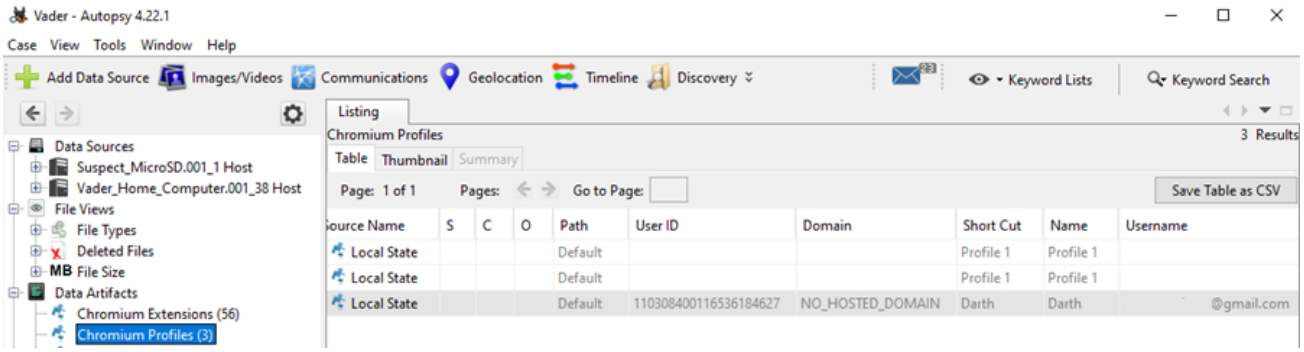


Рис. 112. Chromium Profiles в Autopsy

Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки щодо адреси електронної пошти?

Перейдіть Data Artifacts > Web History.

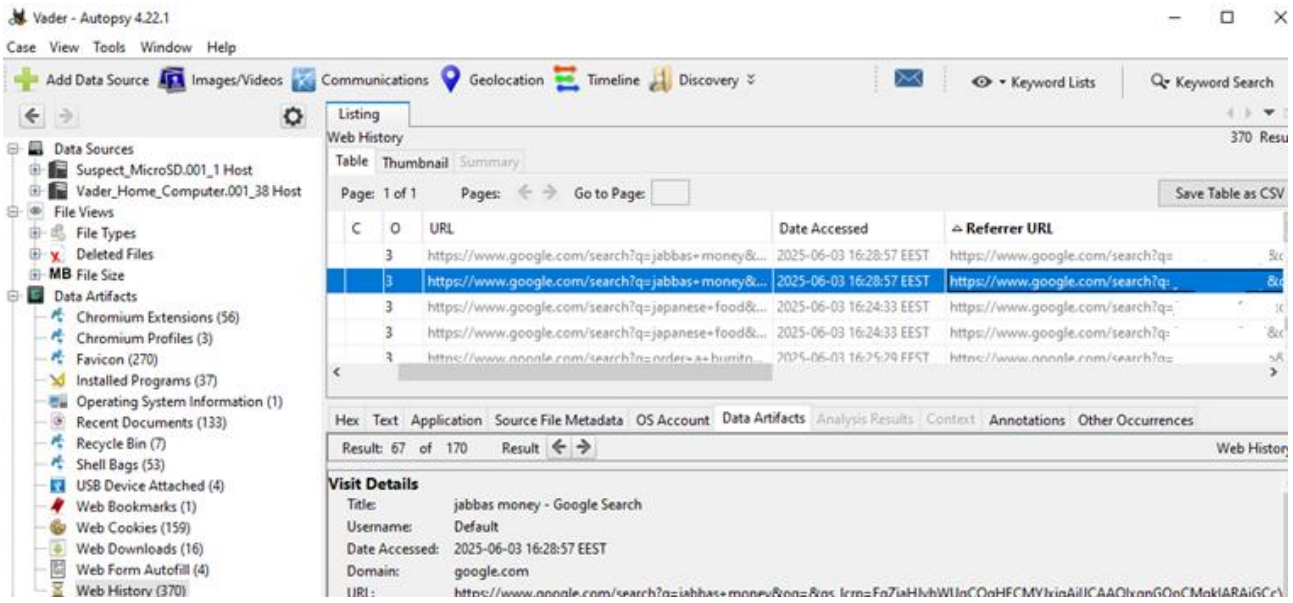


Рис. 113. Web History в Autopsy

Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки?

Перейдіть Data Artifacts > Web Search.

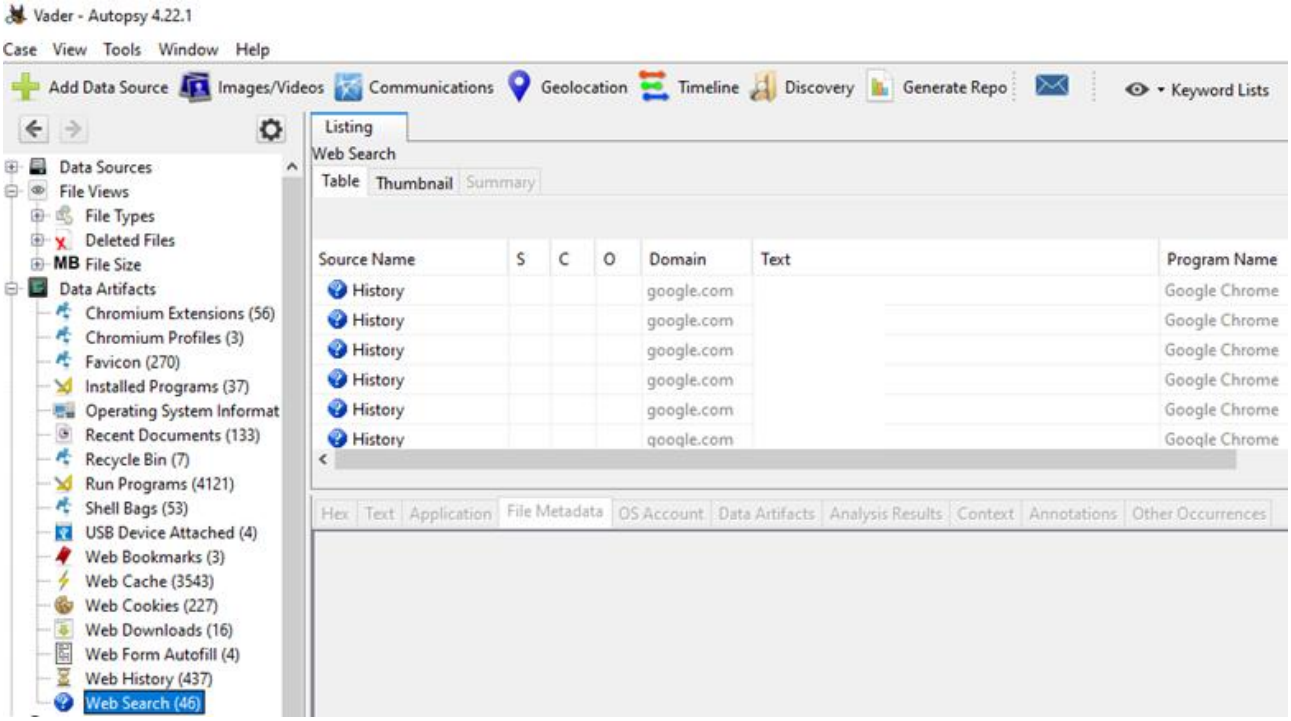


Рис. 114. Web Search в Autopsy

Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки?

_____

Контрольні питання

1. Що таке аналіз інтернет-активності?
2. Які основні джерела цифрових доказів під час аналізу інтернет-активності?
3. Які дані можуть бути отримані з історії браузера?
4. Яку інформацію містить історія відвідування вебсторінок?
5. Яку інформацію може містити кеш браузера?
6. Яку інформацію можна отримати з історії завантажень браузера?
7. Яку інформацію містять журнали вебсерверів?
8. Яку інформацію можна отримати з журналів файєрвола?
9. Яку інформацію містять журнали DNS-сервера?
10. Що таке ARP-кеш?
11. Яку інформацію містить ARP-кеш?
12. Для чого використовується команда netstat -a?
13. Яку інформацію можна отримати за допомогою Диспетчера завдань Windows?
14. Що таке Whois?
15. Яку інформацію можна отримати за допомогою сервісу Whois?

16. Для чого використовується сканування портів?
17. Які можливості має програма Nmap?
18. Для чого використовується програма Wireshark?
19. Що таке Honeypot?
20. Що таке Canarytokens?
21. З яких основних частин складається електронний лист?
22. Яку інформацію містять заголовки (Headers) електронного листа?
23. Які проблеми виникають під час дослідження хмарних сервісів?
24. Що таке мережа Tor?
25. Чим VPN відрізняється від проксі-сервера?
26. Які переваги та недоліки використання Tor?
27. Які переваги та недоліки використання VPN?
28. Що таке Browser Fingerprinting?
29. Які основні методи деанонімізації користувачів існують?
30. Що таке Dark Web?

Список рекомендованої літератури

1. Bowne S. CNIT 121: Computer Forensics. San Francisco: City College of San Francisco. URL: https://samsclass.info/121/121_F23.shtml
2. Easttom C., Butler W., Phelan J., Bhagavatula R.S., Steuber S., Rodriguez K., Balkissoon V.I., Naseer Z. Windows Forensics: Understand Analysis Techniques for Your Windows, 2024. 484p. https://learning.oreilly.com/library/view/windows-forensics-understand/9798868801938/
3. Gehlot A., Singh R., Singh J., Sharma N.R. Digital Forensics and Internet of Things, 2022. 288p. https://learning.oreilly.com/library/view/digital-forensics-and/9781119768784/
4. Muhiballah M. Windows Forensics Analyst Field Guide, 2023. 318p. https://learning.oreilly.com/library/view/windows-forensics-analyst/9781803248479/
5. Oettinger W. Learn Mobile Forensics, 2024. 295p. https://learning.oreilly.com/library/view/learn-mobile-forensics/9781835889602/
6. Parasram Shiva V. N. Digital Forensics with Kali Linux - Third Edition, 2023. 414p. https://learning.oreilly.com/library/view/digital-forensics-with/9781837635153/
7. Ramakrishnan G., Haqanee M. Cloud Forensics Demystified, 2024. 384p. https://learning.oreilly.com/library/view/cloud-forensics-demystified/9781800564411/
8. TryHackMe. URL: https://tryhackme.com/
9. Головня О.С. Основи операційних систем: навч. посіб. Житомир: «Житомирська політехніка», 2023. 126 с. URL: https://eztuir.ztu.edu.ua/handle/123456789/8321
10. Зоріло В. В. Конспект лекцій з дисципліни «Цифрова криміналістика» для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 125 Кібербезпека. Нац. ун-т "Одеська політехніка". Одеса, 2024. 253 с. URL: https://op.edu.ua/mlib/m/16681
11. Карчевський М. Кримінальне право в умовах цифрової трансформації. Від несанкціонованого доступу до «jailbreak» штучного інтелекту : монографія / Микола Карчевський ; Ун-т Короля Данила ; Ін-т інформації, безпеки і права Нац. акад. прав. наук України. Харків : Право, 2025. 176 с.
12. Кіберзлочинність та електронні докази: навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Електрон. вид. Львів : ЛНУ ім. Івана Франка, 2022. 298 с.
13. Климчук М. П., Комісарчук Ю. А., Марко С. І., Стецик Б. В. Судова комп’ютерно-технічна експертиза у кримінальному провадженні: навч. посіб. Львів : Львівський державний університет внутрішніх справ, 2022. 112 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/4399

14. Практичні аспекти реагування на ІТ інциденти та розслідування цифрових загроз : навч. посіб. / О. В. Коваленко та ін. Кропивницький : ЦНТУ, 2026. 320 с. URL: https://dspace.kntu.kr.ua/items/8eeb5b11-1c08-43f9-a129-cacfb179b7cc
15. Степанюк Р.Л., Гусєва В.О., Кікінчук В.В. та ін. Криміналістика: криміналістична техніка: навч. посіб. Харків: ХНУВС, 2023. 388 с. URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi75/0055786.pdf
16. Чепинога А.В., Єфіменко А.А., Рудаков К.С., Лавданський А.О., Ланських Є.В., Фауре Е.В. Комп'ютерні мережі: навч. посіб. Житомир: Державний університет «Житомирська політехніка», 2025. 386 с. URL: https://eztuir.ztu.edu.ua/handle/123456789/8801
17. Щур Н.О., Покотило О.А. Основи криптології: навч. посіб. Житомир: «Житомирська політехніка», 2021. 120 с. URL: https://eztuir.ztu.edu.ua/handle/123456789/8092