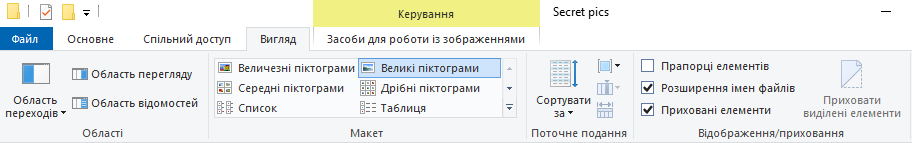
**Лабораторна 1. Хешування**

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



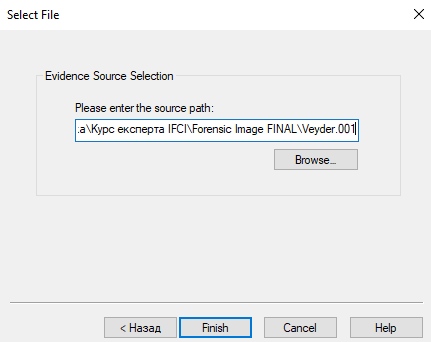
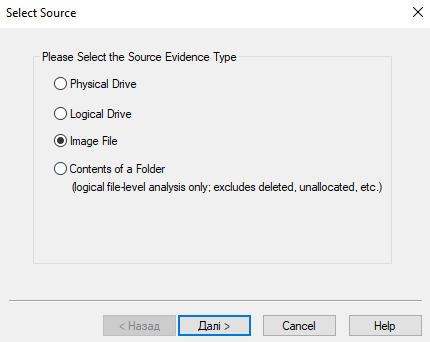
Завантажте з архів образу досліджуваного диска Vader\_Home\_Computer.zip (https://drive.google.com/file/d/1ptqbPdTLPGvQ6WzT22AJtobVGkECqdO9)

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

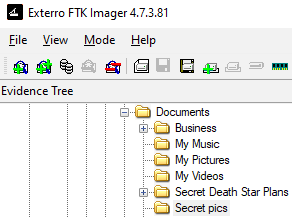
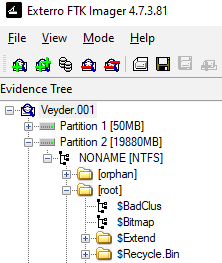
Разархівуйте його. Vader\_Home\_Computer.001, Vader\_Home\_Computer.002 … Vader\_Home\_Computer.005.

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.

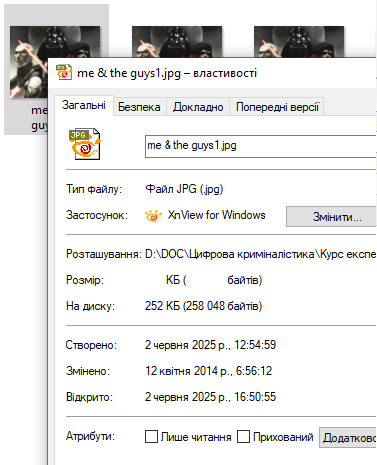


Перейдіть до папки C:\Users\Owner\Documents\Secret pics.



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.



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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

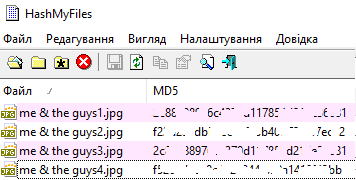
me & the guys3.jpg Опис: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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.



Запишіть хеш-значення MD5 для кожного файлу.

me & the guys1.jpg Хеш MD5: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

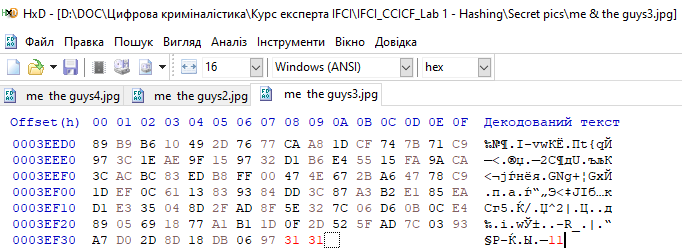
me & the guys2.jpg Хеш MD5: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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.



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?

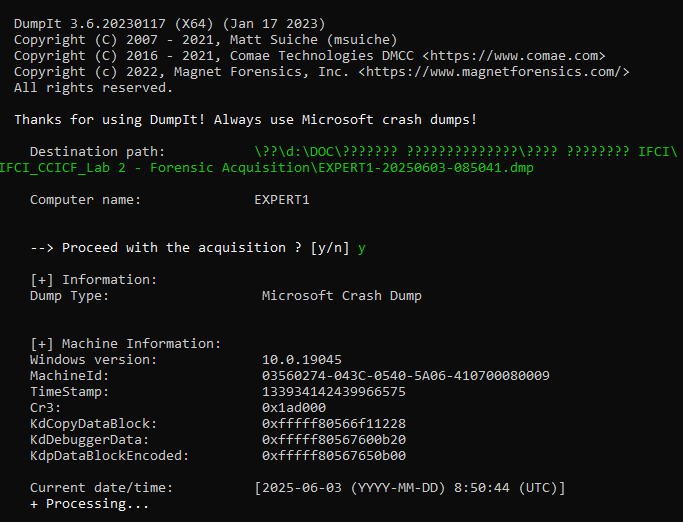
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Лабораторна 2. Дамп ОЗП та образ носія.**

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.



Розмір створеного дампу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

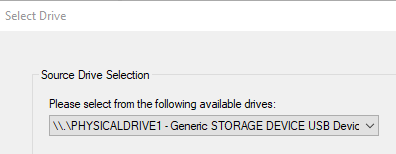
Візьміть невеликий USB-накопичувач або MicroSD картку (бажано менше 8 ГБ, чим більше, тим більше триватиме процес) і вставте його в комп’ютер.

Скопіюйте папку з файлами на ваш вибір на зовнішній накопичувач.

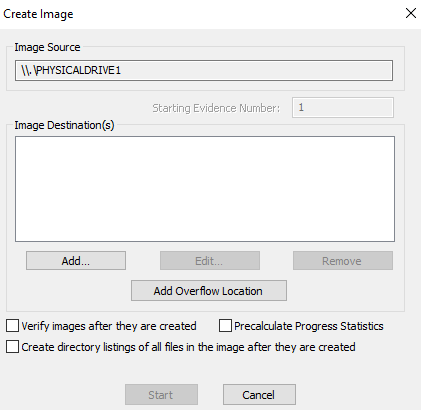
Відкрийте FTK Imager.

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

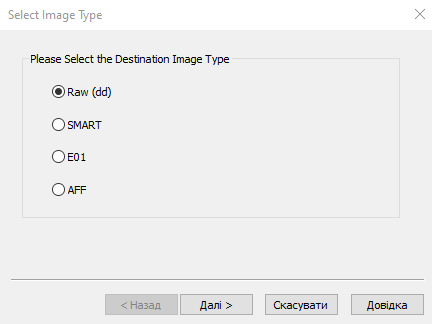
Виберіть фізичний пристрій, який представляє ваш зовнішній накопичувач. (Імовірно \\.\PHYSICALDRIVE1). Натисніть Finish.



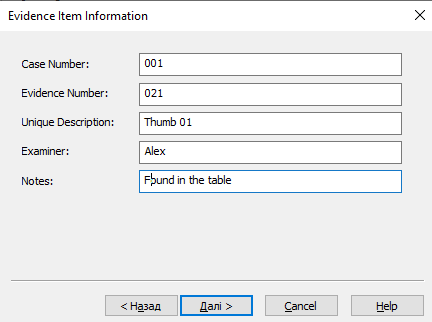
Під полем призначення образу Image Destination(s) натисніть кнопку Add.



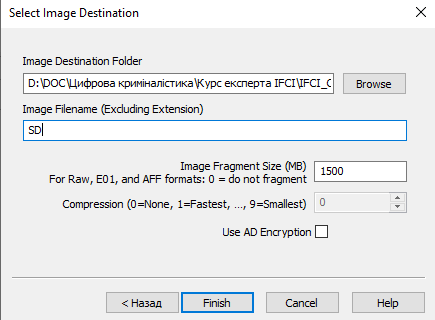
Виберіть Raw (dd) і натисніть Далі.



Додайте інформацію про справу за власним вибором.



Виберіть папку призначення для криміналістичного образу та дайте йому назву файлу.



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 зображення натисніть Image Summary. Запишіть наступну інформацію:

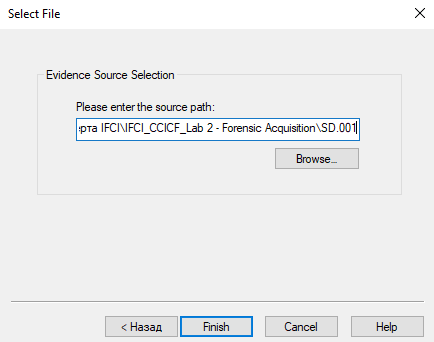
Хеш MD5: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Розмір вихідних даних (Source data size): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

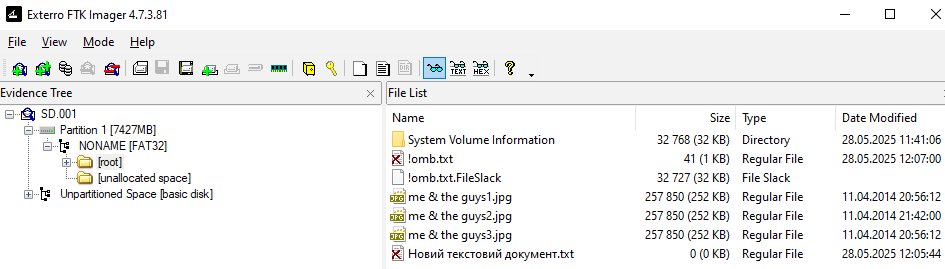
Кількість секторів (Sector count): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

Перейдіть до файлу криміналістичного зображення. Якщо він багатосегментний, виберіть лише перший (.001).



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



**Лабораторна 3. Відновлення файлів**

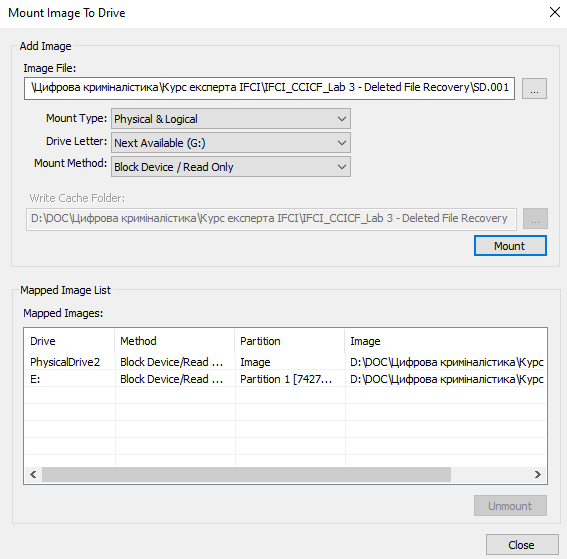
Завантажте архів образу підозрілого зовнішнього накопичувача

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.

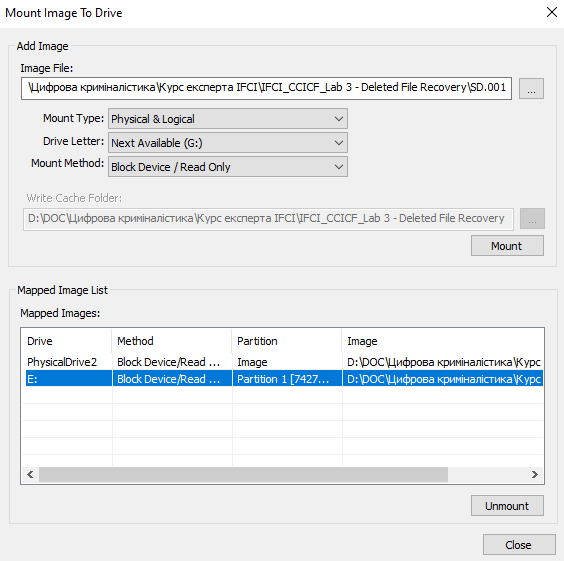


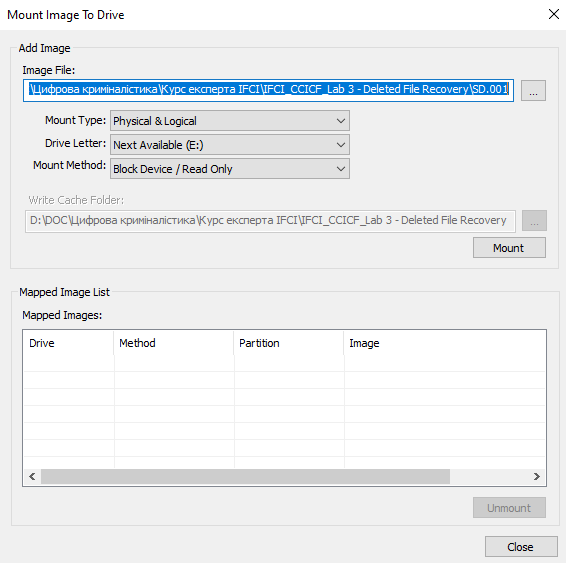
Перейдіть до Провідника Windows і відкрийте диск «E:».

\*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.





Натисніть Close.

Відкрийте шістнадцятковий редактор «HxD».

Виберіть Інструменти > Відкрити образ диска та Suspect\_MicroSD.001.

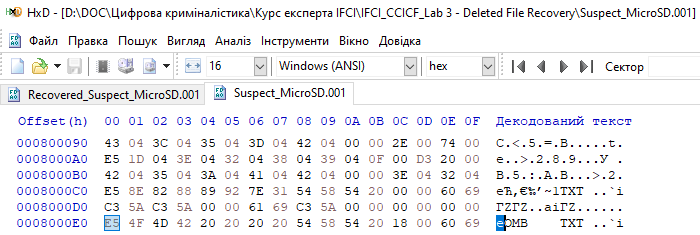
Здійсніть пошук за запитом txt Пошук > Знайти або Ctrl + F

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

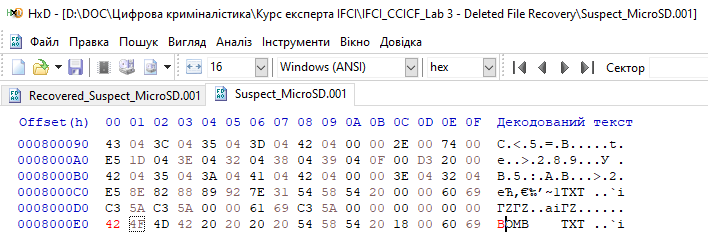
Потім за запитом omb.

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.



Виберіть символ E5 та замініть його на B.



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.

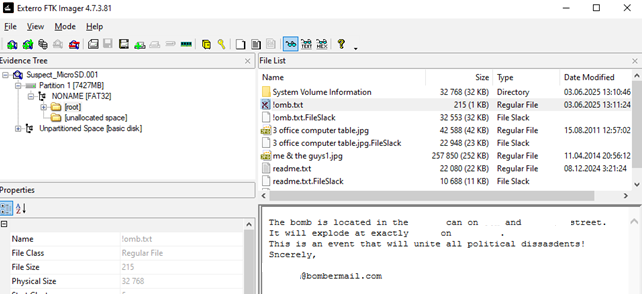
\*ПРИМІТКА: Новий файл «bomb.txt» тепер видно з усіма його метаданими (відкрийте властивості файлу через контекстне меню). Однак фізичне розташування файлу все ще обнулено в таблиці FAT. Тому ми не зможемо фактично відкрити цей файл.

Поверніться до FTK Imager знову відмонтуйте диск та закрийте монтування образу.

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.



Бомба знаходиться:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

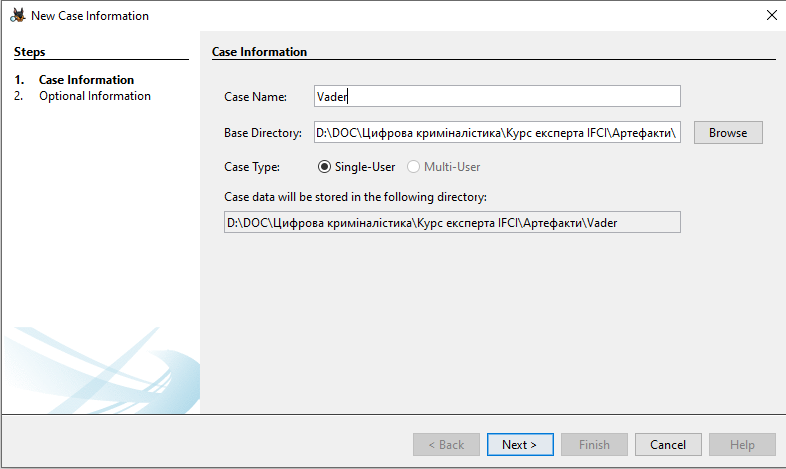
Вибух станеться:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Автор листа:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

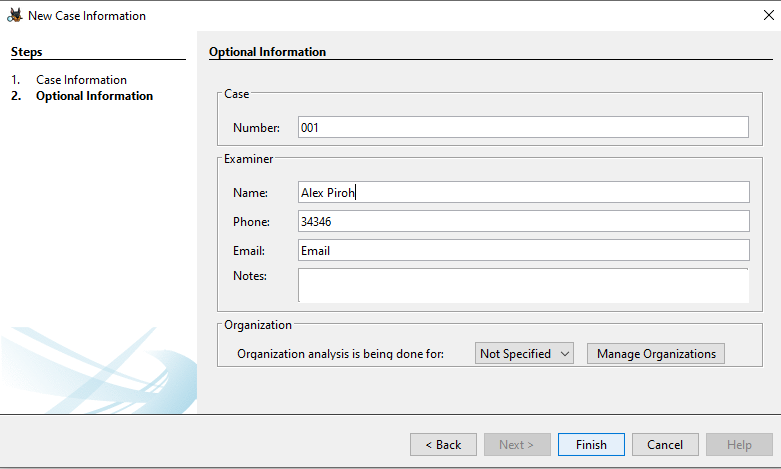
Встановіть та відкрийте Autopsy (https://www.autopsy.com/download/)

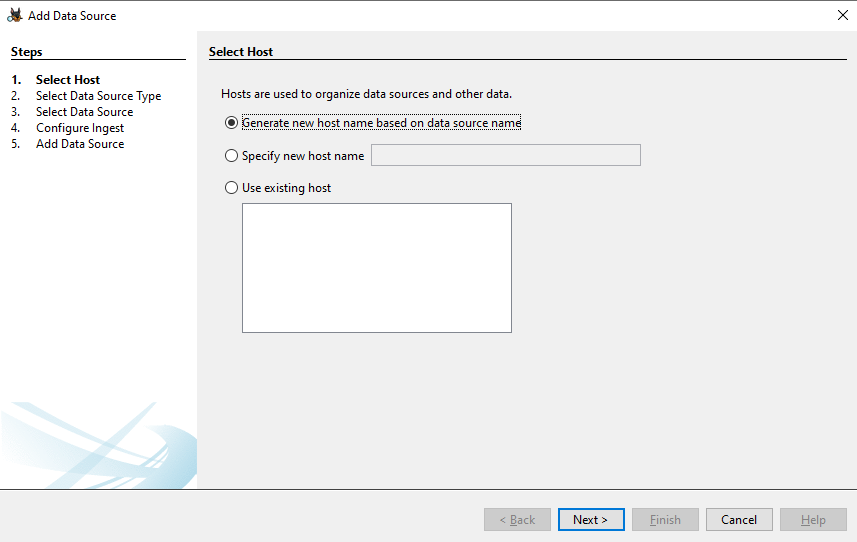


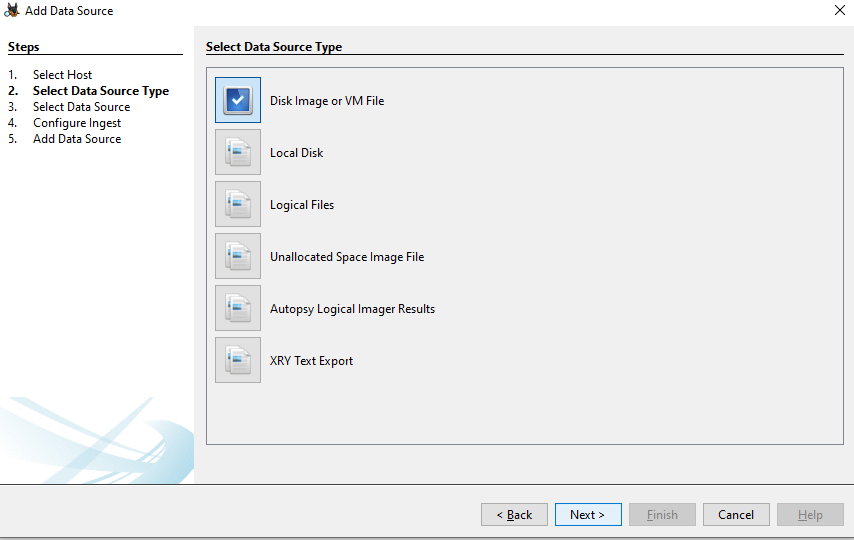
Введіть назву справи (Case Name:) та через Brows вкажіть папку, де будуть зберігатися файли справи. Next



Введіть свою інформацію.

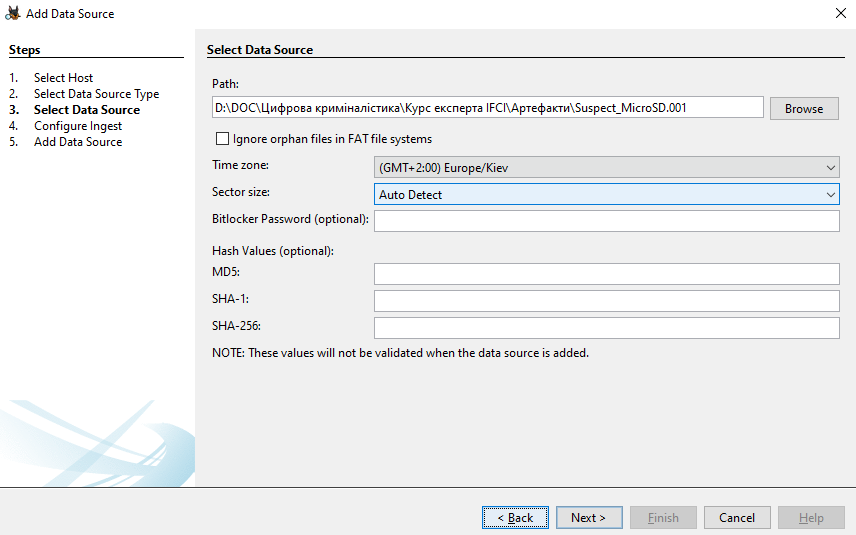






Disk Image or VM File

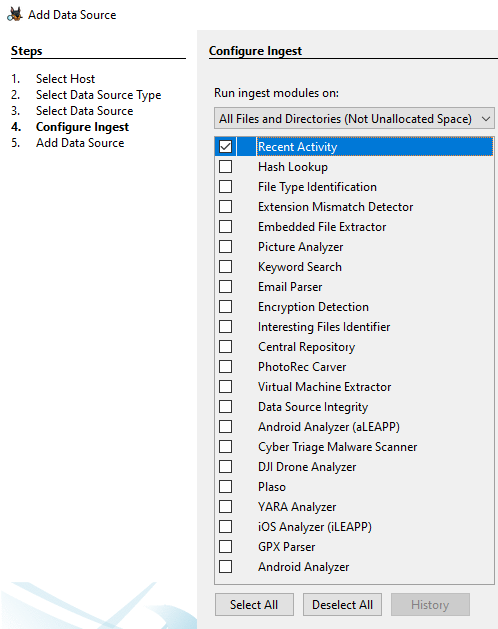
Browse та вкажіть файл образу Suspect\_MicroSD.001.



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

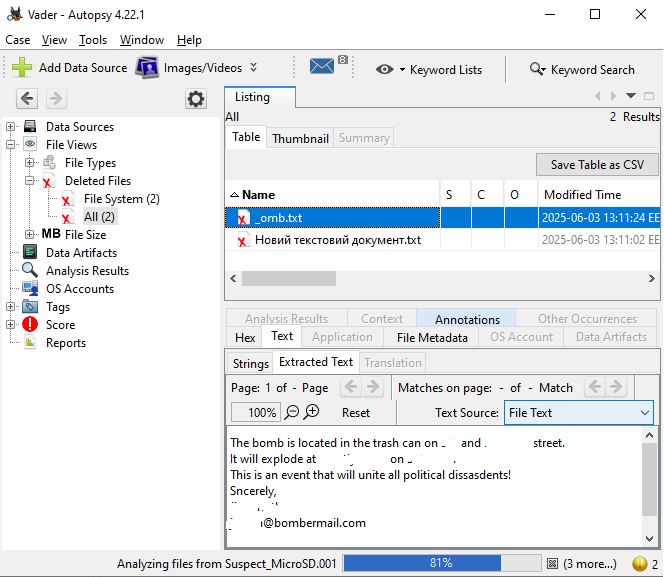
Залиште лише: Recent Activity

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



Finish

Подивиться видалені файли.



Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки?

\_\_\_\_\_\_\_\_\_\_\_\_\_

**Лабораторна 4. Аналіз основних артефактів Windows 10**

Відкрийте програму FTK imager.

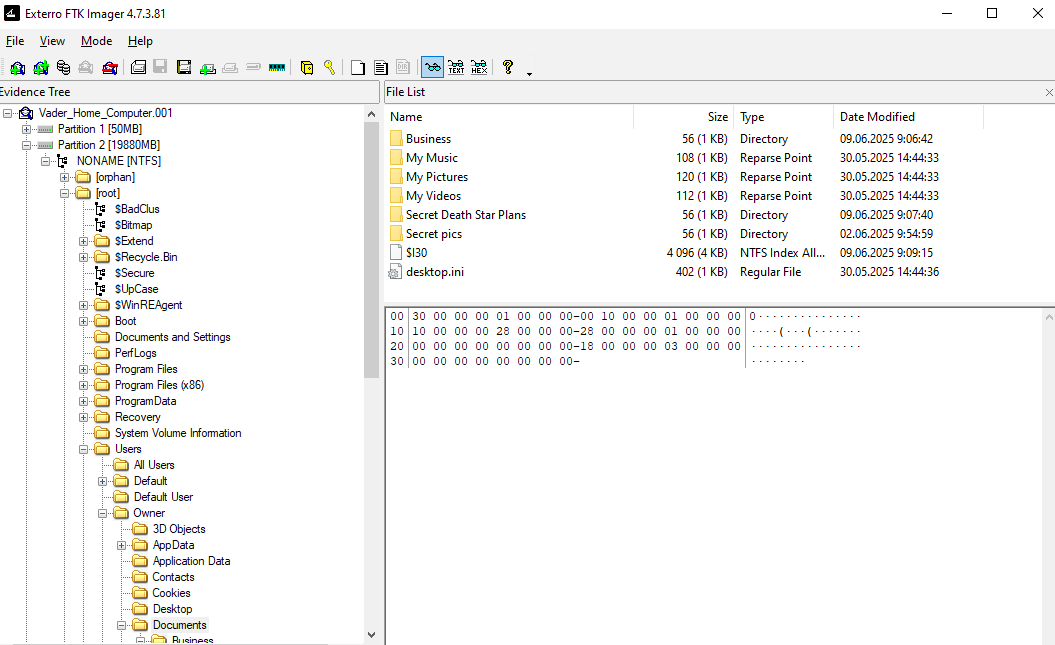
Додайте підозріле зображення (Vader\_Home\_Computer.001) до програми FTK imager.

File > Add Evidence Item > Image File та Далі > Browse та вибрати файл образу, 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\Documents\



Які файли можуть свідчити про злочинну діяльність?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Що це за злочинна діяльність?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

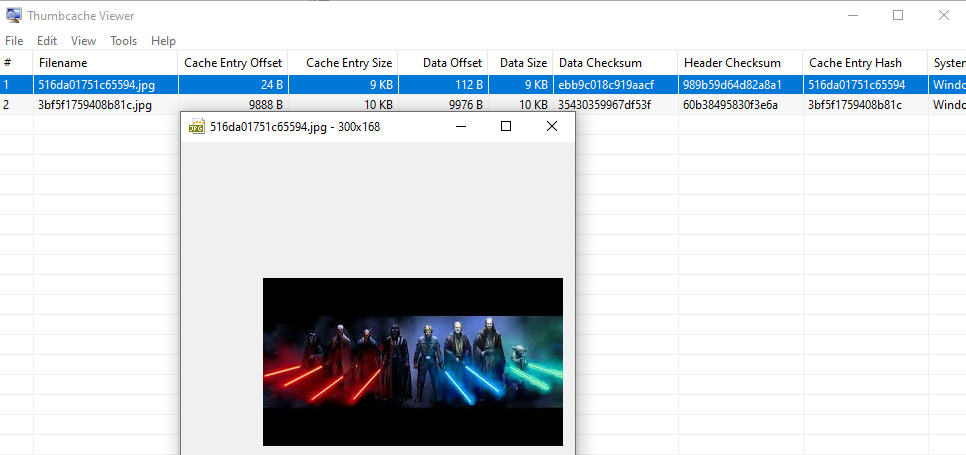
Перейдіть до папки \Users\Owner\AppData\Local\Microsoft\Windows\Explorer\

Експортуйте її на ваш комп’ютер.

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

Відкрийте завантажені файли в Thumbcache Viewer

File > Open > Папка на вашому комп’ютері, де ви зберегли Explorer > thumbcache\_768.db



Чим можуть допомогти в розслідуванні файли мініатюр (thumbcache\_\*.db)? Чому?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Відкрийте Autopsy.



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

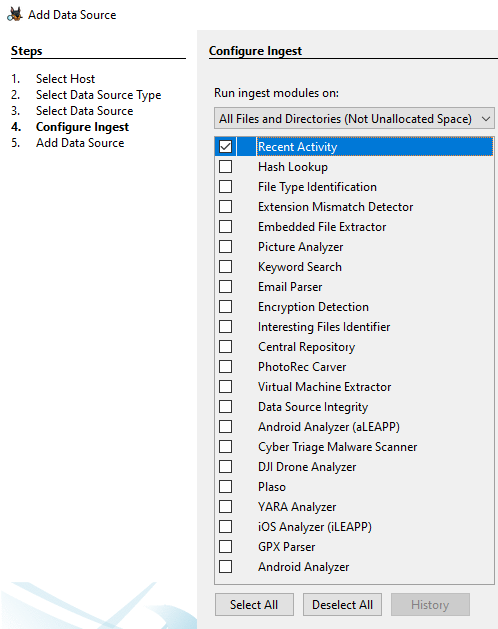
Додайте нове джерело – Add Data Source

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)

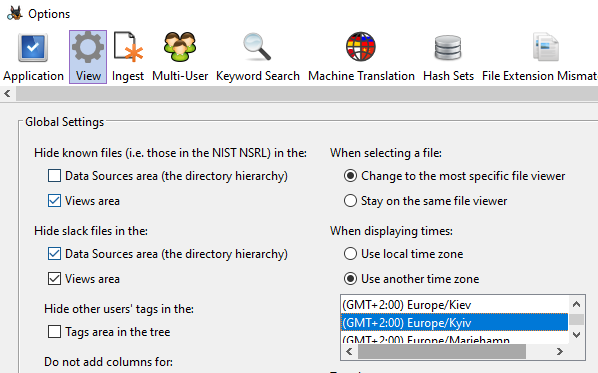


Finish

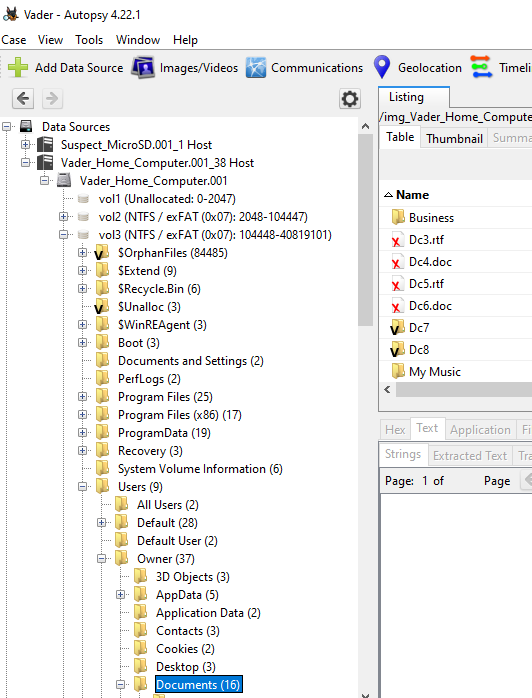
Дочекайтеся завершення аналізу!

Це може зайняти значний час.

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



Перейдіть Data Sources > Vader\_Home\_Computer.001 > vol3 > \Users\Owner\Documents\

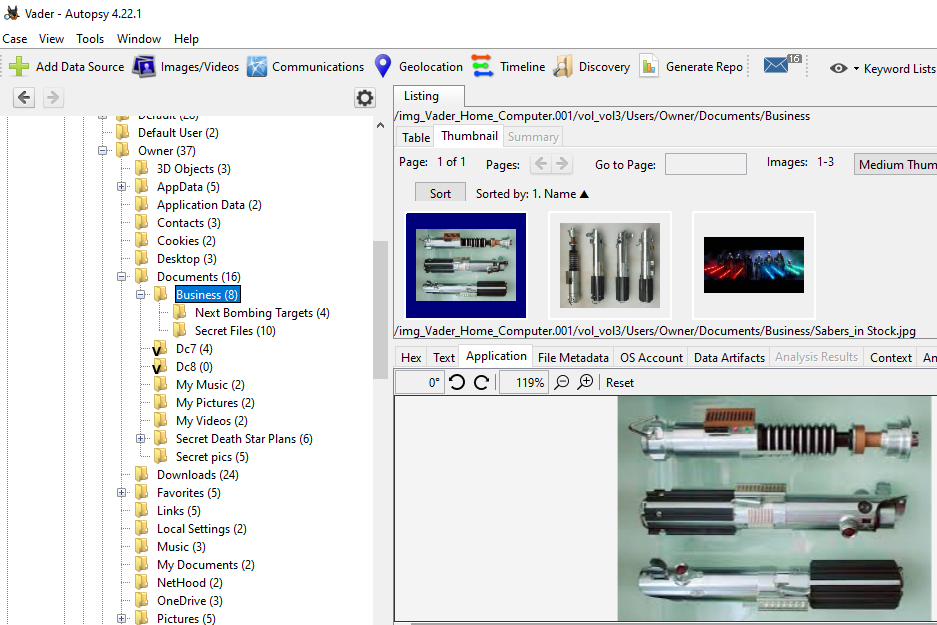


Передивіться документи.

Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки?

\_\_\_\_\_\_\_\_\_\_\_\_\_

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



Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки?

\_\_\_\_\_\_\_\_\_\_\_\_\_

**Лабораторна 5. Аналіз кошику**

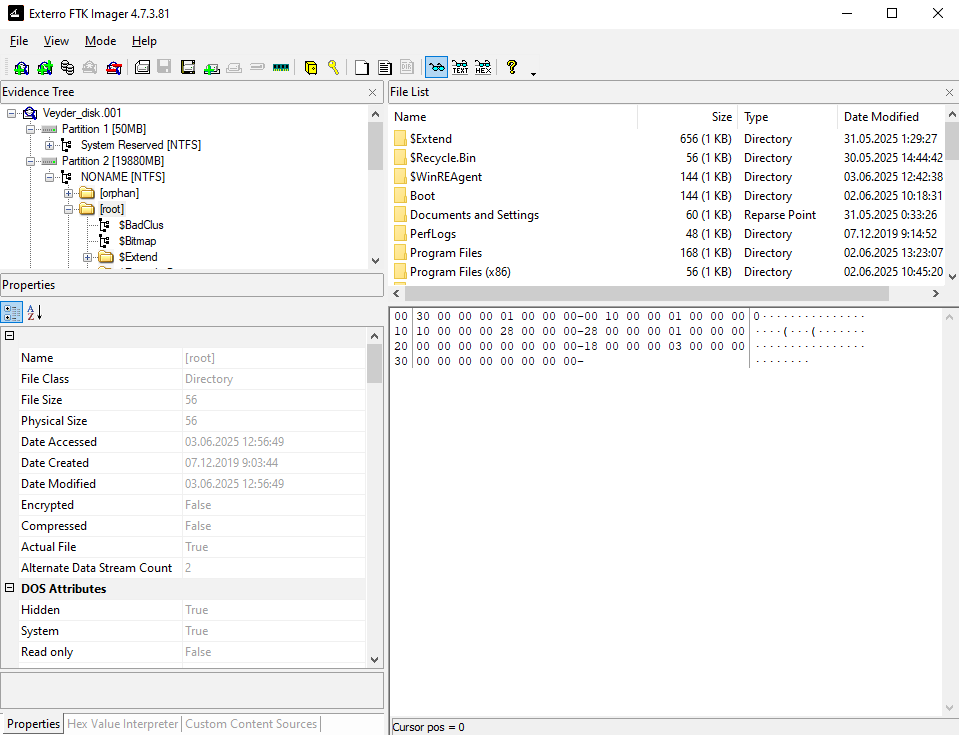
Відкрийте програму FTK imager.

Додайте підозріле зображення (Vader\_Home\_Computer.001) до програми FTK imager.

File > Add Evidence Item > Image File та Далі > Browse та вибрати файл образу, вибрати Vader\_Home\_Computer.001 та відкрити > Finish.

Натисніть кнопки + для навігації по зображенню.

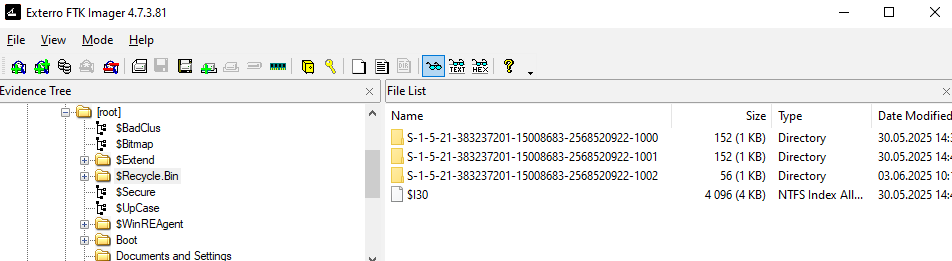
Перейдіть до кореневого каталогу Розділу 2 (root Partition 2).



Яка назва та файлова система цього розділу?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Перейдіть до папки $Recycle.Bin



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?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

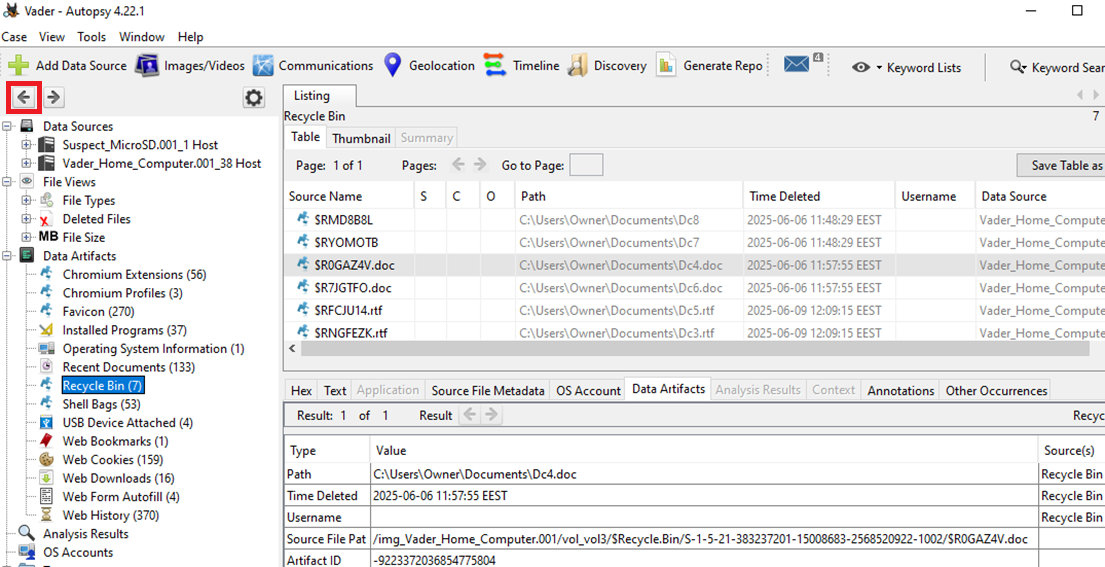
Які були шляхи до файлів, ім'я, розмір і дата видалення підозрілих файлів?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Відкрийте Autopsy.

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

Перейдіть Data Artifacts > Recycle Bin



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?

\_\_\_\_\_\_\_\_\_\_\_\_\_

**Лабораторна 6. Аналіз посилань на недавно відкриті файли (Recent) та файлів попереднього завантаження (Prefetch)**

Відкрийте FTK imager

Відкрийте підозрілий образ (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.

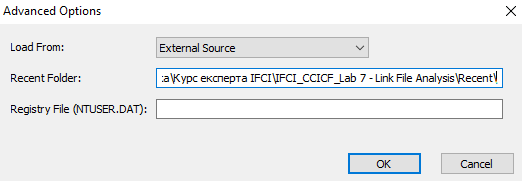
Встановіть / відкрийте RecentFileView від Nirsoft. (https://www.nirsoft.net/utils/recent\_files\_view.html)

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?

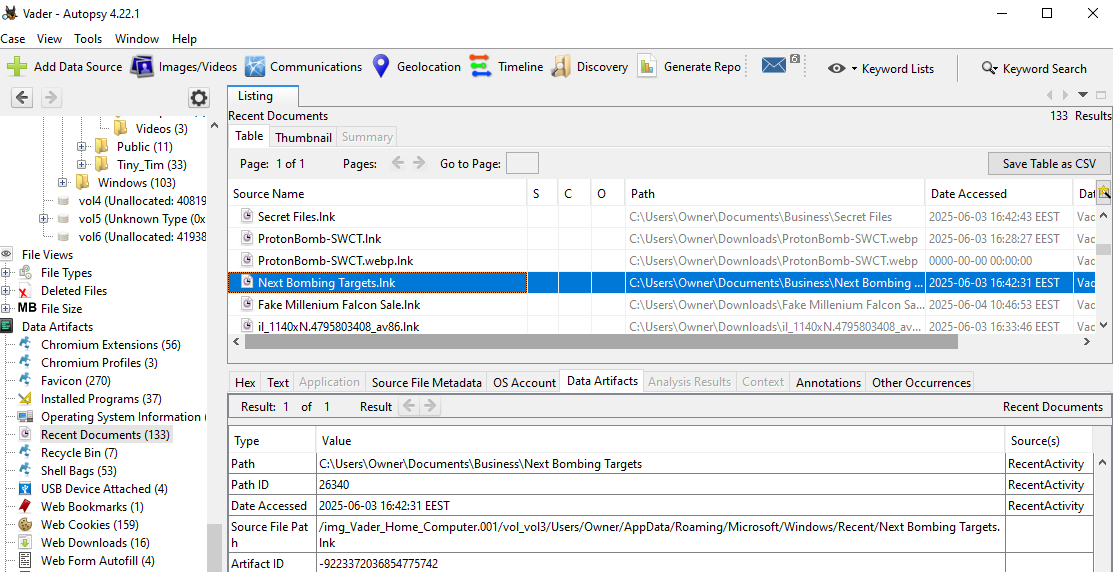
Де він знаходився і як ви могли б знайти цей файл?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Відкрийте Autopsy.

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

Перейдіть Data Artifacts > Recent Documents



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

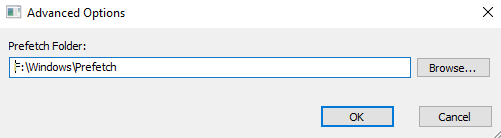
Змонтуйте підозрілий образ (Vader\_Home\_Computer.001) до локального диска.

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.

**Лабораторна 7. Аналіз сигнатур файлів**

Відкрийте FTK Imager

Відкрийте підозрілий образ (Vader\_Home\_Computer.001) у FTK imager.

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

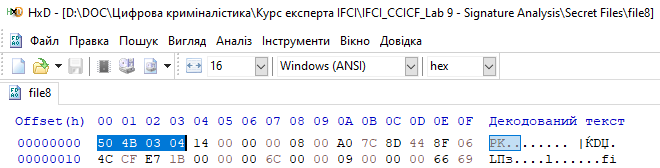
Експортуйте папку Secret Files на локальний жорсткий диск.

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.



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?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Лабораторна 8. Аналіз метаданих файлів**

Відкрийте FTK Imager

Відкрийте підозрілий образ (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.



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

Яка марка та модель камери, якою було зроблено фотографію?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

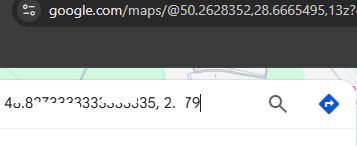
Яка дата та час зйомки фотографії?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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). 

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.

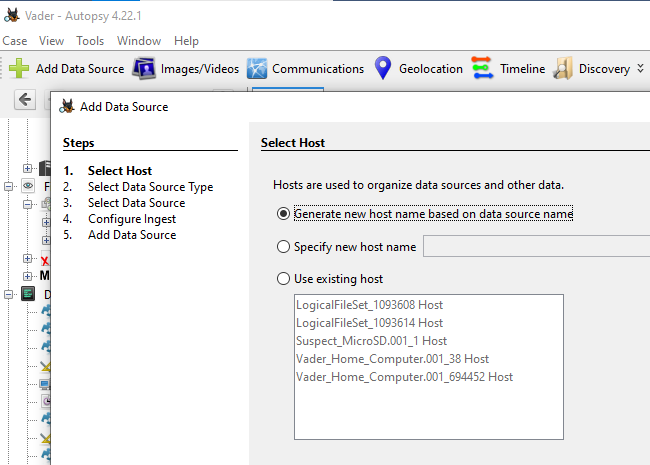
(Пам’ятайте: N = додатна, S = від’ємна, E = додатна, W = від’ємна).

Де саме знаходиться друга ціль теракту?

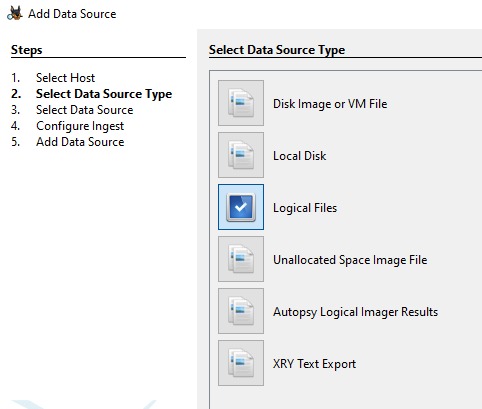
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Відкрийте Autopsy.

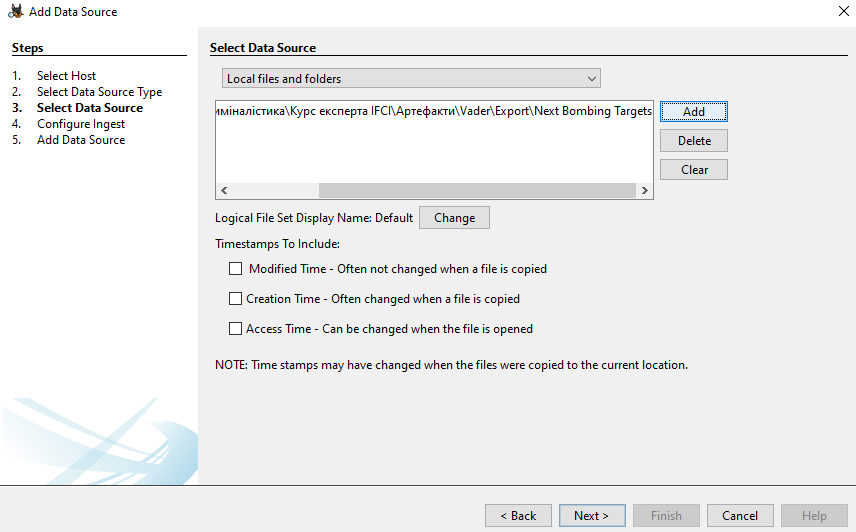
Відкрийте справу, що ви завели у попередніх лабораторних – Open Recent Case



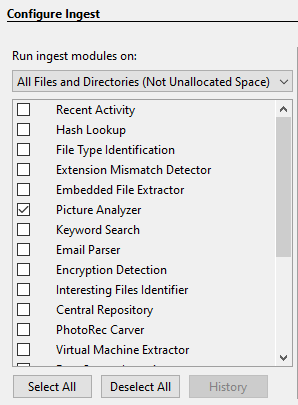
Logical Files



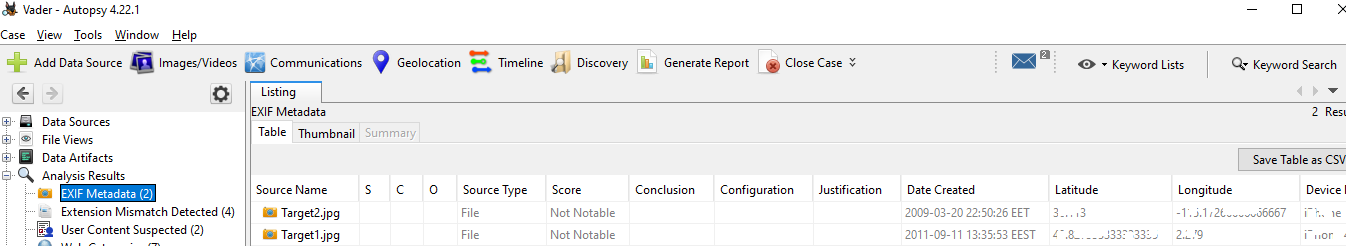
Add > вкажіть шлях до збереженої папки Next Bombing Targets



Виберіть тільки Picture Analyzes



Analysis Results > EXIF Metadata



Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки?

\_\_\_\_\_\_\_\_\_\_\_\_\_

**Лабораторна 9. Аналіз журналу подій**

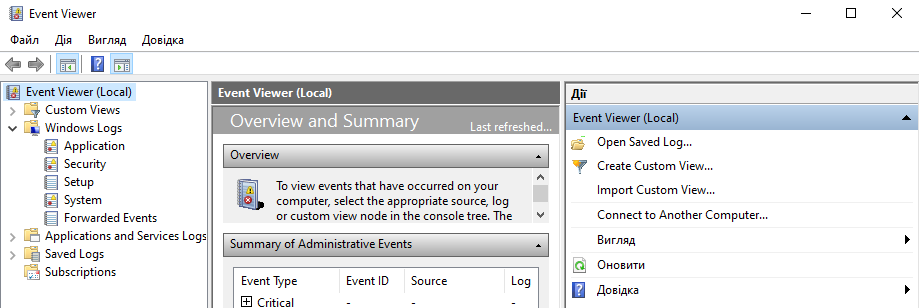
Відкрийте FTK Imager

Відкрийте підозрілий образ (Vader\_Home\_Computer.001) у FTK imager.

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

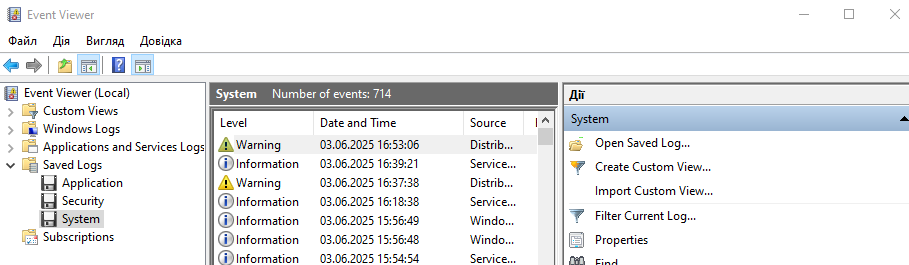
Експортуйте три журнали подій (Application.evtx Security.evtx System.evtx) на ваш комп’ютер.

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



У меню оберіть Дія > Open Saved Log

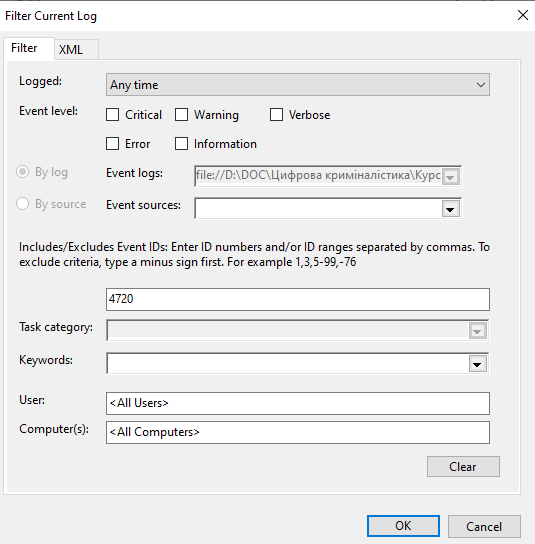
Виберіть експортовані файли .evtx.



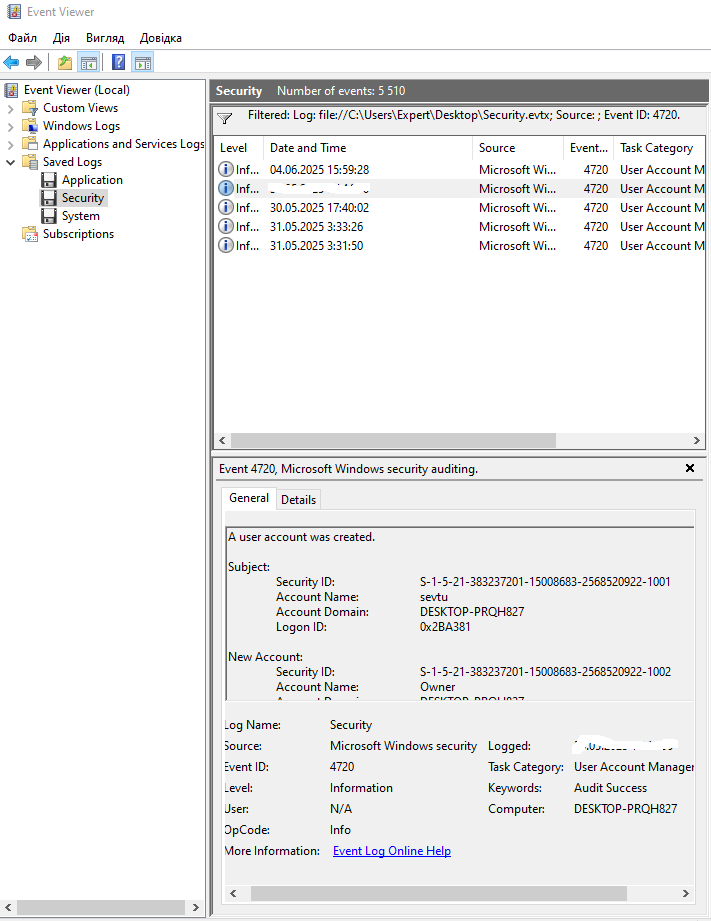
Перегляньте журнал Security.

Event ID 4720 – створення облікового запису.

Скористайтеся фільтром Дія > Filter Current Log



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



Коли було створено профіль користувача Owner?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Коли було створено профіль користувача Tiny\_Tim?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Для скидання фільтру Дія > Clear Filter.

Event ID 4624 – вхід до облікового запису.

Скористайтеся фільтром Дія > Filter Current Log

Потім Скористайтеся пошуком Дія > Find



Коли Owner входив до свого акаунту востаннє?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Що означає Logon Type: 2?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Коли Tiny\_Tim входив до свого акаунту востаннє?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Лабораторна 10. Аналіз реєстру**

Відкрийте FTK Imager

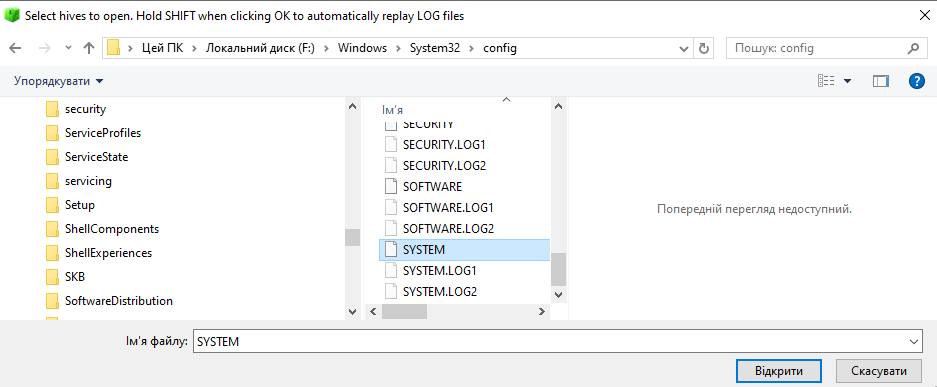
Змонтуйте підозріле зображення File > Image Mounting > Vader\_Home\_Computer.001

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

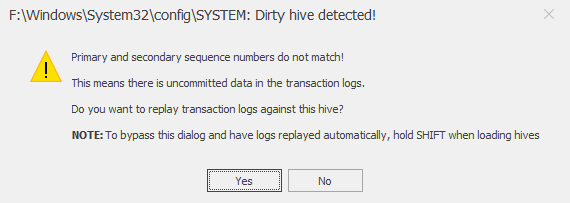
Можливо під час встановлення потрібно буде завантажити та довстановити .NET

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

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

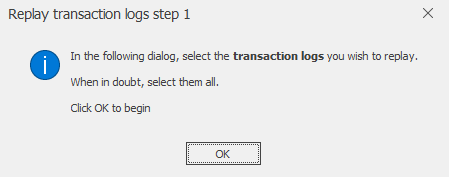


Відкрити.



\*\*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.



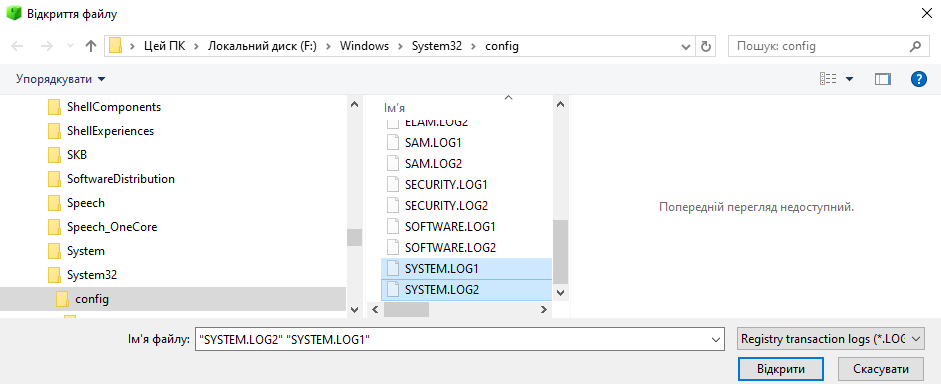
OK

У наступному діалозі позначте всі запропоновані LOG-файли:

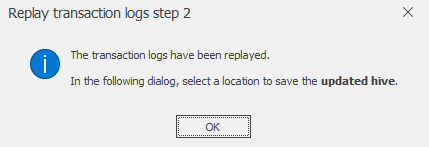
SYSTEM.LOG1

SYSTEM.LOG2

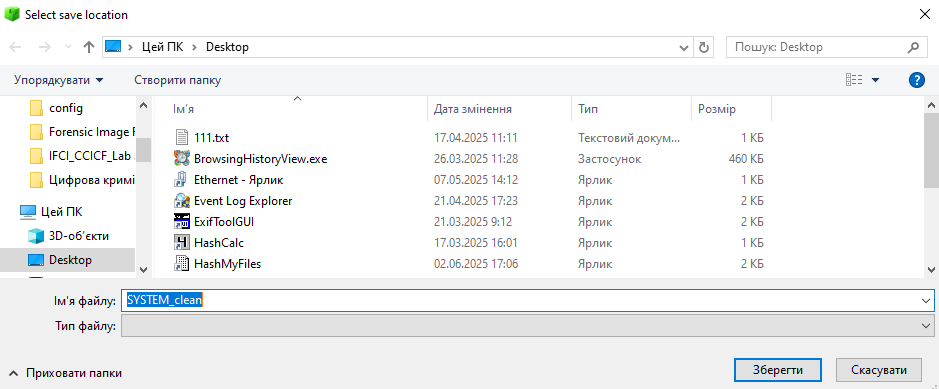
(Ctrl + ліва кнопка миші)



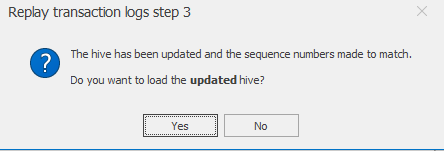
Відкрити.



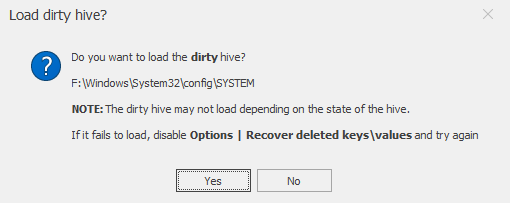
OK



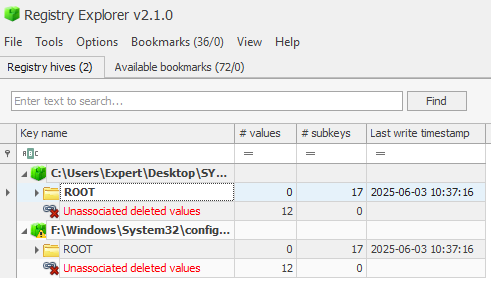
Зберегти.



Yes

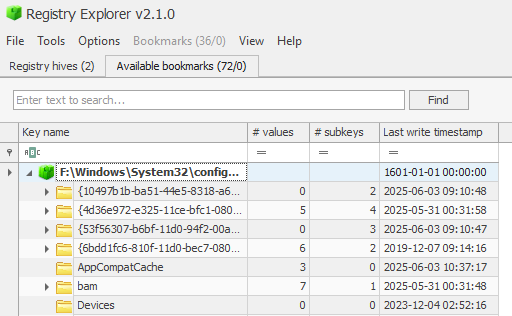


Yes

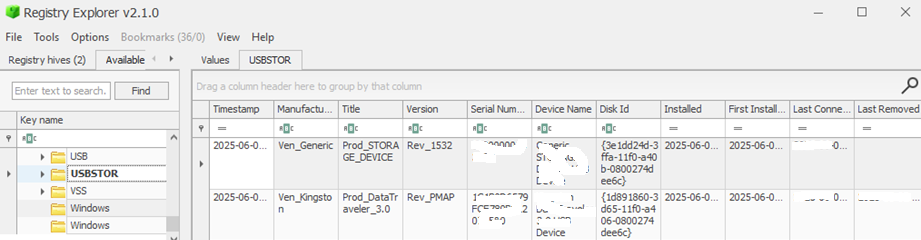


Перейдіть у вкладку Available bookmarks

F:\Windows\System32\config\SYSTEM



USBSTOR



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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

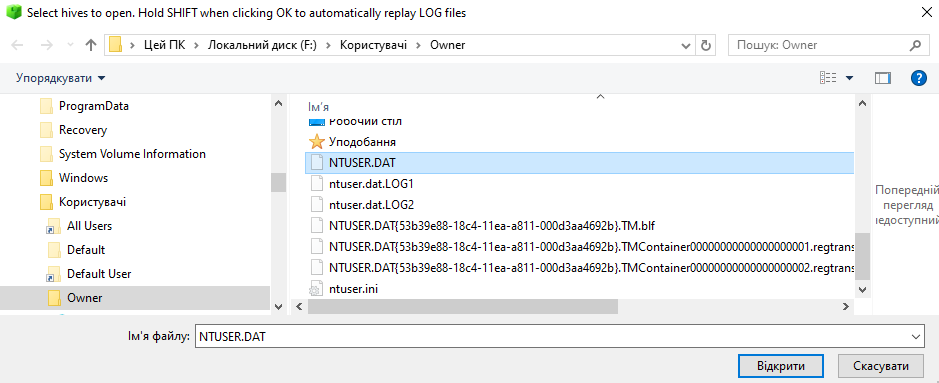
Які серійні номери пристроїв (Serial Number)?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

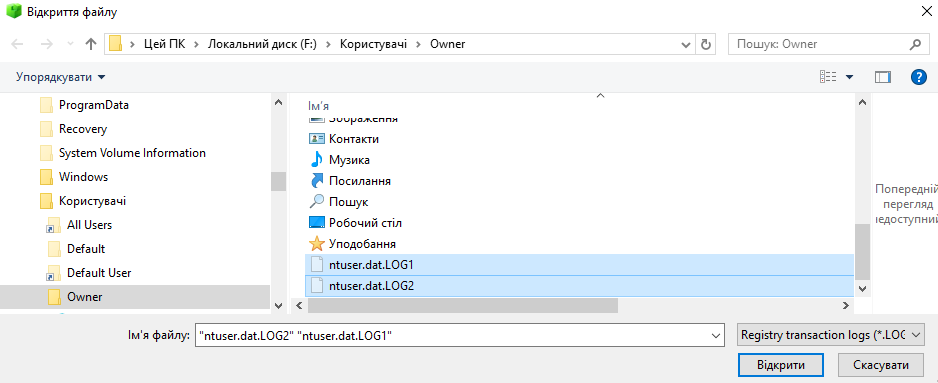
Коли відбувалося останнє підключення цих накопичувачів до системи?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

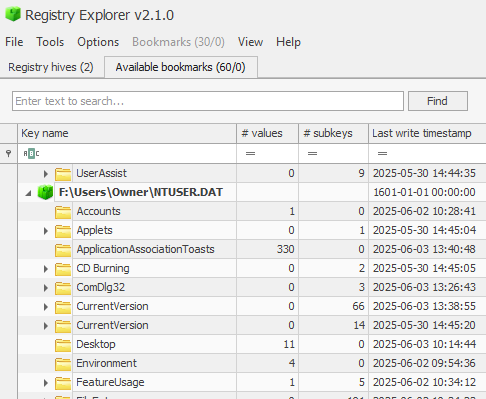
File > Load hive > F:\Users\Owner\NTUSER.DAT



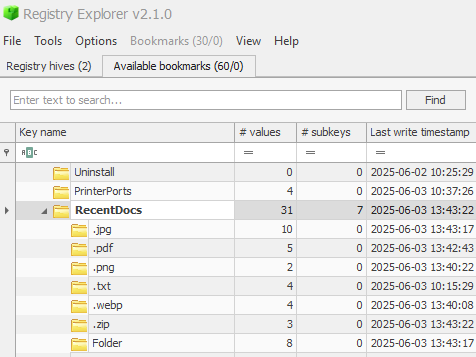
Далі по аналогії з попереднім процесом.



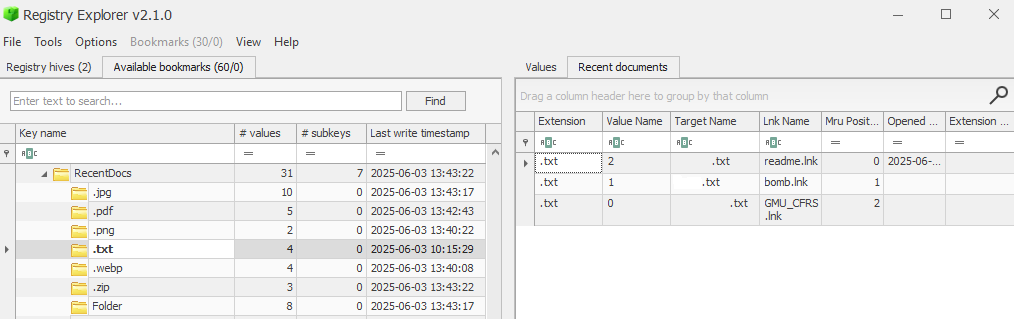
F:\Users\Owner\NTUSER.DAT



RecentDocs



.txt



Які файли .txt відкривалися в цій системі?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

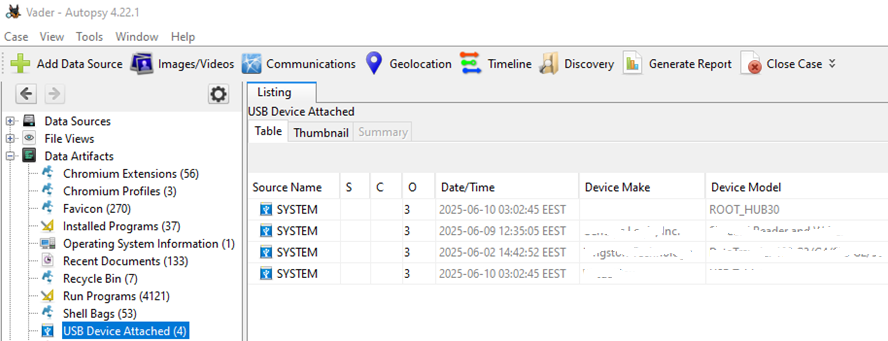
Які файли .zip відкривалися в цій системі?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Відкрийте Autopsy.

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

Перейдіть Data Artifacts > USB Dtvice Attaches



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

\_\_\_\_\_\_\_\_\_\_\_\_\_

**Лабораторна 11. Аналіз оперативної пам’яті**

Завантажте архів дампу оперативної пам’яті VaderRAM.zip (https://drive.google.com/file/d/1OJ8G5Majx2AMJ3I80V86-6v\_9EI9pbCm). Розархівуйте його.

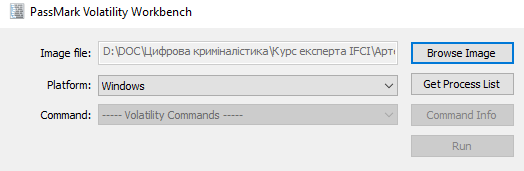
Завантажте Volatility Workbench V3.0.1012 (16,4 МБ)

(https://www.osforensics.com/tools/volatility-workbench.html)

Запустити VolatilityWorkbench.exe

Image file: > Browse Image > Вибрати файл дампу VaderRAM.dmp

Platform: Windows



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 ІРv4-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?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Лабораторна 12. Аналіз мобільного телефона**

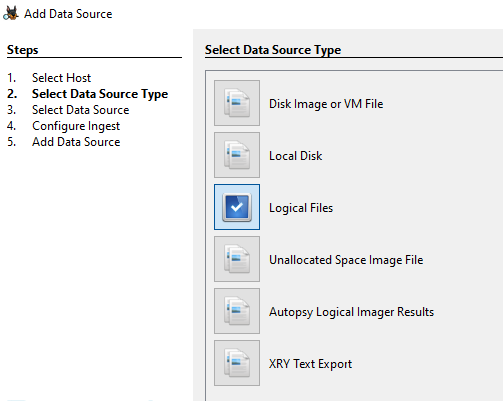
Завантажте архів пам’яті мобільного телефона Vader\_Phone.zip (https://drive.google.com/file/d/19XgxWGRa1Ez9e-gQrAwM7VCONojRSLAH).

Розархівуйте його.

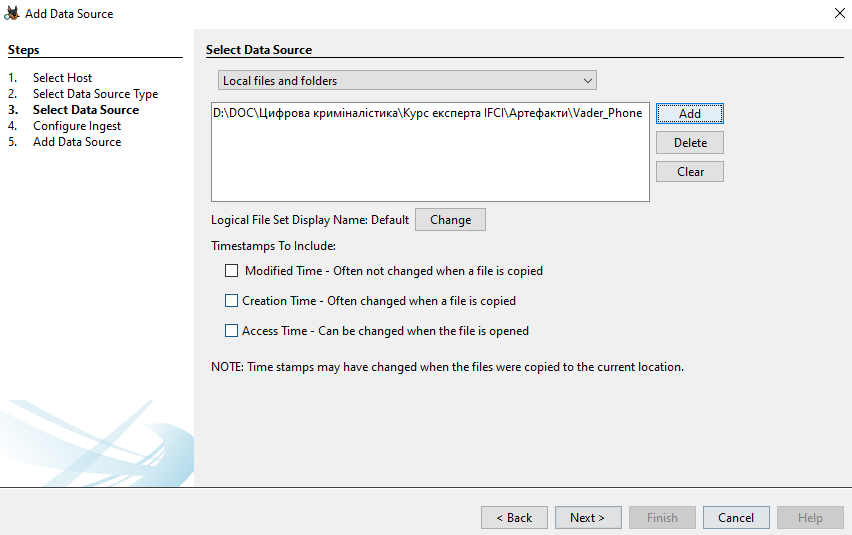
Відкрийте Autopsy.

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

Logical Files

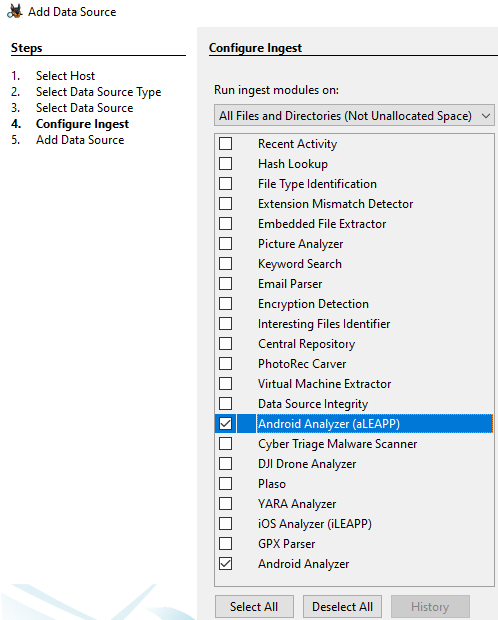


Add > вкажіть шлях до збереженої папки Vader\_Phone

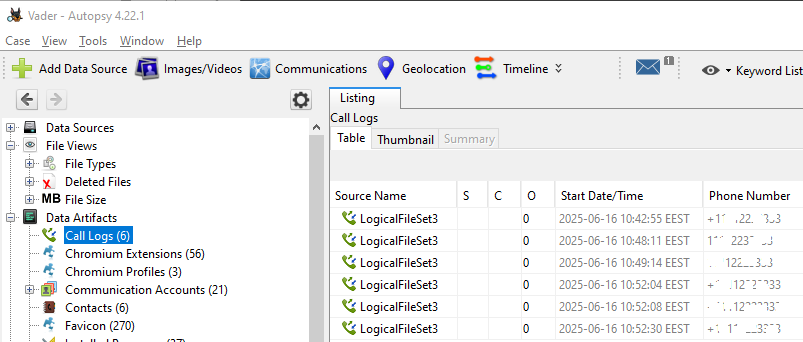


Виберіть:

* Android Analyzer (aLEAPP)
* Android Analyzer



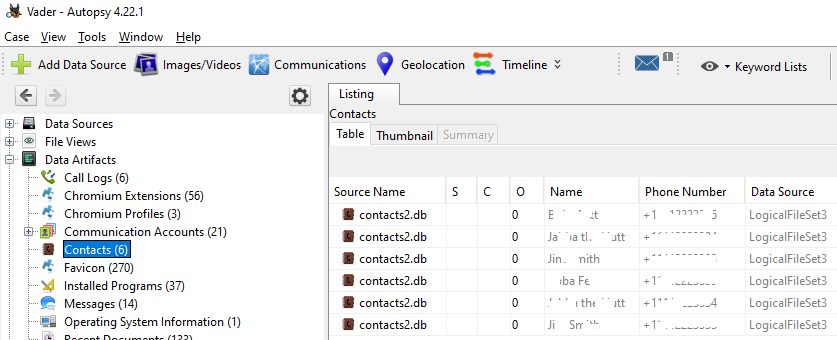
Data Artifacts > Call Logs



Який номер абонента, з яким велося спілкування?

\_\_\_\_\_\_\_\_\_\_\_\_\_

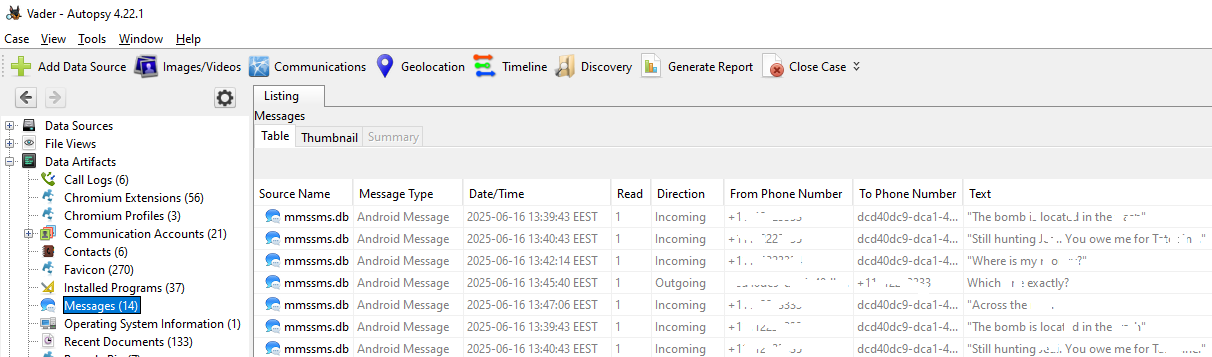
Data Artifacts > Contacts



Які контакти абонента?

\_\_\_\_\_\_\_\_\_\_\_\_\_

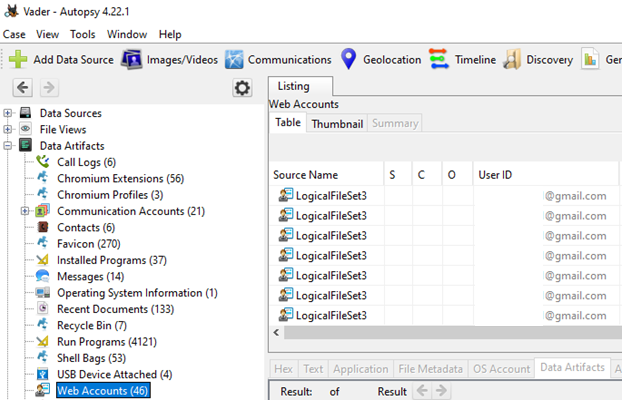
Data Artifacts > Messages



Відновіть листування абонента?

\_\_\_\_\_\_\_\_\_\_\_\_\_

Data Artifacts > Web Accounts



До якого акаунту підключений абонент?

\_\_\_\_\_\_\_\_\_\_\_\_\_

**Лабораторна 13. Аналіз інтернет-активності**

Відкрийте програму FTK imager.

Додайте підозріле зображення (Vader\_Home\_Computer.001) до програми FTK imager.

File > Add Evidence Item > Image File та Далі > Browse та вибрати файл образу, 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)!

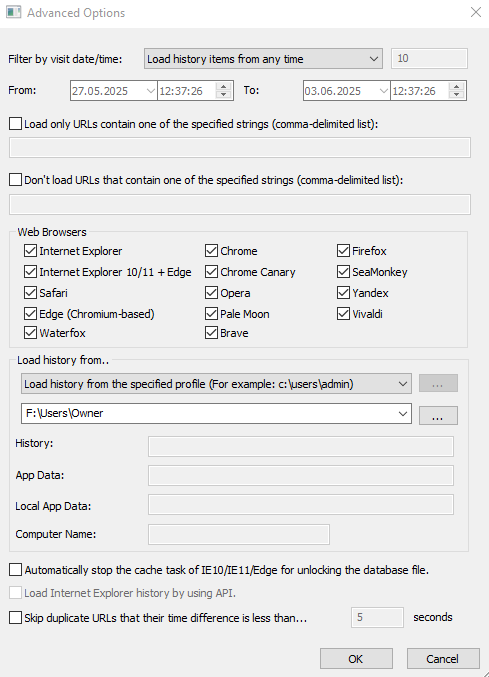
У полі Advanced Options зверніть увагу на поле Filter by visit date/time та виберіть Load History Items from any time.

Залиште позначеними всі веббраузери.

У розділі Load history from.. виберіть: Load history from the specified profile (For

example: 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.



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?

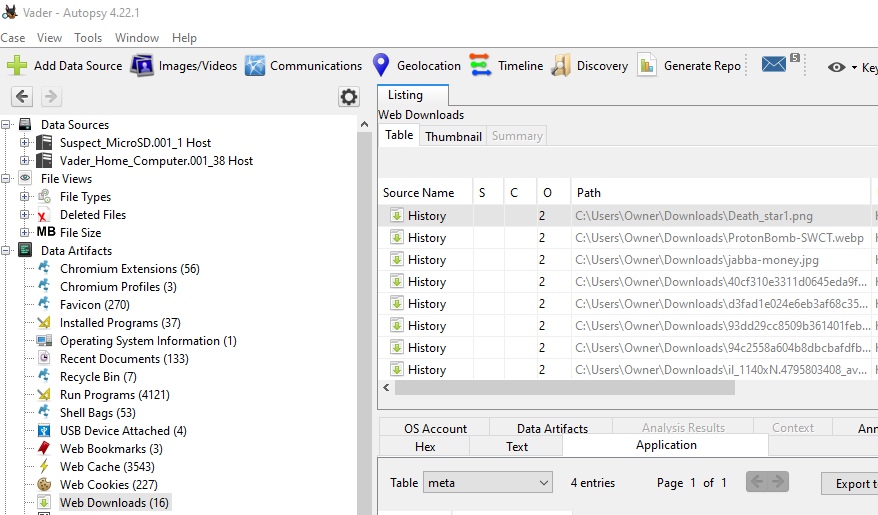
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Перед закриттям FTK Imager відмонтуйте всі змонтовані диски.

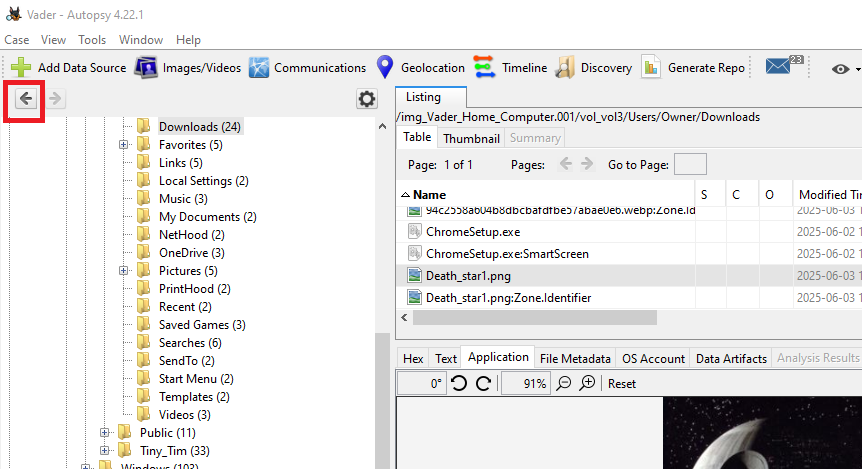
Відкрийте Autopsy.

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

Перейдіть Data Artifacts > Web Downloads



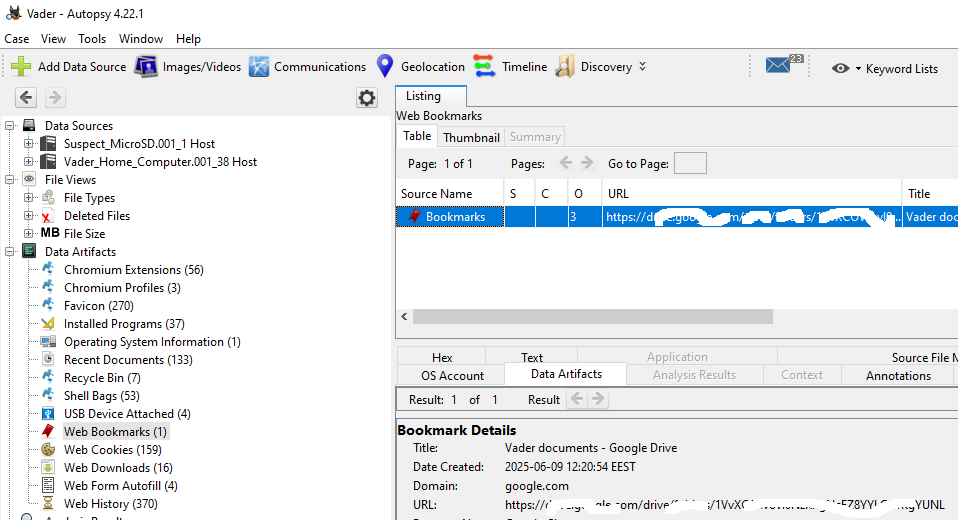
Через контекстне меню виберіть для знайдених файлів View Downloaded File in Directory, щоб подивитися їх. Повернення назад за допомогою стрілки у лівому верхньому куті.



Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки?

\_\_\_\_\_\_\_\_\_\_\_\_\_

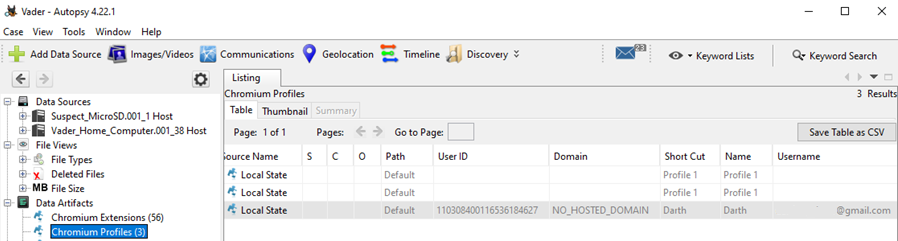
Перейдіть Data Artifacts > Web Bookmarks



Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки?

\_\_\_\_\_\_\_\_\_\_\_\_\_

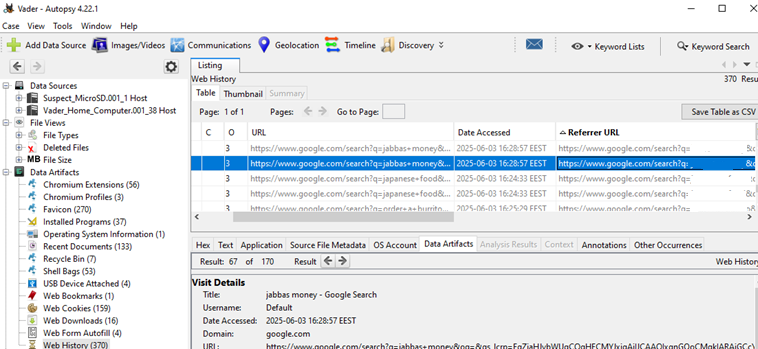
Перейдіть Data Artifacts > Chromium Profiles



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

\_\_\_\_\_\_\_\_\_\_\_\_\_

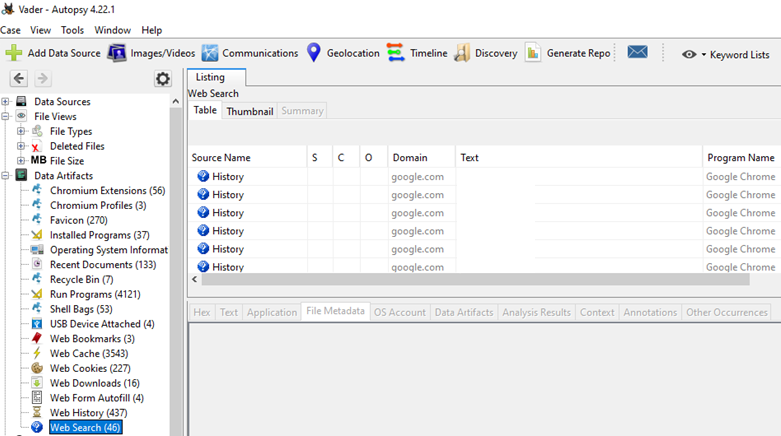
Перейдіть Data Artifacts > Web History



Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки?

\_\_\_\_\_\_\_\_\_\_\_\_\_

Перейдіть Data Artifacts > Web Search



Чи підтверджуються раніше зроблені в цієї лабораторній роботі висновки?

\_\_\_\_\_\_\_\_\_\_\_\_\_