МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра Інформаційної Безпеки

Аналіз та моніторинг кібербезпеки

Практичне завдання №1

Аналіз пам’яті та отримання видалених файлів в операційній системі Windows

Перевірив:
Козленко О. В.

Виконав:
студент IV курсу
групи ФБ-01
Сахній Н. Р.

Київ 2024

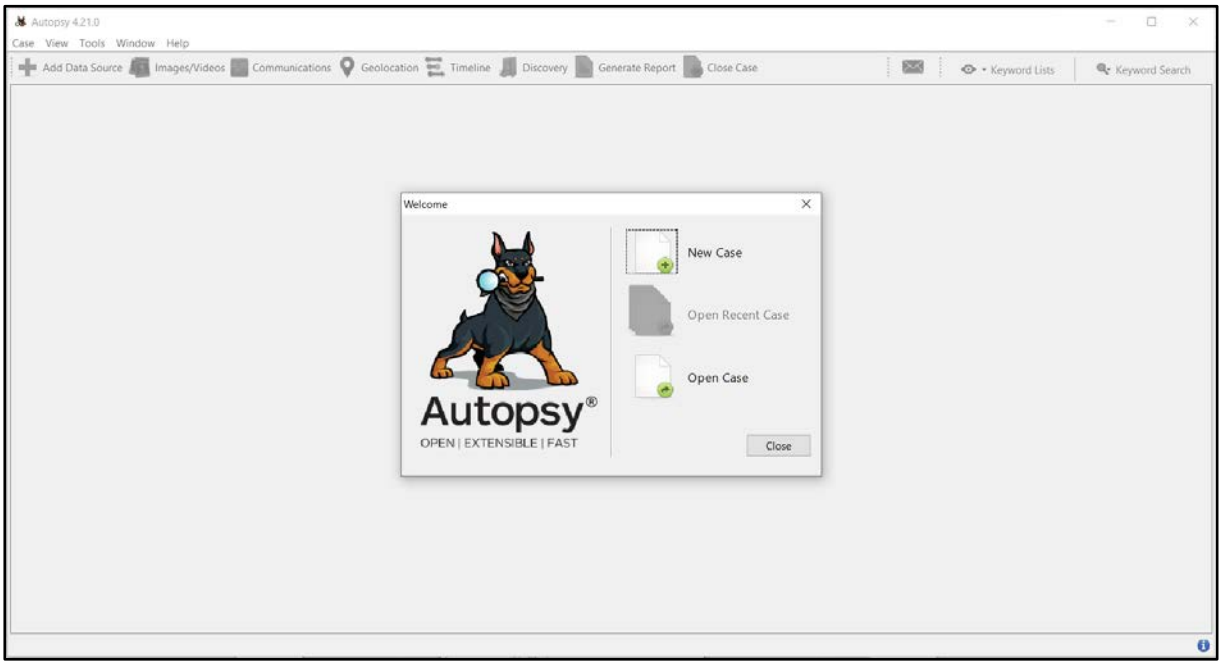
Мета: Знайомство з елементами комп’ютерної криміналістики (форензіки), отримання практичних навичок з пошуку та збору цифрових артефактів в ОС Windows.

Завдання: На бажаному образі пам’яті за допомогою утиліти Autopsy проаналізувати стан, отримати основну інформацію щодо даного образу, сформувати звіт. За допомогою утиліти Recurva відновити видалені файли у системі.

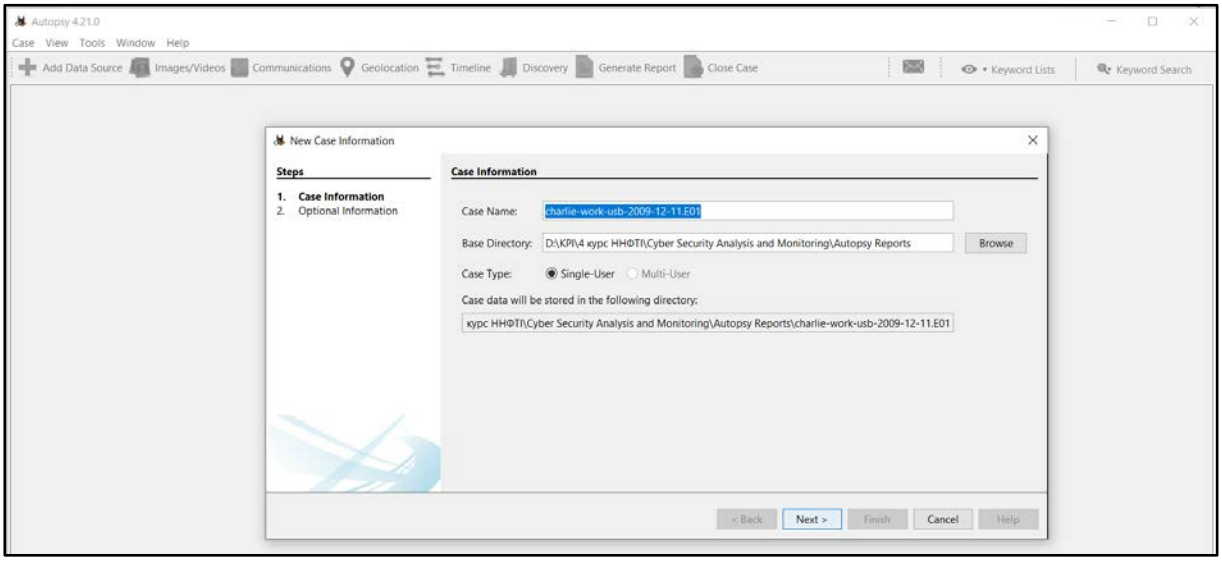
❖ Аналіз стану образу пам’яті за допомогою утиліти Autopsy

***** Образ для аналізу (charlie-work-usb-2009-12-11.E01) завантажимо звідси.

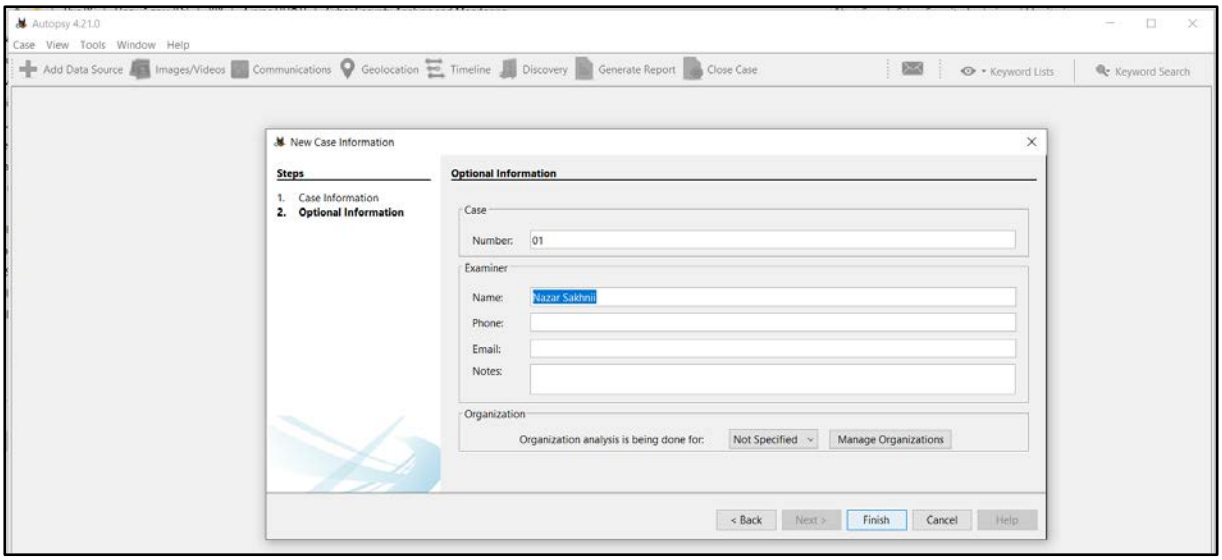
1. Відкриємо Autopsy в Windows як адміністратор і натиснемо «New Case»:



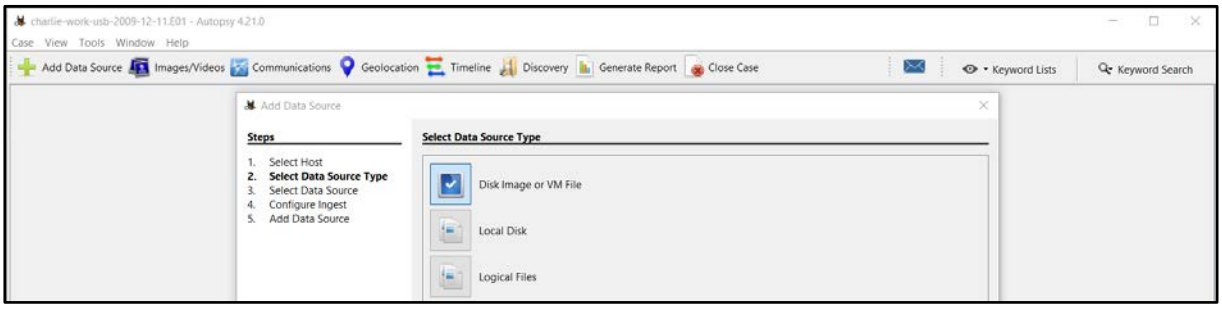
2. Дамо справі ім'я та базовий каталог для збереження файлів:



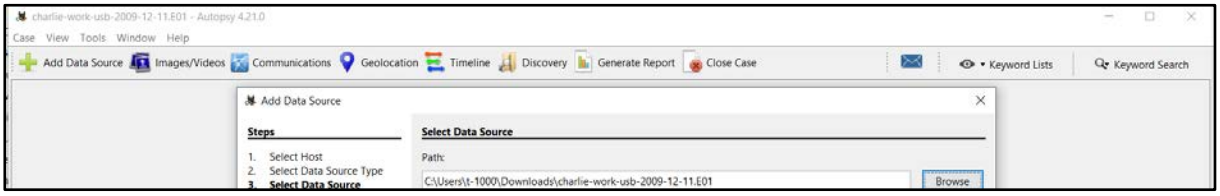
3. Введемо номер справи та ім’я дослідника:



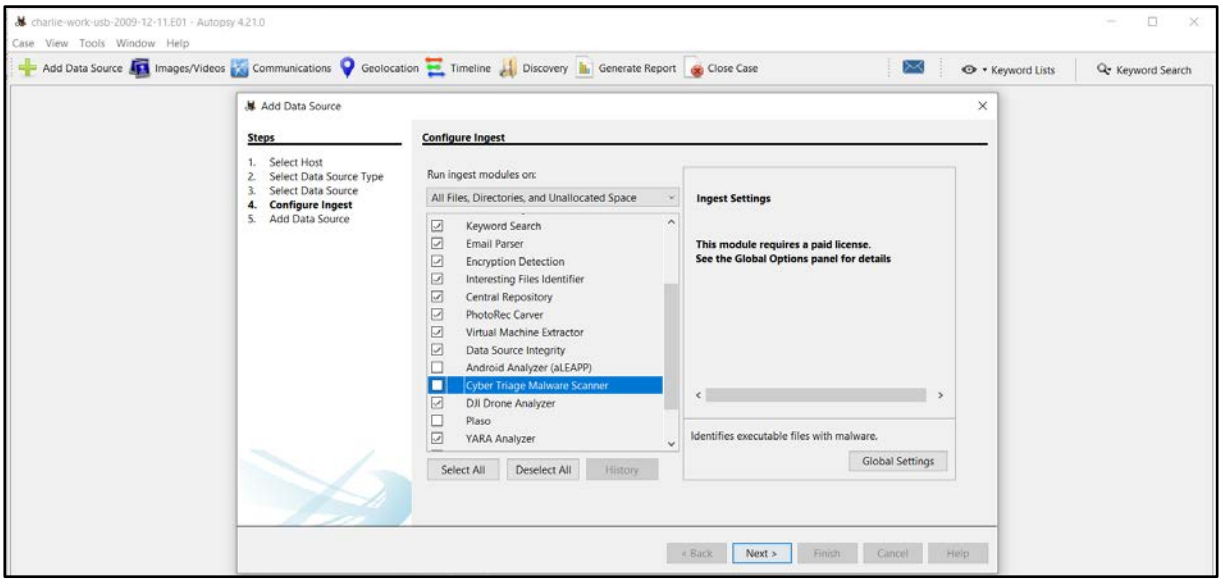
4. Виберемо джерело: Image / Physical / Logical та часовий пояс:



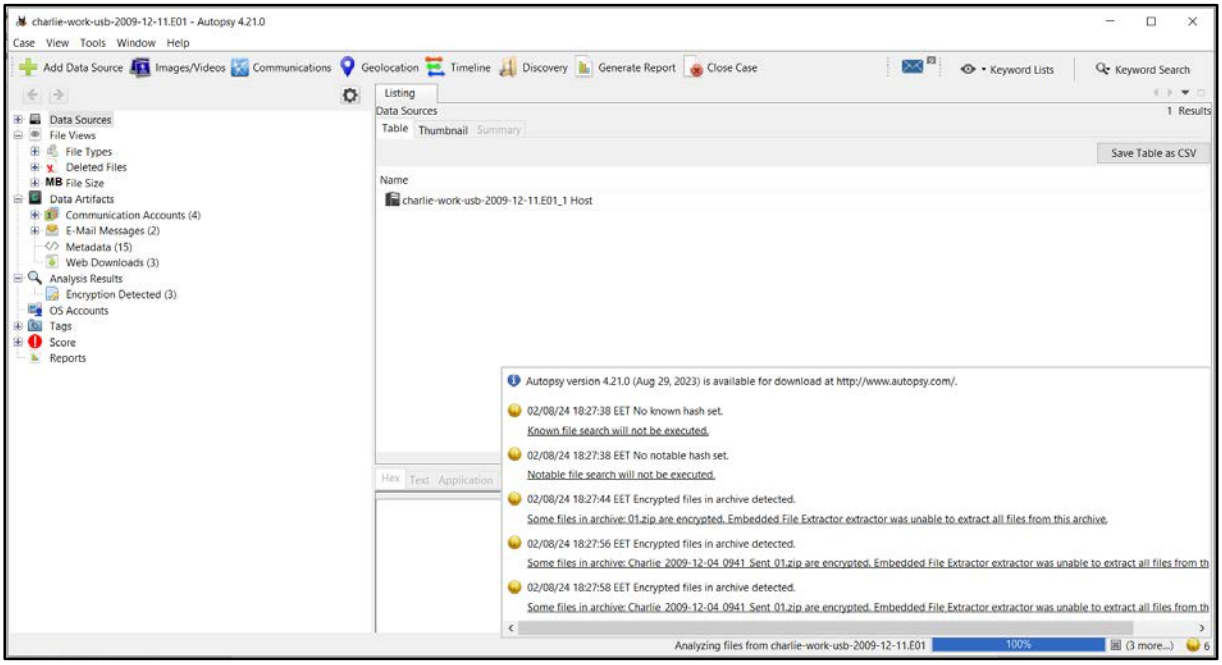
5. Оберемо образ для аналізу та виберемо відповідні модулі:



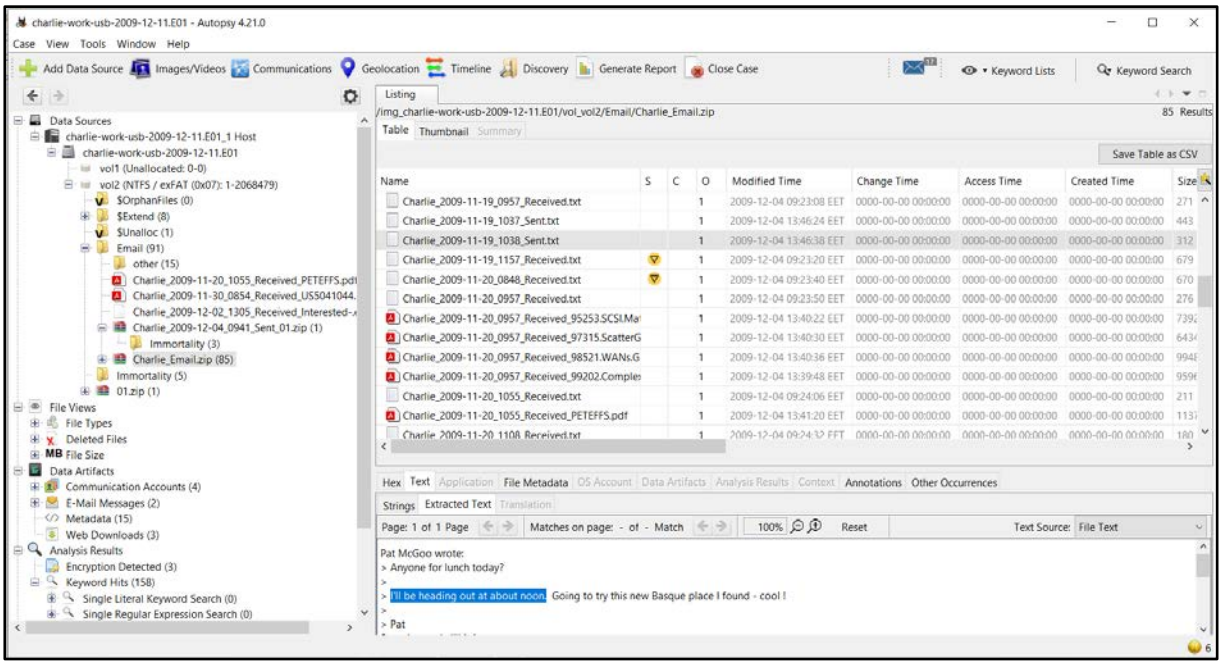
6. Виберемо модулі, які ви хочете використовувати для аналізу:



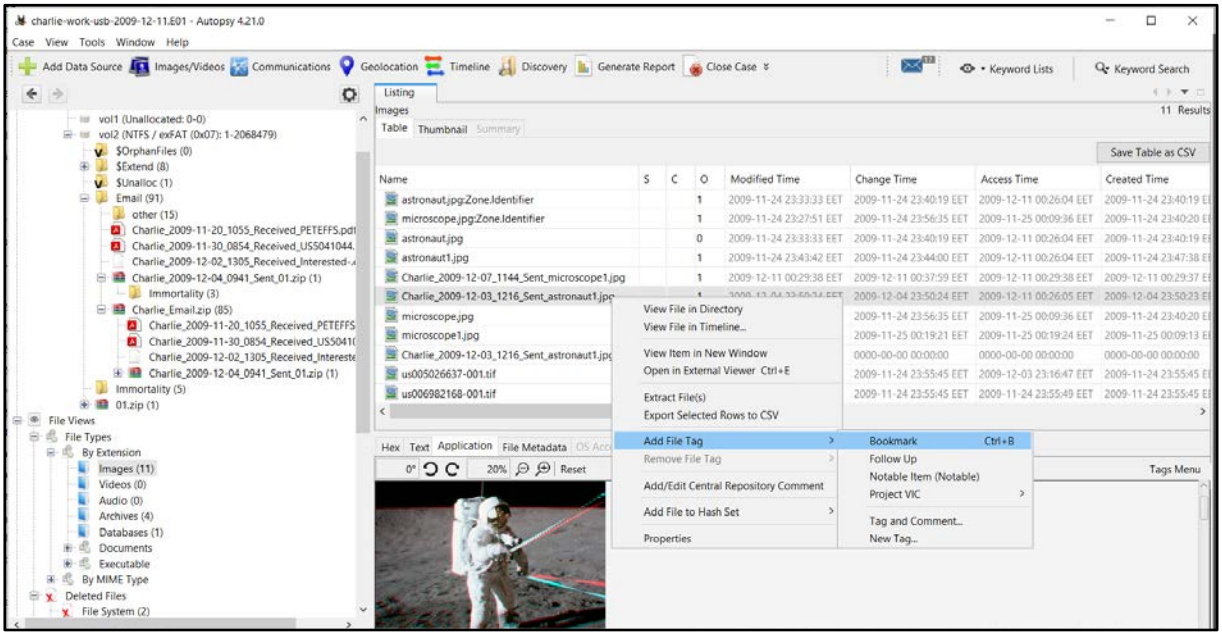
7. Дочекаємось, поки аналіз буде завершено:



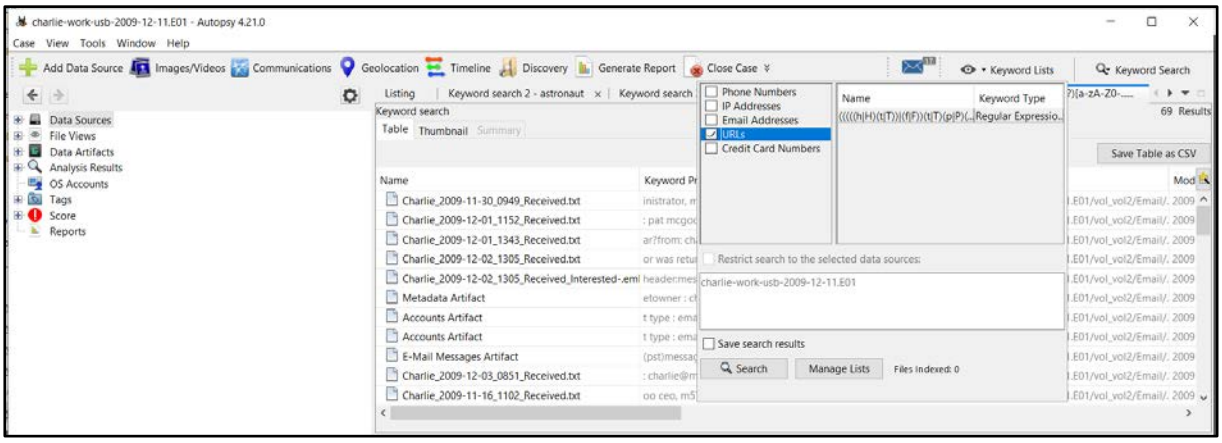
8. Тепер ознайомимося з доказами (наприклад, натиснемо «Data Sources >> … >> vol 2 (NTFS…) >> Email», щоб переглянути надіслані листи):



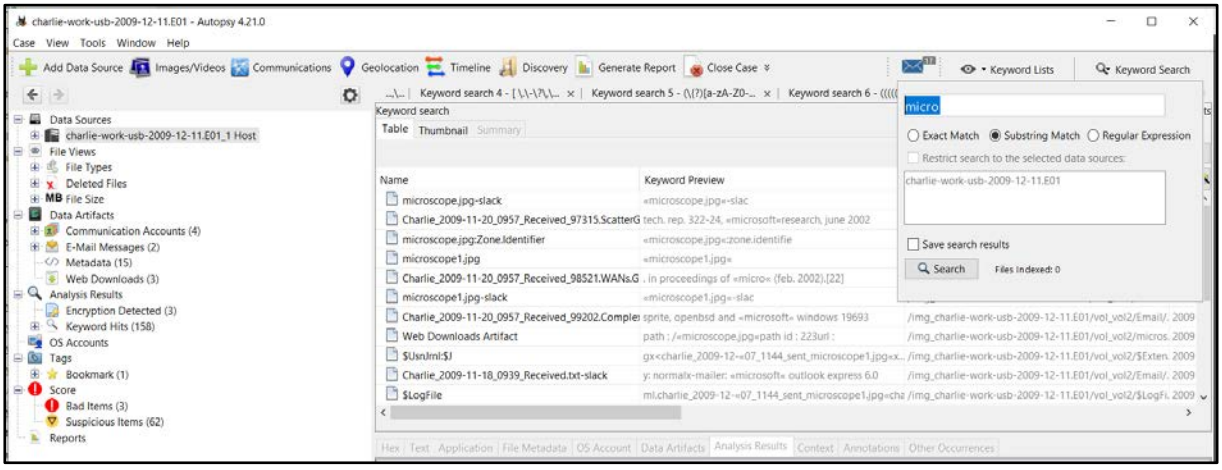
9. Позначимо файл для створення звітів:



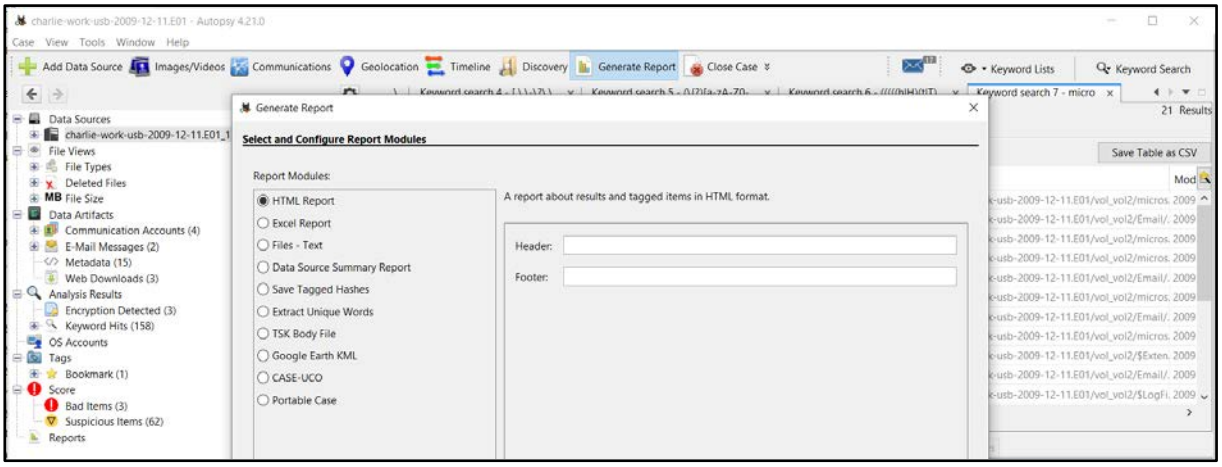
10.Відсортуємо докази за допомогою попередньо визначеного Predefined Keyword List:



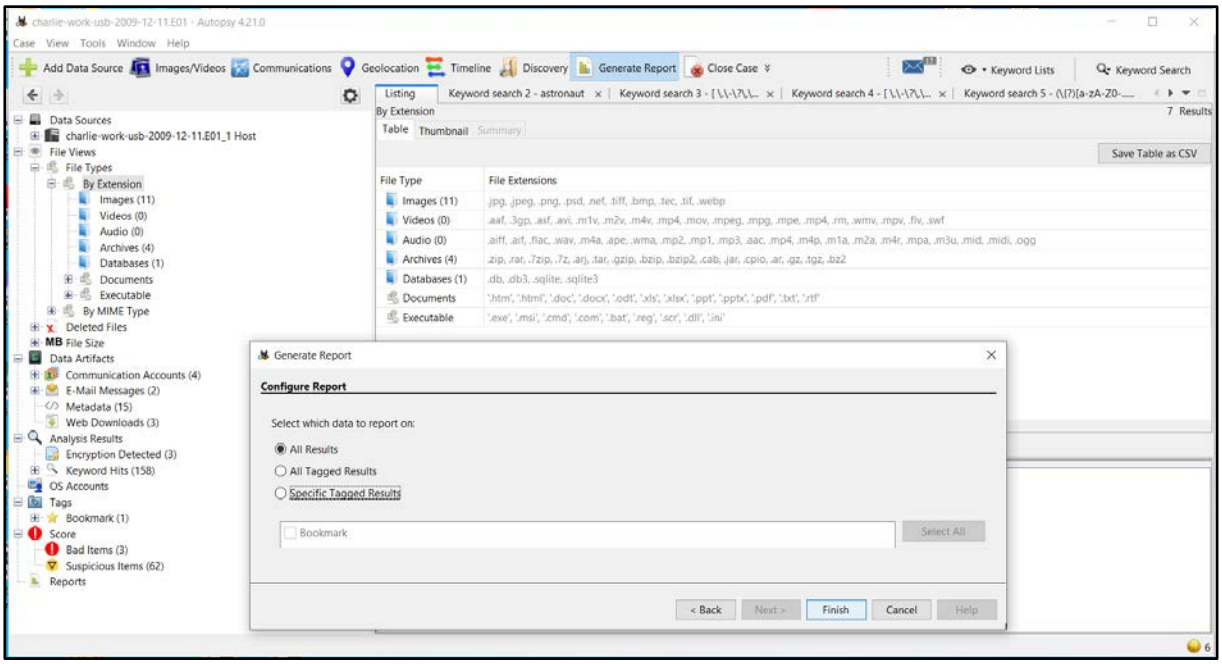
11.Пошукаємо файли за пошуком відносно слова та подивимось результат:



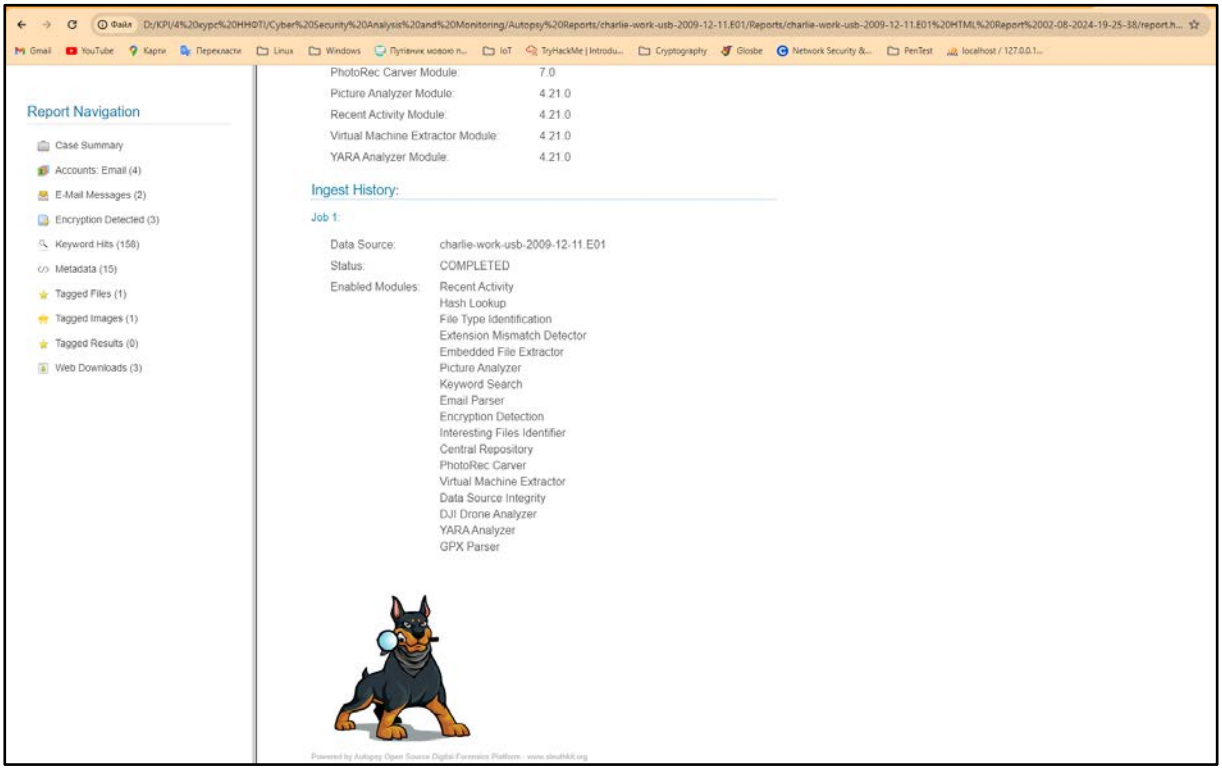
12.Створимо звіт, натиснувши вкладку Generate Report:



13.Натиснемо на All Results:

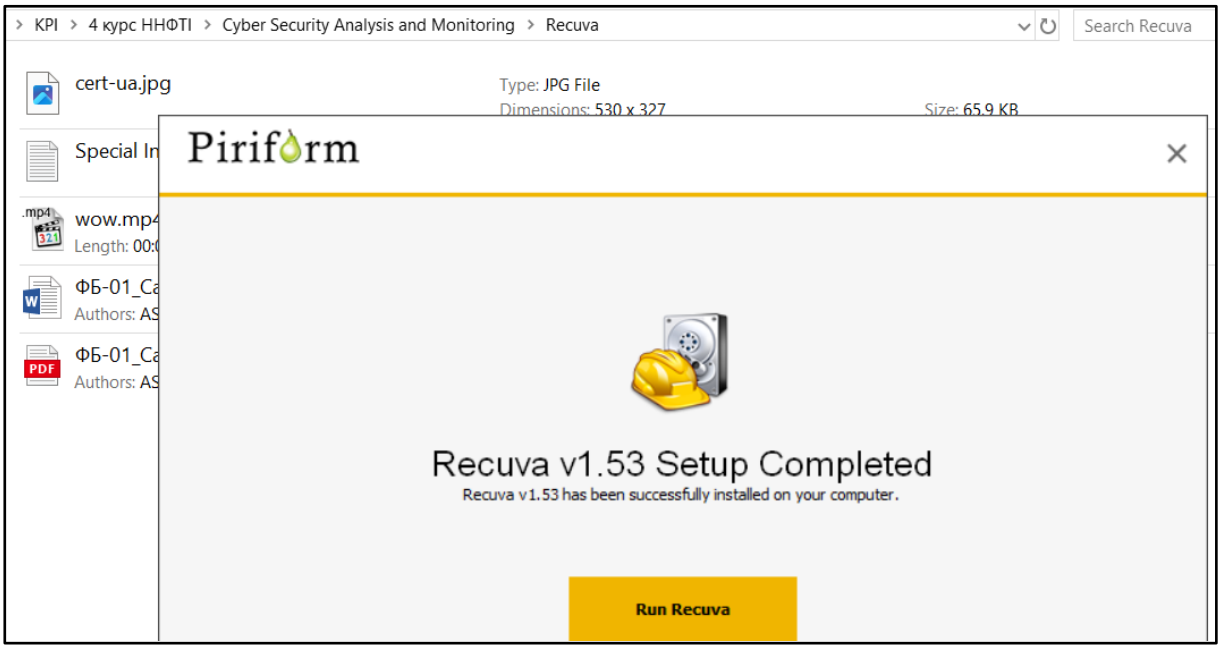


14.Натиснемо на надане посилання HTML і відкрийте його у веб-браузері:

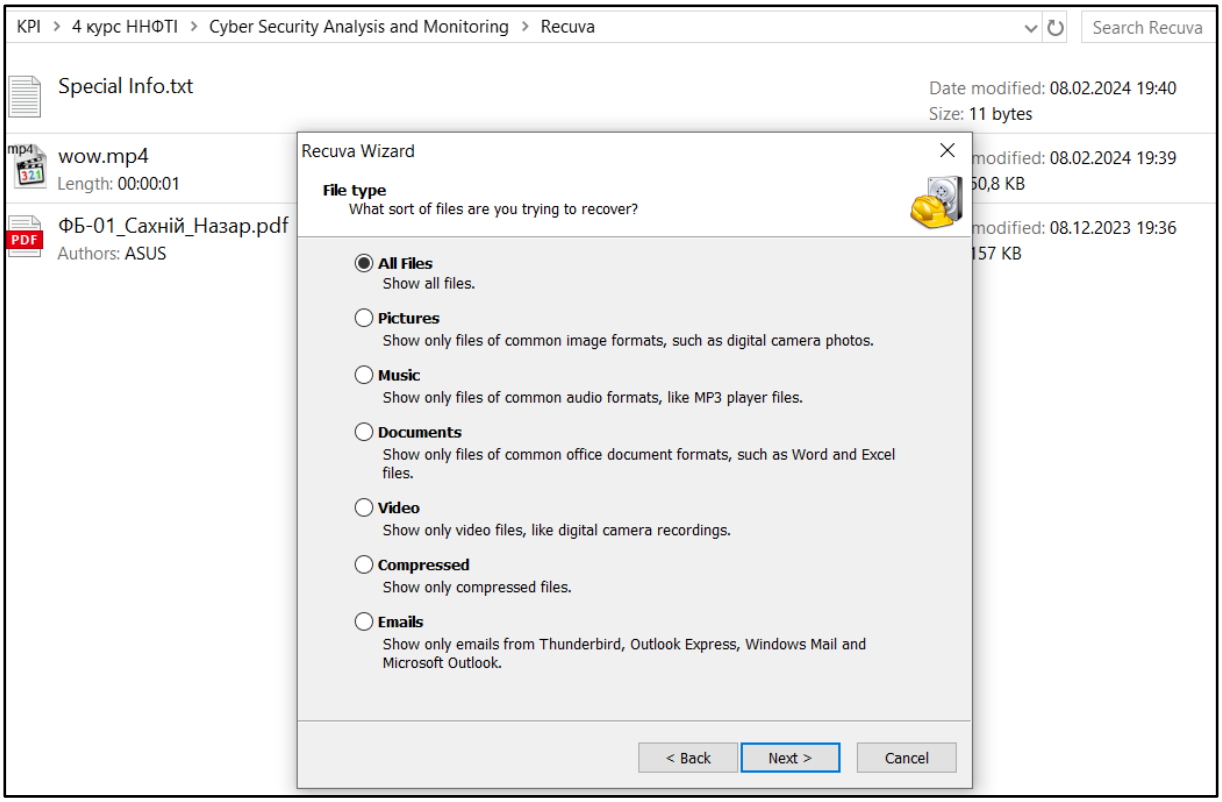


❖ Відновлення видалених файлів за допомогою Recuva

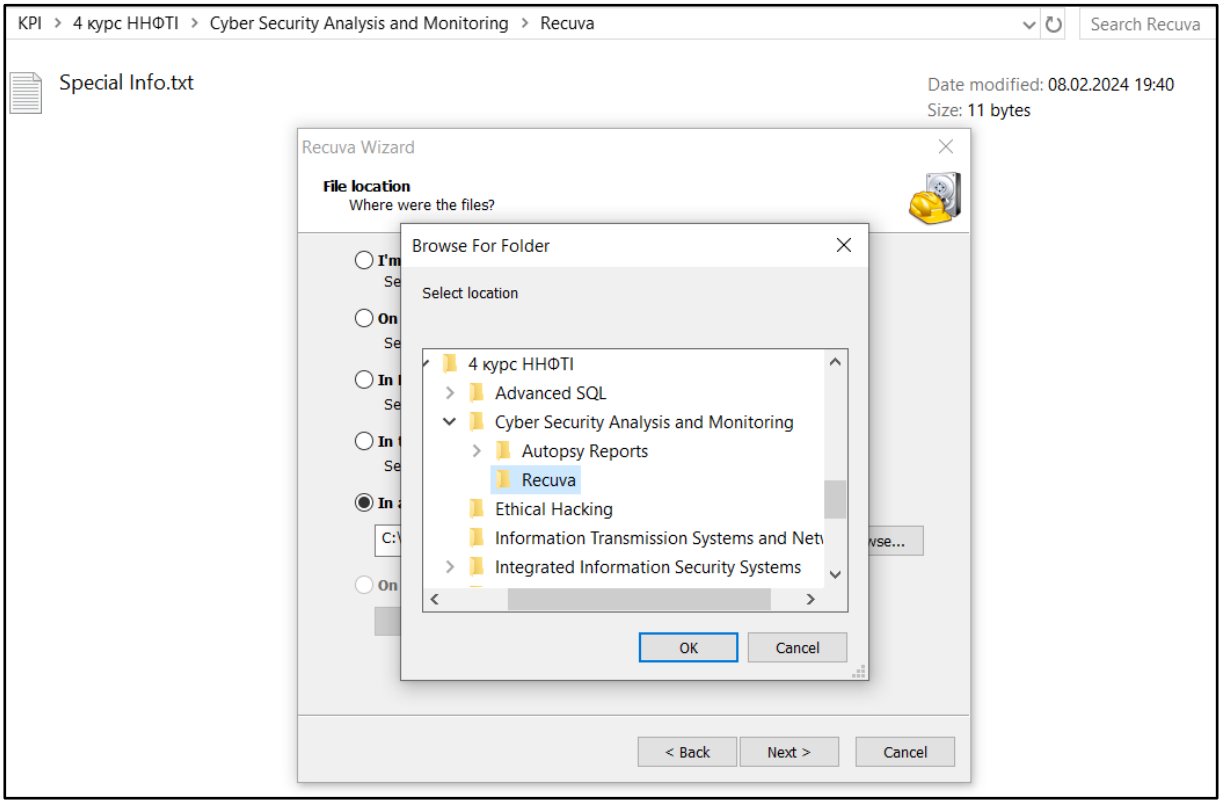
* Для демонстрації попередньо видалимо деякі файли із папки “Recuva/”:



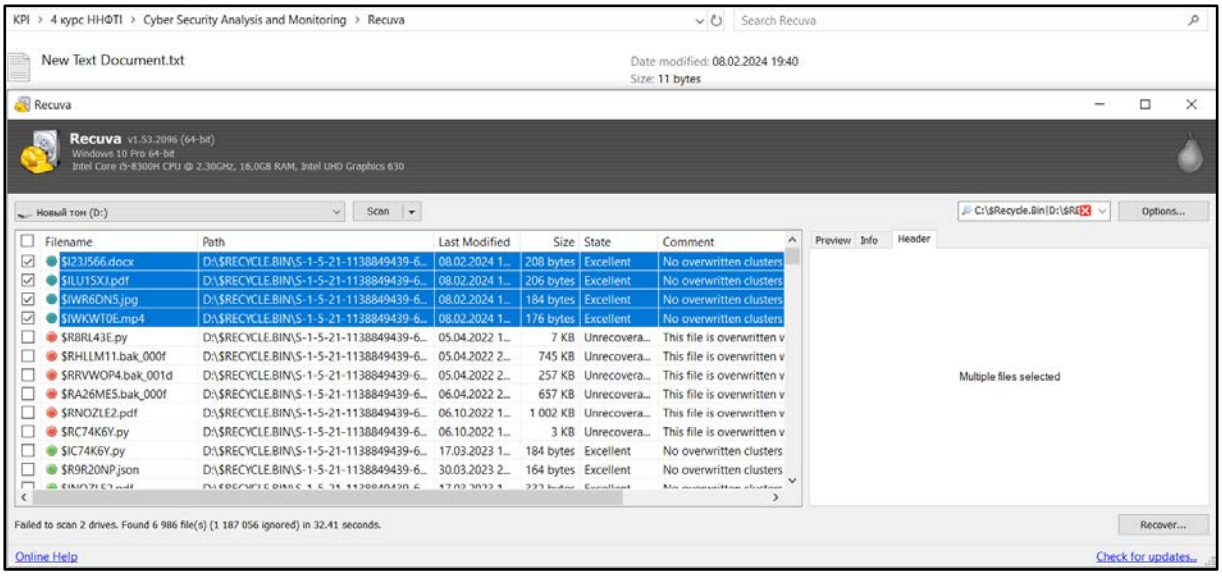
1. Запустимо утиліту і виберемо тип файлів, які потрібно відновити:



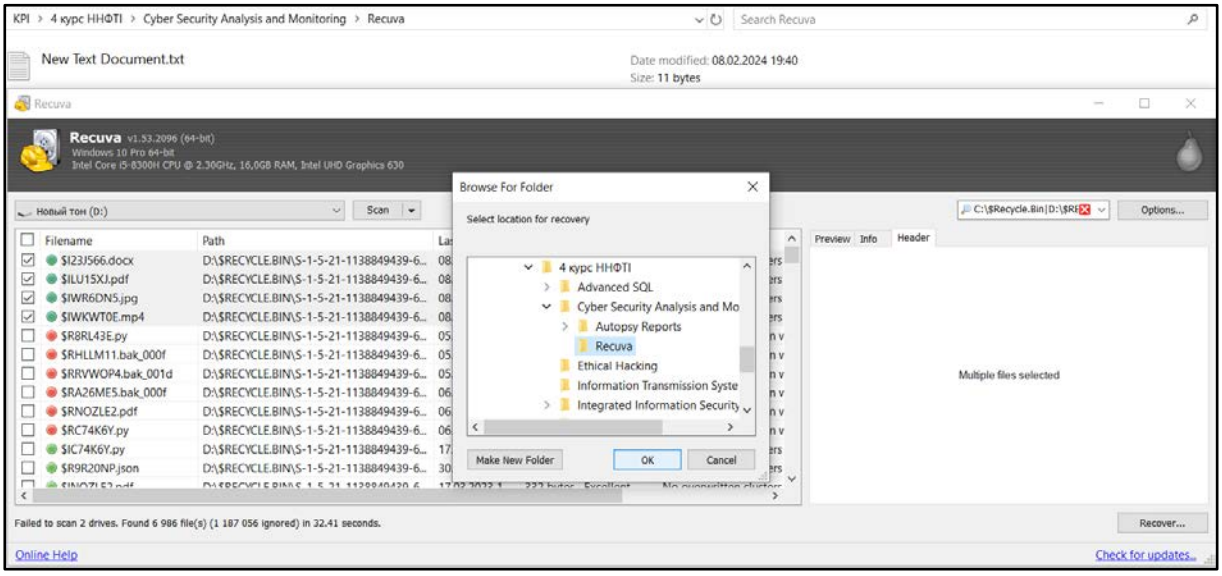
2. Виберемо каталог, де знаходились видалені файли:



3. Виберемо файли, які потрібно «відновити», і натиснемо «Recover»:



4. Вкажемо місце, де ми хочемо зберегти відновлені файли:



5. Переглянемо відновлені файли в каталозі: