ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Рекомендації щодо розслідування кіберінцидентів з використанням Autopsy»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Вікторія САГАЧ
(підпис)

Виконала: здобувачка вищої освіти групи БСД-41
САГАЧ Вікторія
(прізвище, ім'я)

Керівник д.ф., МАРЧЕНКО Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ВСТУП

Актуальність дослідження. У сучасних умовах зростання кількості кіберзагроз розслідування кіберінцидентів набуває особливого значення. Пристрої, зокрема персональні комп'ютери, ноутбуки та мобільні пристрої, є основними засобами обробки, зберігання та передавання інформації. У разі компрометації цих пристроїв можливий витік критичних даних, несанкціонований доступ до корпоративних ресурсів, або зупинка бізнес-процесів.

Одним із ключових інструментів для дослідження інцидентів безпеки та отримання цифрових доказів є Autopsy – програмне забезпечення з відкритим кодом для цифрової криміналістики. Autopsy дозволяє здійснювати аналіз кнцевих точок після інциденту, витягувати цифрові артефакти, зокрема історію браузерів, листування, метадані файлів, видалені об'єкти та іншу критичну інформації, яка може слугувати доказовою базою у кіберрозслідуванні.

У ході розслідування інцидентів безпеки Autopsy забезпечує фахівцям з кібербезпеки структурований підхід до аналізу цифрових носіїв, дозволяючи не лише виявити факти компрометації, а й відтворити повну картину подій. Це робить даний інструмент надзвичайно актуальним у контексті зростаючих вимог до забезпечення інформаційної безпеки в організаціях.

Об'єкт дослідження – розслідування кіберінцидентів.

Предмет дослідження – методи за засоби для розслідування кіберінцидентів на базі Autopsy.

Мета роботи розробити варіант застосування системи цифрової криміналістики на базі Autopsy для виявлення, аналізу та документування інцидентів інформаційної безпеки та розробити рекомендації щодо застосування методів та засобів для розслідування кіберінцидентів.

Наукові завдання:

дослідити сутність проблеми розслідування кіберінцидентів;

проаналізувати основні підходи до розслідування кіберінцидентів;

проаналізувати існуючі інструменти для розслідування кіберінцидентів;

проаналізувати методи та засоби для розслідування кіберінцидентів на базі Autopsy;

розробити рекомендації щодо застосування методів та засобів для розслідування кіберінцидентів;

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів на їх порівняння.

Практичне значення одержаних результатів: розроблення рекомендації щодо застосування методів та засобів для розслідування кіберінцидентів, а також розроблення рекомендації фахівцям з кібербезпеки щодо їх реалізації.

1 АНАЛІЗ ПРОБЛЕМИ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ

1.1. Аналіз сучасних загроз та методів кібератак

У сучасному цифровому світі розслідування кіберінцидентів стало невід'ємною частиною стратегії інформаційної безпеки. Кожна спроба несанкціонованого доступу, витоку даних чи шкідливої активності вимагає швидкої реакції та всебічного аналізу. Саме завдяки грамотному розслідуванню організації можуть виявити джерело інциденту, зменшити шкоду та попередити повторення подібних атак у майбутньому.

Загроза - будь-яка подія або обставина, які можуть негативно вплинути на конфіденційність, цілісність або доступність даних, комп'ютерних систем, мереж чи пристроїв. Перелік інформаційних загроз в наш час дуже широкий і їх список щодня розширюється. Сьогодні ці загрози можна поділити на дві основні групи: внутрішні і зовнішні.

Зовнішні загрози виходять з «зовнішнього світу» (зазвичай з мережі Інтернет), тоді як внутрішні загрози виходять з самої організації. Сьогодні також виділяють ще й деяку «проміжну» групу загроз, які пов'язані з роботою провайдерів послуг. Цими послугами користуються організації, і вони доповнюють її інформаційні ресурси.

Внутрішні загрози. Згідно даних Глобального дослідження тенденцій інформаційної безпеки помітна тенденція зростання внутрішніх загроз від колишніх співробітників компаній. При цьому, серед усіх джерел загроз найбільший приріст (58%) був відзначений у інцидентів, що пов'язані з колишніми постачальниками послуг і сервісів. Незважаючи на це необхідно відзначити, що помітна тенденція спаду кількості інцидентів інформаційної безпеки (ІБ) щодо діючих співробітників. такий немаловажний факт, як витік інформації або її поширення з вини чинного співробітника досі актуальний і передбачається, залишиться таким, поки існує конкуренція і суперництво. Причиною стрімкого

зростання рівня внутрішніх загроз є швидке зростання кількості мобільних пристроїв і популярності хмарних обчислень, що істотно розширює горизонт атак.

З появою принципово нових пристроїв і інфраструктур перед зловмисниками відкриваються нові можливості атак, що використовують непередбачені слабкі місця і погано захищені ресурси. так само, повсюдний доступ з мобільних пристроїв до службової інформації компанії або до інформації, яка може зацікавити конкуруючу сторону, збільшує ризик її розкрадання. Таким чином, компанії збільшуючи зростання безконтрольного застосування мобільних пристроїв для скорочення часу виконання завдань і функцій, збільшують імовірнісний відсоток навмисного розкрадання конфіденційних даних або атаки на внутрішні інформаційні ресурси.

Зовнішні загрози. На практиці зустрічаються різні типи шкідливого програмного забезпечення, використовуваного зловмисниками для отримання доступу до корпоративних мереж. Аналіз наукової літератури показав, що найчастіше зустрічається таке шкідливе програмне забезпечення (ПЗ): рекламне, шпигунське, програми небажаного перенаправлення, експлойти, що використовують iFrame, і програми фішингу.

Список ПЗ можна розглядати як програмні коди, що використовуються для отримання початкового доступу. Це найбільш економічні способи, що дозволяють з легкістю скомпрометувати великі обсяги користувачів. Існує багато різних типів кібератак, кожен з яких має свої унікальні характеристики та цілі. Кібератака - цілеспрямована атака на комп'ютери або комп'ютерні мережі. Деякі з найбільш поширених типів кібератак включають:

1. Віруси – це програми, які можуть заражати комп’ютери та інші пристрої, поширюватися через мережі та завдавати різних видів шкоди, таких як знищення даних, блокування роботи системи та навіть крадіжка конфіденційної інформації. Число вірусів продовжує збільшуватися. Джерелами вірусної загрози є електронна пошта, переважна більшість вірусів проникає за допомогою послань через e-mail.

2. Черв’яки – це програми, які здатні поширюватися самостійно через мережі і заражати безліч комп’ютерів. Вони можуть завдати серйозної шкоди, блокуючи роботу системи та видаляючи файли.

3. Троянські коні – це програми, які можуть маскуватися під звичайні файли та заражати комп’ютери, надаючи зловмисникам віддалений доступ до пристрою та конфіденційної інформації.

4. Фішинг – це атака, яка призначена для отримання конфіденційної інформації, такої як паролі та номери кредитних карток, шляхом обману користувачів та надання їм неправдивої інформації.

5. DDoS-атаки – це атаки, які спрямовані на блокування роботи системи шляхом перевантаження її трафіком, що унеможливлює доступ до ресурсу. Прикладом може бути атака на сайт компанії Twitter в 2016 році, коли ботнет Mirai перевантажив сайт і його сервіси.

6. Атаки на інфраструктуру – це атаки, спрямовані на руйнування фізичної інфраструктури, такої як електронні системи управління транспортом або електроживлення.

Крім того, існують і інші типи кібератак, такі як атаки на мобільні пристрої, атаки на хмарні сховища даних і багато інших. Важливо розуміти, що кожен тип кібератаки має свої унікальні методи та інструменти, і необхідно вжити відповідних заходів захисту, щоб запобігти їх проведенню та захистити свою систему та конфіденційну інформацію [8].

1.2. Аналіз сучасних підходів до цифрової криміналістики

Цифрова криміналістика використовується як у компаніях для розслідувань інцидентів захисту даних, так і в розслідуваннях правоохоронними органами. Відділ поєднує технічну експертизу з аналітичними навичками та надає важливу інформацію для захисту цифрових активів і розуміння динаміки кіберінцидентів.

Цифрова криміналістика вирішує такі завдання: створення методів, апаратних і програмних інструментів для збору та дослідження доказів

комп'ютерних злочинів; розробка тактико-оперативно-розшукових заходів та слідчих дій, пов'язаних із комп'ютерною інформацією; встановлення криміналістичних характеристик правопорушень, пов'язаних із комп'ютерною інформацією.

Основою цифрової криміналістики є її технічна складова, інакше кажучи, засоби і методи техніко-криміналістичного дослідження цифрових доказів. Ця галузь характеризується широким інструментарієм, як комерційним, так і з відкритим кодом. Вона має власний міжнародний стандарт, опублікований у 2012 р. Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC). Згаданий стандарт стосується поводження з цифровими доказами (ISO/IEC 27037 Інформаційні технології – Методи безпеки – Керівництво з ідентифікації, збирання, одержання і збереження свідчень, представлених у цифровій формі) [6]. Він пропонує такі чотири етапи поводження з цифровими доказами:

1. Ідентифікація – передбачає пошук і розпізнання відповідних доказів та їх документування. На цьому етапі пріоритетні завдання збору доказів визначаються на основі цінності й мінливості доказів. Варто звернути увагу, що ідентифікація виступає важливим кроком у процесі цифрової криміналістики, тому що це лише частина більшого, складнішого процесу розслідування;

2. Збирання – передбачає збір усіх необхідних електронних даних із різних джерел, зараховуючи комп'ютери, сервери, мобільні пристрої та інші цифрові носії. Дані збираються за допомогою спеціальних інструментів і методів, що гарантують збереження цілісності та автентичності даних;

3. Отримання. Цифрові докази мають бути отримані без порушення цілісності даних. Для цього робиться копія вмісту цифрового пристрою (процес, відомий як створення неспотвореного образу) з використанням пристрою (блокувальника запису), призначеного для того, щоб гарантувати, що дані не будуть змінені під час процесу копіювання. Для того, щоб визначити, чи є дублікат точною копією оригіналу, значення хеш-функції розраховується з використанням математичних обчислень; у такому випадку для отримання значення хеш-функції

використовується криптографічна хеш-функція. Якщо значення хеш-функції для оригіналу та копії збігаються, це означає, що вміст копії точно відповідає оригіналу;

4. Збереження. Цей етап передбачає захист і збереження електронних доказів, щоб запобігти будь-яким змінам або модифікаціям даних. Процес збереження передбачає створення судово-медичного зображення або копії вихідних даних і збереження копії, щоб забезпечити її незмінність протягом усього розслідування.

Методи цифрової криміналістики включають різні спеціалізовані методи виявлення, аналізу та інтерпретації цифрових доказів. Ці методи включають зворотну стеганографію, стохастичну криміналістику, міждисковий аналіз, аналіз у реальному часі та відновлення видалених файлів.

Стеганографія передбачає приховування інформації в інших, на перший погляд, нешкідливих файлах або даних. Зворотна стеганографія — це процес виявлення та вилучення прихованої інформації з цих файлів. Експерти з цифрової криміналістики використовують різні інструменти та методи для виявлення та відновлення прихованих даних, які можуть бути використані для зловмисних цілей/ Аналізуючи файли носіїв та використовуючи передові алгоритми, зворотна стеганографія допомагає виявляти прихований контент і може допомогти експертам зрозуміти наміри та дії кіберзлочинців.

Стохастична криміналістика використовує статистичні та ймовірнісні методи для аналізу цифрових доказів. Цей метод враховує притаманну цифровим артефактам небезпеку через такі фактори, як шифрування, пошкодження даних та змінні структури даних. Стохастичні моделі можуть оцінювати ймовірність настання певних подій, допомагати у реконструкції подій та підвищувати точність висновків, зроблених під час розслідування. Ці моделі особливо корисні в сценаріях, коли точна послідовність подій неясна або коли традиційні детерміністичні підходи недостатні.

Кросс-дисковий аналіз аналізує та порівнює дані на кількох пристроях зберігання даних. Цей метод дозволяє судово-медичним слідчим виявляти зв'язки, взаємозв'язки або закономірності між різними пристроями, які можуть бути

пов'язані з певною справою. Зіставляючи інформацію з різних джерел, перехресний аналіз даних може виявити приховані зв'язки між людьми, групами чи видами діяльності. Цей метод особливо ефективний, коли йдеться про організовану кіберзлочинність або спільну шкідливу діяльність, поширену на кількох пристроях.

Аналіз у реальному часі передбачає вивчення системи під час її роботи. Цей метод вимагає спеціальних інструментів та досвіду для вилучення летких даних, таких як запущені процеси, мережеві підключення та відкриті файли, з активної системи без шкоди для її функціональності. Аналітика в реальному часі часто використовується, коли збереження нестабільних даних є критично важливим, оскільки відключення системи може призвести до їх втрати. Цей аналіз може надати уявлення про поточні кібератаки, підозрілу активність або наявність шкідливого програмного забезпечення, які можуть бути не очевидними під час традиційного аналізу після інциденту.

Відновлення видалених файлів описує процес відновлення файлів, які були навмисно або випадково видалені з пристрою зберігання даних. Навіть якщо файли здаються видаленими, сліди їхнього існування часто залишаються на носіях інформації, доки їх не перезапишуть. Для виявлення цих залишків можна використовувати судово-медичні інструменти та методи, щоб слідчі могли отримати важливі докази, які могли бути приховані злочинцями. Відновлення видалених файлів важливе, коли підозрювані намагалися замести сліди, оскільки це може дати цінну інформацію про їхню діяльність та наміри.

Інші джерела виділяють такі напрями сучасної цифрової криміналістики: 1) дослідження застосунків (месенджерів та інших застосунків для смартфонів, що використовуються для обміну інформацією); 2) дослідження хмарних сховищ; 3) дослідження мобільних пристроїв (телефонів); 4) дослідження інтернет-речей (IoT); 5) дослідження новітніх пристроїв та застосунків (Alexa від Amazon, Google Assistant, Siri від Apple); 6) дослідження мереж; 7) цифровий аналіз поведінки окремих осіб, груп людей та їхніх стосунків і взаємовідносин; 8) дослідження застосунків, що не призначені для використання іншими особами; 9) мережеві

дослідження; 10) цифрова криміналістична розвідка та розвідка на основі відкритих джерел [7].

1.3. Аналіз існуючих рішень для цифрової криміналістики

На початку 90-х років, дослідження проводились наживо в реальному часі, використання дослідного пристрою здійснювалось без будь-яких засобів захисту даних. Зі змінами інформаційних технологій, з'явилась тенденція до зменшення пристроїв зберігання інформації, а інформаційний простір накопичувачів збільшувався. З часом використання пристроїв наповнених величезною кількістю інформації, зробило криміналістичний аналіз даних наживо, неефективним. Час потребував нових засобів дослідження даних, що спонукало експертів та фахівців з кібербезпеки, розробляти нові аналітичні програмні засоби з відкритим кодом, що давали можливість використання їх у розслідуваннях, не змінюючи інформаційної структури дослідних носіїв, здобувати цифрові докази. Також на комерційному ринку почали з'являтися програмні та апаратні засоби забезпечення розслідування кіберзлочинів. Шляхом таких розробок, що поєднали загальні методи криміналістики з новими сучасними цифровими методами відстеження, відновлення, фіксування даних, що об'єднали цифрове віртуальне середовище з фактичною об'єктивною реальністю та дають можливість збирати артефакти та за сукупності логічних складових яких, можна довести факт кіберзлочину.

Найпопулярніші цифрові криміналістичні інструменти з відкритим кодом, які охоплюють багато реалізацій процесів з оптимальним часом здобування артефактів, розробниками групуються та інтегруються у динамічні портативні дистрибутиви операційних систем (Linux, Unix, Mac), що вміщуються у повному зліпку файлів та налаштувань цієї самої системи, розміщені у файл образ (ISO), або містяться у дистрибутивах, що інсталюються в існуючі операційні системи, як окремі програми та утілити.

Форензика як окрема сфера послуг та продуктів – відносно нове явище. Проте вже зараз сформувалися основні лідери ринку, які добре зарекомендували себе як

експерти та розробники ПЗ з форензики. Зокрема, привертають увагу такі продукти:

- Autopsy.
- Forensic Toolkit (FTK) Imager.
- Wireshark.
- Volatility Framework.
- Velociraptor.

Autopsy [1] – це платформа цифрової криміналістики та графічний інтерфейс для різних цифрових криміналістичних інструментів від компанії Basis Technology. Платформа з відкритим вихідним кодом швидка, проста у використанні та здатна аналізувати всі типи мобільних пристроїв та цифрових носіїв (рис. 1.1).

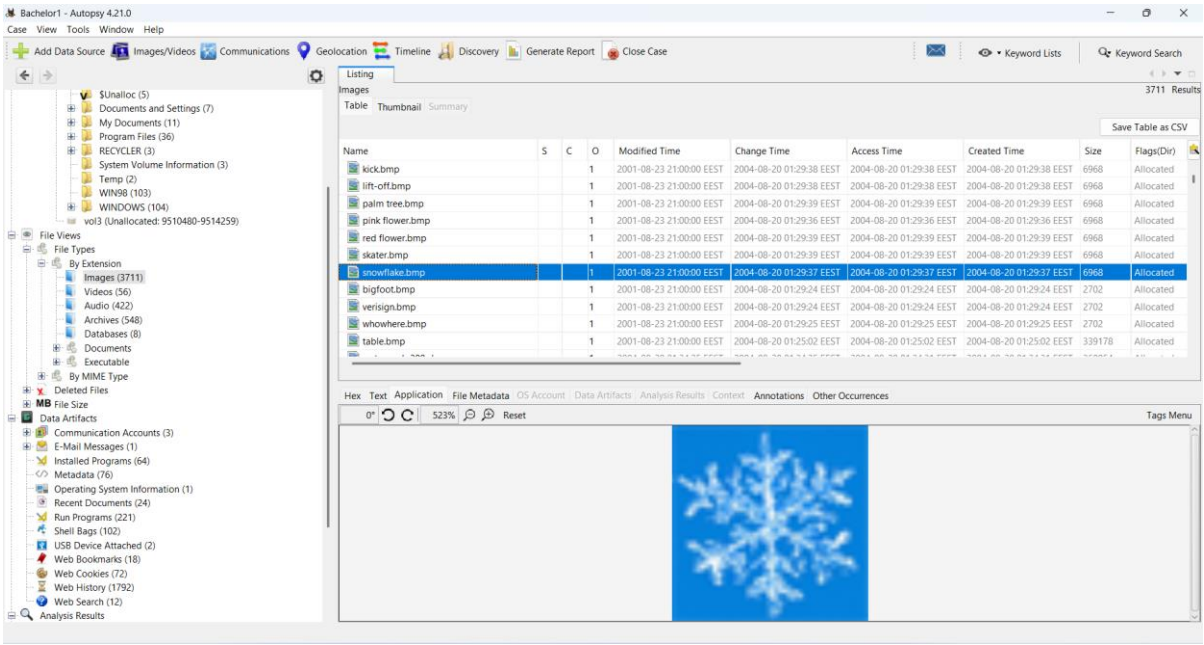

Рис. 1.1. Інтерфейс програми Autopsy

Програма призначена для дослідження доказів з кіберзлочинів, проте має також великий спектр функцій для відновлення та аналізу даних.

Переваги:

- безкоштовна платформа з відкритим кодом для комплексної цифрової криміналістики;
- підтримує різні методи аналізу файлових систем та обробки даних;
- генерує звіти для ефективного документування справ.

Недоліки:

- набір функцій може бути приголомшливим для початківців;
- продуктивність може бути повільнішою на машинах з обмеженими ресурсами.

Forensic Toolkit (FTK) Imager [2] - ретельно створює образи дисків для судово-медичної експертизи, забезпечуючи збереження цілісності доказів протягом усього розслідування (рис. 1.2).

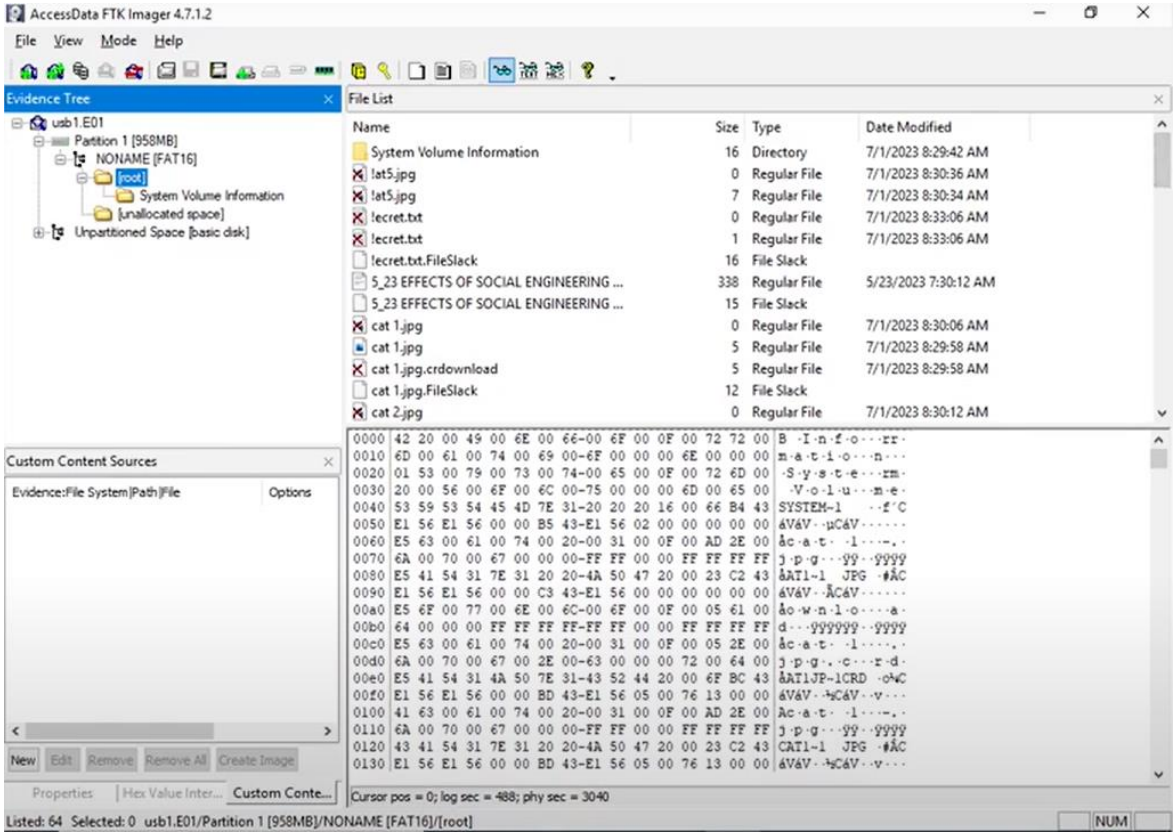

Рис. 1.2. Інтерфейс Forensic Toolkit (FTK) Imager

Плюси:

- створює образи дисків для судово-медичної експертизи, зберігаючи цілісність даних;
- пропонує функції для хешування та перевірки автентичності зображень.

Мінуси:

- комерційний інструмент з платною ліцензією;
- багатофункціональні інтерфейси можуть мати крутішу криву навчання для нових користувачів.

Wireshark [3] - глибокий аналізатор пакетів, що забезпечує мікроскопічне уявлення про мережевий трафік, аналізуючи протоколи та виявляючи складні деталі даних, що передаються мережею (рис. 1.3).

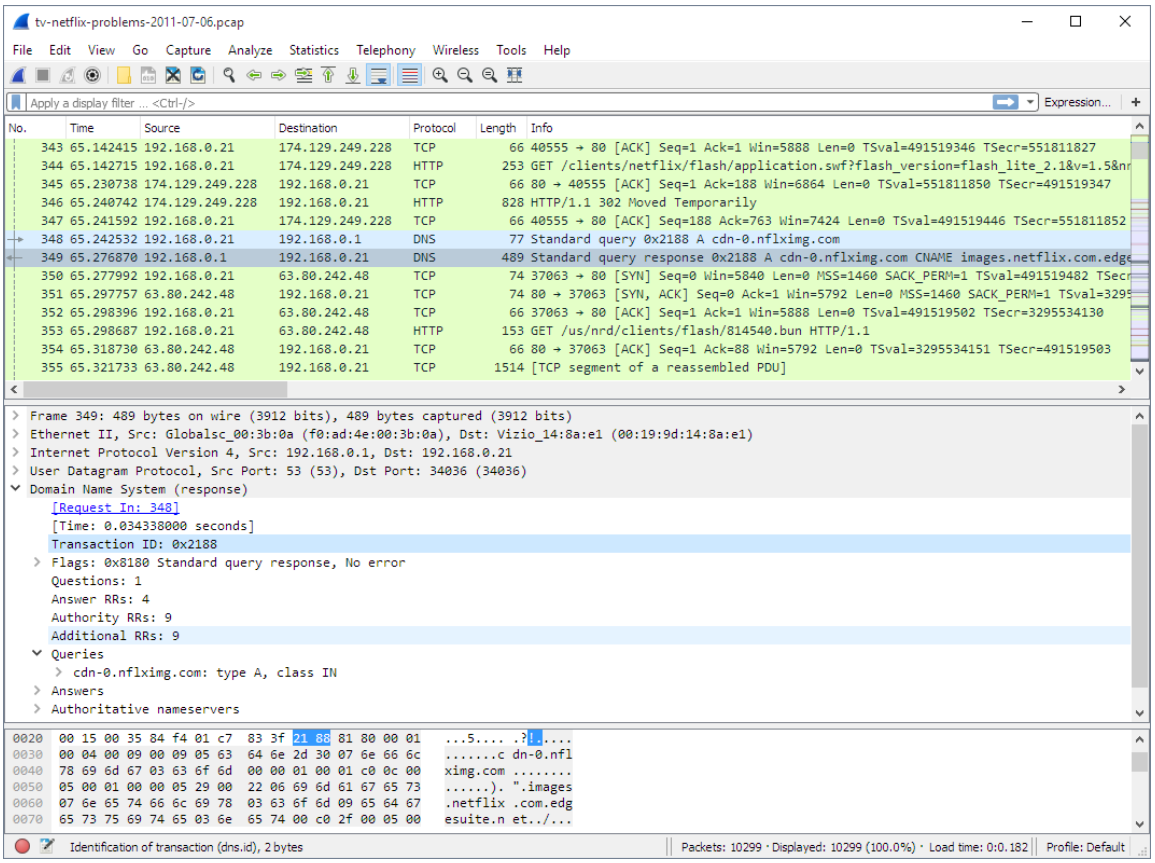

Рис. 1.3. Інтерфейс програми Wireshark

Плюси:

- стандартний інструмент для глибокого аналізу мережевих пакетів;
- розшифровує різні протоколи, надаючи детальну інформацію про мережевий трафік.

Мінуси:

- складне навчання через складність мережевих протоколів;
- можливості захоплення в реальному часі вимагають високого рівня знань про мережу.

Volatility Framework [4] дозволяє слідчим аналізувати оперативну пам’ять комп’ютера, скарбницю швидкоплинних даних, навіть якщо система була

вимкнена. Volatility може виявити процеси, завантажені драйвери та мережеві з’єднання, надаючи знімок стану системи в певний момент часу (рис. 1.4).

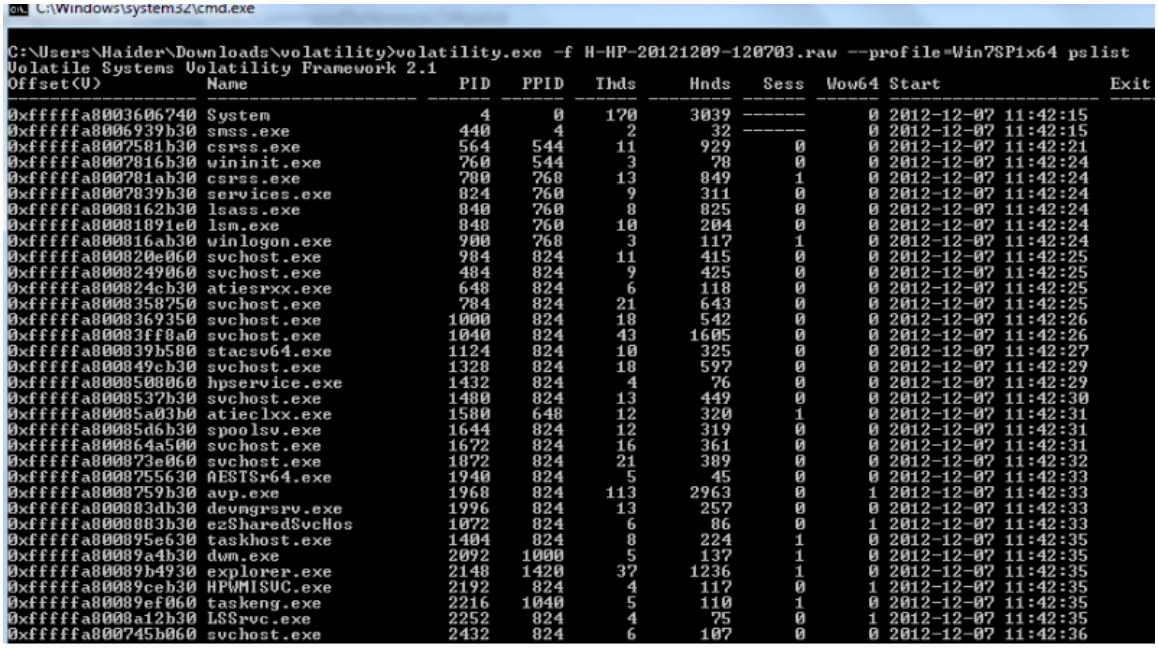

Рис. 1.4. Інтерфейс програми Volatility Framework

Плюси:

- аналізує енергозалежну пам'ять, виявляючи швидкоплинні дані навіть після вимкнення системи;
- безкоштовно та з відкритим вихідним кодом.

Мінуси:

- потрібне знайомство з інтерфейсом командного рядка;
- обмежені можливості графічного інтерфейсу користувача (GUI) можуть ускладнити виконання складних завдань для початківців.

Velociraptor [5] — це вдосконалений цифровий інструмент криміналістики та реагування на інциденти, який покращує видимість кінцевих точок. Дозволяє групам реагування на інциденти швидко збирати та досліджувати артефакти по всій мережі, а також надавати криміналістичні дані після інциденту безпеки (рис. 1.5).

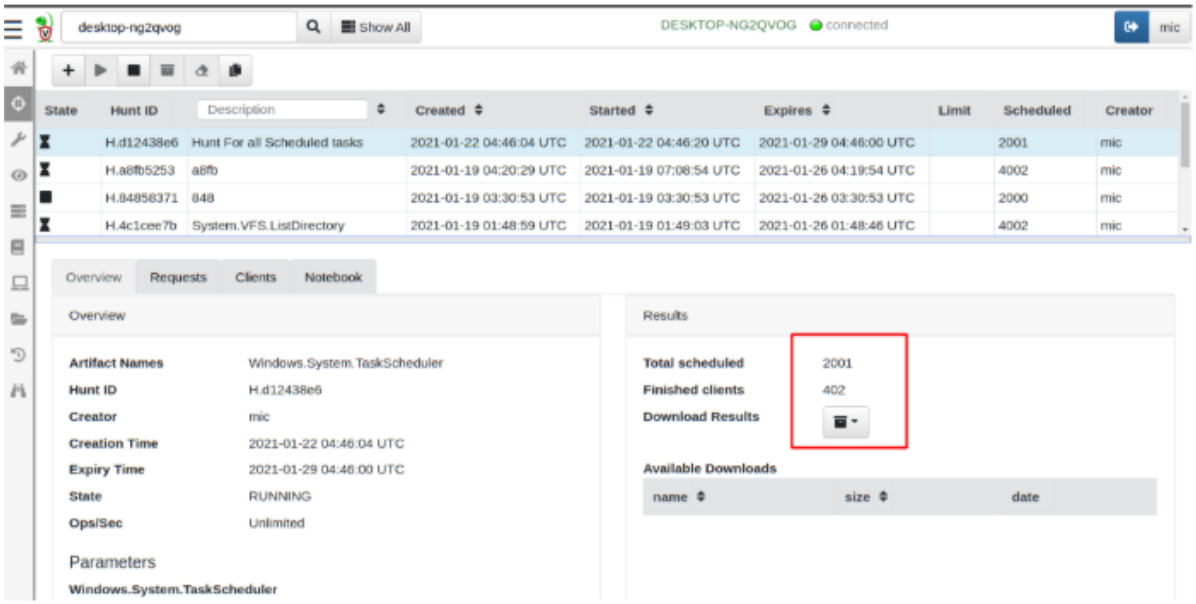

Рис. 1.5. Інтерфейс програми Velociraptor

Переваги:

- відкритий код;
- збирає артефакти з багатьох систем у мережі;
- можна проводити аналіз без вилученого жорсткого диска.

Недоліки:

- складна для новачків специфічна мова запитів.

Взагалі існує дуже багато інструментів, які використовуються в цифровій криміналістиці. З їх допомогою спеціалісти можуть монітори хости, збирати артефакти, працювати з реєстром, журналами, з пам’яттю, образами системи та метаданими. Кожен спеціаліст, або організація самостійно повинна обирати інструментарій для розслідування кіберінцидентів в залежності від потреб та ресурсів.

Отже, розглянуто сучасні загрози у сфері кібербезпеки та проаналізовано сучасні підходи до цифрової криміналістики, яка дозволяє виявляти, зберігати та аналізувати цифрові докази після кіберінцидентів. Крім того, проведено огляд популярних інструментів цифрової криміналістики, зокрема Autopsy, Wireshark? Velociraptor та інші. Було визначено їх переваги та недоліки.

Цей розділ створює базу для кращого розуміння проблем і рішень у сфері цифрового розслідування та підкреслює важливість використання спеціалізованих інструментів у боротьбі з кіберзагрозами.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ НА БАЗІ AUTOPSY

2.1. Архітектура та компоненти Autopsy

Autopsy – це платформа цифрової криміналістики та графічний інтерфейс для різних цифрових криміналістичних інструментів від компанії Basis Technology. Платформа з відкритим вихідним кодом швидка, проста у використанні та здатна аналізувати всі типи мобільних пристроїв та цифрових носіїв. Програмне забезпечення є вільним у розповсюдженні, для встановлення на Windows використовується інсталятор msi, підтримується Linux та MacOS.

Інтерфейс має просту структуру (рис. 2.1):

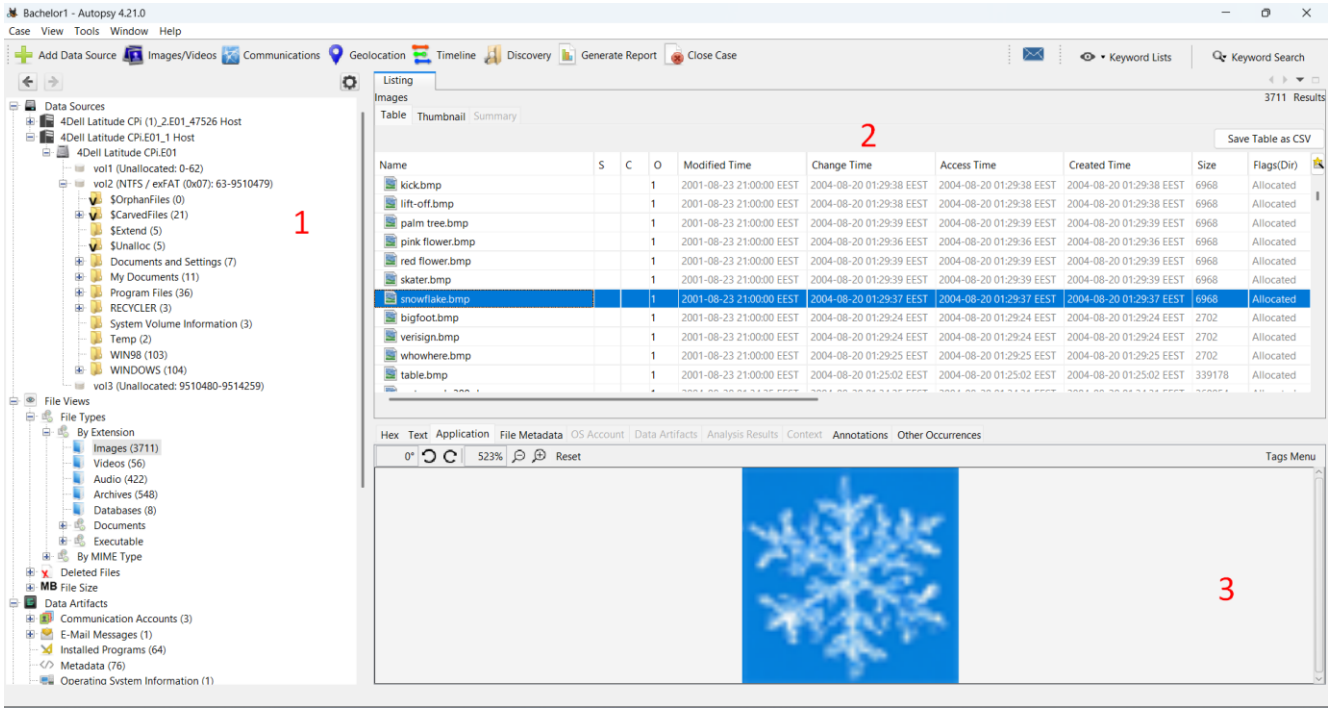

Рис. 2.1 Інтерфейс програми Autopsy

1. Це Вікно дерева результатів роботи модулів. Тут представлені загальні результати того, що було знайдено і дані розбиті на відповідні категорії. Є можливість розгортати потрібні гілки для більш детального розуміння результатів.

2. Вікно огляду результатів. Обравши у гільці результатів певну папку можемо побачити її вміст.

3. Вікно даних. Дає можливість побачити детальнішу інформацію про обрану папку, або файл з цієї папки, наприклад метадані, зображення (для фото), хеш та інше.

Дерево результату має таку структуру (рис. 2.2):

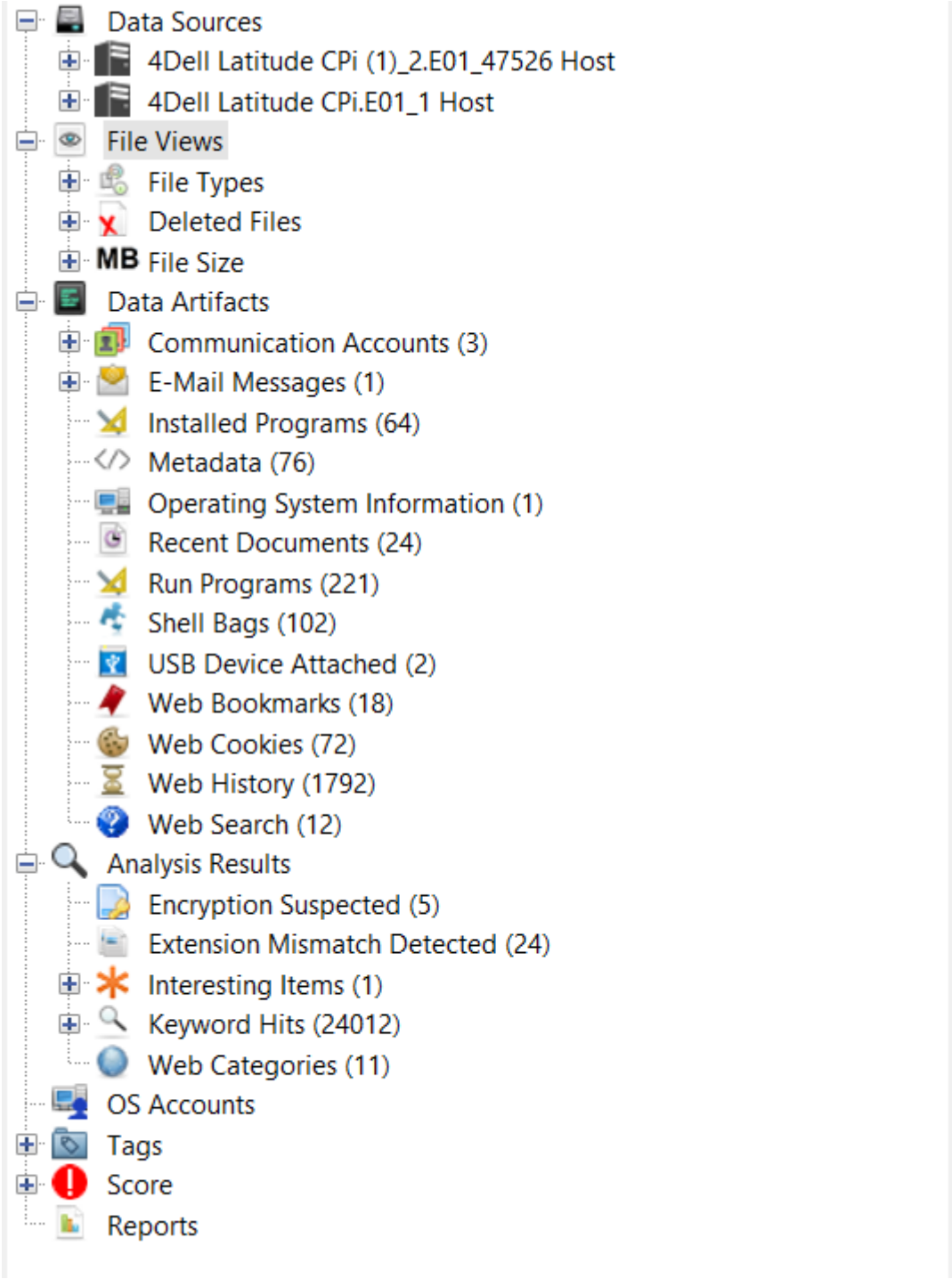

Рис. 2.2. Дерево результату

В розділі Data Sources відображені всі диски, які були додані для аналізу та папки на цих дисках.

В розділі File Views присутні три підрозділи: File Types. Тут знайдені файли сортуються в залежності від типу. Є два поділки: з розширення (зображення, відео, аудіо, архіви, бази даних) та MIME.

Deleted Files. Тут файли, які були виявлені як віддалені.

MB File Size. Тут файли сортуються в залежності від розміру.

Якщо у вікні огляду вибрати закладку Thumbnail, можна переглядати мініатюри знайдених файлів.

В розділі Data Artifacts зібрані знайдені сліди активності користувачів. У тому числі дані операційної системи, веб-активність у вигляді закладок, кукісів, історії пошуку та відвідування сайтів. Також сюди будуть додані знайдені акаунти та адреси електронних пошт, та листи якщо такі будуть знайдені.

Розділ Analysis Results. Тут зібрані результати роботи деяких модулів на які Autopsy вважає, що потрібно звернути увагу.

Наприклад, у розділі Encryption Detected зібрані файли, які були розпізнані як захищені. До таких належать, наприклад, запаролені архіви або офісні документи, а також зашифровані розділи диска. Вибравши потрібний файл у списку, у вкладці Analysis Results можна переглянути причину додавання файлів до цього списку.

У розділі Extension Mismatch Detector показані результати роботи однойменного модуля, він шукає файли, у яких розширення не відповідає типу файла. Тобто, наприклад, якщо аудіо-файл змінити на розширення txt, модуль це визначить. У списку файлів показаний сам файл і те, як він розпізнаний модулем.

У розділі Interesting Files буде показано все те, що знайшов модуль Interesting Files Identifier. Результат залежить від того, які набори правил були додані.

Розділ Keyword Hits. Це знайдені збіги для пошуку за ключовими словами. Сюди потрапляє все те, що було знайдено за заданими словниками, при включенні модуля Keyword Search. Пошук здійснюється у тому числі і за вмістом документа.

Шукати можна як на повний збіг, так і використовуючи регулярні вирази. Крім стандартних словників, можна створювати власні під конкретну ситуацію.

2.2. Призначення та основні функції модулів Autopsy

Autopsy може використовуватися як для банального відновлення даних, так і для проведення розслідувань інцидентів інформаційної безпеки, збору доказової бази. Інструмент використовується правоохоронними органами, військовими та корпоративними експертами для розслідування того, що сталося на комп'ютері [9].

Як зазначалось раніше, Autopsy використовує певні модулі (тобто інструменти) для проведення аналізу. Деякі з них працюють автоматично, деякі вимагають додаткового налаштування або параметрів. Чим більше модулів обирається, тим довше триватиме процес аналізу:

Recent Activity – модуль який визначає нещодавні дії користувача. Він отримує дані операційної системи, а також інформацію про останні дії користувача, включаючи інформації з веб-браузерів (закладки, історія завантажень, сайтів, що відвідувались). Також може отримати інформацію про встановлені програми і які зовнішні пристрої підключались до комп’ютера.

Hush lookup – допоможе виявити «хороші файли» (в основному це файли операційної системи), «погані файли» (наприклад з шкідливих програмним забезпеченням) та «невідомі файли» (це ті які не потрапили ні в одну з інших категорій). Цей модуль потребує додаткового налаштування, а саме, треба завантажити та додати базу даних хешей, з допомогою якої і працює модуль (виявляє хеш-суму для файлів та порівнює з базою даних).

File Type Identification – ідентифікує тип файлу.

Extension Mismatch Detector – шукає файли тип яких не відповідає типу файлу.

Embedded File Extractor – відкриває архіви.

Picture Analyzer – аналізує зображення та виводить метадані.

Keyword Search – модуль пошуку за ключовими словами. Для його роботи потрібні словники, але в самій програмі присутні налаштовані на пошук телефонних номерів, IP адрес, адрес електронної пошти, посилань та номерів банківських карток.

Email Parser – ідентифікує файли електронних повідомлень, а також отримує вкладені файли.

Encryption Detection – шукає зашифровані файли.

Interesting Files Identifier – шукає цікаві файли (пошук файлів хмарних сховищ, пошук файлів криптогаманців та інше) шукає за допомогою правил.

PhotoRec Carver – якщо є не розподілене середовище то знайде файли які там були та спробує відновити.

Virtual Machine Extractor – шукає файли віртуальних машин.

Plaso – аналізує файли, щоб знайти часові мітки і побудувати таймлайни всіх подій в системі.

GPX Parser - цей модуль шукатиме файли GPX і витягуватиме з них дані GPS. GPX — це формат обміну даними GPS між програмами та веб-службами.

Android Analyzer – може аналізувати файли дампа з пристрою Android. Виймає контакти, списки дзвінків, повідомлення та дані GPS із браузера та карт.

У верхній частині вікна програми є кнопки, які якраз і дають додаткові можливості (рис. 2.3):

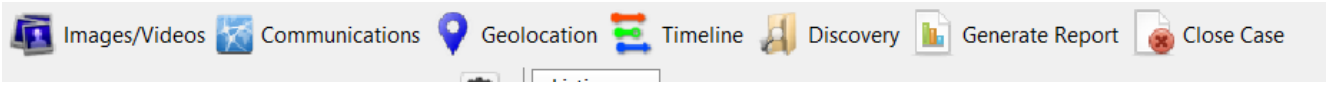

Рис. 2.3. Додаткові функції

Image/Videos - це модуль для роботи з галереями зображень. При запуску цей модуль згрупує всі знайдені фото та відео файли в одну галерею, а також у дереві каталогів позначить ті, у яких було знайдено файли.

Communications модуль візуалізації комунікацій відображає знайдені засоби спілкування, такі електронні пошти та телефони.

Geolocation. Якщо в ході аналізу з будь-яких файлів вдалося отримати дані геолокації, то ця інформація буде додано в цей модуль. Включивши який, можна побачити на карті позначки отриманих координат. Натиснувши на одну з позначок, можна переглянути докладну інформацію.

Timeline - це графічний інструмент вивчення активностей, що показує, коли і які події відбулися в системі.

- червоний – це дії файлової системи;
- зелений - Інтернет активність;
- бірюзовий - все інше, наприклад дії додатків.

Discovery це модуль пошуку зображень, відео, документів або доменів за заданими параметрами.

Autopsy дозволяє створювати дослідникам додаткові типи звітів за допомогою останнього модулю Generate Report. Під замовчуванням доступні звіти в файлах HTML, XLS і Body (рис. 2.4). Слідчі можуть згенерувати більш ніж один звіт за раз, а також редагувати існуючі або створювати нові модулі для настройки поведінки під їх специфічні потреби.

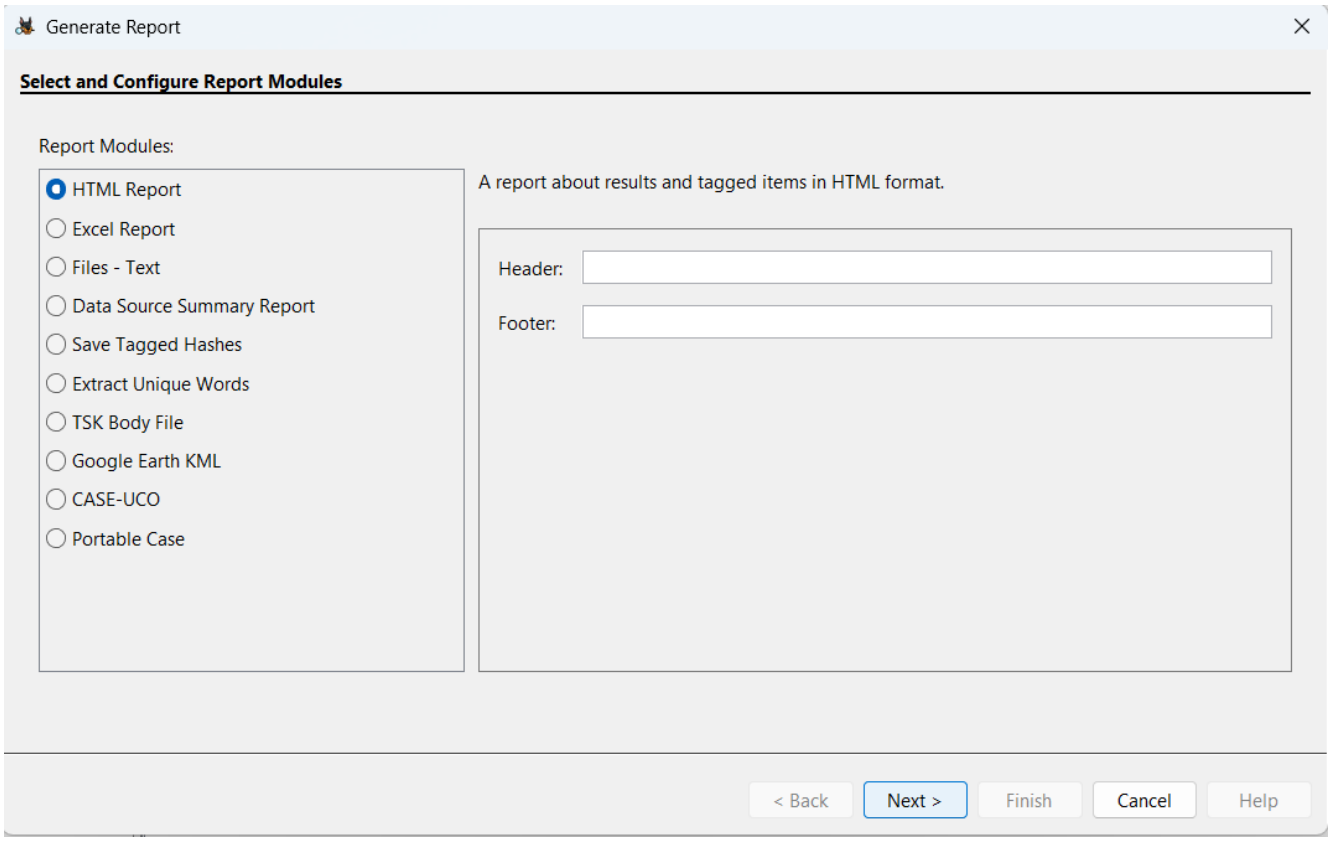

Рис. 2.4. Генерування звіту

Autopsy аналізує образи дисків, локальні диски або папки з локальними файлами. Образи дисків можуть бути як в dd, так і в E01 форматі (рис. 2.5):

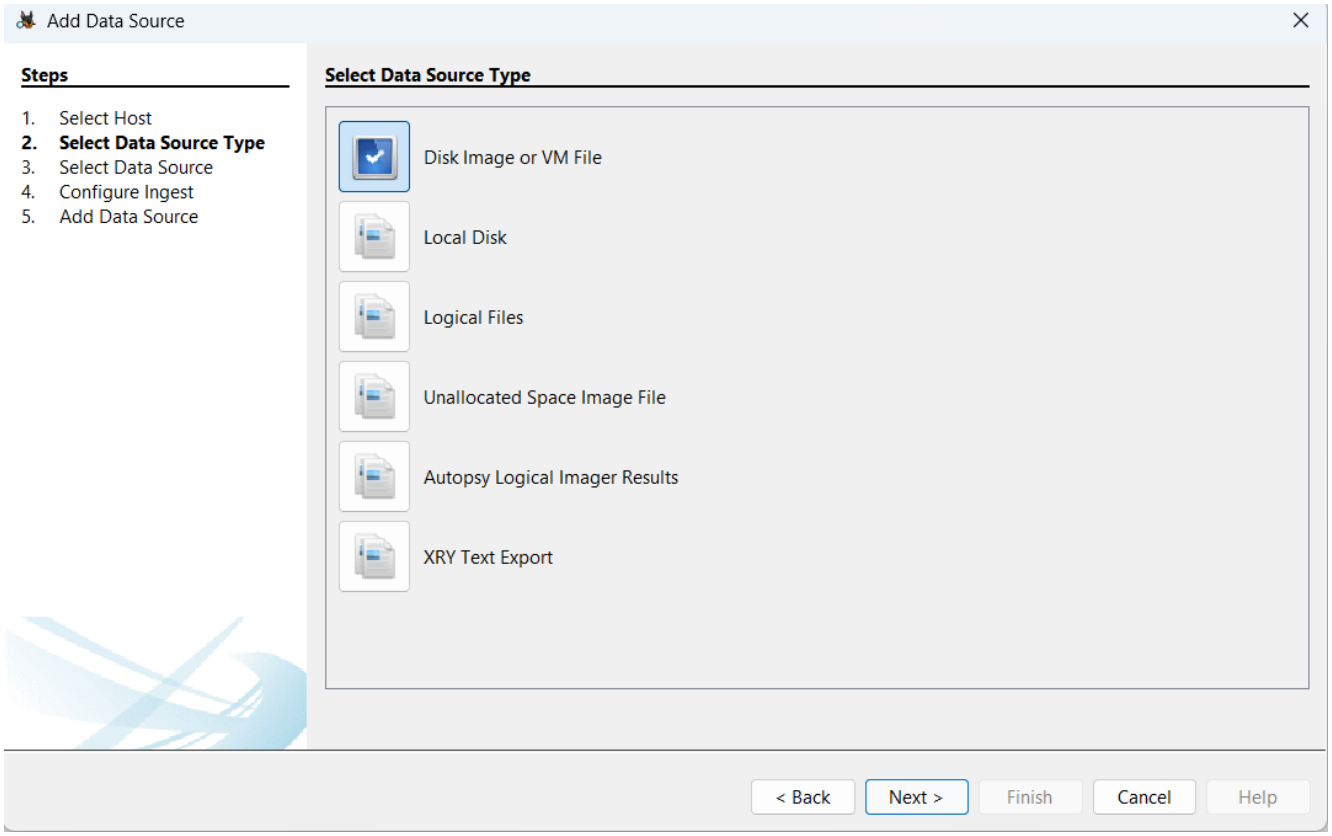

Рис. 2.5. Тип зберігання даних

2.3. Процес використання Autopsy для розслідування кіберінцидентів

Розслідування кіберінцидентів за допомогою Autopsy відбувається за декілька кроків:

1. Перш за все інструмент потрібно інсталювати. Для цього потрібно скористатися посиланням [1], щоб завантажити з офіційного сайту останню версію, яка може включати в себе більшу кількість модулів для розслідування.

2. Після завантаження, відкрити інструмент та створити новий кейс для розслідування (рис. 2.6).

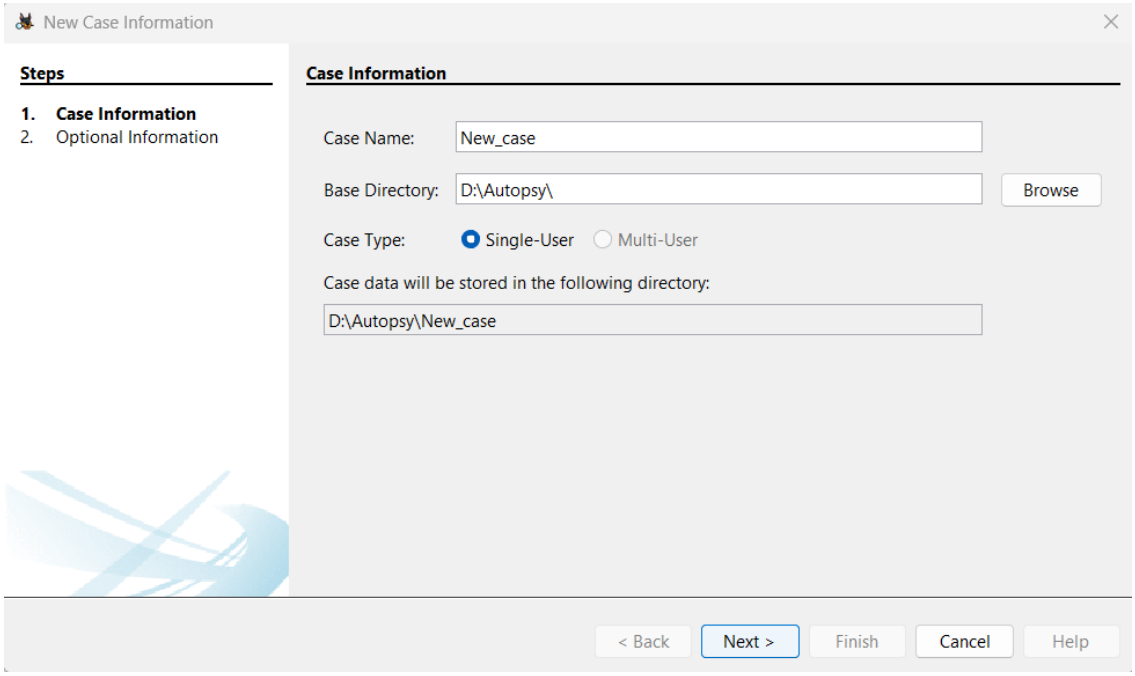

Рис. 2.6. Створення нового кейсу

3. Дати назву кейсу, обрати потрібну директорію для зберігання та вказуємо номер розслідування, контакти аналітика та організацію для якої проводимо розслідування (рис. 2.7)

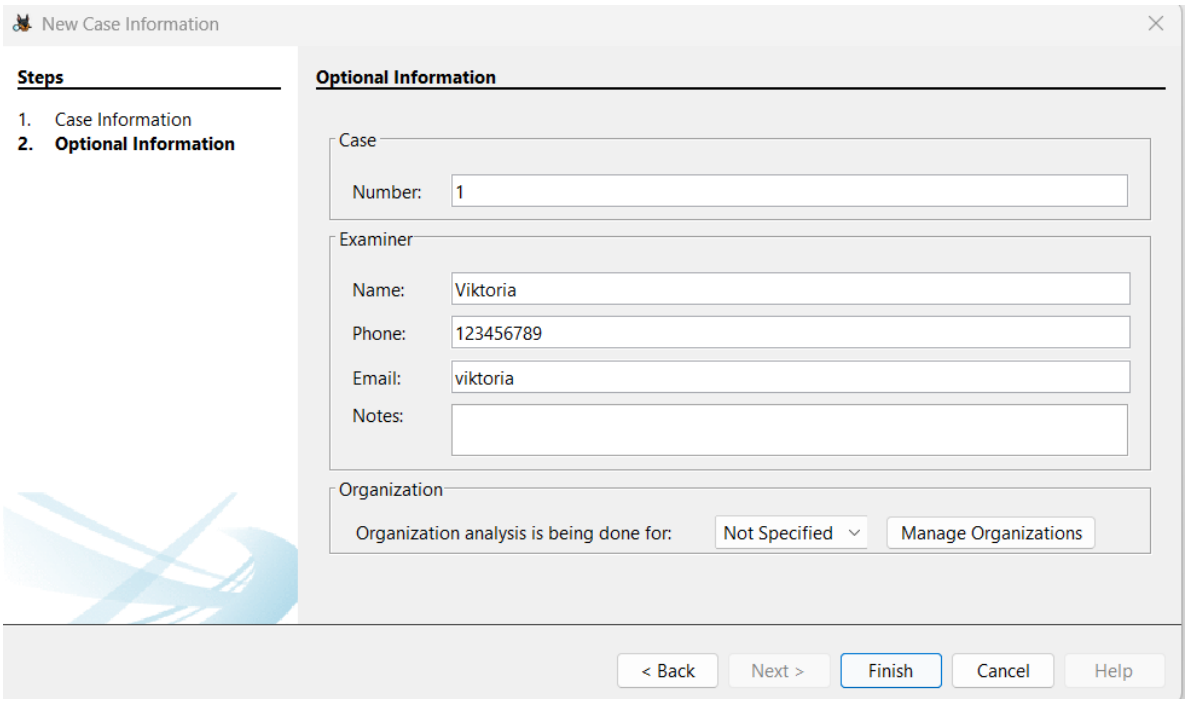

Рис. 2.7. Додаткова інформація

4. Обрати тип джерела даних (рис. 2.8) на якому потрібно провести розслідування (образ диску, локальний диск, файли), встановити відповідний часовий пояс та завантажити обране раніше джерело даних (рис. 2.9).

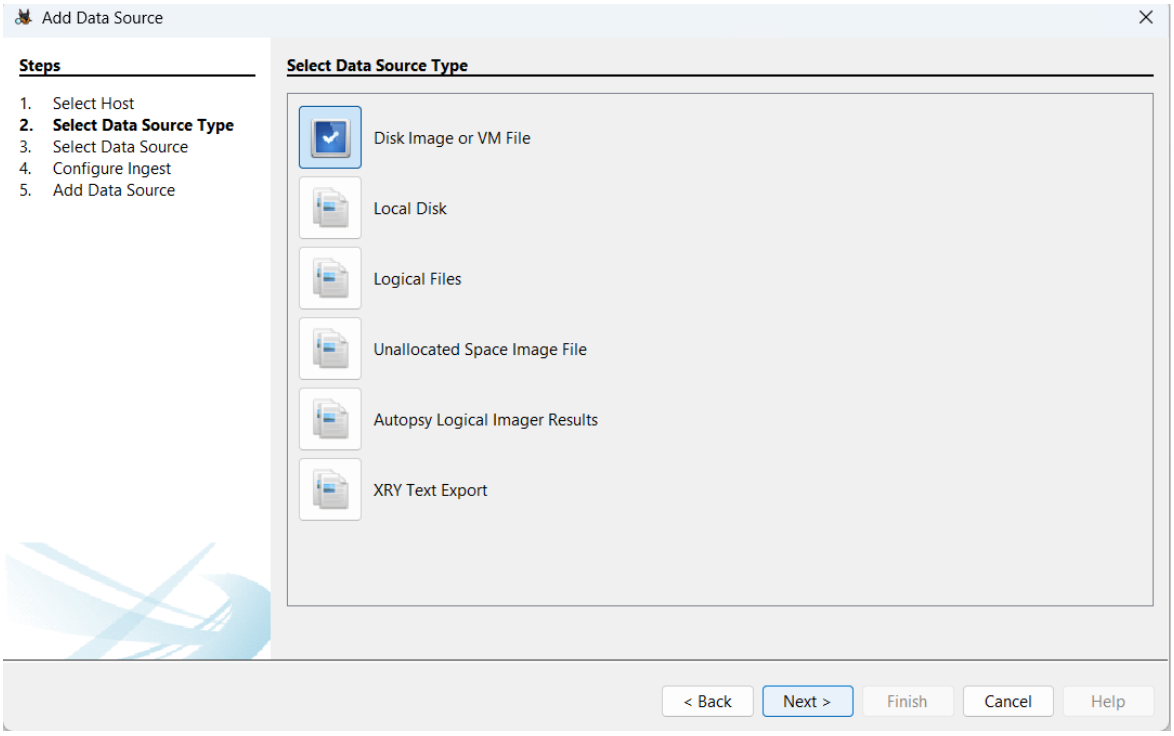

Рис. 2.8. Тип джерела даних

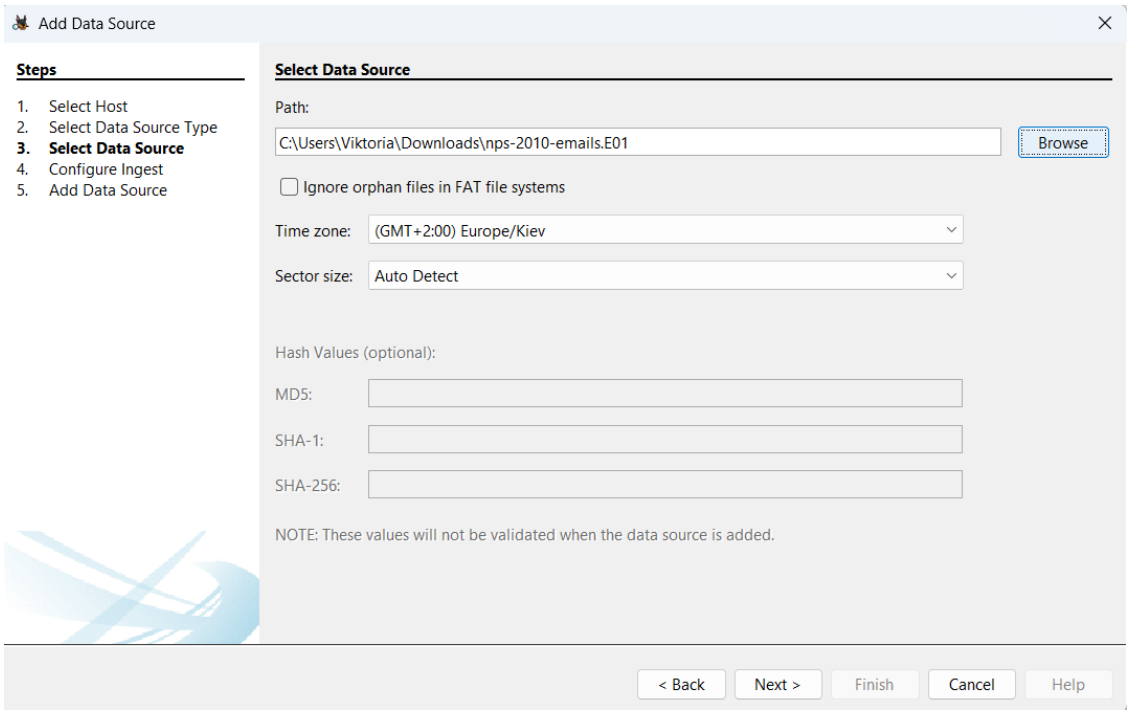

Рис. 2.9. Завантаження джерела даних та налаштування часового поясу

5. Обрати потрібні модулі для аналізу (рис. 2.10). Обираються згідно поставлених задач, аби не навантажувати комп’ютер. При необхідності розгорнути модулі та проставити прапорці, для отримання більш детального результату аналізу.

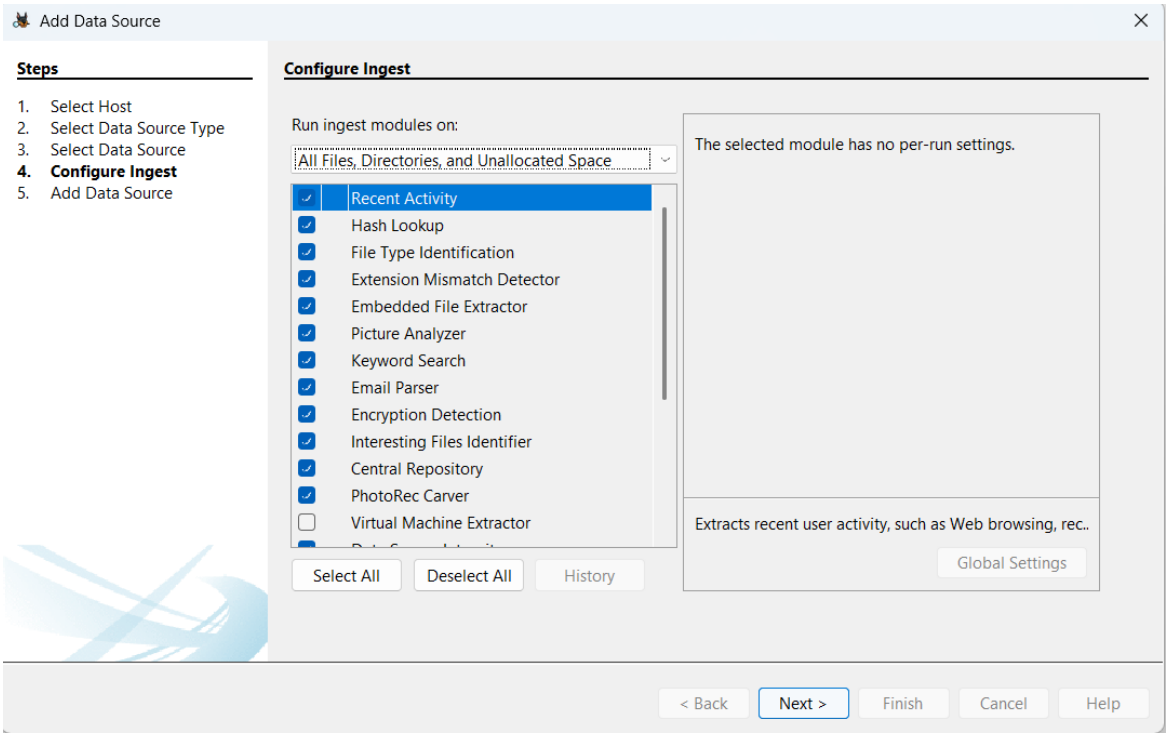

Рис. 2.10. Обирання модулів для аналізу

6. Після цих 5-ти пунктів йде аналіз джерела даних. Далі можна проводити розслідування отриманого результату.

7. Дослідивши потрібний диск, та знайшовши всі потрібні докази створюється звіт [10], який подається до керівництва для подальшого його опрацювання (рис. 2.11).

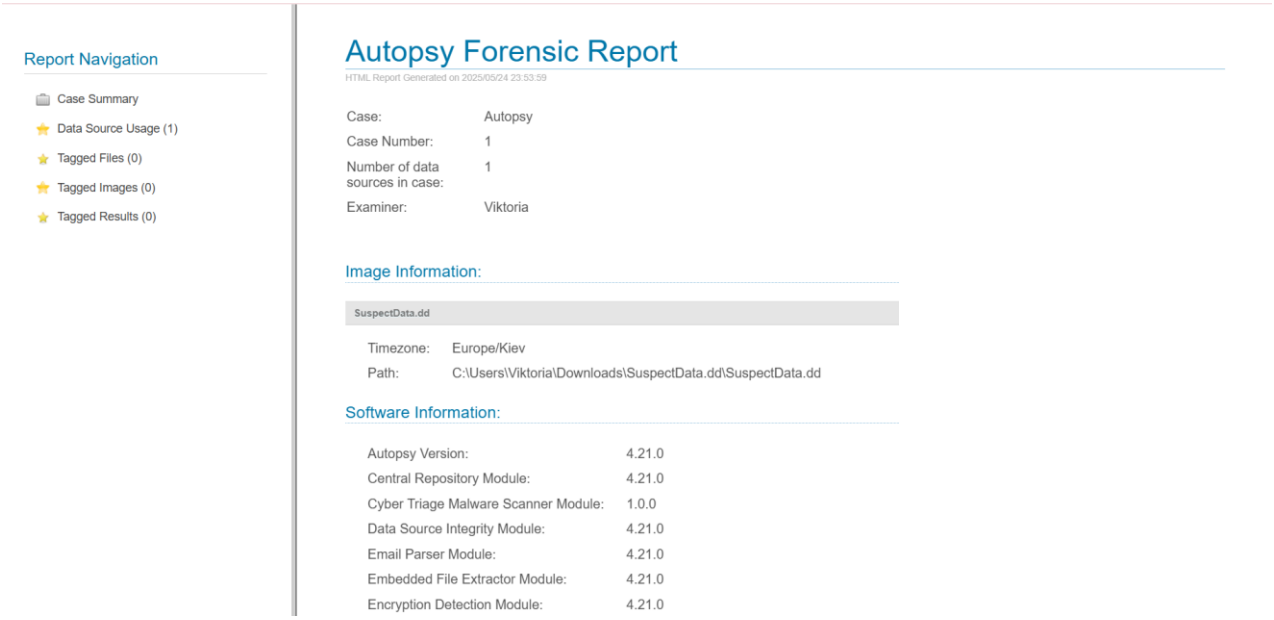

Рис. 2.11. Звіт

Отже, було розглянуто, як працює програма Autopsy та які функції вона виконує під час розслідування кіберінцидентів. Розібрано її архітектуру та основні модулі, які допомагають знаходити та аналізувати цифрові докази, такі як видалені файли, історію браузера, електронну пошту та інші сліди активності.

Також було описано послідовність дій при використанні Autopsy – від створення кейсу до перегляду результатів та формування звіту. Це показало, що програма дуже зручний та корисний інструмент для фахівців, які ведуть розслідування інцидентів у сфері кібербезпеки.

Загалом, Autopsy дозволяє ефективно проводити розслідування та швидко знаходити важливу інформацію.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПРОВЕДЕННЯ РОЗСЛІДУВАНЬ З ВИКОРИСТАННЯМ AUTOPSY

3.1. Методологія розслідування кіберінцидентів за допомогою Autopsy

Згідно з NIST SP 800-61 версії 2 та 3 [11, 12] існує модель життєвого циклу реагування на інциденти (рис. 3.1):

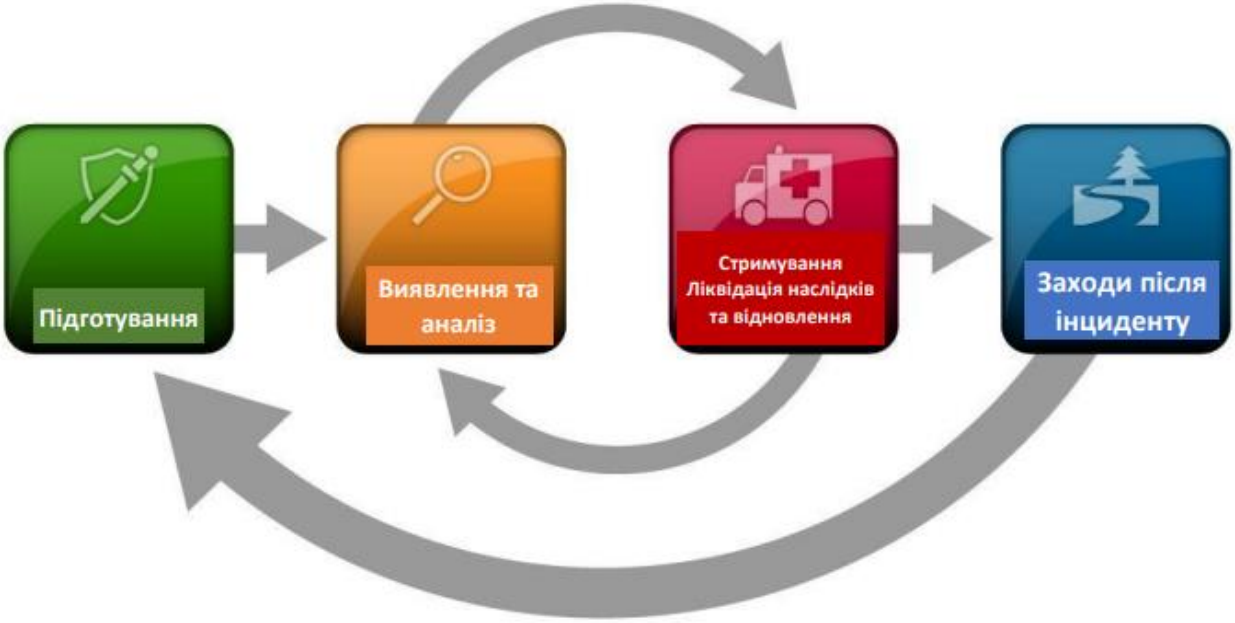

Рис. 3.1. Модель життєвого циклу реагування на інциденти

З цього рисунку ми маємо кроки реагування на інциденти:

1. Підготовка
2. Виявлення та аналіз
3. Стримування
4. Ліквідація
5. Відновлення
6. Огляд після інциденту

Підготовка

Ця початкова фаза реагування на інцидент також є безперервною фазою. CSIRT обирає найкращі можливі процедури, інструменти та методи для реагування

на інцидент, його виявлення, локалізації та відновлення після нього якомога швидше та з мінімальними перебоями в роботі.

Шляхом регулярних оцінок ризиків CSIRT визначає бізнес-середовище, яке потребує захисту, потенційні вразливості мережі та різні типи інцидентів безпеки, що становлять ризик для мережі. Команда визначає пріоритетність кожного типу інциденту на основі його потенційного впливу на компанію.

CSIRT може відпрацювати кілька різних стратегій атаки у військових іграх, а потім створити шаблони для найефективніших відповідей, щоб мати змогу швидко діяти у разі реальної атаки. Час реакції можна відстежувати для створення показників для майбутніх навчань та потенційних атак. На основі цієї повної оцінки ризиків команда реагування на надзвичайні ситуації може оновити існуючі плани дій у надзвичайних ситуаціях або створити нові.

Виявлення та аналіз

На цьому етапі члени команди безпеки моніторять мережу на наявність підозрілої активності та потенційних загроз. Вони аналізують дані, сповіщення та тривоги, зібрані з журналів пристроїв та різних інструментів безпеки (антивірусного програмного забезпечення, брандмауерів), щоб виявити поточні інциденти. Команда працює над тим, щоб відфільтрувати неправдиві повідомлення від реальних інцидентів та ранжує фактичні сповіщення за ступенем їхньої серйозності.

Сьогодні більшість компаній використовують одне або декілька рішень безпеки, таких як: Управління інформацією та подіями безпеки (SIEM) та виявлення та реагування на кінцеві точки (EDR) для моніторингу подій безпеки в режимі реального часу та автоматизації заходів реагування.

План комунікації також вступає в гру на цьому етапі. Після того, як команда реагування на надзвичайні ситуації визначить тип загрози або порушення безпеки, вона повідомляє відповідний персонал, а потім переходить до наступного етапу процесу реагування.

Стримування

Команда реагування на надзвичайні ситуації вживає заходів, щоб запобігти подальшому пошкодженню мережі внаслідок інциденту чи іншої зловмисної діяльності. Після цього набувають чинності плани дій у надзвичайних ситуаціях. Існує дві категорії заходів щодо стримування:

Короткострокові заходи стримування зосереджені на запобіганні поширенню поточної загрози шляхом ізоляції уражених систем, наприклад, шляхом відключення уражених пристроїв.

Довгострокові заходи стримування зосереджені на захисті неуражених систем шляхом встановлення посилених заходів безпеки навколо них, таких як: сегментація конфіденційних баз даних від решти мережі.

Під час цього етапу CSIRT також може створювати резервні копії уражених та неуражених систем, щоб запобігти подальшій втраті даних та зберегти судово-медичні докази інциденту для майбутніх розслідувань.

Ліквідація

Після того, як загрозу буде локалізовано, команда переходить до повного її усунення із системи. Це може включати видалення шкідливого програмного забезпечення або завантаження мережі неавторизованого чи зловмисного користувача. Команда також перевіряє як уражені, так і неушкоджені системи, щоб переконатися, що не залишилося слідів порушення безпеки.

Відновлення

Як тільки аварійно-рятувальна група переконається, що загрозу повністю усунуто, уражені системи будуть повернуті до нормального режиму роботи. Це виправлення може включати встановлення виправлень, відновлення систем з резервних копій та повернення систем і пристроїв до працездатності. Запис атаки та її вирішення зберігається для аналізу та вдосконалення системи.

Огляд після інциденту

На кожному етапі процесу реагування на інциденти CSIRT збирає докази порушення та документує кроки, які вона вживає для стримування та усунення загрози. Під час цього етапу CSIRT переглядає цю інформацію, щоб зрозуміти інцидент та винести уроки. CSIRT намагається визначити причину атаки, як вона

успішно проникла в мережу, та виправити вразливості, щоб запобігти подібним інцидентам у майбутньому.

CSIRT також оцінює, які заходи були успішними, та шукає шляхи вдосконалення систем, інструментів та процесів для посилення можливостей реагування на майбутні інциденти. Залежно від обставин порушення, правоохоронні органи також можуть бути залучені до розслідування після інциденту.

В загальному Autopsy використовується на всіх етапах реагування на інциденти.

3.2. Порядок проведення розслідування кіберінцидентів з використанням Autopsy

Розглянуто таку ситуацію: Увімкнено 20.09.04 , ноутбук Dell CPi із серійним номером VLQLW був знайдений покинутим разом із бездротовою картою PCMCIA та зовнішньою саморобною антеною 802.11b. Підозрюється, що цей комп'ютер використовувався для хакерських цілей, хоча його не можна пов'язати з підозрюваним у хакерстві G=r=e=g S=c=h=a=r=d=t. (Знаки рівності призначені лише для того, щоб веб-сканери не індексували це ім'я; у файлах зображень знаків рівності немає.). Шардт також має онлайн-прізвисько «Містер Зло», і деякі з його соратників казали, що він паркував свій автомобіль у зоні дії точок бездротового доступу (таких як Starbucks та інші точки доступу T-Mobile), де потім перехоплював інтернет-трафік, намагаючись отримати номери кредитних карток, імена користувачів та паролі [2].

Для цього було завантажено образ диску формату E01, та проаналізовано за допомогою Autopsy. Першим кроком, звичайно, було створення кейсу (рис. 3.2-3.3).

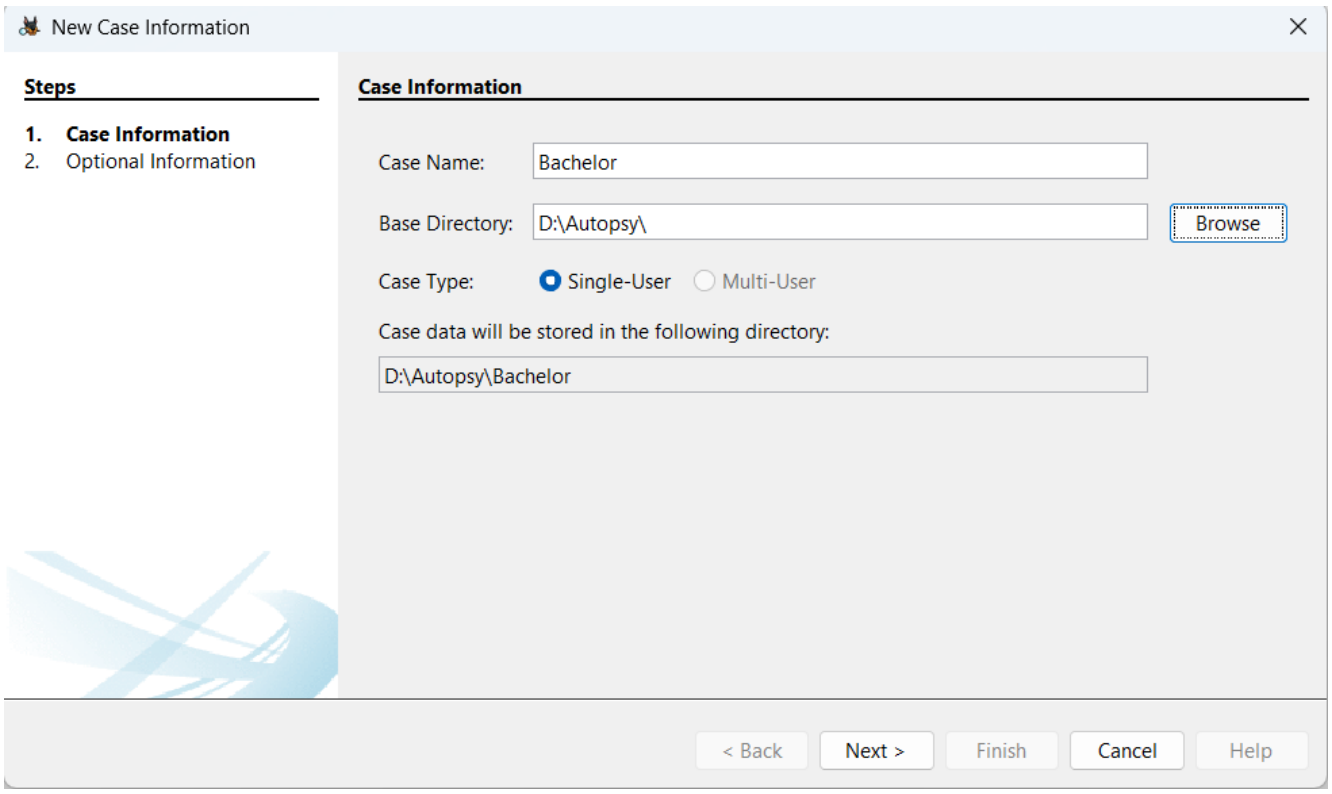

Рис. 3.2. Створення кейсу

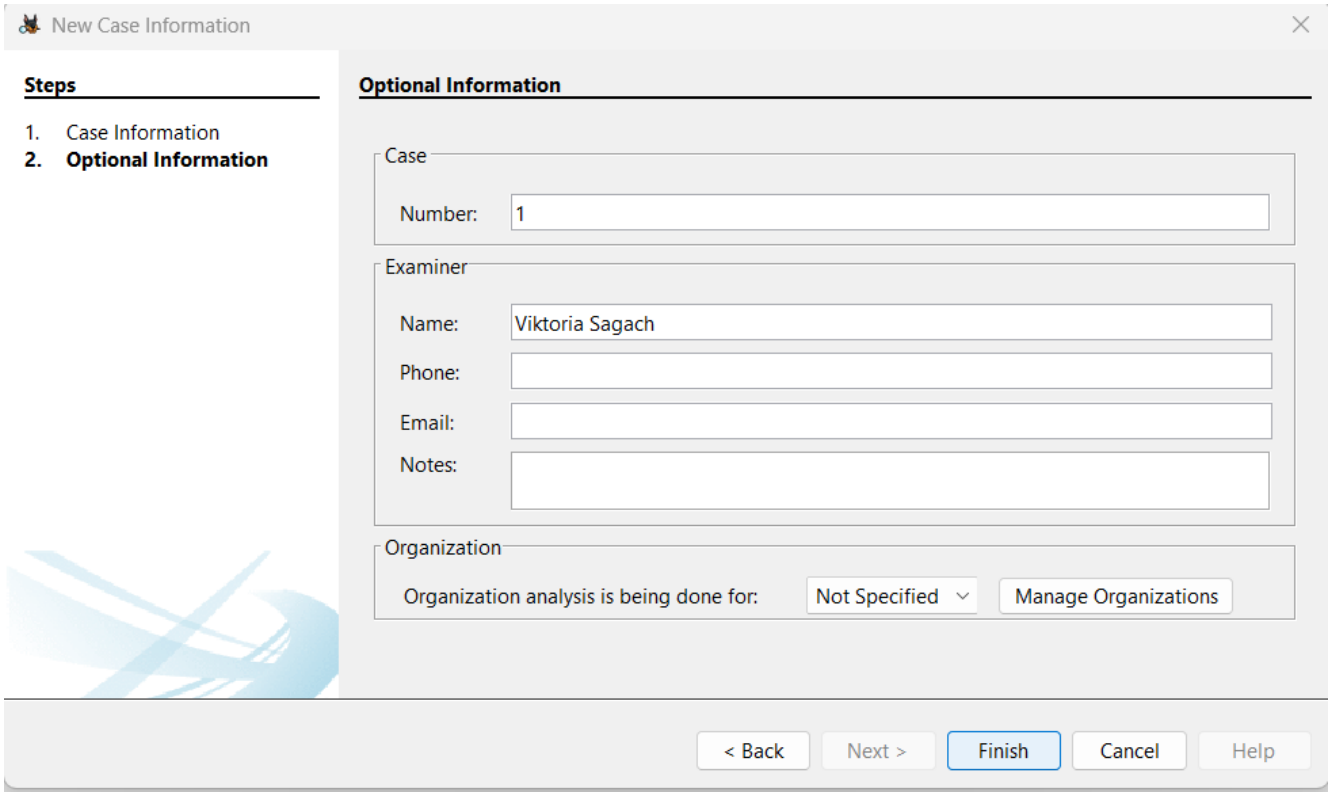

Рис. 3.3. Введення додаткової інформації

Наступний крок, це завантаження образу диску до програми та обирання модулів аналізу. Обираємо всі модулі, оскільки треба провести детальний аналіз. Гілка результату дуже об’ємна, тому потрібно детально перевіряти кожен з файлів, які ми маємо, щоб знайти будь-яку інформацію причетності до хакерства (рис. 3.4).

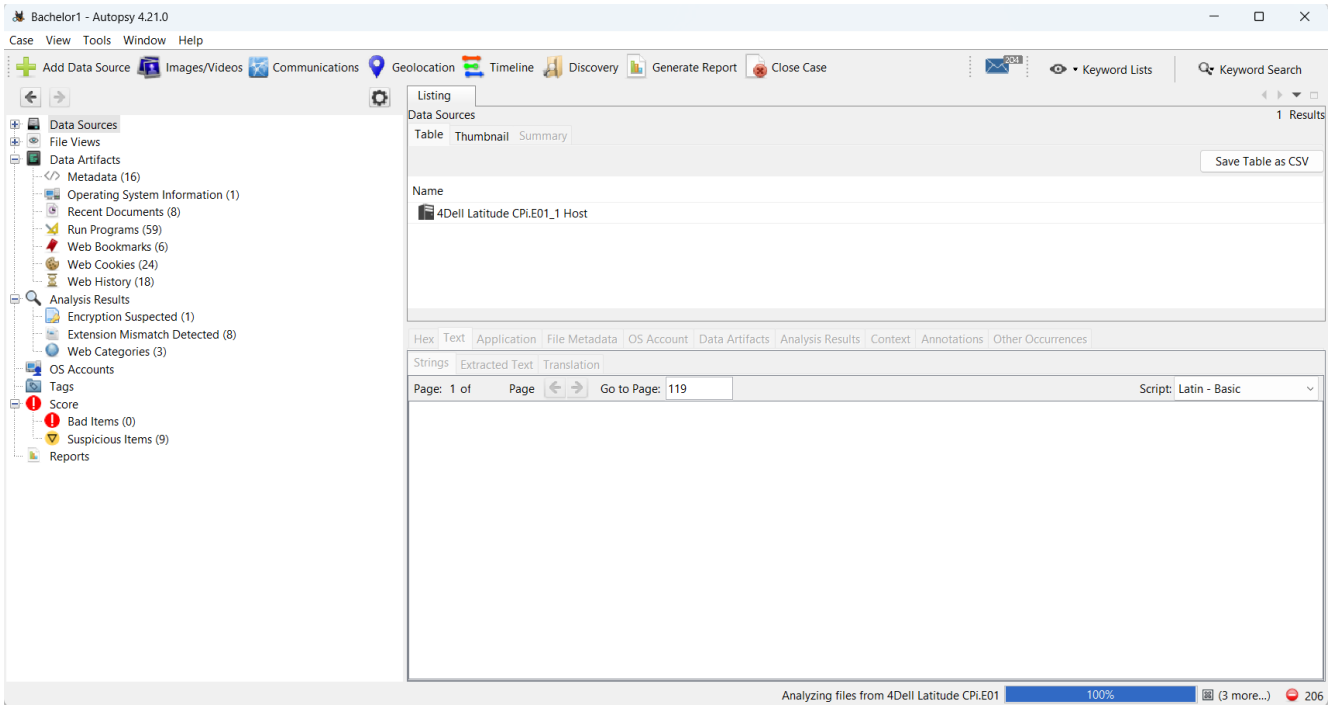

Рис. 3.4. Гілка результату

Згідно [10] будь-які дії у ході розслідування, збору та аналізу доказів, усі виконані дії з файлами, даними та інформацією, що досліджуються, необхідно ретельно документувати. Оскільки справа пов’язана з хакерством потрібно задокументувати використовувану операційну систему, ім’я облікового запису, основного домену тощо, аби потім можна було справу передати до суду.

Перелік деяких питань наступний [13]:

1. Яка операційна система використовувалася на комп'ютері?
2. Коли була дата встановлення?
3. Які налаштування часового поясу?
4. Хто є зареєстрованим власником?
5. Яке ім'я облікового запису комп'ютера?
6. Яке ім'я основного домену?
7. Коли була остання зареєстрована дата/час вимкнення комп'ютера?

8. Скільки облікових записів зареєстровано (загальна кількість)?

9. Яке ім'я облікового запису користувача, який здебільшого користується комп'ютером?

10. Хто був останнім користувачем, який входив у систему комп'ютера?

11. Знайдіть 6 встановлених програм, які можуть бути використані для злому.

12. Чи є на комп'ютері віруси?

Для документування основної інформації найкраще створити додатково файл txt. Докази будуть додані до звіту який створюється в Autopsy.

Почнемо розслідування. Для початку дізнаємося чи дійсно Greg Schardt пов’язаний з чим комп’ютером. Для цього відкриваємо гілку «Data Sources», наш проаналізований комп’ютер, та опиняємось у вікні, де доступно ще 3 диски з папками. Тут нам необхідно перейти до «Summary» та «Container». У рядку «Details» ми побачимо потрібну інформацію (рис. 3.5).

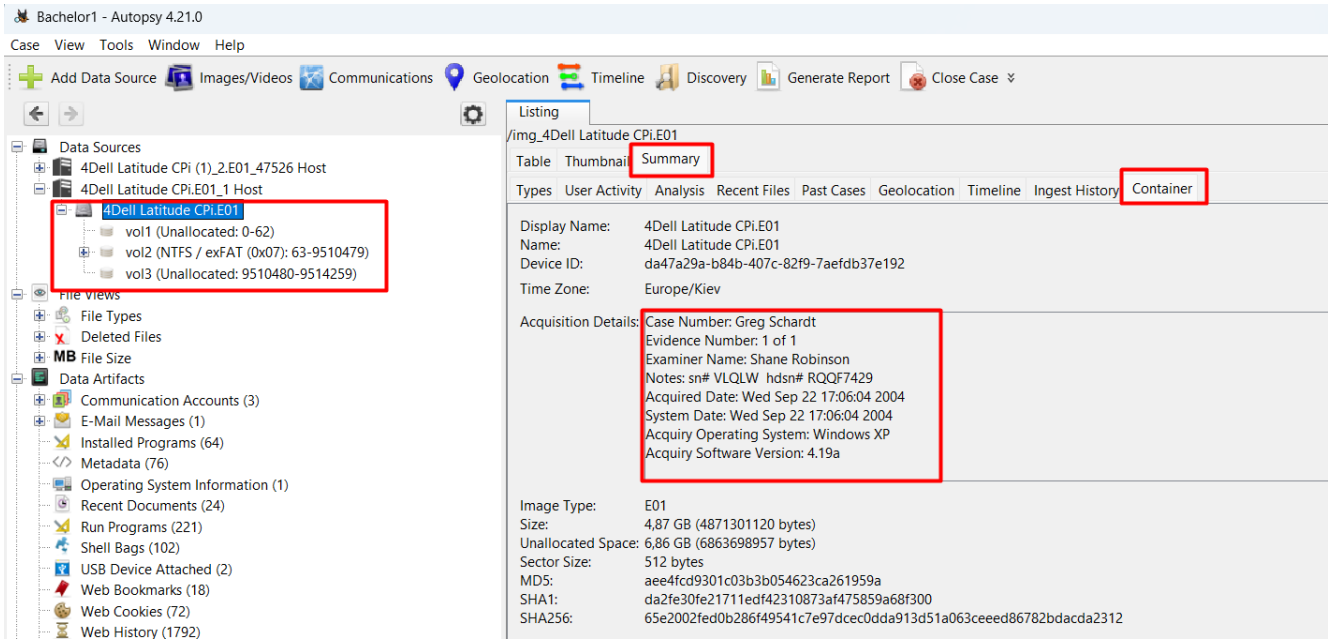

Рис. 3.5. Інформація

Також бачимо, яка операційна система була на комп’ютері (Windows XP). Наступне, що можемо дізнатися – ім’я облікового запису та основний домен. Для цього використовуємо такий шлях: vol2/WINDOWS/system32/config/software.sav/Microsoft/WindowsNT/CurrentVersion/Winlogon

Зі скріншоту (рис. 3.6) бачимо, ім’я облікового запису та основний домен.

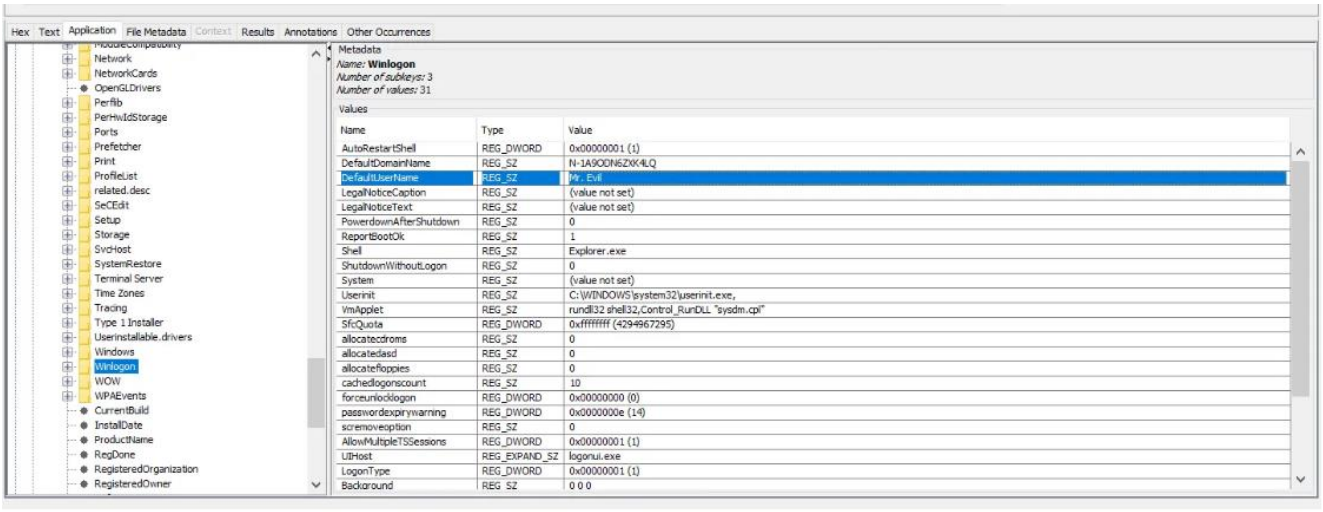

Рис. 3.6. Обліковий запис та домен

Щоб визначити кількість зареєстрованих облікових записів необхідно в гільці результату знайти «OS Accounts» (рис. 3.7):

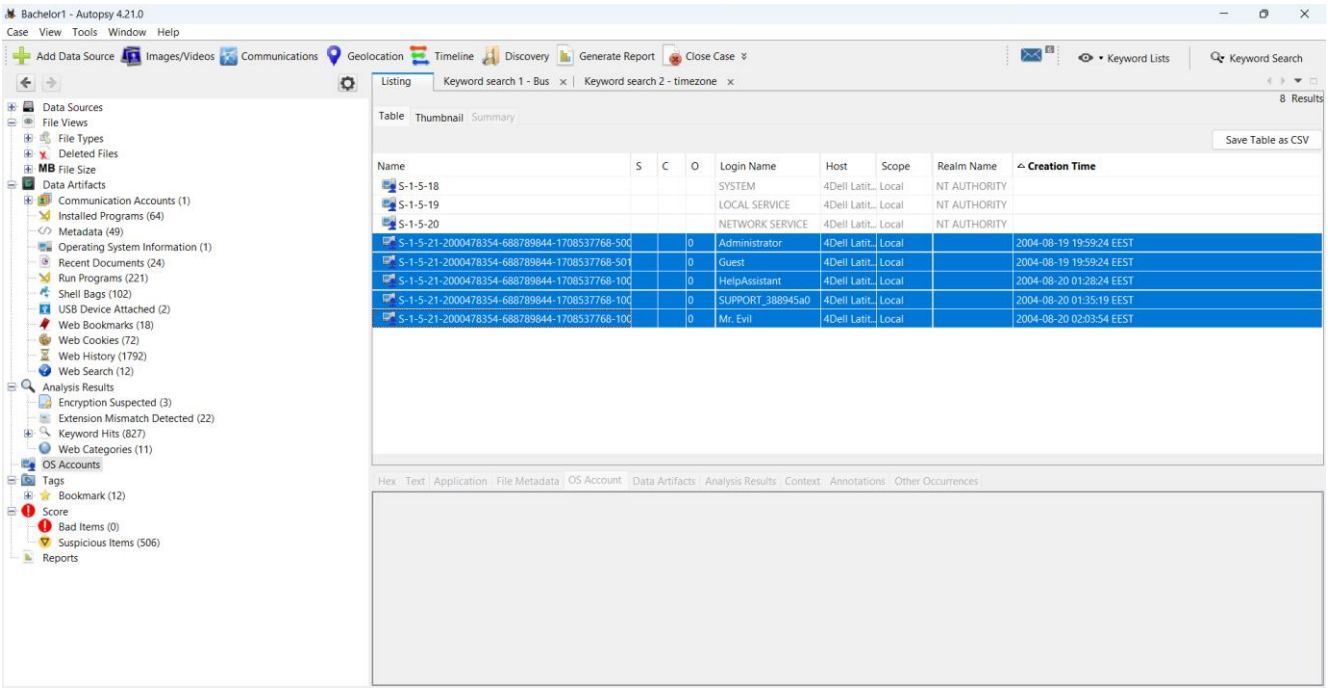

Рис. 3.7. Облікові записи

Проглянувши кожен обліковий запис, який є, можна побачити Login Count – тобто кількість входжень в обліковий запис. З цього можна зробити висновок, що частіше користується комп’ютером – Містер Зло, було 15 входжень (рис. 3.8).

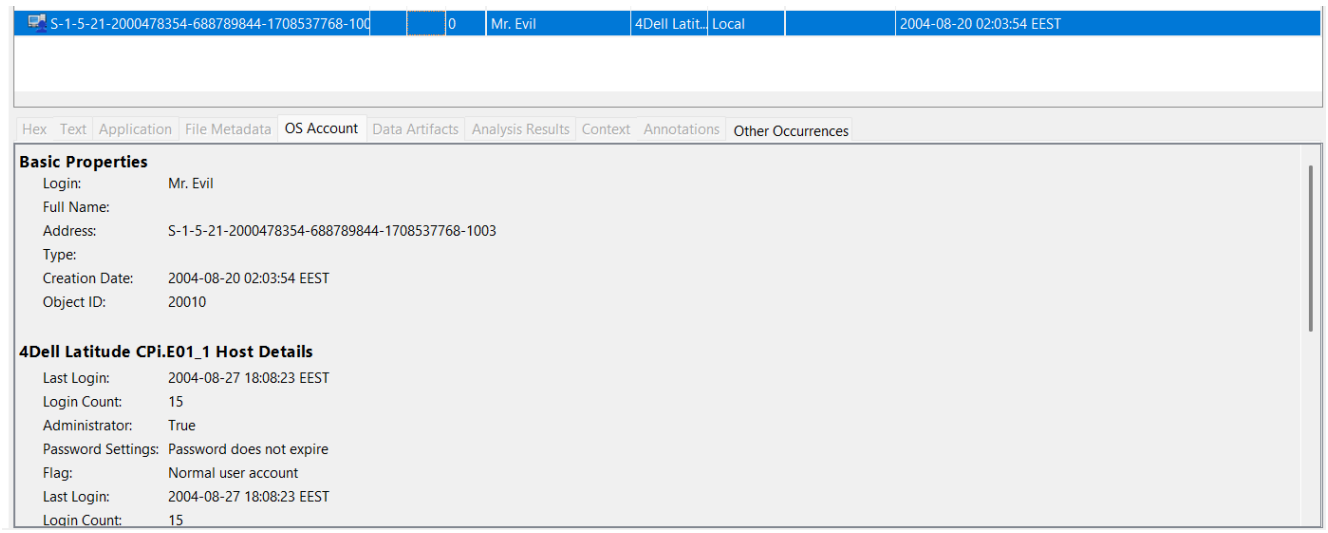

Рис. 3.8. Користувач, який частіше користується комп’ютером

Далі виявлено встановлені файли на комп’ютері. Їх можна знайти також у гілці результату (рис. 3.9).

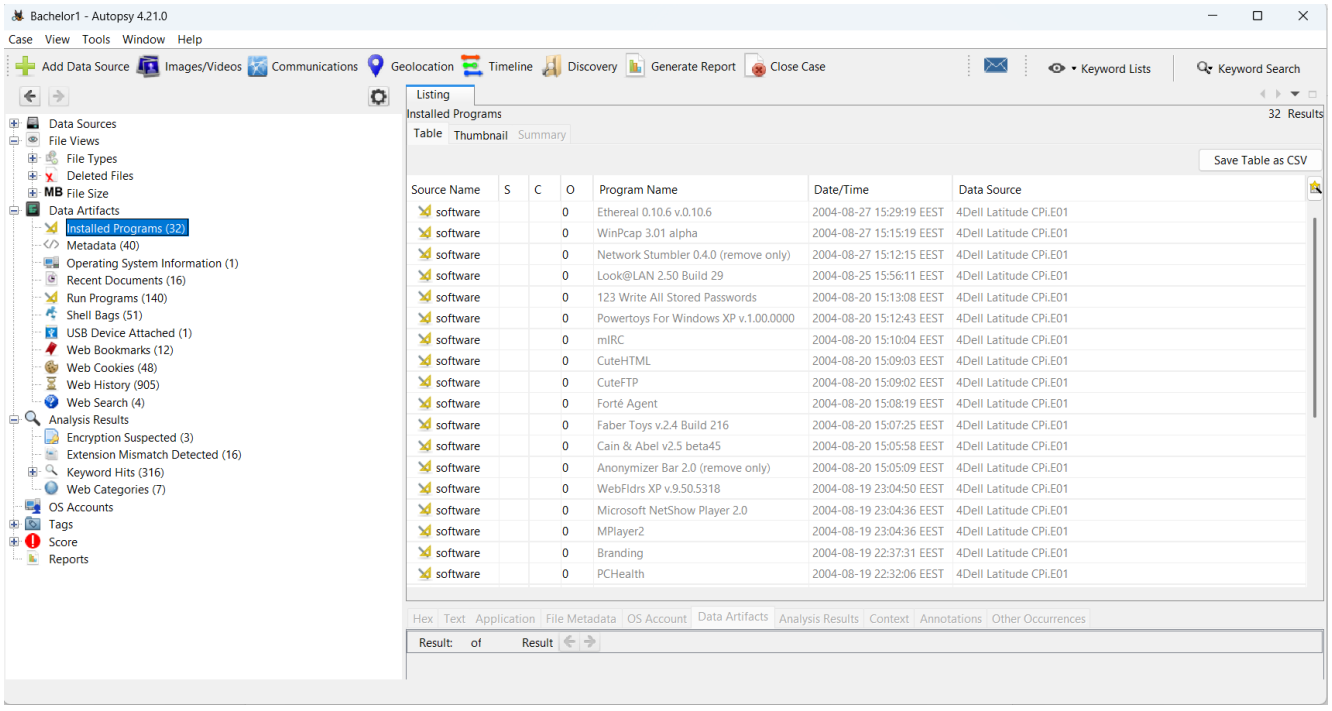

Рис. 3.9. Встановлені програми

Переглянувши інформацію в Інтернеті про кожну з цих програм виявлено:

- Ethereal (сучасний Wireshark) – програма, яка може перехоплювати всі пакети, які відправлялися через мережеве з’єднання, щоб потім відобразити інформацію про них і переглядати що відбувалось в мережі.

- Network Stumbler – інструмент, який облегшує виявлення безпровідних локальних мереж з використанням стандартів бездротової локальної мережі 802.11b, 802.11a, 802.11g.

- Anonymizer – інструмент, що використовується для приховування особи та місцезнаходження користувача в Інтернеті шляхом маскування IP-адреси.

- LOOK@LAN – програмне забезпечення, яке дозволяє контролювати та бачити пристрої підключені до нашої локальної мережі.

Це лише частина завантажених програм, які можна було використовувати для хакерських цілей. Їх потрібно виокремити, щоб потім побачити їх у звіті від Autopsy. Для цього ставимо на них прапорці – права кнопка миші – «Add Result Tag», та обрати прапорець. Також можна просто натиснути комбінацію клавіш «Ctrl + B».

В ході подальшого розслідування було виявлено файл з інструкцією інсталяції програми, яка дає змогу віддалено керувати комп'ютерною системою по мережі, а саме NetBus. Його було знайдено у гілці «Data Artifacts» – «Metadata» (рис. 3.10):

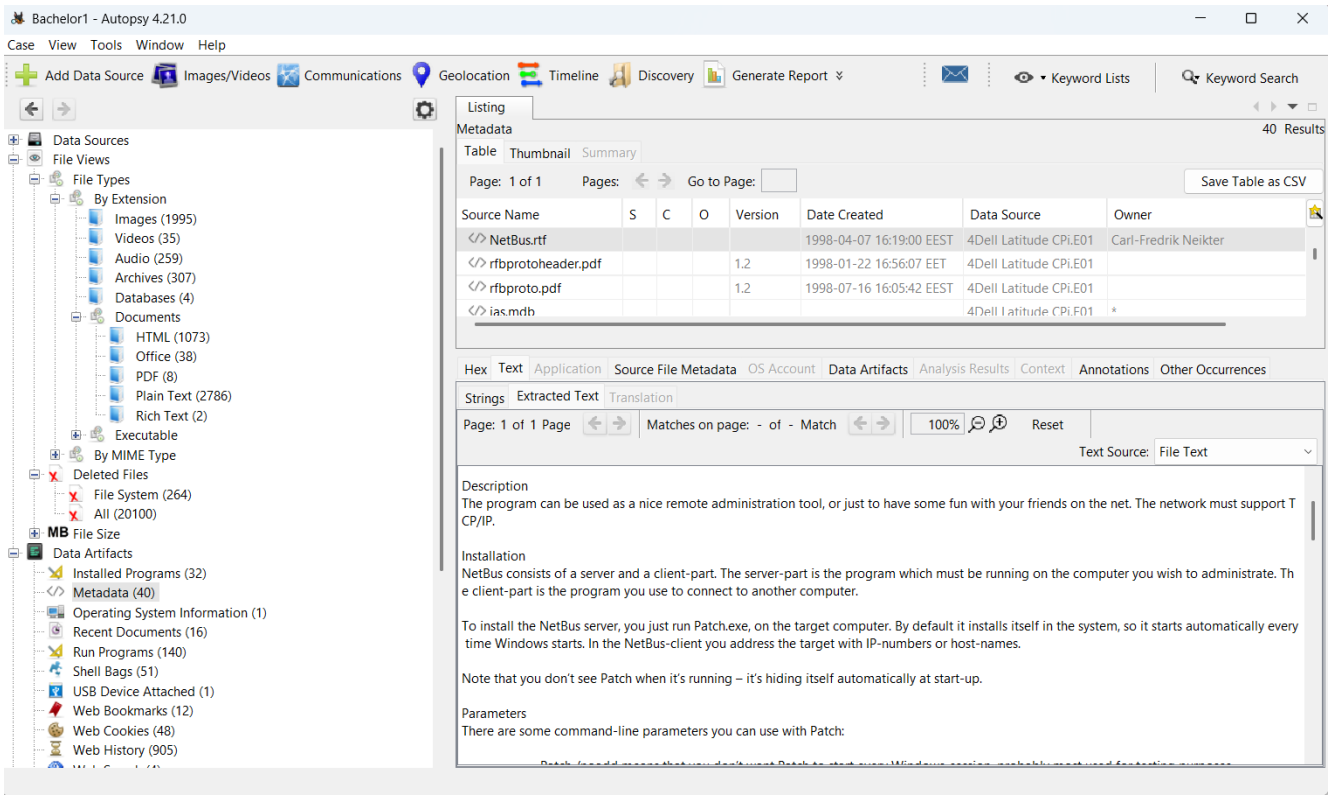

Рис. 3.10. Інструкція програми

В списку інстальованих програм її немає, але краще виокремити її.

Також, як зазначалось раніше, програма Autopsy може знаходити інформацію за ключовими словами. В нашому випадку слово «Bus» зустрічається доволі часто.

Попередньо було виявлено, що встановлено Ethereal, популярну програму для перехоплення дротових та бездротових інтернет-пакетів. Знайдено папку з цією програмою vol2/Documents and Settings/Mr.Evil/Application Data/Ethereal/recent. В цьому файлі міститься наступне посилання Documents and Settings/Mr. Evil/interception з текстом про те, що всі перехоплені файли знаходяться там (рис. 3.11):

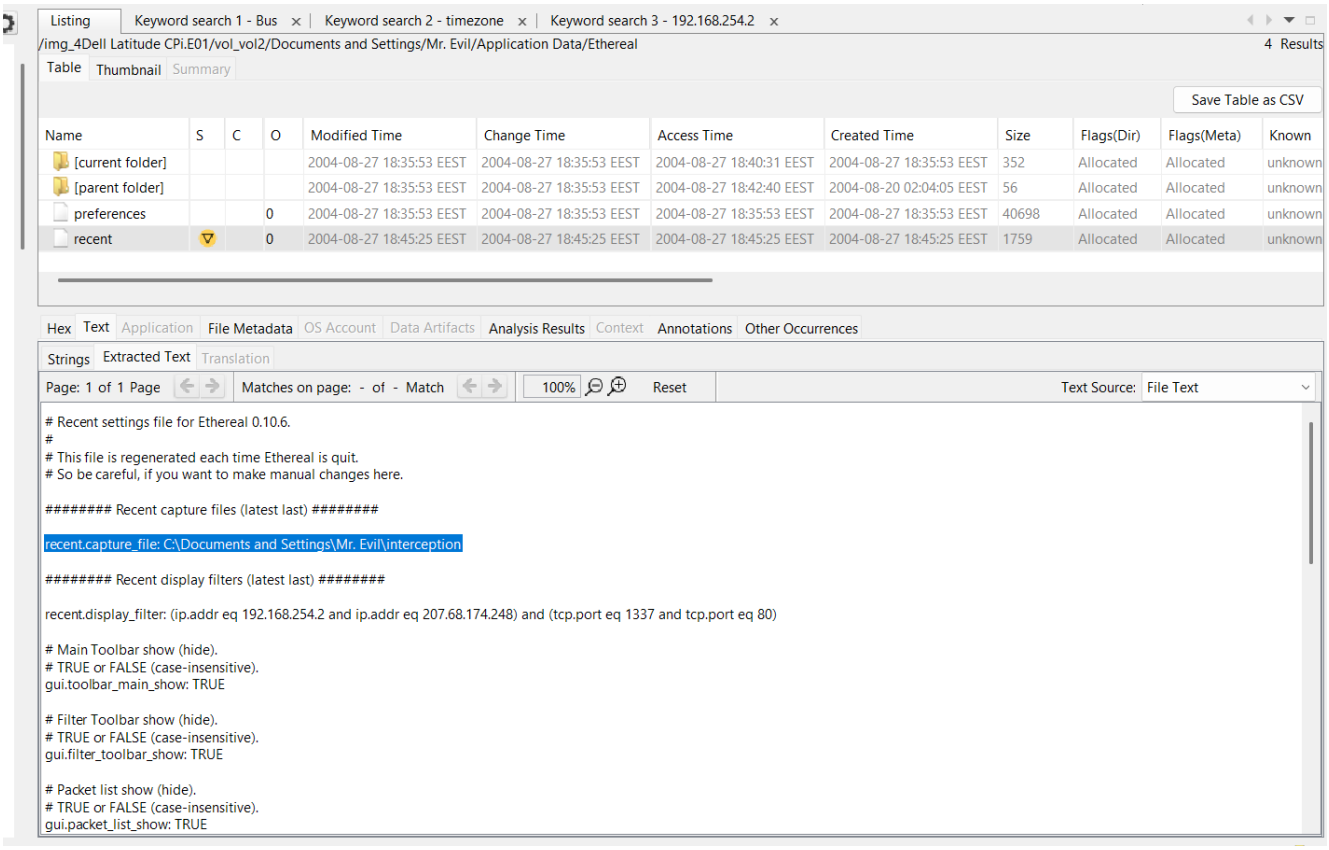

Рис. 3.11. Шлях до перехоплених даних

Переходимо за цим напрямком та маємо перехоплені дані жертви. З цього можна зробити висновок, що жертва намагалася отримати доступ до вебсайтів (рис. 3.12).

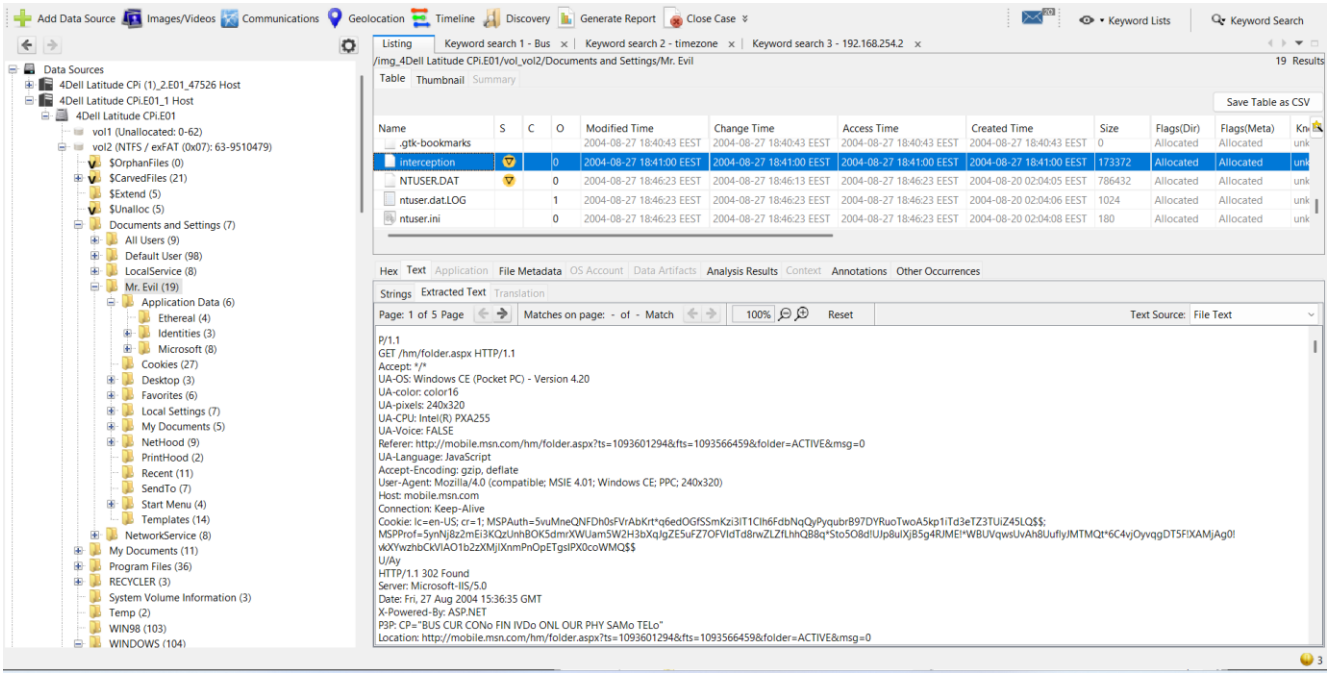

Рис. 3.12. Перехоплені дані

З цього можна зробити висновки, що все ж таки Грег отримав доступ до ПК жертви, та перехоплював дані про веб-активність.

Після розслідування та збирання потрібної інформації робимо два звіти: один, що писався власноруч (рис. 3.13) та другий зроблений з допомогою Autopsy (рис. 3.14):

Файл Редагувати Переглянути

1. Яка операційна система використовувалася на комп'ютері?
   Windows XP
2. Коли була дата встановлення?
   08/19/04 05:48:27 PM
3. Які налаштування часового поясу?
   Central Daylight Time (-05hrs GMT)
4. Хто є зареєстрованим власником?
   Greg Schardt
5. Яке ім'я облікового запису комп'ютера?
   N-1A9ODN6ZXK4LQ
6. Яке ім'я основного домену?
   Evil
7. Коли була остання зареєстрована дата/час вимкнення комп'ютера?
   08/27/04 10:46:33 AM
8. Скільки облікових записів зареєстровано (загальна кількість)?
   5
9. Яке ім'я облікового запису користувача, який здебільшого користується комп'ютером?
   Mr. Evil
10. Хто був останнім користувачем, який входив у систему комп'ютера?
    Mr. Evil
11. Знайдіть 6 встановлених програм, які можуть бути використані для злому.
    Cain & Abel v2.5 beta45
    Ethereal
    123 Write All Stored Passwords
    Anonymizer
    CuteFTP
    Look&LAN_1.0
    NetStumbler
12. Чи є на комп'ютері віруси?
    Yes

Рис. 3.13. Звіт-txt

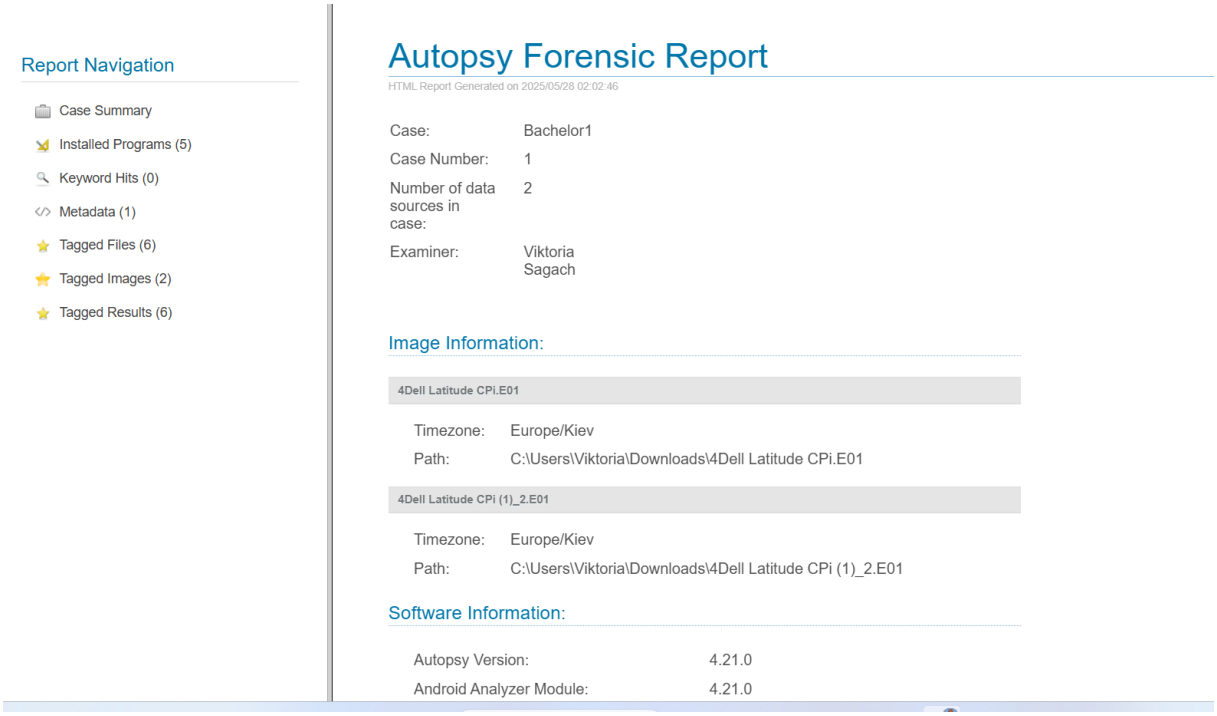

Рис. 3.14. Звіт-Autopsy

В цьому звіті зліва представлені всі знайдені артефакти. Їх можна ще раз передивитися. Інстальовані програми (рис. 3.15), метадані про NetBus(рис. 3.16):

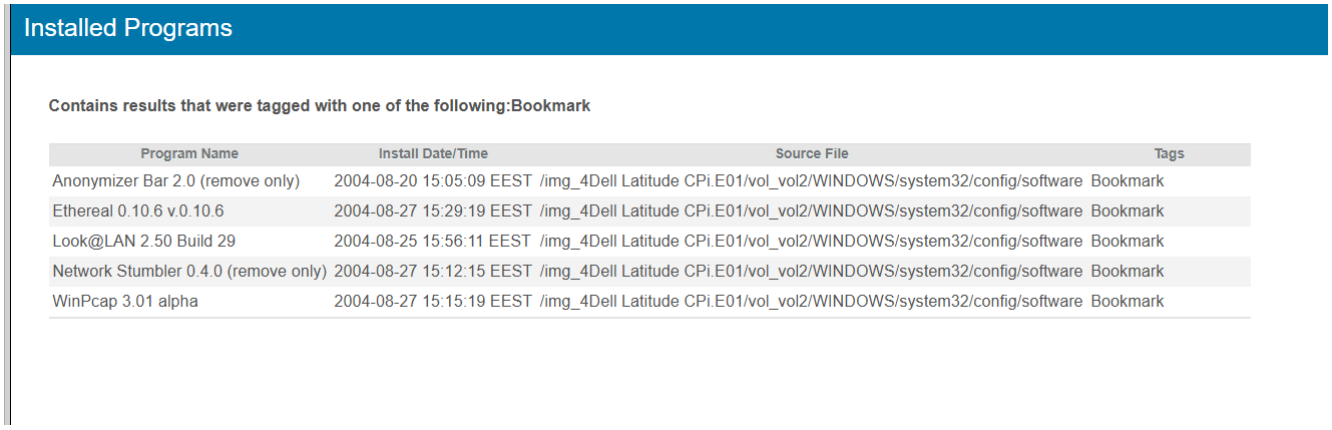

Рис. 3.15. Звіт-інстальовані програми

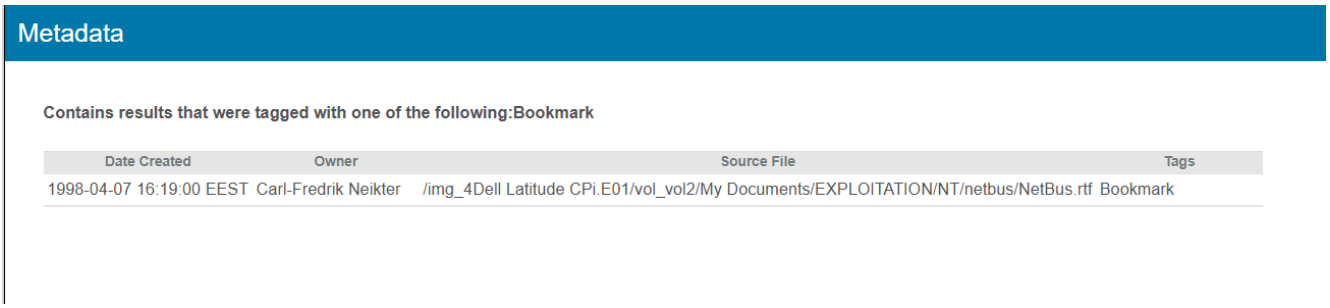

Рис. 3.16. Звіт-метадані

Також, підозрілі на мою думку файли, які були знайдені під час проведення розслідування. Тут є файли з великою кількістю паролів (словники), інструкція до Brutus – онлайн взломник паролів та дивні htm файли, на яких є можливість залишити персональні дані(рис. 3.17):

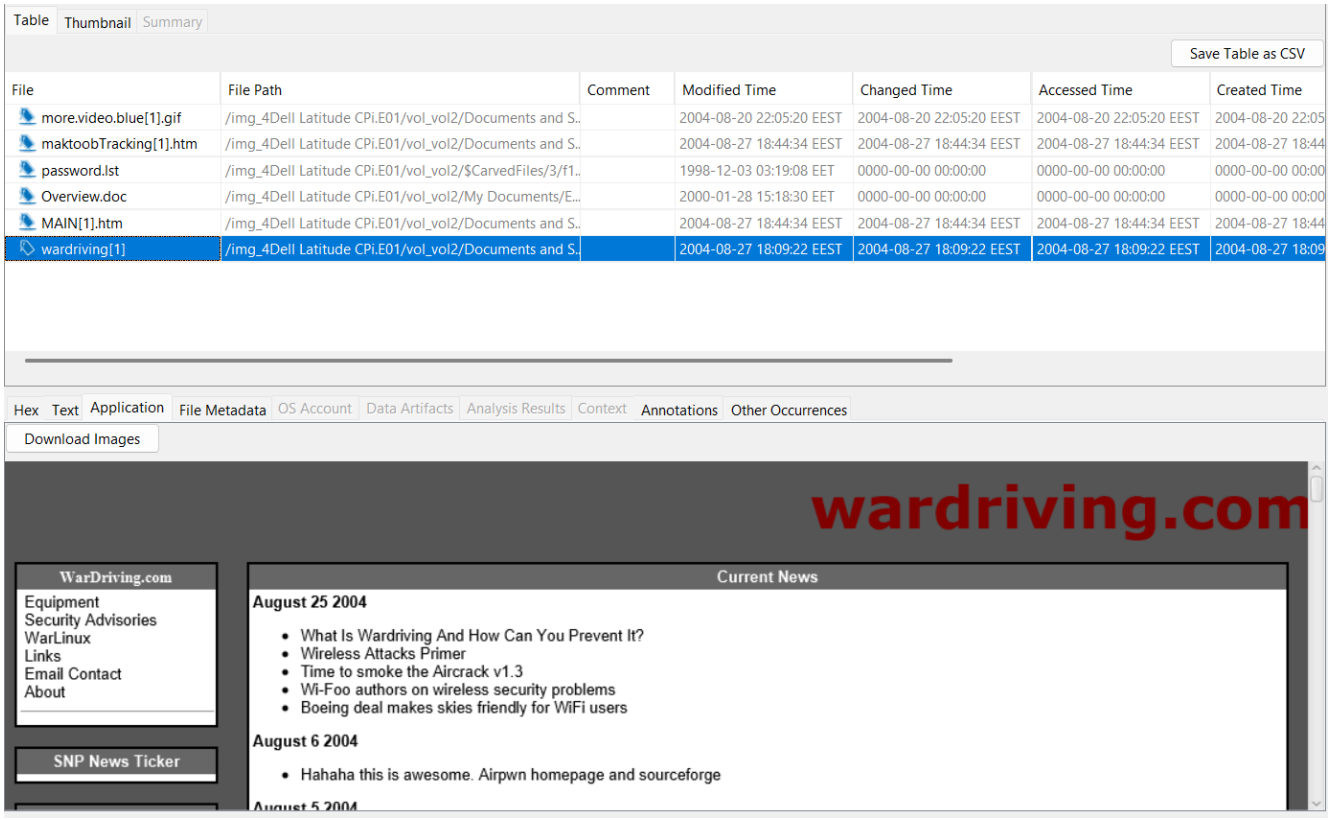

Рис. 3.17. Підозрілі файли

Так чи винен Грег у хакерстві чи ні? Оскільки прямих доказів знайдено не було (файли з паролями, даними карток), то сказати точно, що він винен неможливо. Програми могли використовуватися лише в навчальних цілях, а перехоплений користувач міг бути його знайомим. В такому випадку потрібно провести співбесіду з підозрюваним і вирішити все має суддя. Проводячи останній аналіз було також виявлено Zip-бомбу (зловмисний архівний файл, який при розпаковці може перевантажити систему, споживаючи надмірну кількість пам’яті або ресурсів процесора), що може говорити про те, що 1) він міг «підкидати» таку бомбу своїм жертвам, 2) він сам став жертвою, через що в його комп’ютері було знайдено багато дивних файлів (рис. 3.18).

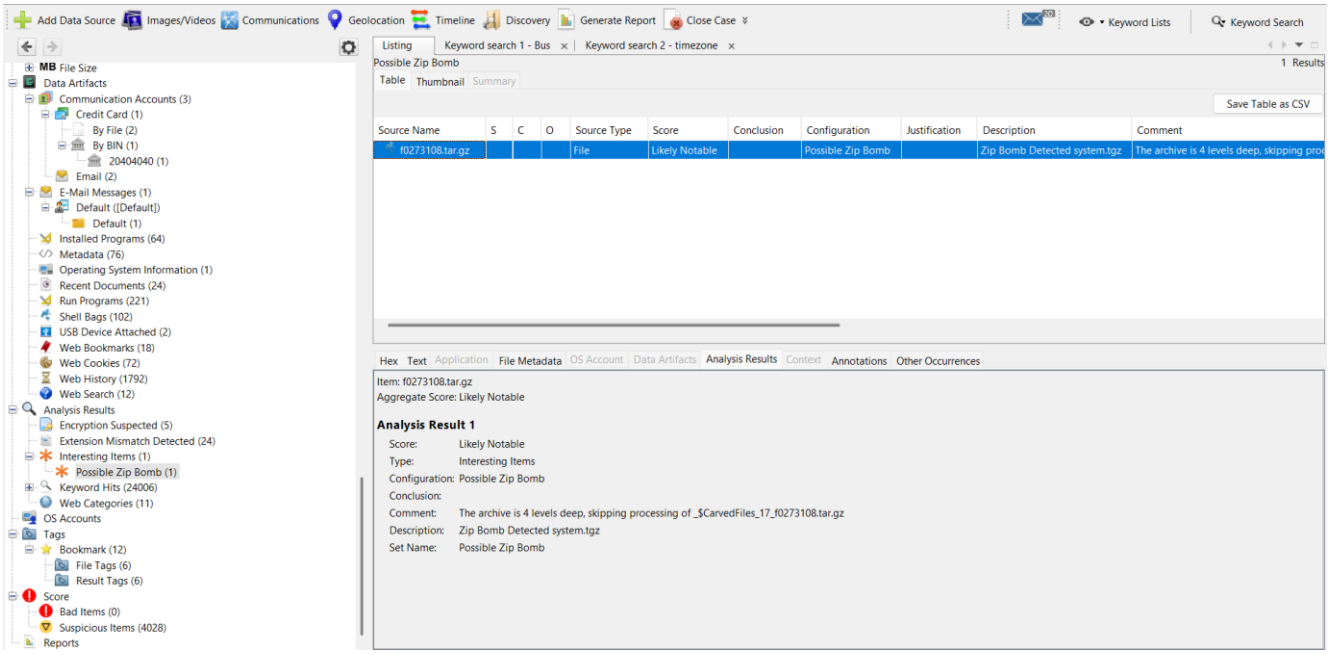

Рис. 3.18. Zip-бомба

Отже, висновок: неможливо звинувачувати людину без прямих доказів його причетності. Справа Грега повинна розслідуватися далі, з залученням свідків та, якщо це можливо, жертв.

3.3. Рекомендації щодо застосування Autopsy у практичній діяльності

Розслідування будь-яких кіберінцидентів з використанням Autopsy (і взагалі будь-якого іншого інструмента) краще виконувати на окремому комп’ютері, аби захистити дані організації. Деякі образ дисків можуть містити в собі шкідливе програмне забезпечення і тому аби не було інцидентів в самій організації, краще виконувати все окремо. Додатковим засобом захисту буде слугувати антивірусна програма, яка зможе виявити шкідливе ПЗ та допомогти з його усуненням.

Рекомендація до пристрою на якому ведеться розслідування кіберінциденту перш за все - достатній обсяг оперативної пам’яті, оскільки Autopsy при аналізі використовує більше ніж 3 ГБ. Найкращим варіантом буде 8 ГБ і більше. І бажано при цьому не відкривати сторонні програми, які також займають оперативну пам’ять. До цього обов’язково потрібен продуктивний багатоядерний процесор, оскільки повільний та старий процесор може викликати зниження швидкості

аналізу або «зависання» комп'ютера під час дослідження. Всі образи дисків бажано записувати на окремі носії інформації, але якщо носіїв немає, то звичайно, на комп'ютері має бути достатня кількість пам'яті і обов'язково антивірусна програма, як зазначалося раніше.

Для ефективного розслідування кіберінцидентів з використанням саме Autopsy перш за все потрібно слідкувати за оновленнями інструменту, оскільки нова версія програми може містити нові модулі, які покращують і/або полегшують розслідування.

Після завантаження досліджуваного диску до Autopsy можна його вже аналізувати та шукати докази, але краще дочекатися повного аналізу з боку програми, щоб не навантажувати комп'ютер. Звичайно, чим більше обсяг пам'яті у диску, тим довше він буде аналізуватися інструментом. Але якщо дочекатися повного аналізу, то не буде проблем з «зависанням» та буде доступна повна інформація з цього диску.

Наступне та також важливе – вміння користуватися пошуком за ключовими словами, адже можуть бути громіздкі жорсткі диски (на кілька терабайт) і власноруч такий диск буде складно аналізувати та шукати докази. Тому потрібно розуміти який інцидент трапився та використовувати «популярні пошукові запити». Наприклад, якщо фішинг (викрадення облікових записів, номерів карток та паролів), то можна використати ключові слова «credit card», «cvv», «password» або їх аналоги. Звичайно, якщо хакер - професіонал, то він може не використовувати такі слова в своїх документах/папках з викраденими даними, але все одно краще перевірити.

При використані програми обов'язковим є ведення звіту. Тому важливо створити окремо файл (txt, word), або використовувати шаблони організації та додатково виділяти доказові файли у програмі, а потім генерувати звіт у Autopsy, щоб потім справу можна було надіслати до суду, для продовження розслідування або відразу для судового процесу. Програма дає можливість вказати ім'я особи яка веде розслідування. При ведені звіту у форматі txt або word обов'язково повинні бути додані докази у вигляді скріншотів.

Отже, було розглянуто практичне застосування інструменту Autopsy для розслідування кіберінцидентів. Описано загальну методології проведення розслідування, включаючи етапи підготовки, збору та аналізу цифрових доказів.

Детально подано порядок використання Autopsy на кожному етапі розслідування, зокрема показано, як створюється кейс, додаються джерела даних, проводиться пошук артефактів, переглядаються журнали подій, веб-активність, файлові зміни та формується звіт.

Сформульовано рекомендації щодо ефективного використання Autopsy для розслідування інцидентів у різних ситуаціях.

ВИСНОВКИ

У роботі проведено дослідження проблематики цифрової криміналістики як одного з ключових компонентів забезпечення захисту кінцевих точок. Визначено мету та завдання розслідування інцидентів інформаційної безпеки з використанням сучасних інструментів криміналістичного аналізу. На сьогодні організації стикаються з серйозними викликами, пов’язаними з ефективним розслідуванням складних кіберінцидентів, зо потребують швидкого, точного та структурованого аналізу великої кількісті цифрових даних з кінцевих точок.

Проведено аналіз існуючих методів та інструментів цифрової криміналістики, які застосовуються для витягнення, дослідження та збережння цифрових доказів. Особливу увагу приділено інструменту Autopsy, яке є потужним і водночас доступним інструментом із відкритим кодом для цифрового аналізу. Autopsy дозволяє здійснювати глибоке дослідження вмісту жорстких дисків, файлових систем, журналів подій, браузерної активності, пошти та інших артефактів, які можуть вказувати на факт компрометації системи.

Завдяки інтуїтивному графічному інтерфейсу та широкому функціоналу Autopsy може бути ефективно використаний не лише експертами з цифрової криміналістики, а й фахівцями з кібербезпеки під час розслідувань інцидентів безпеки. Виявлення видалених файлів та можливість формування детальних звітів роблять інструмент корисним засобом у реагуванні на інциденти та документуванні цифрових доказів.

Таким чином, цифрова криміналістика з використанням Autopsy є важливою складовою сучасної стратегії кіберзахисту. Застосування цього інструменту сприяє ефективному реагуванню на інциденти, відновленню хронології подій, локалізації вразливих ділянок системи та наданню доказової бази для подальших дій.

Autopsy дозволяє організаціям підвищити рівень підготовки персоналу до роботи з цифровими доказами, а також забезпечити відповідність вимогам інформаційної безпеки та аудиту. Таким чином, правильне впровадження та використання Autopsy у процесах кібербезпеки є вагомим кроком до розслідування кіберінцидентів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Autopsy. URL: https://www.autopsy.com/ (дата звернення 20.05.2025).

2. FTK Imager. URL: https://www.exterro.com/digital-forensics-software/ftk-imager (дата звернення 28.05.2025).

3. Wireshark. URL: https://www.wireshark.org/ (дата звернення 28.05.2025).

4. Volatility Framework. URL: https://volatilityfoundation.org/ (дата звернення 28.05.2025).

5. Velociraptor. URL: https://docs.velociraptor.app/ (дата звернення 28.05.2025).

6. ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/standard/44381.html (дата звернення 21.05.2025).

7. Братішко Н. Напрями використання цифрової криміналістики в умовах військового стану. *Науковий вісник Дніпровського державного університету внутрішніх справ.* 2023. № 2. С. 282-288. URL: https://doi.org/10.31733/2078-3566-2023-6-282-288 (дата звернення 21.05.2025).

8. Фесьоха Н. О. Стан та тенденції розвитку кібербезпеки в епоху цифрової трансформації – аналіз сучасних загроз та заходів захисту. *Вісник Херсонського національного технічного університету*. *Інформаційні технології*. Херсон, 2024. № 2. С. 235-241. URL: https://doi.org/10.35546/kntu2078-4481.2024.2.33 (дата звернення 21.05.2025).

9. Козачок, В., Драпатий, М. Аналіз технології розслідування інцидентів безпеки на об’єктах критичної інфраструктури. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2024. № 26 Т. 2. С. 374–391. URL: https://doi.org/10.28925/2663-4023.2024.26.699 (дата звернення 22.05.2025).

10. Гончаренко М. Ф., Стежко М. В. Розслідування кіберінцидентів в корпоративній інформаційній системі на основі рішень Autopsy та Volatility. *Державний університет телекомунікацій. Сучасний захист інформації*. 2022. № 50. Т. 2. С. 22-29. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2635/2534 (дата звернення 24.05.2025).

11. Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-61 Revision 2. Paul R. Cichonski, Thomas Millar, Timothy Grance, Karen Scarfone. URL: https://www.nist.gov/publications/computer-security-incident-handling-guide (дата звернення 25.05.2025).

12. Incident Response Recommendations and Considerations for Cybersecurity Risk Management NIST Special Publication 800-61 Rev. 3: Alex Nelson, Sanjay Rekhi, Murugiah Souppaya, Karen Scarfone. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf (дата звернення 25.05.2025).

13. Computer Forensic Reference Data Sets (CFReDS). Hacking Case. URL: https://cfreds-archive.nist.gov/ (дата звернення: 20.05.2025).