КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій

(факультет)

Кібербезпеки та комп'ютерної інженерії

(назва випускової кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

на тему:

OSINT - сценарії виявлення цифрового сліду організації в умовах навчального кіберполігону

_____Гінзбург Данило Юрійович_____
(прізвище, ім’я та по батькові здобувача повністю)

Київ 2026р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)

Кібербезпеки та комп'ютерної інженерії
(назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
___Делембовський М.М.
„___" _____2026 року

КВАЛІФІКАЦІЙНА РОБОТА ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

OSINT - сценарії виявлення цифрового сліду організації в умовах навчального кіберполігону
(назва)

Я як здобувач вищої освіти КНУБА розумію і підтримую політику закладу з академічної доброчесності. Я не надавав(-ла) і не одержував(-ла) недозволену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Здобувач Гінзбург Данило Юрійович
Спеціальнсть 125 «Кібербезпека»
Освітня програма «Безпека інформаційних і комунікаційних систем»
Група БІКС-22
Керівник Делембовський М. М., доцент
Рецензент_____
(прізвище та ініціали)

Ідентичність підтверджую

Київ 2026р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: Автоматизації і інформаційних технологій
Випускова кафедра: Кібербезпеки та комп'ютерної інженерії
Ступінь вищої освіти: бакалавр
Спеціальність: 125 «Кібербезпека»
Освітня програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

Делембовський М.М.
„___”_____2026 року

З А В Д А Н Н Я
ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

Гінзбург Данило Юрійович
(прізвище, ім’я та по батькові здобувача)

1. Тема роботи OSINT – сценарії виявлення цифрового сліду організації в умовах навчального кіберполігону
затверджена наказом ректора КНУБА № 576/52-15/13.2/26 від «14» травня 2026 року.
2. Керівник роботи Делембовський М. М., доцент
(прізвище, ім’я та по батькові, науковий ступінь, вчене звання)
3. Термін подання здобувачем роботи до захисту _____
4. Зміст пояснювальної записки за розділами:
Р. 1. Аналіз предметної області та постановка задачі
Р. 2. Обґрунтування та розробка рішення
Р. 3. Практична реалізація та тестування сценарію ідентифікації цифрового сліду

5. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Розділ 1	08.05.2026
Розділ 2	14.05.2026
Розділ 3	25.05.2026
Остаточне оформлення роботи	08.06.2026
Направлення роботи для перевірки на плагіат	10.06.2026
Попередній захист роботи	12.06.2026
Направлення роботи на рецензування	12.06.2026

6. Дата видачі завдання «14» травня 2026 року

Керівник _____ Делембовський М. М

Здобувач _____ Гінзбург Д. Ю.

<table>
<tr><td>РЕЗЮМЕ
(SUMMARY)
до кваліфікаційної випускової роботи здобувача</td><td colspan="3">Гінзбург Данило Юрійович
Ginzburg Danylo Yuriyovych
здобувача українською та англійською мовами</td></tr>
<tr><td>ЗВО</td><td colspan="3">Київський національний університет будівництва і архітектури</td></tr>
<tr><td>Тема (українською та англійською)</td><td colspan="3">OSINT - сценарії виявлення цифрового сліду організації в умовах навчального кіберполігону
OSINT - scenarios for detecting an organization's digital footprint in a cyber training ground</td></tr>
<tr><td>Освітній ступінь</td><td colspan="3">Бакалавр</td></tr>
<tr><td>Факультет</td><td colspan="3">Автоматизації і інформаційних технологій</td></tr>
<tr><td>Випускова кафедра</td><td colspan="3">Кібербезпеки та комп’ютерної інженерії</td></tr>
<tr><td>Спеціальність</td><td colspan="3">125 “Кібербезпека”</td></tr>
<tr><td>Освітня програма</td><td colspan="3">Безпека інформаційних і комунікаційних систем</td></tr>
<tr><td>Керівник</td><td colspan="3">Делембовський Максим Михайлович</td></tr>
<tr><td rowspan="2">Обсяг роботи:</td><td>Пояснювальна записка, стор.</td><td>Розділів</td><td>Презентація, кількість слайдів</td></tr>
<tr><td>84</td><td>3</td><td>11</td></tr>
<tr><td>Розділ 1</td><td colspan="3">Аналіз предметної області та постановка задачі</td></tr>
<tr><td>Розділ 2</td><td colspan="3">Обґрунтування та розробка рішення</td></tr>
<tr><td>Розділ 3</td><td colspan="3">Практична реалізація та тестування сценарію ідентифікації цифрового сліду</td></tr>
<tr><td>Висновки по роботі</td><td colspan="3">У ході роботи практично доведено критичну небезпеку накопичення цифрових слідів та розроблено комплексний навчальний сценарій з п'яти OSINT завдань для безпечного тренування фахівців в умовах локального кіберполігона на базі платформи CTFd.</td></tr>
<tr><td>Ключові слова:
Keywords:</td><td colspan="3">OSINT, цифровий слід, кіберполігон, кібербезпека, CTFd, метадані, стеганографія, криптографія.
OSINT, digital footprint, cyber range, cybersecurity, CTFd, metadata, steganography, cryptography.</td></tr>
</table>

Здобувач Гінзбург Д.Ю./ _____

Керівник Делембовський М.М./ _____

Анотація

Кваліфікаційну роботу присвячено дослідженню цифрового сліду об'єктів за допомогою методів OSINT. Розроблено практичний сценарій для локального кіберполігона на базі платформи CTFd. Сценарій складається з п’яти етапів розвідки. Етапи охоплюють технічний аналіз метаданих графічних файлів. Проведено пошук профілів у соціальних мережах. Застосовано методи стеганографії та криптографічного розшифрування PGP ключів. Виконано статичний аудит вихідного коду для знаходження IP адрес. Створено синтетичну особистість за допомогою генеративних моделей для імітації цифрової активності. Отримані результати формують готовий інструментарій для тренування фахівців. Робота допомагає розробляти заходи з мінімізації витоків конфіденційних даних.

Ключові слова: OSINT, цифровий слід, кіберполігон, кібербезпека, CTFd, метадані, стеганографія, криптографія.

Abstract

The qualification graduation work is dedicated to the development of a practical scenario for identifying a company digital footprint in an educational cyber range environment. The relevance of the topic is determined by the growing number of confidential data leaks due to personnel negligence. The situation requires preparing cybersecurity specialists for threats applying OSINT methods. The work implements a five stage scenario based on the CTFd platform. This scenario covers the analysis of graphic file metadata, social media profiling, steganographic analysis, PGP key decryption, and source code auditing. To simulate a real environment, a synthetic digital persona was generated via the Nano Banana Pro artificial intelligence model. The practical significance of the work lies in preparing a ready training complex for specialists and forming recommendations for minimizing digital presence.

Keywords: OSINT, digital footprint, cyber range, cybersecurity, CTFd, metadata, steganography, cryptography.

ЗМІСТ

Вступ

Актуальність теми

Стрімкий розвиток інформаційних технологій змінює методи взаємодії бізнесу та суспільства. Компанії переносять більшість своїх бізнес процесів у цифрове середовище, отже, це спричиняє появу значного обсягу інформації про діяльність організацій у відкритому доступі. Персонал компаній активно застосовує соціальні мережі та різноманітні платформи для комунікації та обміну досвідом. Співробітники часто публікують дані про робочі процеси та технічні рішення. Такі публікації формують цифровий слід компанії в мережі Інтернет. Ці відомості стають доступними для аналізу без прямого проникнення в корпоративну інфраструктуру.

Зловмисники застосовують методи OSINT для ідентифікації критичних активів організації. Вони шукають імена користувачів та структури програмних репозиторіїв. Правопорушники аналізують метадані зображень для визначення географічного положення об’єктів та ідентифікації обладнання. Витоки через особисті профілі працівників дозволяють зловмисникам проводити атаки за допомогою соціальної інженерії. Питання захисту конфіденційної інформації від витоку через відкриті джерела має критичне значення для виживання бізнесу. Фахівці з кібербезпеки повинні вміти знаходити такі витоки раніше за зловмисників.

Навчальні заклади мають готувати студентів до реальних сценаріїв загроз у кіберпросторі. Застосування навчальних кіберполігонів дозволяє безпечно відпрацьовувати методики пошуку та ідентифікації цифрового сліду. Сценарії у вигляді практичних завдань-головоломок підвищують ефективність навчання майбутніх спеціалістів. Студенти вчаться бачити логічні зв’язки між фрагментами інформації з різних джерел, що, в свою чергу, допомагає розробляти стратегії мінімізації цифрового сліду для реальних компаній.

Об’єкт роботи

Процес формування та накопичення цифрового сліду об’єктів у відкритих інформаційних мережах.

Предмет роботи

Технічні методи аналізу метаданих, методики профілювання у соціальних мережах та програмні засоби аудиту вихідного коду для ідентифікації персональних та мережевих параметрів цільового об’єкта.

Мета роботи

Мета роботи полягає в розробці практичного сценарію для ідентифікації цифрового сліду. Буде створена система з п’яти послідовних завдань для спеціалістів з кібербезпеки. Ці завдання імітують дії зловмисника по збору конфіденційних даних про компанію та її персонал.

Завдання роботи

Для досягнення мети будуть виконуватися такі завдання:

- Оцінка технічних можливостей методів збору інформації з відкритих джерел.
- Дослідження функціональних параметрів інструментів для мережевого
- профілювання та аналізу метаданих.
- Розробка логічної структури сценарію з п’яти послідовних етапів розвідки.
- Генерація синтетичного візуального контенту та підготовка цифрових артефактів для імітації активності.
- Розгортання платформи CTFd та конфігурація параметрів валідації прапорів.
- Аналіз результатів практичного тестування та оцінка надійності задіяних програмних засобів.

Методи аналізу

Застосування системного аналізу для вивчення загроз кібербезпеці. Впровадження методів OSINT для ідентифікації цифрових об’єктів. Задіяння стеганографії для приховування інформації в межах завдань. Застосування

криптографічних методів для захисту та розшифрування ключів доступу. Технічний аналіз програмного коду для пошуку конфіденційних даних.

Практична цінність

Створення готового технічного інструментарію для тренувань у кіберполігоні. Сценарій дозволяє здобути практичні навички ідентифікації прихованих витоків даних. Організації отримують методологічну базу для проведення самостійного аудиту власного цифрового сліду.

Структура роботи

Пояснювальна записка складається з вступу, трьох розділів, висновків, списку джерел та додатків. Перший розділ містить аналіз стану галузі OSINT та постановку задачі. Другий розділ описує архітектуру сценарію та вибір інструментів. Третій розділ присвячений процесу реалізації завдань у кіберполігоні та аналізу результатів тестування.

Розділ 1. Аналіз предметної області та постановка задачі

1.1 Сучасний стан методології пошуку даних у відкритих мережах

Сучасна методологія пошуку даних у відкритих мережах спирається на системні принципи обробки інформації. Цей напрямок має назву Open Source Intelligence або OSINT. Дисципліна охоплює аналіз відомостей з публічних джерел. Глобальні мережі щоденно генерують величезні масиви даних. Фахівці з кібербезпеки застосовують ці масиви для захисту об’єктів. Методологія трансформується разом із розвитком програмних засобів. Спеціалісти з кібербезпеки вивчають ці підходи для протидії загрозам.

Інформаційний простір поділяють на кілька рівнів доступу. Перший рівень складає видима мережа або Surface Web. Пошукові системи індексують ці ресурси автоматично. Другий рівень охоплює глибоку мережу або Deep Web. Вміст цих сторінок не потрапляє до загальних пошукових результатів. Глибока мережа містить закриті форуми та бази даних компаній. Третій рівень складає темна мережа або Dark Web. Ця частина мережі потребує спеціальних анонімних протоколів для входу. Аналітики шукають на цих рівнях сліди витоків конфіденційної інформації.

Цикл розвідки на основі відкритих даних включає п’ять основних етапів:

1. Визначення вимог та планування. Аналітик формує список об’єктів для перевірки. Встановлюються пріоритети пошуку та визначаються часові межі проведення аналізу.
2. Активний збір відомостей. Спеціалісти застосовують технічні інструменти для автоматизації процесу. Збираються дані з сайтів та соціальних мереж. Фіксуються мережеві параметри систем.
3. Обробка отриманих фрагментів. Дані структуруються та сортуються за пріоритетами. Проводиться очищення від дублікатів та неактуальної інформації. Текст перекладається на зрозумілу аналітику мову.
4. Аналіз зв’язків. Фахівець встановлює логічні ланцюжки між різними джерелами. Застосовується метод мозаїчного складання картини [4], де кожен фрагмент доповнює загальний портрет цифрового сліду.

5. Підготовка звіту. Формуються висновки з рекомендаціями щодо захисту інформації. Результати передаються відповідальним особам для вжиття заходів.

Розвідка в соціальних медіа або SOCMINT (Social Media Intelligence) займає центральне місце в сучасній методології. Соціальні мережі накопичують персональні дані мільйонів користувачів. Профілі в різноманітних мережах дають інформацію про технологічний стек організації.

Співробітники публікують фотографії з робочих місць у популярних мережах. Аналіз цих зображень дозволяє ідентифікувати моделі серверного обладнання. Публікації допомагають зловмисникам зрозуміти внутрішню структуру компанії. Навіть коротке повідомлення містить дані про географічне розташування об’єкта.

Технічна частина методології фокусується на аналізі метаданих файлів. Метадані EXIF у зображеннях містять координати GPS та час зйомки. Ці дані допомагають встановити фізичне розташування офісів компанії. Репозиторії коду на порталах типу GitHub часто містять забуті паролі або API ключі. Програмісти залишають у коді адреси тестових серверів для відлагодження. Спеціалісти з безпеки аналізують ці вразливості для запобігання атакам. Вивчення історії комітів у репозиторіях дозволяє знайти дані які були видалені раніше.

Автоматизація збору даних значно підвищує швидкість ідентифікації об’єктів. Скрипти на мовах програмування дозволяють перевіряти сотні сайтів за лічені хвилини. Деякі утиліти шукають акаунти за унікальним іменем користувача. Ці інструменти показують присутність особи на різних онлайн платформах. Методологія передбачає застосування спеціалізованих баз даних [1] для перевірки поштових адрес, що дозволяє встановити факти попередніх витоків облікових записів. Програмні комплекси візуалізують зв’язки між людьми та технічними пристроями.

Навчальні кіберполігони забезпечують безпечну платформу для відпрацювання методик. Студенти моделюють дії зловмисників у

контрольованому середовищі. Практичні завдання у формі головоломок розвивають аналітичне мислення майбутніх фахівців. Сценарії включають пошук цифрового сліду через складні ланцюжки перехідних даних, це готує фахівців до реальних викликів. Кіберполігон імітує роботу реальних веб сервісів та баз даних. Така підготовка формує практичні навички захисту корпоративних ресурсів.

Етичні норми та законодавство України формують межі пошуку інформації. Збір даних має відбуватися без порушення приватності осіб. Фахівці дотримуються норм закону про захист персональних даних. Методологія OSINT не передбачає несанкціонованого доступу до закритих систем. Робота ведеться виключно з даними які власники зробили доступними для перегляду. Фахівець несе відповідальність за коректне застосування отриманих результатів. Аналітична праця базується на принципах об’єктивності та точності висновків.

Методологія пошуку у відкритих мережах постійно вдосконалюється. З’являються нові алгоритми для аналізу великих масивів неструктурованих даних. Фахівці поєднують ручні методи перевірки з інструментами автоматичного пошуку, це дозволяє ефективно знаходити приховані загрози для діяльності бізнесу. Постійний моніторинг цифрового сліду є обов’язковим елементом сучасної системи безпеки. Данна сфера вимагає глибокого розуміння цих процесів для надійного захисту інформаційного простору.

Розвиток методів OSINT зумовлює появу нових інструментів для ідентифікації прихованих об’єктів. Аналіз цифрових слідів потребує уваги до дрібних деталей. Кожен підрозділ компанії формує власну частину загального інформаційного поля. Співробітники відділів кадрів або маркетингу стають джерелом витоку технічних подробиць. Методологія передбачає регулярне проведення аудитів публічних ресурсів. Це допомагає виявляти конфіденційні дані до їх застосування зловмисниками. Знання методів розвідки дозволяє будувати ефективні бар’єри для витоків інформації.

1.2 Аналіз ризиків безпеки для компанії через наявність цифрового сліду персоналу

Цифровий слід персоналу є сукупністю даних які працівники залишають у мережі під час професійної діяльності або приватного життя. Ці дані формують інформаційний портрет організації. Кожна публікація чи коментар працівника може містити фрагменти конфіденційних відомостей. Зловмисники аналізують ці фрагменти для пошуку вразливостей у системі захисту компанії. Людський фактор залишається одним із найбільш критичних елементів у забезпеченні кібербезпеки.

Основним ризиком є проведення цілеспрямованої розвідки на основі відкритих джерел. Зловмисники збирають дані про структуру компанії через особисті профілі працівників у соціальних мережах. Профілі на професійних платформах часто містять детальний опис обов’язків та технологічного стеку. Працівники вказують конкретні версії програмного забезпечення чи моделі обладнання з якими вони працюють. Ця інформація дозволяє правопорушникам підібрати специфічні експлойти для атаки на корпоративну мережу. Вивчення списків контактів працівників допомагає зловмисникам зрозуміти ієрархію підпорядкування та ідентифікувати ключових осіб що мають доступ до критичних даних.

Ризик застосування методів соціальної інженерії [6] значно зростає при наявності детального цифрового сліду. Зловмисники вивчають уподобання та хобі працівників. Вони аналізують місця відпочинку та графіки активності персоналу. Ці відомості стають основою для створення персоналізованих фішингових повідомлень. Працівник з більшою ймовірністю відкриє шкідливий файл чи перейде за посиланням якщо тема листа відповідає його актуальним інтересам. Використання професійної термінології та імен реальних колег у таких повідомленнях підвищує рівень довіри жертви. Це призводить до компрометації робочих станцій та проникнення всередину периметра безпеки.

Технічні витоки через візуальний контент складають окрему групу ризиків. Працівники часто публікують фотографії з робочих місць або селфі в

офісних приміщеннях. На задньому фоні таких зображень можуть бути зафіксовані монітори з відкритими вікнами програм чи корпоративною поштою. Іноді на фото потрапляють паперові стікери з логінами та паролями або схеми мережі на дошках для нарад. Аналіз таких зображень дозволяє зловмисникам отримати прямі доступи до внутрішніх ресурсів без технічних зусиль. Метадані цифрових фотографій містять координати GPS які вказують на точне розташування офісів або віддалених об’єктів компанії.

Публікація робочих фрагментів коду в особистих репозиторіях персоналу несе пряму загрозу безпеці. Програмісти застосовують публічні платформи для зберігання напрацювань або тестування скриптів. У коді випадково залишаються конфіденційні параметри такі як токени доступу чи адреси баз даних. Навіть після видалення таких даних історія комітів дозволяє відновити первинні версії файлів. Зловмисники автоматизовано сканують репозиторії на наявність подібних витоків. Це дає можливість миттєво отримати контроль над серверами компанії або внести шкідливий код у продукти організації.

Ризик ідентифікації внутрішніх процесів через цифрову активність персоналу впливає на загальну стійкість бізнесу. Коментарі працівників на форумах щодо технічних проблем допомагають правопорушникам зрозуміти слабкі місця інфраструктури. Обговорення планових робіт чи впровадження нових засобів захисту дає зловмисникам час для підготовки атак до моменту завершення налаштування систем. Опис процедур безпеки в оголошеннях про пошук нових співробітників також стає джерелом цінних відомостей для зовнішньої розвідки. Компанія втрачає перевагу прихованості своїх оборонних механізмів.

Використання однакових облікових даних для приватних та робочих сервісів є поширеною помилкою персоналу. Зловмисники отримують бази паролів від скомпрометованих сторонніх сайтів. Вони застосовують ці логіни та паролі для спроб входу в корпоративні системи. При відсутності багатофакторної автентифікації цей метод дозволяє отримати доступ до робочої пошти чи хмарних сховищ. Цифровий слід працівника на сумнівних ресурсах

збільшує ймовірність того що його дані будуть використані для масових атак на організацію.

Репутаційні ризики пов’язані з поведінкою персоналу в мережі впливають на довіру клієнтів та партнерів. Негативні відгуки чи нецензурна лексика працівників від імені компанії псують її імідж. Зловмисники можуть використовувати ці конфлікти для дискредитації організації. Вони створюють фейкові профілі на основі реальних даних персоналу для поширення дезінформації. Це спричиняє фінансові втрати та юридичні ускладнення для бізнесу.

Навчальний кіберполігон є місцем де фахівці вчаться аналізувати ці складні ланцюжки ризиків. Завдання на основі ідентифікації цифрового сліду допомагають студентам зрозуміти як одна помилка працівника ставить під загрозу всю компанію. Моделювання ситуацій витоку даних дозволяє розробити протоколи реагування на інциденти. Студенти відпрацьовують навички пошуку прихованих зв’язків між публічними профілями та технічними параметрами мережі.

Аналіз ризиків має бути регулярним процесом у межах стратегії кібербезпеки [7]. Організації повинні впроваджувати політику безпечної поведінки працівників у мережі Інтернет, це включає обмеження на публікацію робочої інформації та перевірку налаштувань приватності в соціальних мережах. Навчання персоналу основам цифрової гігієни зменшує ймовірність реалізації описаних загроз. Розуміння механізмів формування цифрового сліду дозволяє фахівцям будувати захищені інформаційні системи. Компанії що ігнорують ризики пов’язані з людським фактором стають легкими цілями для сучасних кібератак.

Постійний моніторинг відкритого інформаційного простору допомагає виявити витоки на ранніх етапах. Аналітична робота з цифровим слідом вимагає уваги до деталей та знання методів соціальної інженерії. Фахівці з кібербезпеки застосовують системний підхід для оцінки впливу кожної знайденої деталі на загальний стан захисту. Результатом такого аналізу є розробка рекомендацій

щодо мінімізації цифрової присутності критичних об’єктів. Це зміцнює стійкість компанії до зовнішніх впливів та підвищує рівень довіри до її цифрової інфраструктури.

1.3 Огляд програмних засобів для автоматизації збору інформації та аналізу метаданих

Автоматизація процесів збору та аналізу даних є критичною умовою успішного проведення OSINT досліджень. Сучасні обсяги інформації в мережі унеможливлюють ефективний ручний пошук. Фахівці з кібербезпеки застосовують спеціалізований інструментарій для прискорення ідентифікації об’єктів. Програмні засоби забезпечують точність обробки технічних параметрів файлів та мережевих профілів. Кожна утиліта має вузьку спеціалізацію та вирішує конкретні завдання в межах загального сценарію.

Програмний засіб ExifTool [8] є стандартом у галузі аналізу метаданих цифрових об’єктів. Це незалежна бібліотека та додаток командного рядка для читання та запису метаінформації. Автор програми Філ Харві забезпечив підтримку понад тисячі різних форматів файлів. Інструмент працює із зображеннями, відео, аудіо та документами. Основна перевага ExifTool полягає в можливості витягувати дані які не відображаються стандартними засобами операційних систем. Сюди належать теги EXIF, IPTC, XMP [2] та специфічні дані виробників обладнання. Фахівець отримує доступ до параметрів пристрою, серійних номерів та налаштувань програмного забезпечення для редагування. Особливе значення мають GPS координати та часові мітки створення файлу. Ці дані дозволяють встановити точне місце розташування та час події. Утиліта надає можливість пакетної обробки директорій, що дозволяє аналізувати тисячі фотографій за один цикл роботи. Результати аналізу можна експортувати у формати JSON, CSV або XML для подальшої автоматизованої обробки іншими системами.

Утиліта Sherlock [9] призначена для ідентифікації присутності користувача на різних онлайн платформах за його унікальним іменем. Програма

написана на мові Python та використовує асинхронні запити до мережевих ресурсів. Логіка роботи базується на перевірці наявності сторінки за конкретною адресою через HTTP статус коди. Sherlock аналізує понад 350 популярних сайтів, форумів та соціальних мереж. Користувачі часто використовують один і той самий нікнейм для реєстрації на різних ресурсах. Це дозволяє аналітику зв’язати професійні профілі з приватними акаунтами. Програма автоматично видає прямі посилання на знайдені сторінки. Технічна особливість утиліти полягає у використанні специфічних User-Agent для імітації дій реального браузера. Це допомагає уникати блокувань з боку систем захисту сайтів. Швидкість роботи Sherlock забезпечує миттєве отримання результатів навіть при великому списку ресурсів для перевірки.

Утиліта Maigret [10] представляє собою прогресивний засіб для проведення розвідки за іменем користувача на основі відкритих джерел. Програма здійснює автоматизований пошук профілів на понад 3000 веб ресурсах. Головна технічна перевага maigret полягає в проведенні глибокого контентного аналізу сторінок. Інструмент не обмежується лише перевіркою HTTP статус кодів відповідей серверів. Програма аналізує HTML теги. Метадані та текстові фрагменти для підтвердження реальної присутності об’єкта. Утиліта підтримує функцію рекурсивного пошуку. Це дозволяє автоматично ідентифікувати додаткові нікнейми. Поштові адреси або посилання на інші ресурси. Результати роботи maigret включають формування детальних звітів у форматах HTML. JSON або PDF. Спеціалісти задіюють цей інструмент для побудови складних логічних зв’язків між акаунтами в різних соціальних мережах та на тематичних форумах. Технічна база програми постійно оновлюється через активну спільноту розробників на GitHub [3], що забезпечує високу точність ідентифікації цифрового сліду в умовах постійних змін структури веб сайтів.

Засоби стеганографії дозволяють реалізувати методи прихованої передачі даних усередині цифрових контейнерів. Утиліта Steghide [11] є ефективним інструментом для впровадження та вилучення зашифрованої інформації. Вона

працює із зображеннями форматів JPEG та BMP, а також аудіо файлами WAV та AU. Програма використовує метод найменш значущого біта для приховування даних, що забезпечує візуальну ідентичність файлу після впровадження повідомлення. Steghide застосовує алгоритми стиснення та шифрування перед початком процесу вбудовування. Це захищає інформацію від випадкового виявлення. Для доступу до прихованого вмісту необхідне знання пароля. Програма підтримує шифрування за алгоритмом Rijndael-128, що гарантує конфіденційність навіть при виявленні факту наявності стеганографії. Фахівці застосовують цей інструмент для створення складних завдань у кіберполігоні. Студенти вчаться ідентифікувати приховані дані які не відображаються при звичайному перегляді файлів.

Програмний комплекс GnuPG забезпечує [12] реалізацію стандартів криптографічного захисту через систему PGP ключів. Це вільний аналог комерційного ПЗ PGP для захисту цифрової комунікації. Інструмент базується на системі асиметричного шифрування з використанням відкритих та закритих ключів. Користувачі застосовують GnuPG для шифрування текстових повідомлень, файлів та створення цифрових підписів. Програма дозволяє підтверджувати авторство контенту та забезпечувати цілісність даних. У межах OSINT досліджень GnuPG стає засобом для аналізу знайдених шифрів та ключів у репозиторіях. Фахівець може ідентифікувати власника ключа через ідентифікатор користувача в структурі PGP сертифіката. Утиліта підтримує гнучке управління кільцями ключів та рівнями довіри, це дозволяє будувати захищені канали зв’язку в межах сценаріїв кіберполігона.

Вибір конкретного інструментарію для ідентифікації цифрового сліду вимагає детального порівняння з існуючими аналогами. Кожна обрана програма проходить оцінку за технічними параметрами та зручністю впровадження в автоматизовані ланцюжки.

Аналіз можливостей ExifTool демонструє значну перевагу над інструментами FOCA [13] та Exiv2 [14]. ExifTool має підтримку запису метаданих та обробки рідкісних форматів файлів. Програма FOCA потребує

графічного середовища Windows та обмежує гнучкість налаштувань. Утиліта Exiv2 має менший набір доступних тегів для обробки та гіршу підтримку скриптів. Отже, обрано ExifTool для забезпечення максимальної глибини аналізу медіа контенту. Детальні критерії та результати порівняння цих засобів наведено в таблиці 1.1.

Таблиця 1.1 - Порівняння засобів обробки метаінформації

ПАРАМЕТР	**EXIFTOOL**	**FOCA**	**EXIV2**
Кількість форматів	Понад 1000	Близько 15	Близько 30
Робота в терміналі	Повна підтримка	Відсутня	Обмежена
Функція запису даних	Наявна	Відсутня	Наявна
Підтримка скриптів	Висока	Відсутня	Середня
Кросплатформність	Висока	Низька	Середня

Порівняння Sherlock із утилітами Maigret та Social Analyzer підтверджує раціональність швибору. Sherlock забезпечує високу швидкість обробки запитів через легку структуру програмного коду але періодично видає помилкові дані. Програма Maigret надає велику кількість посилань, але, так само, періодично видає помилкові результати через специфіку алгоритмів. Social Analyzer [15] потребує значних обсягів оперативної пам’яті та складного налаштування додаткових модулів. Отже, задіяно Sherlock для миттєвого отримання списку профілів без зайвого навантаження на систему. Зведені характеристики інструментів для мережевого пошуку представлено в таблиці 1.2.

Таблиця 1.2 - Порівняння засобів мережевого пошуку

ПАРАМЕТР	**SHERLOCK**	**MAIGRET**	**SOCIAL ANALYZER**

Продовження таблиці 1.2

Кількість ресурсів	Понад 350	Понад 2000	Понад 1000
Швидкість роботи	Висока	Середня	Низька
Системні вимоги	Мінімальні	Середні	Високі
Складність налаштування	Низька	Середня	Висока
Формат звітів	Текст та JSON	Текст та HTML	Графічний та текст

Вивчення Steghide на фоні OpenStego та Stegsolve виявляє унікальні переваги для захисту даних. Steghide впроваджує криптографічний захист усередину контейнера автоматично. Програма OpenStego [16] лише ховає дані без додаткового перетворення. Утиліта Stegsolve [17] призначена для візуального вивчення шарів зображення та не підтримує автоматизацію через командний рядок. Отже, застосовано Steghide для гарантованої конфіденційності прапорів у межах кіберполігона. Технічне порівняння обраних засобів стеганографії наведено в таблиці 1.3.

Таблиця 1.3 - Порівняння засобів стеганографії

ПАРАМЕТР	**STEGHIDE**	**OPENSTEGO**	**STEGSOLVE**
Тип контейнерів	JPEG, BMP, WAV	Лише зображення	Лише зображення
Вбудований шифр	AES 128	Відсутній	Відсутній
Стиснення даних	Наявне	Наявне	Відсутнє
Робота в терміналі	Наявна	Обмежена	Відсутня

Продовження таблиці 1.3

Робота з аудіо	Наявна	Відсутня	Відсутня

Аналіз GnuPG у порівнянні з OpenSSL та PGP Desktop підкреслює спеціалізацію на захисті документів користувача. GnuPG має відкритий код та повну відповідність актуальним стандартам OpenPGP. Програма OpenSSL [18] орієнтована на роботу з мережевими протоколами та сертифікатами сайтів. Комерційний продукт PGP Desktop [37] має закритий код та високу вартість ліцензії. Отже, впроваджено GnuPG для ідентифікації авторства цифрового контенту через надійне розшифрування ключів. Основні параметри та відмінності засобів криптографічного захисту узагальнено в таблиці 1.4.

Таблиця 1.4 - Порівняння засобів криптографічного захисту

ПАРАМЕТР	**GNUPG**	**OPENSSL**	**PGP DESKTOP**
Вартість ліцензії	Безкоштовно	Безкоштовно	Платно
Тип коду	Відкритий	Відкритий	Закритий
Керування ключами	Зручне	Складне	Автоматичне
Профільна задача	Тексти та файли	Мережеві сертифікати	Корпоративна пошта
Стандарт роботи	OpenPGP	X.509, TLS	Proprietary PGP

Інтеграція цих інструментів у єдиний ланцюжок дозволяє вирішувати комплексні завдання. Аналітик починає з обробки первинного файлу за допомогою ExifTool для отримання технічних зачіпок. Знайдені імена користувачів стають вхідними даними для утиліти Sherlock. Отримані посилання на соціальні мережі та репозиторії GitHub дозволяють знайти додатковий контент. Зображення з цих ресурсів перевіряються через Steghide на наявність прихованих шифрів. Знайдені криптографічні контейнери обробляються за допомогою GnuPG для отримання фінальних прапорів. Така

послідовність дій демонструє логіку переходу від відкритої інформації до глибоко прихованих технічних даних.

Використання засобів автоматизації з відкритим вихідним кодом забезпечує прозорість методів дослідження. Спеціаліст має можливість перевірити вихідний код кожної утиліти на відсутність шкідливих функцій. Це підвищує рівень довіри до отриманих результатів аналізу. Більшість цих програм легко інтегруються в автоматизовані скрипти на мовах Bash або Python. Це дозволяє створювати власні фреймворки для моніторингу цифрового сліду. Навчання роботі з цими інструментами є невід'ємною частиною практичної підготовки аналітиків безпеки.

Сценарії кіберполігона використовують ці інструменти як базові засоби для проходження завдань. Кожна утиліта навчає студента окремому аспекту роботи з даними. Аналіз метаданих формує увагу до деталей. Пошук акаунтів розвиває навички мережевої розвідки. Стеганографія та криптографія дають розуміння методів захисту інформації. Компанії застосовують аналогічні підходи для внутрішнього аудиту та виявлення потенційних каналів витоку даних. Розуміння функціоналу програмних засобів дозволяє фахівцю обирати оптимальний інструмент для конкретної ситуації.

Постійне оновлення програмного забезпечення є обов'язковим через зміни у структурах веб сайтів та форматах файлів. Розробники утиліт вносять правки для підтримки нових алгоритмів обробки даних, отже фахівець з кібербезпеки має стежити за оновленнями та новими можливостями інструментарію, а це гарантує актуальність методів збору інформації у динамічному цифровому середовищі.

1.4 Характеристика середовища навчального кіберполігона як платформи для тестування

Навчальний кіберполігон виступає спеціалізованою платформою для відпрацювання практичних навичок у сфері захисту інформації. Платформи такого типу створюють ізольоване середовище для моделювання кібератак та

перевірки методів оборони. Використання кіберполігона дозволяє студентам працювати з реальними інструментами без загрози для зовнішніх мереж. Сценарії проходження завдань будуються на логічних зв'язках між фрагментами даних.

Для реалізації освітнього проекту обрано платформу CTFd (Capture The Flag daemon) [19]. Це програмне забезпечення з відкритим вихідним кодом для організації змагань із кібербезпеки. Вибір даної платформи зумовлений потребою у гнучкому налаштуванні мережевих параметрів. Професійні OSINT утиліти потребують стабільного з'єднання з мережею Інтернет для звернення до баз даних соціальних платформ. Локальне розгортання CTFd забезпечує повний контроль над технічним стеком та мережевою доступністю. Платформа підтримує створення інтерактивних завдань із автоматичною перевіркою текстових прапорів.

Технічна база полігона включає використання засобів віртуалізації Oracle VirtualBox [20]. Робоче середовище базується на операційній системі Kali Linux [21]. Це забезпечує наявність попередньо встановлених утиліт для проведення розвідки та технічного аналізу. Використання локальної віртуальної машини дозволяє уникнути обмежень хмарних платформ щодо зовнішнього трафіку. Студенти отримують стабільний доступ до об'єктів дослідження та інструментів ідентифікації цифрового сліду.

Розгортання платформи CTFd виконується за допомогою технології контейнеризації Docker [22]. Застосування Docker Compose дозволяє ізолювати компоненти системи та забезпечити швидку відбудову середовища у випадку технічних збоїв. Архітектура рішення включає окремі контейнери для веб сервера та бази даних, що гарантує надійність збереження результатів тестування та статистики проходження сценарію. Контейнеризація спрощує процес перенесення полігона між різними апаратними конфігураціями.

Процес розробки сценарію у середовищі CTFd передбачає налаштування параметрів кожного з п'яти завдань. Встановлюється категорія OSINT для всіх етапів ідентифікації. Обирається режим User Mode для забезпечення

індивідуального оцінювання знань кожного учасника. Платформа дозволяє додавати детальні описи (Task Content) та посилання на зовнішні артефакти дослідження. Для кожного завдання прописується система підказок та умови нарахування балів.

Гейміфікація процесу навчання реалізується через систему рейтингів та візуалізацію успіхів у реальному часі. Правильне введення прапора призводить до миттєвої зміни позиції студента у загальній таблиці Scoreboard. Це стимулює конкуренцію та підвищує рівень зацікавленості у розв’язанні складних аналітичних задач. Система CTFd дозволяє адміністратору відстежувати час виконання кожного етапу. Аналіз цих даних допомагає виявляти найбільш складні фрагменти сценарію для подальшої корекції навчального матеріалу.

Ізоляція та безпека проведення експериментів є ключовою характеристикою середовища. Студенти застосовують методи ідентифікації профілів та аналізу коду в межах встановленого регламенту. Платформа забезпечує цілісність завдань для кожного користувача. Коректна обробка прапорів незалежно від регістру символів підвищує логічну стійкість системи тестування.

Характеристика кіберполігона підкреслює важливість поєднання теорії з практикою. Платформа CTFd перетворює абстрактні методи розвідки на послідовні технічні операції. Студенти отримують досвід роботи в умовах близьких до реальності, ще розвиває професійну інтуїцію аналітика та формує впевненість у навичках ідентифікації цифрового сліду. Сценарій на базі CTFd та Docker стає вагомим внеском у практичну базу підготовки фахівців.

Кіберполігон виступає надійним містком між академічними знаннями та фаховою діяльністю. Ведення детальних журналів активності дозволяє проводити розбір помилок після завершення сценарію. Система повідомлень сприяє обміну досвідом між учасниками розслідування. Використання сучасних засобів автоматизації перевірки знань підвищує якість освітнього процесу та забезпечує об’єктивність фінальних оцінок.

1.5 Постановка технічного завдання та проведення етапів ідентифікації об’єктів

Технічне завдання, що вказано нижче - описує детальну логіку побудови практичного сценарію для навчального кіберполігона. Розроблено послідовну структуру з п’яти взаємопов’язаних завдань. Кожен етап імітує реальну дію зловмисника під час проведення розвідки на основі відкритих джерел. Метою завдання є повна ідентифікація цифрового профілю особи та місця її перебування.

Завдання 1. Технічний аналіз метаданих графічного контейнера. Надано вхідний файл у форматі зображення для первинного аналізу. Вимагається провести глибоке дослідження внутрішньої структури файлу. Студент застосовує утиліту ExifTool для перевірки всіх доступних тегів метаданих. Основним об’єктом пошуку стає специфічне поле export file name. Це поле часто містить оригінальну назву файлу яка була автоматично згенерована операційною системою під час експорту. З цієї назви студент має виокремити ім’я облікового запису користувача комп’ютера або username. Отриманий унікальний ідентифікатор стає першим прапором для успішного завершення етапу.

Завдання 2. Мережева розвідка та ідентифікація соціальних профілів. Отриманий на попередньому етапі username є вхідним параметром для масштабного пошуку в мережі. Студент застосовує автоматизовані інструменти, наприклад, Sherlock для сканування глобальних платформ. Метою є знаходження активних акаунтів користувача у соціальних мережах Instagram або X. Після виявлення профілів необхідно провести аналіз публічної інформації в описі сторінки. Студент шукає реальне ім’я та прізвище особи які вказані користувачем для ідентифікації. Знайдене повне ім’я стає текстовим прапором для другого завдання.

Завдання 3. Криміналістичний аналіз візуального контенту [24] та пошук конфіденційних даних.
Увагу студента спрямовется на детальне вивчення публікацій у знайдених соціальних мережах. Серед великої кількості контенту необхідно знайти

специфічне фото робочого простору. На зображенні зафіксований користувач біля персонального комп'ютера. Студент проводить візуальний аналіз об'єктів що знаходяться на столі або приклеєні до монітора. Об'єктом пошуку є паперова наліпка з технічними записами. Студент ідентифікує тестовий User ID та пароль до спеціалізованої програми. Ці дані є ключовим прапором третього етапу.

Завдання 4. Стеганографія та криптографічний аналіз у сховищах коду. Тут вже використовується посилання на GitHub репозиторій яке було знайдено в одному з постів соціальної мережі. Користувач хвалиться розробкою власного скрипта. Студент аналізує вміст репозиторію та знаходить зображення з описом про PGP ключі. Необхідно виконати стеганографічний аналіз цього файлу за допомогою Steghide для пошуку прихованих об'єктів. Студент витягує PGP шифр за допомогою технічних засобів аналізу зображень. Далі проводиться робота з утилітою GnuPG для розшифрування отриманого блоку даних. Результатом операції стає реальна email адреса користувача. Ця адреса є прапором четвертого завдання.

Завдання 5. Статичний аналіз коду та геолокація за мережевими параметрами.

Фінальний етап дослідження всередині того самого GitHub акаунта. Студент аналізує вихідний код утиліти для перевірки мережевого з'єднання про яку згадував користувач. Під час перегляду коду необхідно знайти жорстко закодовану IP адресу яку розробник залишив для тестування. Студент використовує цю адресу для визначення фізичного місця розташування сервера або пристрою. За допомогою баз даних GeoIP проводиться ідентифікація міста де знаходиться об'єкт. Назва міста стає фінальним прапором для завершення всього сценарію в кіберполігоні.

Така постановка завдання забезпечує комплексну перевірку знань студента. Об'єднуються навички роботи з метаданими та знання методів криптографії в одну логічну лінію. Сценарій вчить бачити загрози в розрізнених фрагментах публічної інформації. Кожен крок сценарію є технічно

обґрунтованим та має чіткий критерій виконання.

1.6 Психологічні аспекти формування цифрового сліду та соціальна інженерія

Людський фактор залишається головним джерелом вразливостей у системах кібербезпеки, технічні засоби захисту не здатні повністю нівелювати наслідки недбалої поведінки персоналу. Користувачі формують власний цифровий слід через глибокі психологічні потреби та когнітивні викривлення. Розуміння цих механізмів дозволяє фахівцям прогнозувати можливі канали витоку конфіденційної інформації.

Головною причиною надмірного поширення контенту є потреба в соціальному визнанні та схваленні. Публікація інформації про професійні успіхи або робоче середовище викликає позитивні емоційні реакції в мережах, це, в свою чергу, стимулює викид дофаміну в головному мозку. Користувачі прагнуть підтримувати свій статус експерта або успішного працівника. Працівники відчувають гордість за свої технічні досягнення. Вони публікують фрагменти коду в репозиторіях для демонстрації навичок колегам. Ця гордість часто переважає над усвідомленням ризиків безпеки.

Когнітивні викривлення спотворюють сприйняття реальних загроз у мережевому просторі. Ефект оптимізму змушує людину вірити в низьку ймовірність кібератаки саме проти неї. Користувач вважає свій аккаунт або діяльність занадто дрібними для уваги професійних зловмисників. Ілюзія анонімності в мережі створює хибне відчуття захищеності під час публікації даних. Люди забувають про неминучість тривалого зберігання цифрових слідів у пошукових архівах. Короткочасна вигода від зручності переважає над довготривалими наслідками для безпеки організації.

Пріоритет зручності над безпекою спричиняє більшість технічних витоків. Працівники записують паролі на фізичних носіях для миттєвого доступу (папірці, блокноти, тощо) до складних систем. Вони сприймають робоче місце як приватну та безпечну зону. Це призводить до появи

конфіденційних даних на фотографіях у соціальних мережах. Користувач фокусується на головному об’єкті зйомки, він не аналізує вміст фону зображення, а зловмисники використовують цю неуважність для отримання ідентифікаторів доступу.

Соціальна інженерія [25] базується на використанні цих психологічних особливостей. Зловмисники застосовують тригери довіри та авторитету. Вони вивчають цифровий слід для створення переконливої легенди спілкування. Знання деталей приватного життя працівника дозволяє маніпулювати його діями. Користувачі легше розкривають дані особам зі схожими інтересами або професійним досвідом. Виявлений цифровий слід стає ключем для обходу технічних бар’єрів через маніпуляцію людиною. Систематизований опис цих психологічних чинників та їх наслідків для кібербезпеки наведено в таблиці 1.5.

Таблиця 1.5 - Порівняльна таблиця психологічних чинників витоку даних

Психологічний чинник	**Опис механізму впливу**	**Наслідок для кібербезпеки**
Потреба у визнанні	Публікація досягнень для отримання лайків	Витік фрагментів коду та планів
Ефект оптимізму	Нехтування правилами через віру в безпеку	Відсутність паролів на пристроях
Пріоритет зручності	Використання паперових нотаток з даними	Паролі на фото робочих місць
Ілюзія приватності	Віра в обмежене коло читачів постів	Публікація робочих email адрес
Професійна гордість	Бажання похвалитися написаним скриптом	IP адреси у відкритих репозиторіях

Філософія цифрової присутності вимагає балансу між відкритістю та захищеністю. Повна відсутність цифрового сліду в сучасному світі майже

неможлива. Організації мають прищеплювати персоналу навички цифрової гігієни. Це включає критичне ставлення до кожного опублікованого фрагмента даних. Навчання методам соціальної інженерії допомагає працівникам впізнавати спроби маніпуляції на ранніх стадіях.

Навчальний кіберполігон імітує ці сценарії людських помилок. Завдання з пошуку пароля на папірці або email адреси в PGP ключі базуються на реальних кейсах. Студенти вчаться бачити за технічними параметрами поведінкові патерни користувачів. Така підготовка зміцнює стійкість компанії до атак із застосуванням людського фактора.

Розділ 2. Обґрунтування та розробка рішення

2.1 Розробка алгоритму та детального сценарію практичного завдання

Формування практичного сценарію для платформи CTFd базується на створенні послідовного ланцюжка завдань. Кожен етап має чіткий технічний взаємозв'язок із результатами попередніх кроків. Сценарій імітує реальну ситуацію витоку конфіденційних відомостей через недотримання правил цифрової гігієни. Алгоритм проходження включає п'ять основних етапів (дивитися рисунок 2.1).

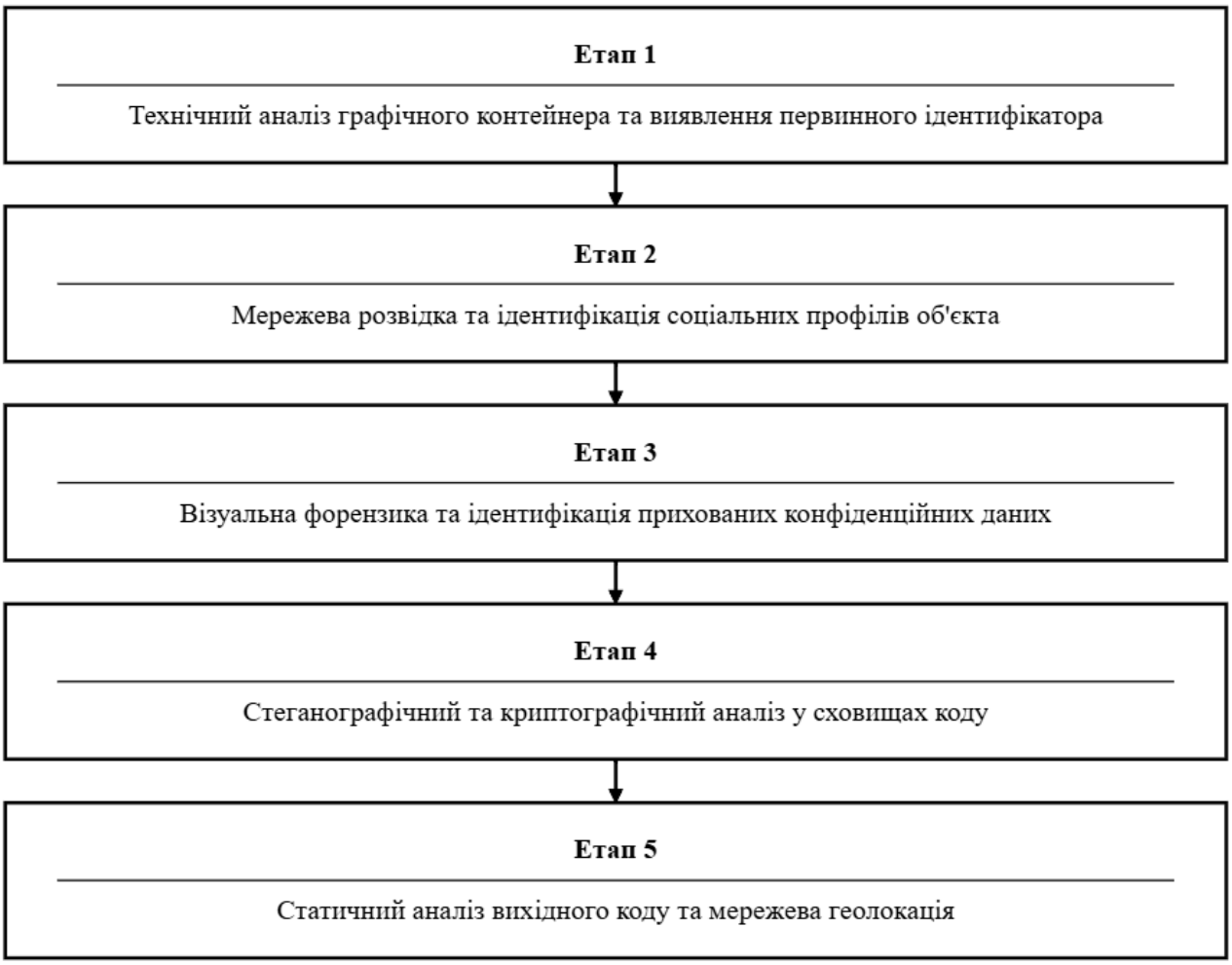

Рисунок 2.1 - П'ять етапів сценарію

Етап 1. Для початку проходження сценарію готується вхідний цифровий артефакт. Обирається файл у форматі зображення без застосування алгоритмів стиснення даних. Це дозволяє зберегти оригінальну структуру технічних

заголовків. Створюється стандартне портретне фото паспортного формату. На зображенні представлено чоловіка у діловому костюмі на білому фоні. Фотографія слугує відправною точкою для ідентифікації прихованої інформації.

Головна мета етапу полягає у виявленні технічних слідів створення файлу. Користувачі часто ігнорують факт наявності метаданих у медіафайлах перед їх публікацією, що стає першою точкою входу для проведення розвідки. Для виконання завдання використовується утиліта ExifTool. Цей інструмент дозволяє отримати доступ до повного переліку тегів графічного контейнера.

Завантажується зображення в ізольоване середовище кіберполігона. Студент запускає процес аналізу метаданих через командний рядок. Проводиться детальний огляд вихідного тексту програми. Серед великого обсягу системних параметрів увага фокусується на полях Source та Preserved Filename. Ці поля часто містять дані про первинне розташування об’єкта на файловій системі пристрою автора.

У результаті виконання команди знаходиться шлях х до файлу. Шлях має вигляд C:\Users\cjlarksonn\Desktop\J.Clarkson.png. Аналізується структура цього рядка. Папка всередині розділу Users в операційних системах Windows ідентифікує ім’я облікового запису користувача. Виокремлюється рядок cjlarksonn як унікальний нікнейм об’єкта. Цей ідентифікатор стає першим прапором для завершення завдання. Отриманий username стає основою для проведення подальших етапів мережевої розвідки.

Етап 2. На другому етапі використовується знайдений нікнейм cjlarksonn для розширення зони пошуку в мережі Інтернет. Створюється ситуація технічної неочевидності для учасника тестування. Студент має самостійно обрати оптимальний метод ідентифікації акаунтів. Передбачається використання утиліт автоматичного пошуку таких як Maigret або Sherlock. Також залишається можливість застосування методів прямого пошуку через складні запити Google Dorking.

Для реалізації сценарію заздалегідь наповнюються контентом три

цифрові майданчики. Це профілі в соціальних мережах Instagram, X та на платформі зберігання коду GitHub. Застосування автоматизованих засобів дозволяє миттєво підтвердити присутність користувача на цих ресурсах. Кожен знайдений профіль додає нові фрагменти до загального портрета об’єкта.

Проводиться аналіз доступної інформації на знайдених сторінках. Аккаунт у мережі X має обмежену видимість публікацій, але містить опис профілю. Сторінка в Instagram є більш детальною та містить велику кількість візуального контенту. Студент вивчає текстові блоки в розділах біографії акаунтів.

Головним завданням етапу стає встановлення реальних персональних даних особи. Користувачі часто вказують справжнє ім’я та прізвище для ведення професійної комунікації. Ці дані знаходяться в описах профілів Instagram та X. Комбінація імені та прізвища стає текстовим прапором для другого завдання. Цей етап демонструє як використання однакових нікнеймів дозволяє пов’язати технічні дані з реальною особистістю працівника.

Етап 3. Третій етап сценарію вимагає проведення глибокого візуального аналізу публікацій. Об’єктом дослідження стає знайдений аккаунт у мережі Instagram. Проводиться послідовний огляд усіх фотографій у профілі. Серед публікацій знаходиться зображення, де користувач зафіксований поруч із робочим місцем. Ця фотографія містить критичну вразливість пов’язану з людським фактором.

Під час зйомки користувач не звернув уваги на сторонні об’єкти в кадрі. На робочому столі біля монітора знаходиться папірець із записами. Записи візуально нагадують ідентифікатори доступу до інформаційної системи. Створюється технічна складність через обмеження якості зображення на соціальних платформах. Стандартний перегляд у браузері не дозволяє чітко розрізнити символи на папері.

Для вирішення проблеми якості застосовуються спеціалізовані програмні засоби для вивантаження медіафайлів. Використовується онлайн сервіс dumpor.io, оскільки утиліти по типу Gallery DL потребують виконати вхід в

акаунт соц. мережі для завантаження фото. Після завантаження файлу проводиться масштабування та цифрову обробку фрагмента з папірцем.

Об’єктом ідентифікації виступає пароль. Навіть при наявності шумів символи залишаються читабельними для уважного аналітика. Знайдений текстовий пароль стає прапором для третього етапу. Цей крок навчає звертати увагу на дрібні деталі фону публікацій. Завдання ілюструє небезпеку порушення правил фізичної безпеки та ризики випадкової публікації конфіденційних нотаток. Студент отримує практичний досвід роботи з інструментами відновлення візуальних даних.

Етап 4. Проводиться вивчення технічної активності об’єкта на платформі GitHub. Посилання на цей ресурс знаходиться в одному з дописів соціальної мережі. Також проводимо пошук за раніше ідентифікованим нікнеймом. Аналізується повний список репозиторіїв у профілі користувача. Знаходимо специфічний проект під назвою Best PGP. Вміст репозиторію включає графічне зображення та текстовий опис під ним. Опис містить дві окремі кодові фрази.

Припускається наявність прихованих даних через назву проекту. Графічний файл виступає контейнером для стеганографічного вкладення. Застосовується утиліта Steghide для проведення аналізу. Програма вимагає введення пароля для вилучення вмісту. Застосовується методика перебору знайдених фраз як потенційних ключів. Перша фраза дозволяє успішно розпочати процес дешифрування контейнера. У результаті роботи утиліти отримується окремий текстовий файл із PGP шифром. Цей процес демонструє надійність стеганографічних методів приховування технічної інформації.

Наступним кроком проводиться криптографічний аналіз отриманого шифру. Застосовується програмний комплекс GnuPG для роботи з блоком даних. Використовується друга знайдена фраза як пароль для розшифрування повідомлення. Процес базується на алгоритмах симетричного шифрування. Успішне виконання команди відкриває доступ до конфіденційного змісту. Результатом стає email адреса користувача cjlarkson@protonmail.com. Вибір поштового сервісу ProtonMail вказує на прагнення об’єкта до підвищеної

приватності. Ця адреса стає прапором для четвертого етапу. Таким чином демонструється небезпека зберігання паролів поруч із зашифрованими об’єктами. Студенти отримують навички комбінування методів технічного аналізу для виявлення прихованих контактних даних.

Етап 5. Фінальний етап сценарію присвячується аналізу програмних розробок користувача. Продовжується робота з GitHub акаунтом об’єкта. Проводимо ручний огляд усіх наявних репозиторіїв для пошуку критичних витоків. Знаходиться проект, який користувач розробляв для діагностики мережевих параметрів. Аналізується структура файлів усередині репозиторію. Відкривається файл під назвою ping_module.py для вивчення вихідного коду. Ручний аналіз коду дозволяє знайти вразливості які часто пропускають автоматизовані сканери.

Звертається увага на технічні коментарі та змінні в тілі програми. Програмісти часто залишають тестові дані у коді під час відлагодження функцій. Знаходиться жорстко закодована IP адресу 178.136.106.167 у фрагменті коду модуля. Користувач не видалив цю адресу перед публікацією скрипта у відкритий доступ. Ця знахідка стає основою для завершального кроку ідентифікації. Цим підкреслюються ризики пов’язані з наявністю технічних параметрів у публічних сховищах коду.

Проводиться ідентифікація географічного розташування пристрою за знайденою адресою. Застосовується термінальна команда для отримання результатів:

curl ipinfo.io/178.136.106.167

Програма здійснює запит до публічної бази даних GeoIP. Отримуються відомості про інтернет провайдера та координати сервера. Аналізуються вихідні дані для встановлення назви міста. Назва міста стає фінальним прапором для завершення проходження всього сценарію в кіберполігоні. Так доводиться, що невелика помилка в коді веде до розкриття фізичного місцезнаходження розробника. Сценарій завершується успішною ідентифікацією всіх параметрів об’єкта на основі лише відкритої інформації.

2.2 Технічні налаштування інструментів

Процес підготовки практичної частини передбачає попереднє налаштування програмного середовища на базі операційної системи Windows 10. Подальша реалізація сценарію в межах платформи CTFd буде відбуватися у середовищі Kali Linux. Проводимо підготовку всіх цифрових артефактів та інструментів ідентифікації в хронологічному порядку відповідно до логіки завдань.

Для маніпуляцій з метаданими початкового зображення використовується утиліта ExifTool. Проводиться завантаження виконуваного файлу з офіційного сайту розробника. Розпаковується отриманий архів у робочу директорію. Вхідний файл photo.png розміщується у ту саму папку для зручності роботи через термінал. Відкривається оболонка PowerShell безпосередньо в цій директорії.

На першому етапі формується легенда про походження файлу. Вносяться дані про професійне обладнання та програмне забезпечення для редагування. Це створює враження реальної діяльності працівника компанії. Використовується наступна команда:

.\exiftool.exe -Make=Canon -Model=Canon EOS R5 -Software=Adobe Photoshop 2025 (Windows) -DateTimeOriginal=2025:02:15 10:30:00 -CreateDate=2025:02:15 10:30:00 -ModifyDate=2025:02:16 14:20:00 photo.png

Ця команда встановлює марку та модель камери. Вказується версія графічного редактора Adobe Photoshop 2025. Прописуються дати зйомки та створення об’єкта. Це додає текстової глибини метаданим.

На другому етапі впроваджується головна технічна вразливість для першого завдання. Прописується шлях до файлу який містить ім’я користувача системи. Використовується команда для заповнення тегів PreservedFileName та Source:

.\exiftool.exe -PreservedFileName=C:\Users\cjlarksonn\Desktop\J.Clarkson.png -XMP-dc:Source=C:\Users\cjlarksonn\Desktop\J.Clarkson.png photo.png

Цей крок дозволяє залишити цифровий слід cjlarksonn всередині

контейнера. Для перевірки успішності внесених змін запускається фінальна команда:

.\exiftool.exe -g1 photo.png

Програма виводить структурований список усіх активних тегів. Результат демонструє наявність усіх заданих параметрів (дивитися рисунок 2.2).

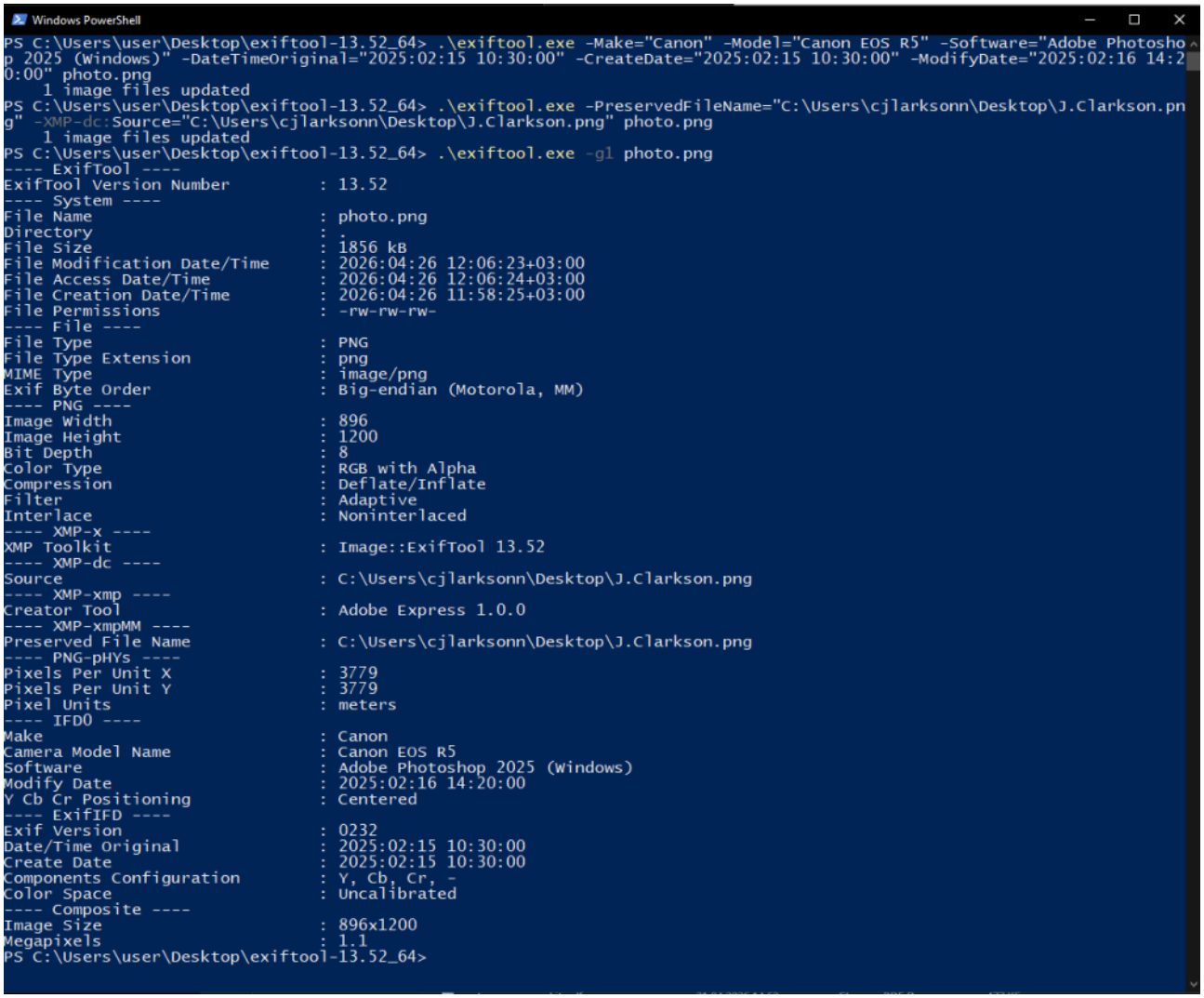

Рисунок 2.2 - Процес налаштування метаданих зображення та перевірка результатів через PowerShell

Для реалізації сценарію з ідентифікацією email адреси проводиться реєстрація нової поштової скриньки. Обирається сервіс ProtonMail [27] через його репутацію серед користувачів що дбають про приватність. Це відповідає психологічному портрету об’єкта розвідки. Створюється адреса cjlarkson@protonmail.com. Під час реєстрації використовується складний

пароль. Проводиться фіксація процесу створення облікового запису (дивитися рисунок 2.3).

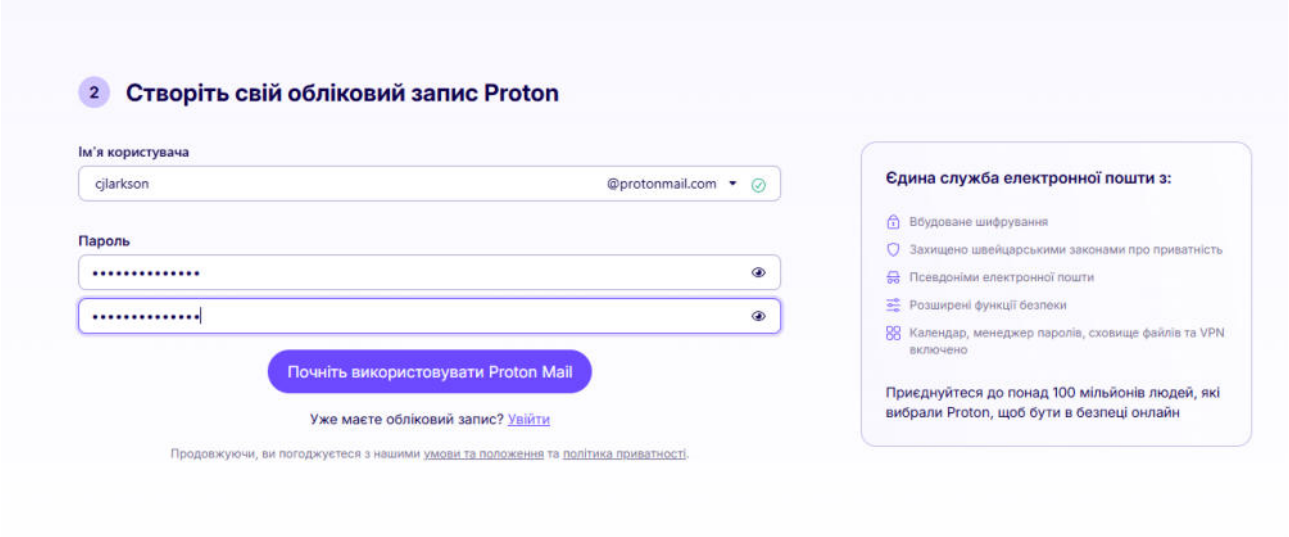

Рисунок 2.3 - Інтерфейс створення поштової скриньки на платформі ProtonMail

Наступним етапом підготовки артефактів є створення захищеного контейнера з адресою електронної пошти. Використовується метод симетричного шифрування для приховування текстових даних. Процес починається з формування вихідного файлу email.txt. Усередині цього документа розміщується раніше створена адресу cjlarkson@protonmail.com. Це буде кінцевим об’єктом пошуку для студента на четвертому етапі сценарію.

Для забезпечення високого рівня стійкості до зламу обирається складна кодова фразу. Було використано вислів: «Work hard, study well, and eat and sleep plenty. That is the Turtle Hermit Way».

Ця фраза запозичена з філософії майстра бойових мистецтв Мутен Роші з всесвіту Dragon Ball (японська манга, аніме-серіал та ігри). Вона символізує всебічний розвиток особистості через баланс між працею, навчанням та відпочинком. Вибір такої цитати відповідає профілю користувача. Студенти часто обирають улюблені вислови з масової культури як основу для своїх паролів. Це додає реалізму в сценарій соціальної інженерії.

Процедура шифрування проводиться за допомогою програмного комплексу GnuPG. Відкривається термінал PowerShell на робочому столі. Застосовується алгоритм AES256 для гарантування максимального захисту інформації. Вводиться наступна команда:

gpg --symmetric --cipher-algo AES256 email.txt

Після введення команди з'являється діалогове вікно для запиту парольної фрази. Вводиться підготовлена цитата та підтверджується (дивитися рисунок 2.4). У результаті виконання операції в робочій директорії з'являється файл email.txt.gpg. Цей об'єкт містить зашифровані дані у двійковому форматі.

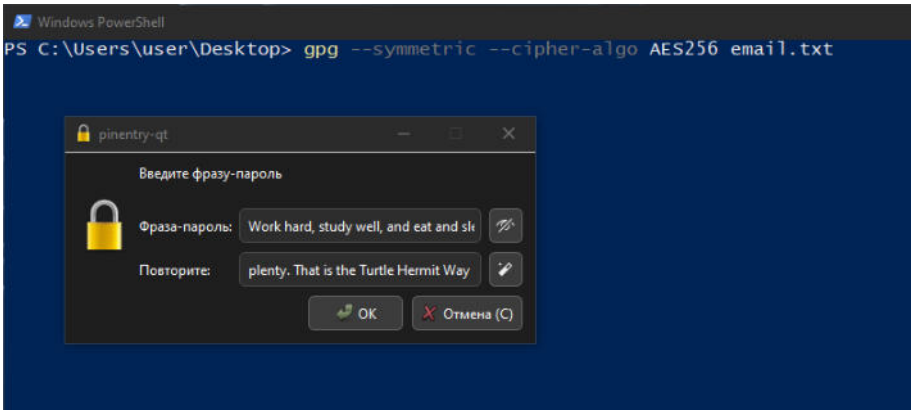

Рисунок 2.4 - Процес створення симетричного шифру за допомогою GnuPG та введення кодової фрази

Завершальним етапом технічної підготовки є впровадження отриманого PGP шифру в графічний контейнер. Обирається зображення cover.jpg для використання як прикриття. Для проведення операції впровадження готується друга кодова фраза: *«Believe in the me that believes in you!»*.

Цей вислів походить із аніме серіалу Gurren Lagann. Він несе глибокий посил про самоідентифікацію через віру іншої людини. Це підкреслює важливість міжособистісної підтримки у подоланні складних викликів. Така фраза є ідеальним ключем для стеганографічного захисту. Вона легко запам'ятовується автором та водночас є складною для автоматизованого підбору.

Використовується утиліта Steghide для об'єднання файлів. Переноситься

криптографічний контейнер email.txt.gpg та зображення cover.jpg у робочу папку програми. Відкривається термінал та вводиться команда для вбудовування даних:

.\steghide.exe --embed -cf cover.jpg -ef email.txt.gpg -sf secret_image.jpg

Програма запитує парольну фразу. Вводиться цитата про віру та підтверджується (дивитися рисунок 2.5). На виході отримується новий файл secret_image.jpg. Це зображення візуально не відрізняється від оригіналу, проте воно містить у собі зашифровану email адресу. Цей файл буде розміщено в GitHub репозиторії об’єкта. Цим демонструється багатоступеневий захист інформації. Студент має спочатку ідентифікувати факт наявності стеганографії. Далі він повинен знайти правильний ключ для вилучення PGP блоку. Лише після цього стає можливим фінальне дешифрування.

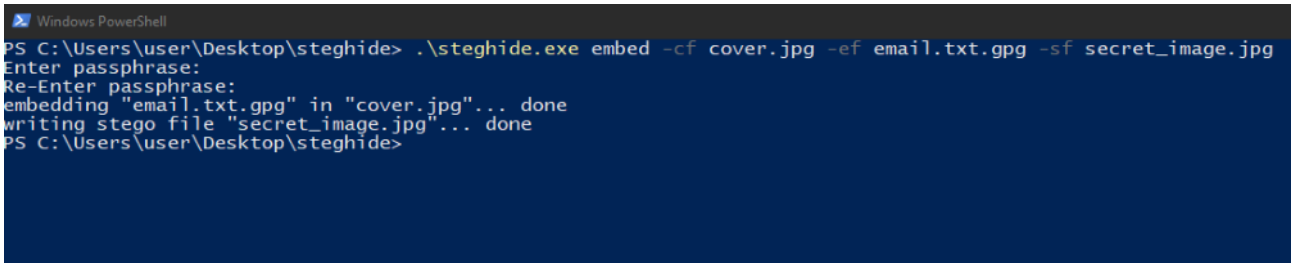

Рисунок 2.5 - Виконання команди впровадження даних у графічний файл за допомогою утиліти Steghide

Цей підхід дозволяє перевірити не лише технічні навички студентів. Цим створюється ситуація де необхідно аналізувати контекст знайденої інформації. Кожна кодова фраза є частиною легенди про користувача. Такий метод побудови завдань робить процес тестування у кіберполігоні змістовним та логічно завершеним. Підготовлені артефакти повністю відповідають технічним вимогам розробленого сценарію ідентифікації цифрового сліду.

2.3 Підготовка інфраструктури та розгортання ctfd

Вибір інфраструктури для проведення тестування сценарію зумовлений технічними вимогами обраних утиліт. Багато засобів потребують стабільного з’єднання з мережею Інтернет для звернення до баз даних соціальних платформ. Хмарні рішення часто обмежують зовнішній трафік у безкоштовних версіях. Прийнято рішення про створення локального середовища на базі засобів віртуалізації. Це забезпечує повний контроль над мережевими параметрами та конфігурацією системи.

Для створення робочого середовища використовується гіпервізор Oracle VirtualBox. Процес починається із завантаження спеціально підготовленого образу Kali Linux із офіційного ресурсу розробників (дивитися рисунок 2.6). Такий образ містить попередньо налаштовані драйвери для коректної роботи у віртуальному просторі.

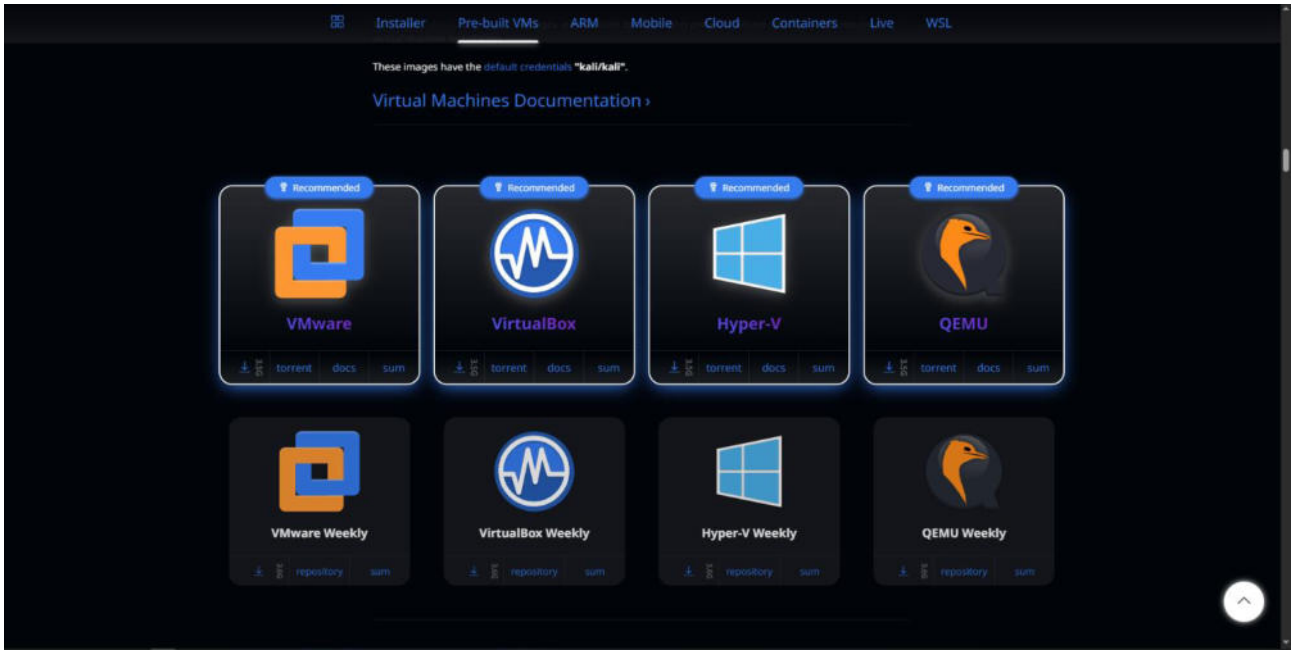

Рисунок 2.6 - Процес завантаження актуального образу Kali Linux для архітектури VirtualBox

Після завершення завантаження проводиться імпорт файлу у середовище VirtualBox. Налаштовуються параметри оперативної пам’яті та кількість ядер процесора для забезпечення швидкодії системи (дивитися рисунок 2.7).

Проводиться перший запуск віртуальної машини та перевірка мережевої доступності.

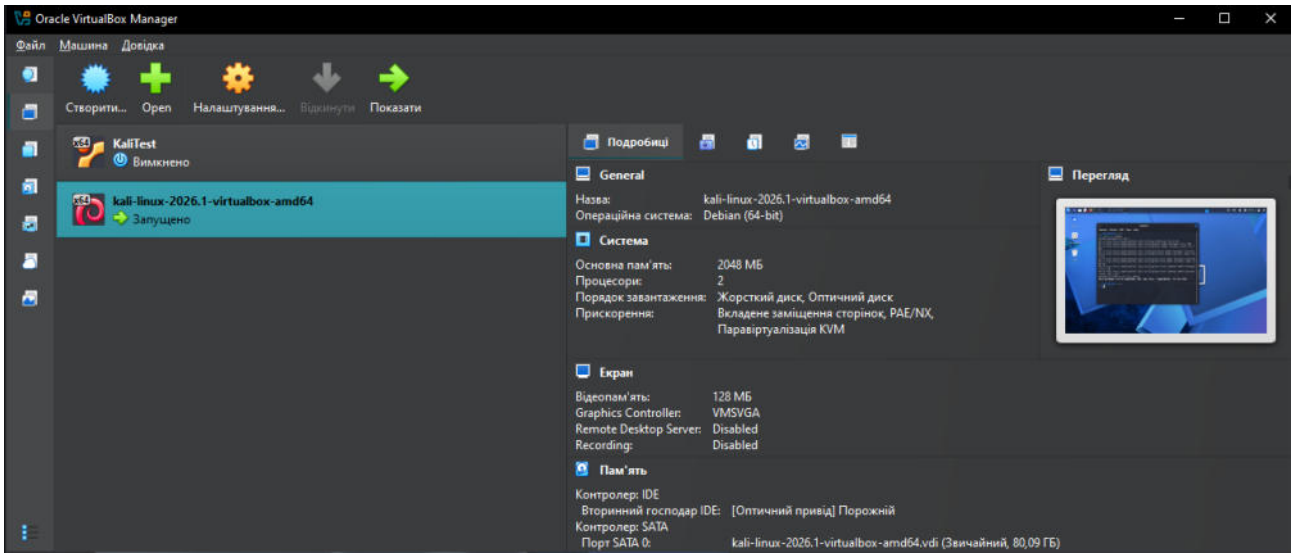

Рисунок 2.7 - Налаштована віртуальна машина Kali Linux у головному меню VirtualBox

Для розгортання серверної частини завдань застосовується технологія Docker. Це дозволяє ізолювати компоненти платформи CTFd та забезпечити стабільність їх роботи. Через термінал Kali Linux проводиться встановлення пакетів Docker та Docker Compose:

```
sudo apt update
sudo apt install docker.io docker-compose -y
```

Наступним кроком проводиться клонування офіційного репозиторію CTFd із порталу GitHub [23]. Здійснюється перехід у директорію проекту та запускається процес побудови контейнерів:

```
git clone https://github.com/CTFd/CTFd.git
cd CTFd
sudo docker-compose up
```

Використовується команда docker-compose up. Система автоматично завантажує необхідні образи бази даних та веб сервера.

Після запуску контейнерів доступ до панелі керування здійснюється через

веб браузер за локальною адресою. Проводиться первинне налаштування системи. Вказується назва заходу та надається детальний опис мети проходження OSINT сценарію (дивитися рисунок 2.8).

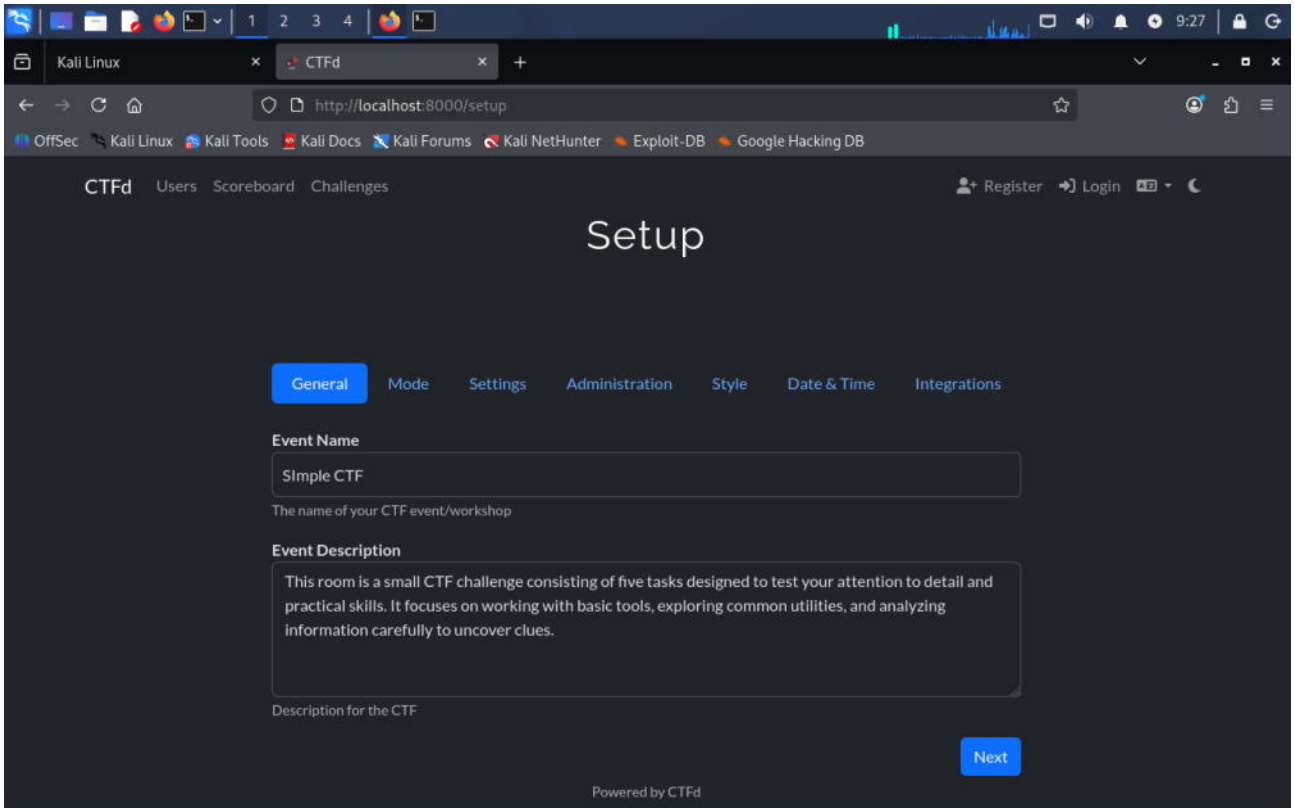

Рисунок 2.8 - Інтерфейс введення назви та технічного опису івенту

У розділі налаштувань обирається режим User Mode. Це передбачає індивідуальну участь кожного студента без об’єднання у команди. Для спрощення реєстрації в умовах навчального полігона відключається обов’язкова верифікація адрес електронної пошти. Створюються облікові дані для адміністратора системи. Також деактивується опція соціальних поширень для дотримання конфіденційності тренувального процесу.

Процес формування сценарію передбачає створення п’яти окремих карток завдань у меню Challenges. Для кожного етапу прописується заголовок, опис завдання та категорія OSINT. Налаштовується система автоматичної перевірки введених рядків.

Особлива увага приділяється третьому завданню. Через візуальні

особливості символів на фотографії робочого місця передбачається можливість помилки при розрізненні літер «е» та «с». Для забезпечення коректності оцінювання створюється два окремих прапори для одного питання. Система зараховує відповідь як правильну при введенні будь якого із цих варіантів (дивитися рисунок 2.9).

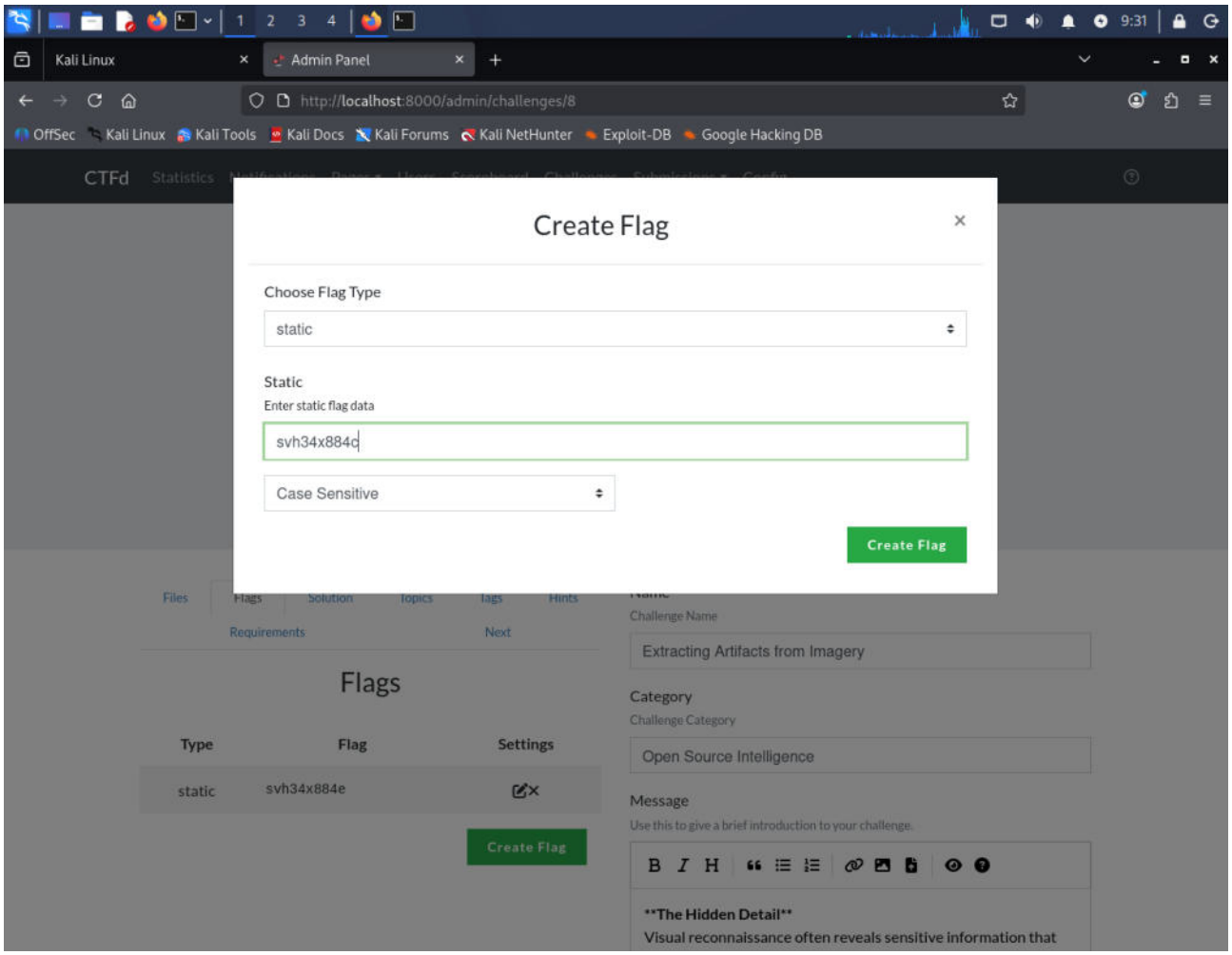

Рисунок 2.9 - Налаштування кількох валідних прапорів для завдання з ідентифікації пароля

Завершальним етапом підготовки інфраструктури є перевірка відображення всіх завдань у загальному списку (дивитися рисунок 2.10). Система готова до прийому підключень та фіксації результатів проходження сценарію. Локальне розгортання на базі Docker та CTFd забезпечує стабільну платформу для практичного вивчення методів ідентифікації цифрового сліду.

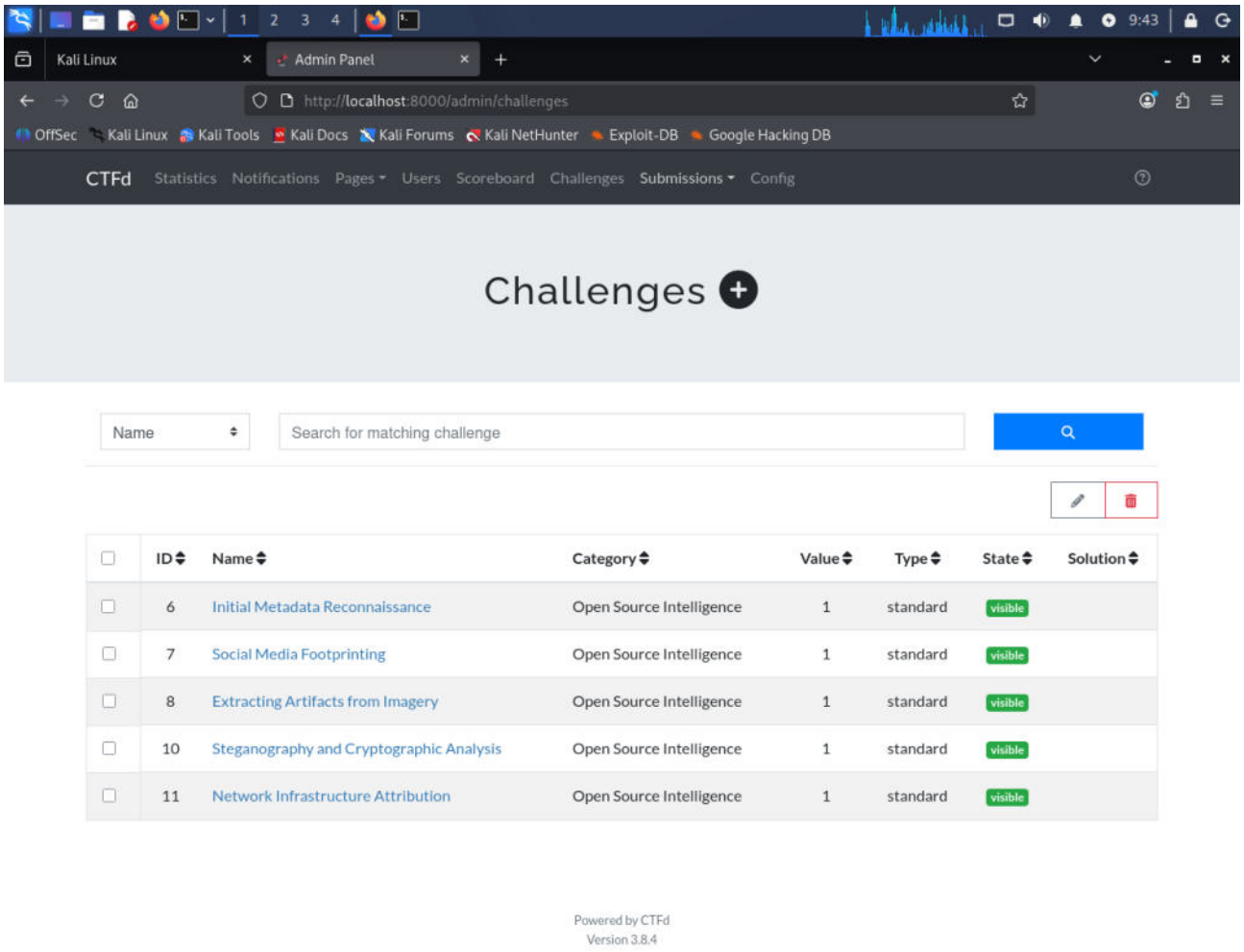

Рисунок 2.10 - Готове меню із п’ятьма послідовними завданнями сценарію

Для кожного з п’яти завдань встановлюються параметри перевірки у панелі керування кімнатою. Використовується функціонал Static Flag для більшості питань. Це означає, що платформа порівнює введену відповідь із чітко визначеним текстовим рядком. Для більш детального ознайомлення з повною інформацією щодо всіх п'яти завдань - від їхніх назв до підказок - див. додаток А.

2.4 Генерація синтетичних профілів та підготовка графічних об’єктів

Для забезпечення максимальної реалістичності практичного сценарію та дотримання етичних норм у межах роботи приймається рішення про створення повної синтетичної особистості. Використання вигаданого персонажа дозволяє уникнути порушення приватності реальних осіб та надає можливість повного

контролю над усіма цифровими артефактами. Процес створення включає генерацію візуального образу за допомогою штучного інтелекту, технічну обробку зображень та наповнення соціальних профілів змістовним контентом.

Як основу для візуального образу обирається скріншот із аніме «Монстр» (автор Наокі Урасава), а саме персонажа Кендзо Тенма (дивитися рисунок Б.1 у додатку Б*)*, де чітко видно обличчя персонажа, риси обличчя та його зачіску.

Вибір цього героя зумовлений його нейтральною зовнішністю, що підходить для створення образу технічного фахівця. Для трансформації аніме-стилістики у реалістичне фото використовується платформа Higgsfield.

Посилання на платформу Higgsfield: https://higgsfield.ai/.

Вибір платформи Higgsfield зумовлений наявністю широкого спектра інструментів для генерації візуального контенту. Платформа забезпечує зручний інтерфейс та доступ до багатьох безкоштовних моделей. Це дозволяє створювати якісні зображення без фінансових витрат. Усі графічні артефакти для роботи створено саме на цьому ресурсі. Використання Higgsfield надає можливість гнучкого налаштування параметрів генерації для отримання реалістичних результатів. Застосовано лише моделі з відкритим доступом для безкоштовного використання.

Генеративні моделі працюють на основі складних математичних алгоритмів. Ці алгоритми пройшли навчання на великих масивах реальних зображень. Принцип роботи базується на дифузії. Процес передбачає поступове видалення випадкового шуму до формування чіткого об’єкта. Для сценарію критичною є здатність моделі зберігати ідентичність обличчя в різних умовах. Обрано конкретну модель на основі технічної ефективності роботи з параметрами Face ID.

Вибір моделі Nano-Banana Pro [28] базується на високій точності збереження рис обличчя при повторних ітераціях. Ця модель застосовує оптимізовані ваги для відтворення антропометричних параметрів. Отримано можливість створювати різні сцени з одним персонажем без втрати візуальної схожості. Інші доступні моделі часто демонструють технічну нестабільність.

Вони генерують анатомічні дефекти або змінюють зовнішність об’єкта. Проведено технічне порівняння для обґрунтування вибору серед безкоштовних варіантів.

Альтернативні безкоштовні моделі Seadream 4.5 [29], GPT Image 2 [30] та Wan 2.2 [31] мають технічні недоліки. Seadream 4.5 створює значні візуальні шуми на фоні зображення. GPT Image 2 видає контент низької чіткості з анатомічними дефектами. Модель Wan 2.2 втрачає стабільність рис обличчя при зміні ракурсу або освітлення. Ці чинники унеможливлюють створення переконливого цифрового образу для OSINT розслідування. Порівняння технічних параметрів цих інструментів наведено нижче у таблиці 2.1.

Таблиця 2.1 - Технічне порівняння параметрів моделей безкоштовної генерації

Модель	**Точність ідентичності**	**Ефективність обробки промптів**	**Архітектурна база**	**Швидкість генерації**
Nano-Banana Pro	> 85%	Висока (SDXL)	GemPix 2 (Diffusion)	30-50 кроків
Seadream 4.5	< 50%	Середня (CLIP)	Proprietary DiT	20-30 кроків
GPT Image 2	< 40%	Низька (Legacy)	Advanced Diffusion	15-25 кроків
Wan 2.2	< 65%	Середня (U-Net)	MoE (Mixture of Experts)	25-40 кроків

Застосовано Nano-Banana Pro як найбільш раціональний технічний інструмент. Ця модель забезпечує необхідну якість для ідентифікації об’єкта студентами.

Для генерації цільового зображення було сформовано промпт, який враховує стилістику, деталізацію освітлення та конкретні параметри персонажа. Детальний текст промпту та отриманий результат наведено у додатку Б (див.

етап генерації для першого зображення, рисунки Б.1, Б.2)

Результат роботи Nano-Banana Pro, отриманий у ході виконання спеціально підготовленого промпту, продемонстровано на рисунок 2.11.

Рисунок 2.11 Сгенероване фото персонажа Джеймс Кларксон

Після отримання базового реалістичного портрета проводиться генерація додаткових зображень у різних ракурсах та умовах. Окрема увага приділяється створенню фотографії паспортного формату 3х4 для профілю в LinkedIn та корпоративних систем (дивитися рисунок 2.12).

Для генерації «корпоративно-паспортного» зображення було сформовано промпт, який враховує всі умови, від освітлення та білого фону, до охайного

одягу і зачіски. Детальний текст промпту та отриманий результат наведено у додатку Б (див. етап генерації для другого зображення, рисунок Б.2, Б.3)

Рисунок 2.12 - Процес перетворення графічного образу в реалістичне зображення на платформі Higgsfield

Також, створено додаткові фото для заповнення профілів у соц. мережах (дивитися додаток Б рисунки Б.4-Б.8).

Для видалення системних водяних знаків платформи Higgsfield використовується сервіс Adobe Express [32].

Посилання на платформу Adobe Express: https://new.express.adobe.com/.

Проводиться ретельне очищення візуального поля для надання знімкам професійного вигляду (дивитися рисунок 2.13).

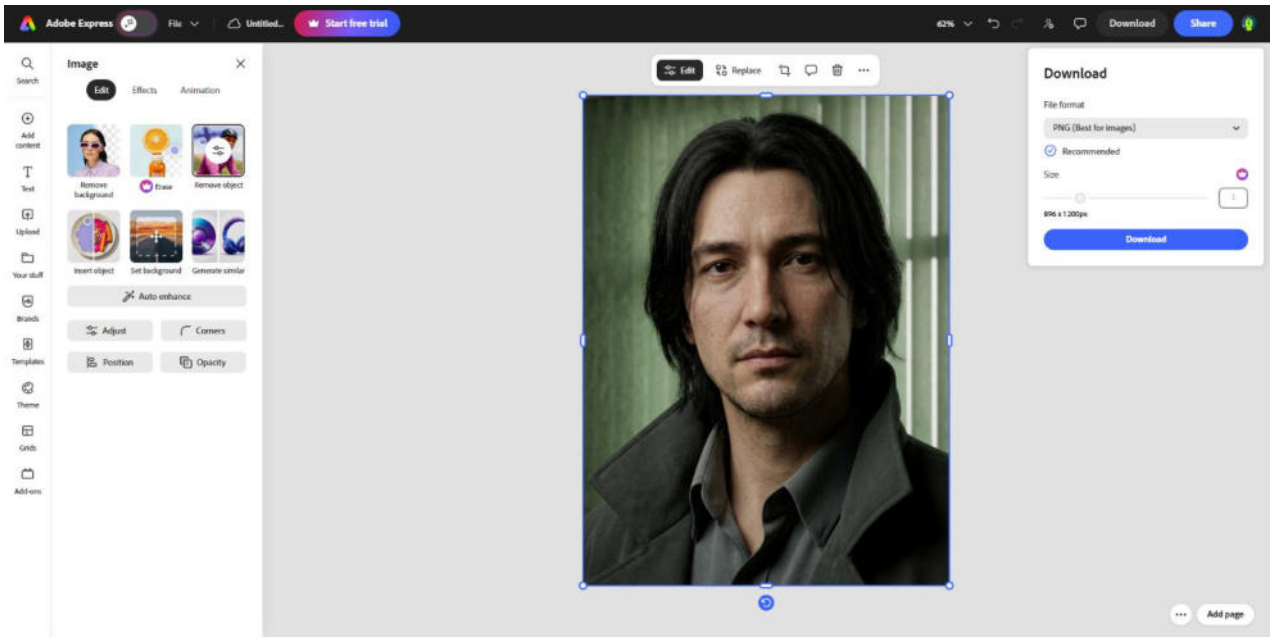

Рисунок 2.13 - Процес видалення водяних знаків із генерованих зображень у сервісі Adobe Express.

Отримані фотографії потребують покращення роздільної здатності, особливо для завдань, що передбачають ідентифікацію дрібних деталей. Використовується платформу upscale.media для збільшення роздільної здатності зображення з робочим місцем у два рази. Це необхідно для забезпечення читабельності прапора на паперовому носії.

Посилання на платформу upscale.media: https://upscale.media/.

Наступним кроком застосовується графічний редактор Adobe Photoshop. Проводиться ретуш об’єктів та виправлення дефектів генерації штучного інтелекту, як приклад - змазані значення на годиннику. На цьому етапі впроваджується прапор для третього завдання - додається на зображення папірець із логіном «JamCla01504» та паролем «svh34x884e» (дивитися рисунок 2.14).

Рисунок 2.14 - Зображення робочого місця після обробки в Adobe Photoshop (впровадження пароля та виправлення дефектів годинника).

Для формування переконливого цифрового сліду реєструються та оформлюються акаунти на трьох платформах:

Профіль у мережі X (Twitter). Здійснюється базове оформлення фону та аватарки. Стрічка наповнюється комбінацією пустих дописів та інформативних повідомлень. В опис додається посиланням на GitHub та Instagram акаунти. Проводиться імітація активності через підписки на тематичні блоги (дивитися рисунок 2.15).

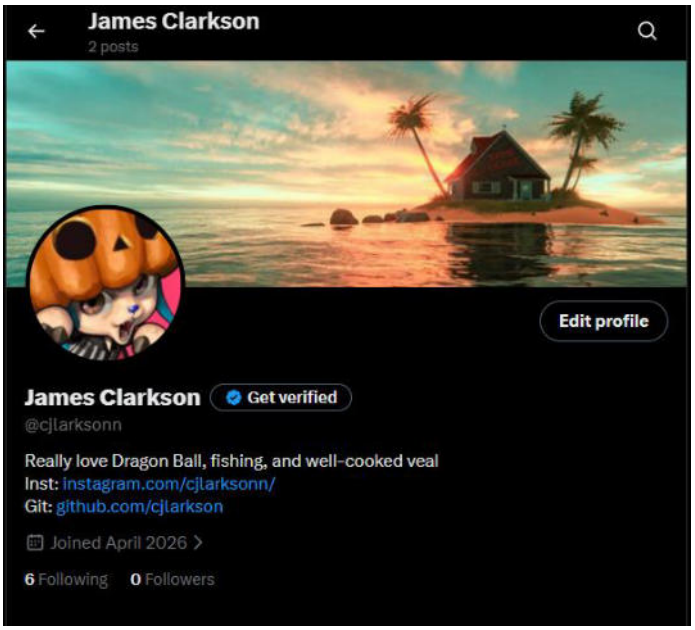

Рисунок 2.15 - Профіль у мережі X

Посилання на профіль у мережі X: https://x.com/cjlarksonn.

Профіль в Instagram. Розміщується серія фотографій персонажа, включаючи знімки робочого середовища. Основний фокус робиться на публікації, що містить ідентифікатори доступу. Налаштовується біографія профілю з вказанням реального імені та прізвища (дивитися рисунок 2.16).

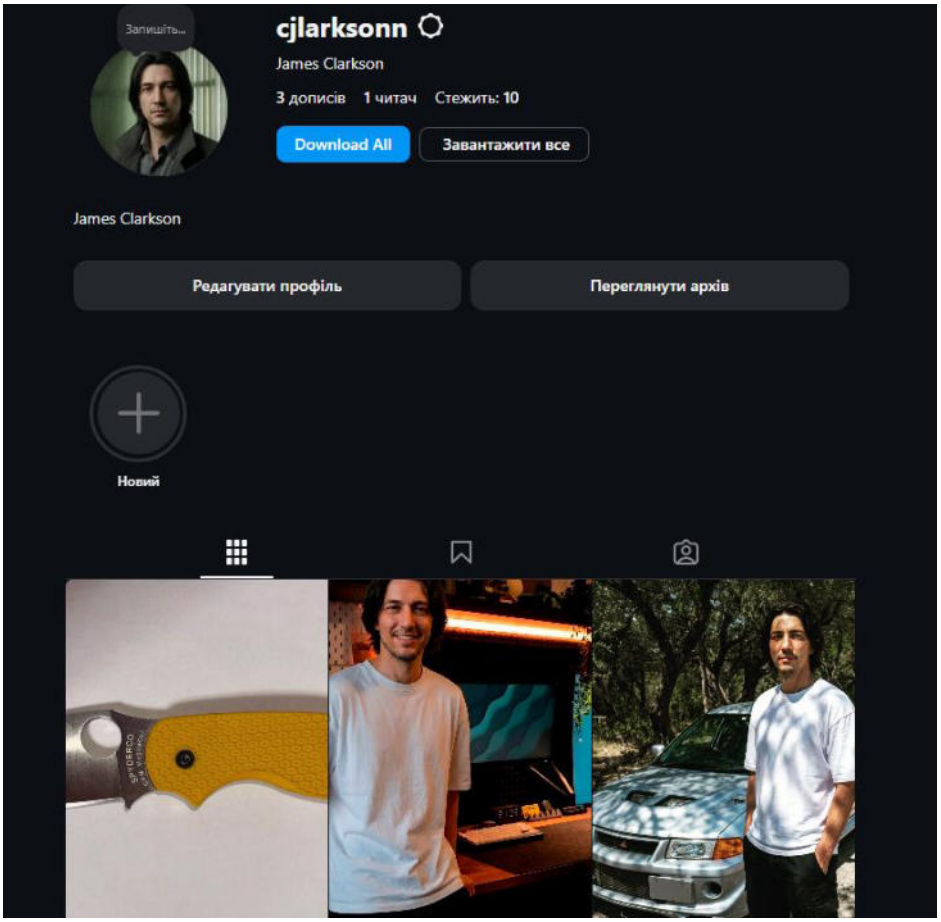

Рисунок 2.16 - Профіль у мережі Instagram

Посилання на профіль у мережі Instagram: https://www.instagram.com/cjlarksonn/.

Профіль на GitHub. Створюється обліковий запис із відповідним нікнеймом. Заповнюється інформація про користувача та аватарку. Для створення ілюзії професійної діяльності розробляється структура з п’яти репозиторіїв (дивитися рисунок 2.17).

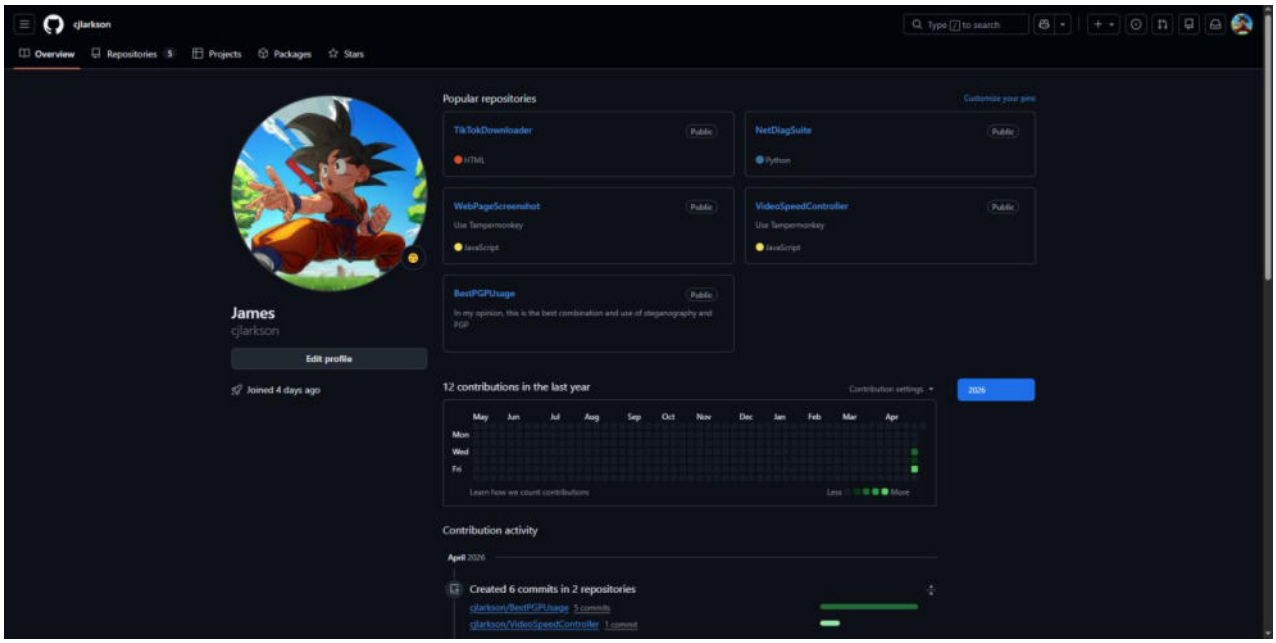

Рисунок 2.17 - Профіль на GitHub

Посилання на профіль на GitHub: https://github.com/cjlarkson.

Для ускладнення завдання та створення інформаційного шуму GitHub профіль наповнюється різноплановими проектами.

1. BestPgpUsage. Репозиторій містить зображення з вбудованим стеганографічним шифром та підказки для дешифрування в README файлі дивитися рисунок 2.16).
   Посилання: https://github.com/cjlarkson/BestPGPUsage
2. NetDiagSuit. Проект утиліти для діагностики мережі. У файлі ping_модуль.py розміщується IP адреса, що є ключем до п’ятого завдання.
   Посилання: https://github.com/cjlarkson/NetDiagSuite
3. Webpage screenshot. Робочий JavaScript скрипт для розширення Tampermonkey [33], що дозволяє створювати знімки екрана.
   Посилання: https://github.com/cjlarkson/WebPageScreenshot
4. Video Speed Controller. Функціональне розширення для регулювання швидкості відтворення відео в браузері.
   Посилання: https://github.com/cjlarkson/VideoSpeedController
5. TikTok Downloader. Складний проект локального додатка для автоматизованого завантаження контенту з описом інсталяції та

структурою папок.

Посилання: https://github.com/cjlarkson/TikTokDownloader.

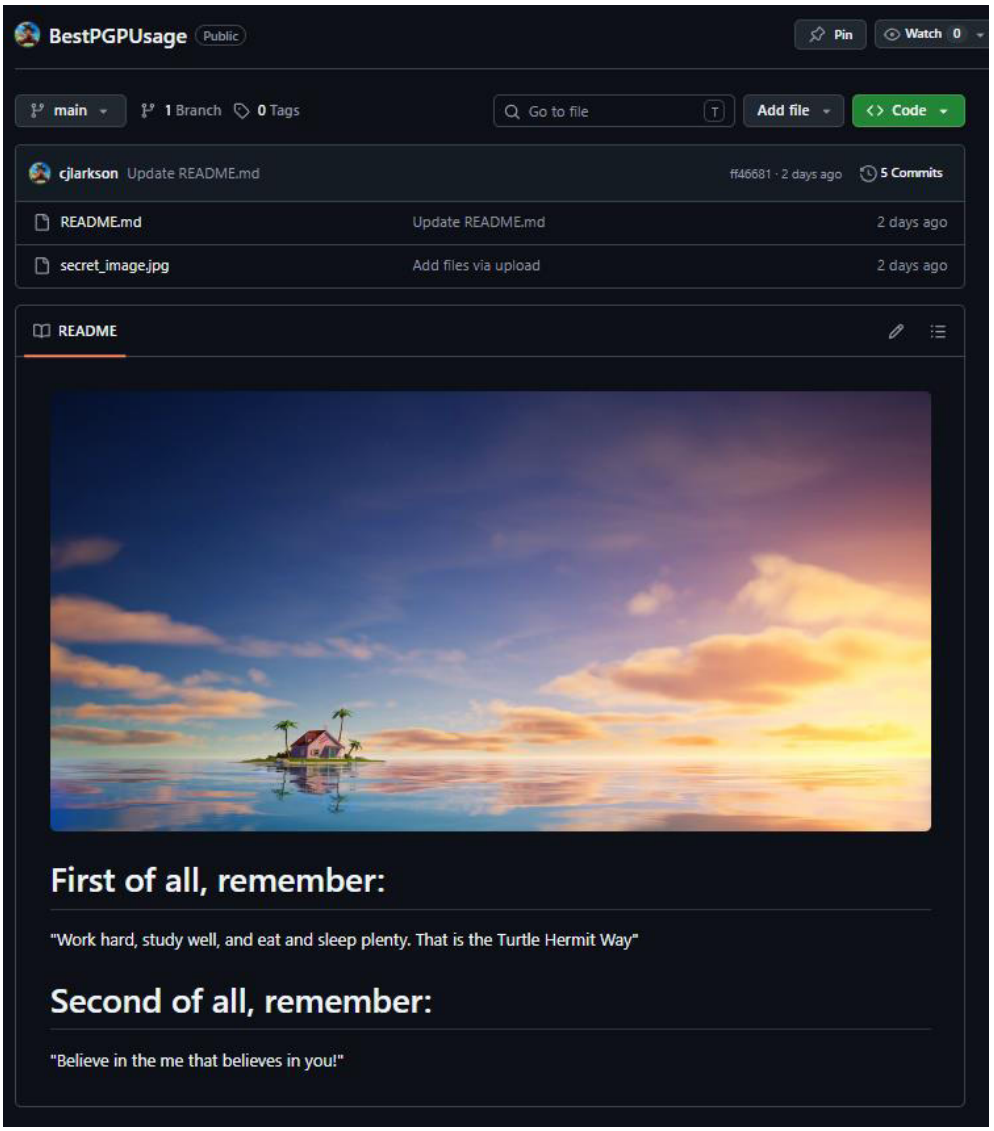

Рисунок 2.16 Структура та вміст репозиторію BestPgpUsage з артефактами для стеганографічного аналізу

Створення такої кількості артефактів дозволяє повністю реалізувати сценарій ідентифікації цифрового сліду. Синтетичні дані забезпечують стабільність результатів тестування та відповідність кожного елемента загальній логіці розслідування.

2.5 Програмування логіки перевірки прапорів та системи оцінювання

Процес автоматизації перевірки результатів у середовищі CTFd базується на зіставленні введених користувачем даних із еталонними значеннями. Надійна логіка валідації забезпечує точність оцінювання навичок ідентифікації цифрового сліду. Система працює в автономному режимі. Це дозволяє студентам отримувати миттєве підтвердження правильності виконання завдань. Налаштування платформи охоплює параметри чутливості до регістру та логіку обробки альтернативних відповідей.

Нарахування балів відбувається за статичною моделлю. Кожне розв’язане завдання додає фіксовану кількість очок до загального рейтингу користувача. Це дозволяє прозоро оцінювати прогрес ідентифікації об’єктів. Платформа CTFd веде детальний журнал спроб введення. Адміністратор має можливість аналізувати типові помилки студентів та час витрачений на кожний етап.

Для фінальної перевірки працездатності розгорнутої інфраструктури проведено повний цикл тестування. Використано окремий обліковий запис тестового студента. Процес імітує реальне проходження сценарію від ідентифікації нікнейма до визначення геолокації об’єкта.

Під час тестування перевірено доступність усіх п’яти завдань. Підтверджено коректну роботу мережевих інструментів усередині Kali Linux при зверненні до сервера CTFd. Результати тестування демонструють повну справність усіх механізмів. Тестовий користувач успішно отримав 5 прапорів із 5 можливих. Система коректно зафіксувала час виконання та нарахувала підсумкову суму балів.

Статистика проходження підтверджує готовність середовища до експлуатації (дивитися рисунок 2.17). Локальна платформа CTFd забезпечує ідентичний досвід для всіх учасників незалежно від зовнішніх факторів. Виявлені під час тестування логічні зв’язки працюють без збоїв. Система готова до прийому підключень для проведення навчання.

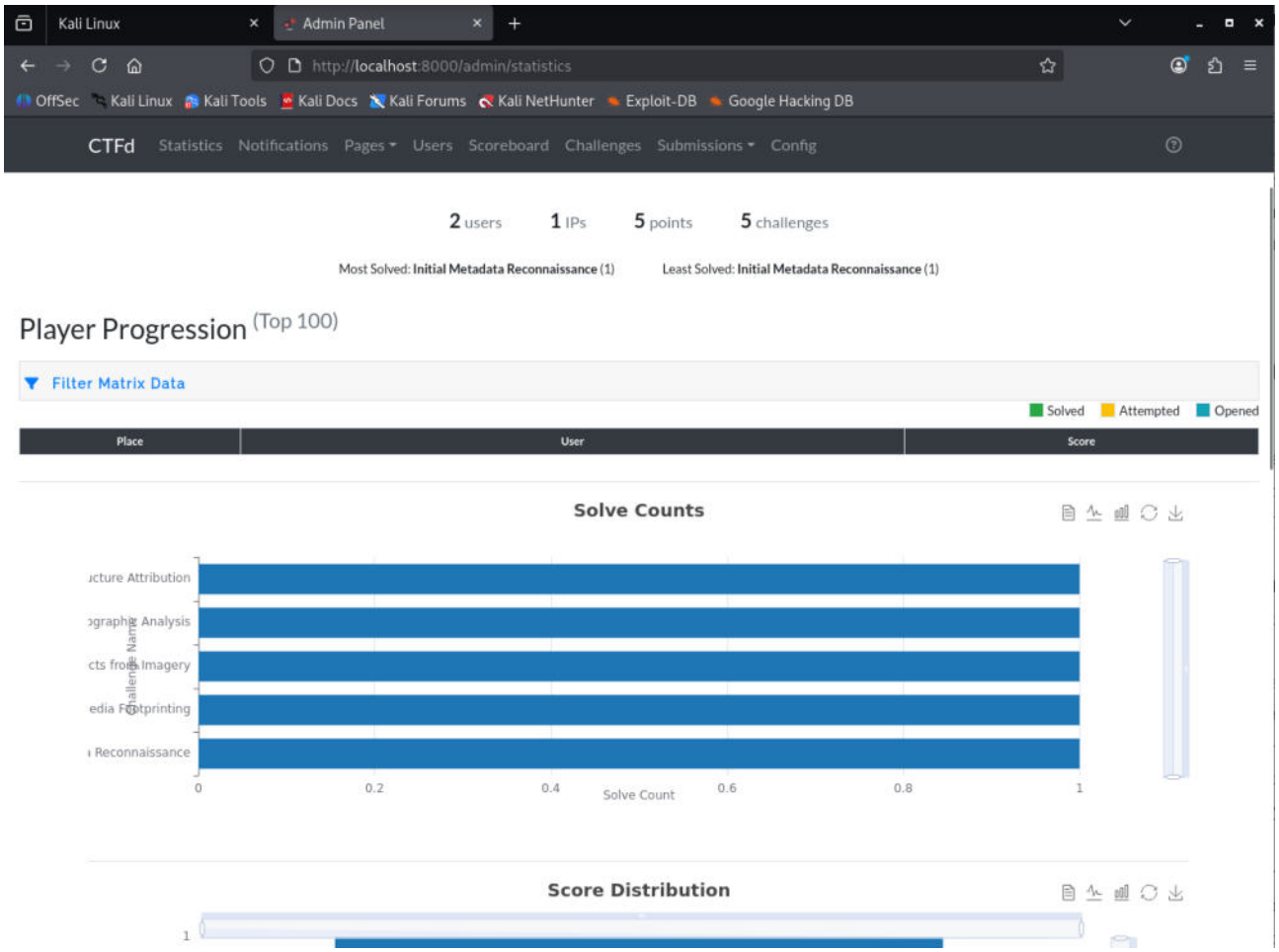

Рисунок 2.17 - Панель загальної статистики із підтвердженням успішного завершення сценарію тестовим обліковим записом

Розділ 3. Практична реалізація та тестування сценарію ідентифікації цифрового сліду

3.1 Практичне проведення етапів ідентифікації цифрового сліду в кіберполігоні

Процес практичного виконання сценарію передбачає послідовне розв’язання п’яти взаємопов’язаних завдань. Кожен етап імітує реальну діяльність аналітика з розвідки на основі відкритих джерел. Тестування проводимо в операційній системі Kali Linux із використанням локально розгорнутої платформи CTFd. Такий підхід забезпечує повну контроль над мережевими параметрами та дозволяє уникнути обмежень хмарних сервісів.

Початок роботи передбачає авторизацію на платформі CTFd (дивитися рисунок 3.1). Використовуються заздалегідь створений облікові дані для входу в систему. Локальне розгортання через технологію Docker Compose гарантує стабільність доступу до завдань без залежності від зовнішніх серверів та швидкості інтернет-з’єднання. Після успішного введення логіна та пароля відкривається головне меню з переліком усіх завдань сценарію. Завдання розміщуються в суворому логічному порядку. Це необхідно для поетапної побудови цифрового профілю об’єкта. Кожен успішно знайдений прапор відкриває нові вихідні дані для наступного кроку розвідки.

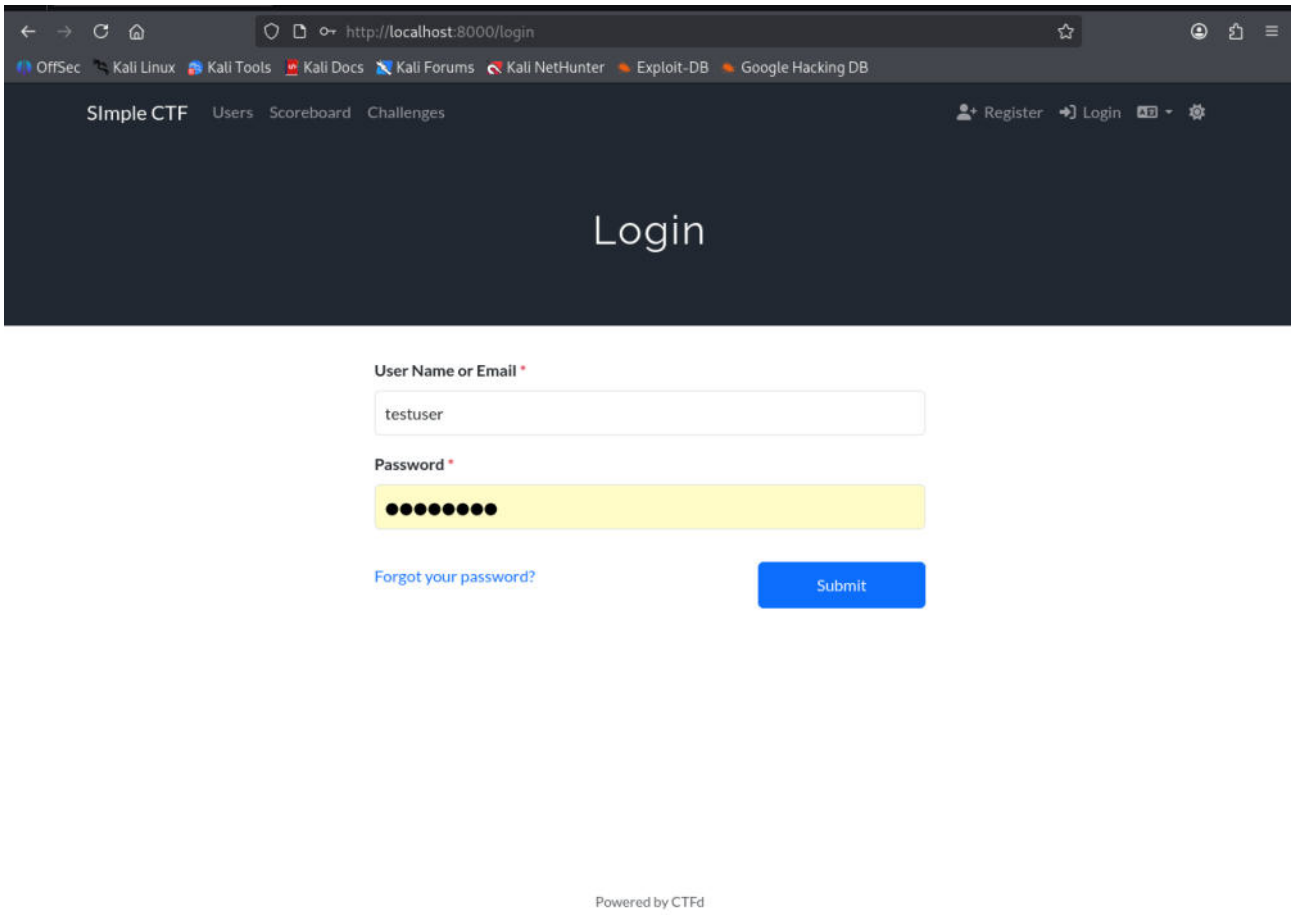

Рисунок 3.1 - Інтерфейс авторизації користувача на локальній платформі CTFd

Етап 1. Технічний аналіз графічного контейнера. Перше завдання Initial Metadata Reconnaissance спрямоване на роботу з метаданими. Кожне цифрове зображення є складним контейнером, який містить приховану технічну інформацію за стандартами EXIF, IPTC та XMP. Отримується посилання на графічний файл у хмарному сховищі Proton Drive (дивитися рисунок 3.2), завантажується зображення на робочу станцію. Це портретне фото вигаданого співробітника компанії. Файл зберігається у форматі без агресивного стиснення. Це дозволяє виявити оригінальну структуру технічних заголовків, які часто видаляються при поширенні через месенджери.

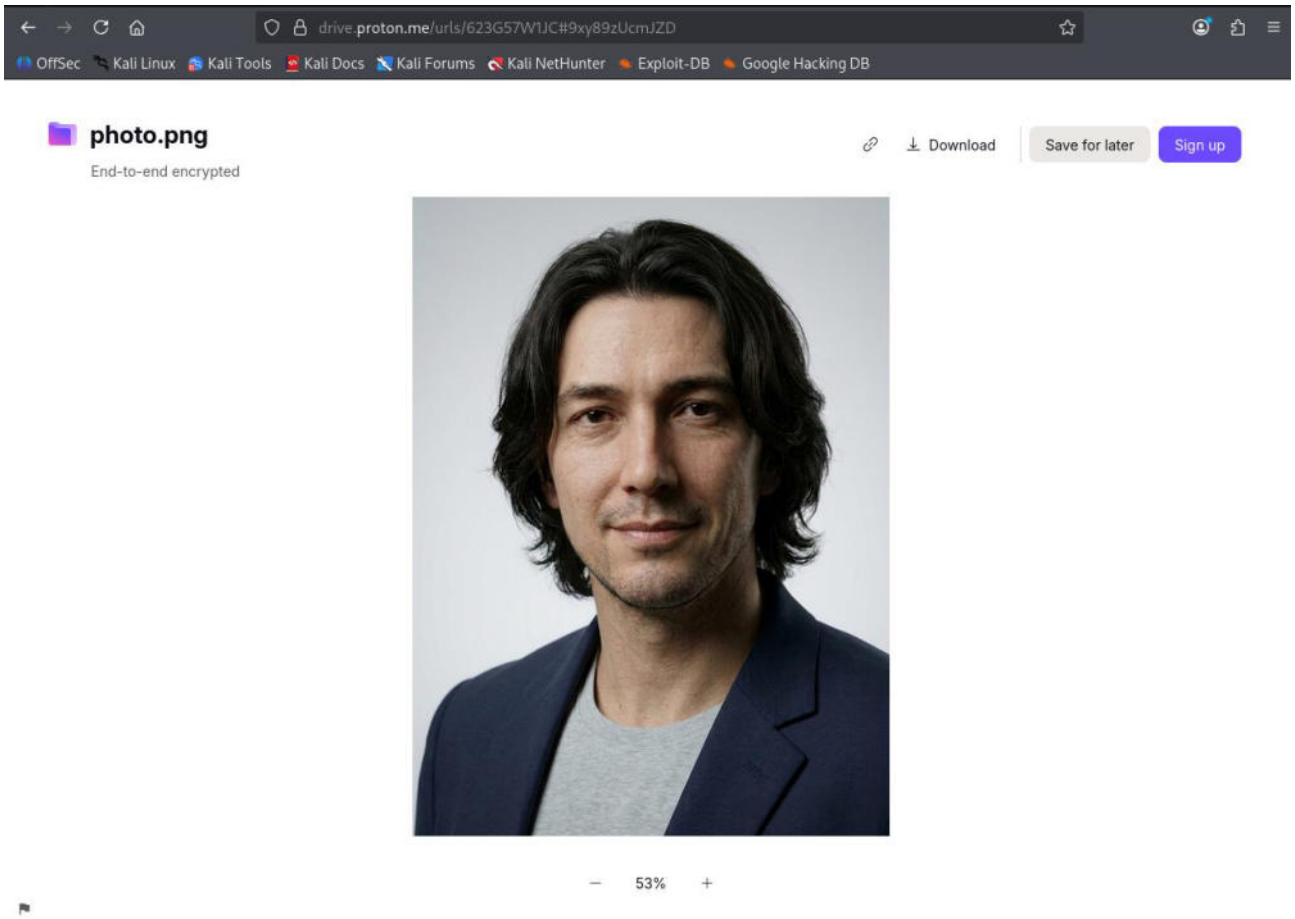

Рисунок 3.2 - Процес завантаження вхідного файлу з хмарного сховища

Для аналізу внутрішньої структури файлу застосовується утиліта exiftool. Програма є галузевим стандартом для криміналістичного дослідження медіафайлів. Вона дозволяє витягувати дані, які не відображаються стандартними засобами провідника операційної системи. Перед початком перевіряється наявність та версію інструменту в системі:

exiftool -ver

При відсутності утиліти або необхідності її оновлення виконується оновлення локальних репозиторіїв та встановлення відповідних пакетів:

sudo apt update && sudo apt install libimage-exiftool-perl

Запускається повний технічний аналіз завантаженого зображення. Програма сканує всі доступні теги метаданих:

exiftool photo.png

Детально аналізуються вихідні дані в терміналі (дивитися рисунок 3.3).

Найбільшу цінність для ідентифікації мають технічні теги Source та Preserved File Name. Ці поля заповнюються графічними редакторами або операційною системою автоматично під час експорту файлу. Вони містять абсолютний шлях до об’єкта на початковому пристрої автора. У цьому рядку виявляється назва папки користувача у структурі Windows. Виокремлюється ім’я cjlarksonn. Це ім’я виступає першим прапором для платформи CTFd. Воно стає ключовим ідентифікатором (username) для проведення всіх подальших етапів розвідки в мережі.

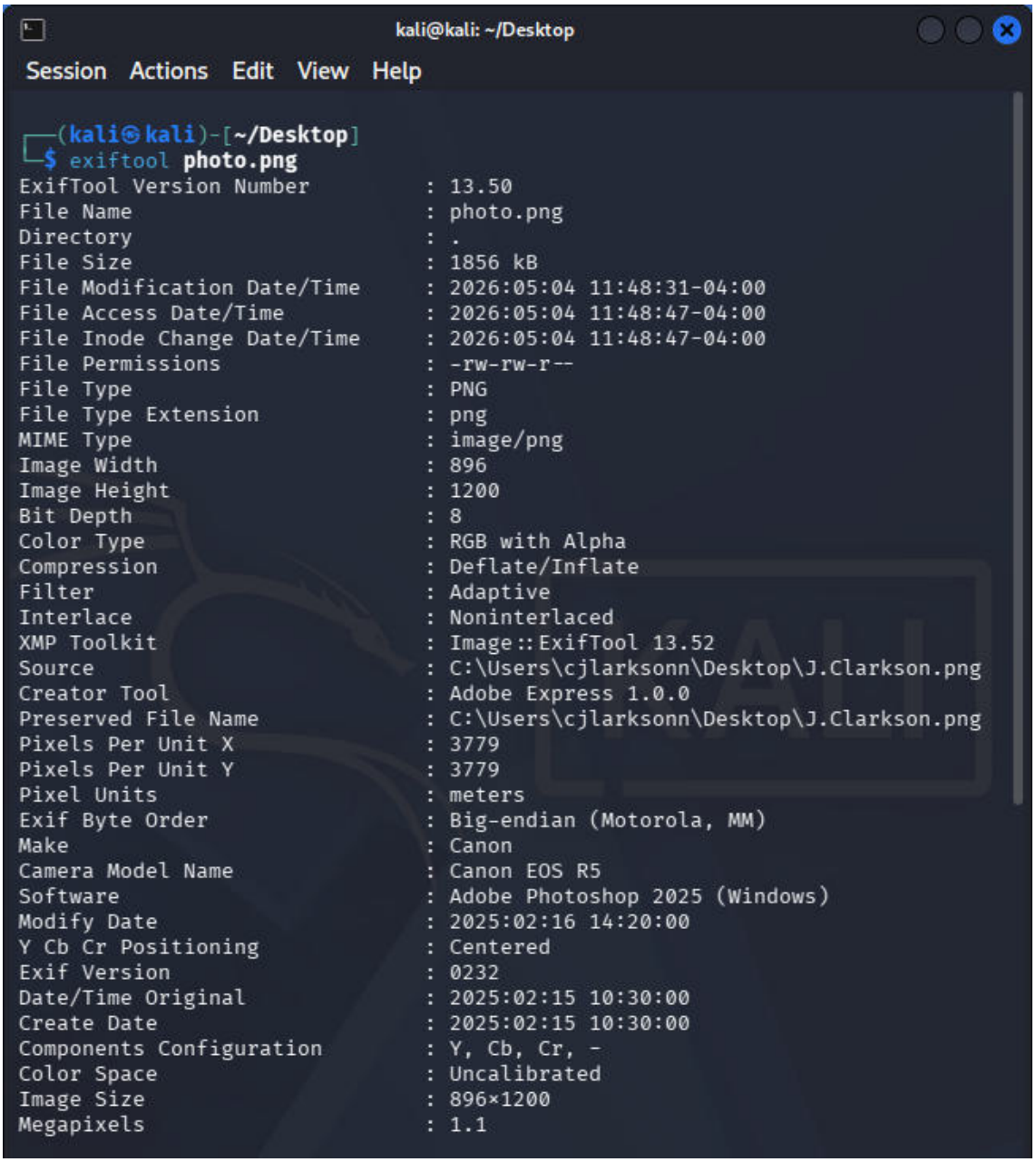

Рисунок 3.3 - Вихідний текст утиліти exiftool із технічним шляхом до файлу

Етап 2. Мережева розвідка та footprinting. На другому етапі Social Media Footprinting проводимо масштабний пошук знайденого нікнейма в глобальних мережах. Техніка базується на психологічному аспекті використання ідентичних імен для реєстрації на різних ресурсах. Починається робота з утиліти Sherlock. Цей інструмент працює за принципом надсилання асинхронних запитів до великої бази даних соціальних сайтів. Перевіряється працездатність програми:

sherlock --version

sudo apt update && sudo apt install sherlock

Запускається автоматизоване сканування соціальних платформ за ідентифікатором: sherlock cjlarksonn.

Під час виконання процесу фіксується проблема технічної недосконалості алгоритмів Sherlock. Програма видає 33 результати (дивитися рисунок 3.4) про нібито існуючі профілі, проте детальна ручна перевірка посилань виявляє велику кількість помилкових спрацювань (false positives). Це відбувається через те, що Sherlock аналізує лише HTTP-коди відповідей серверів (код 200 OK). Багато сайтів видають успішну відповідь навіть при зверненні до неіснуючих сторінок, наприклад, посилання на аккаунт у TikTok веде на пусту сторінку (дивитися рисунок 3.5) або повідомлення про відсутність користувача, що робить результати роботи Sherlock непридатними для швидкого аналізу.

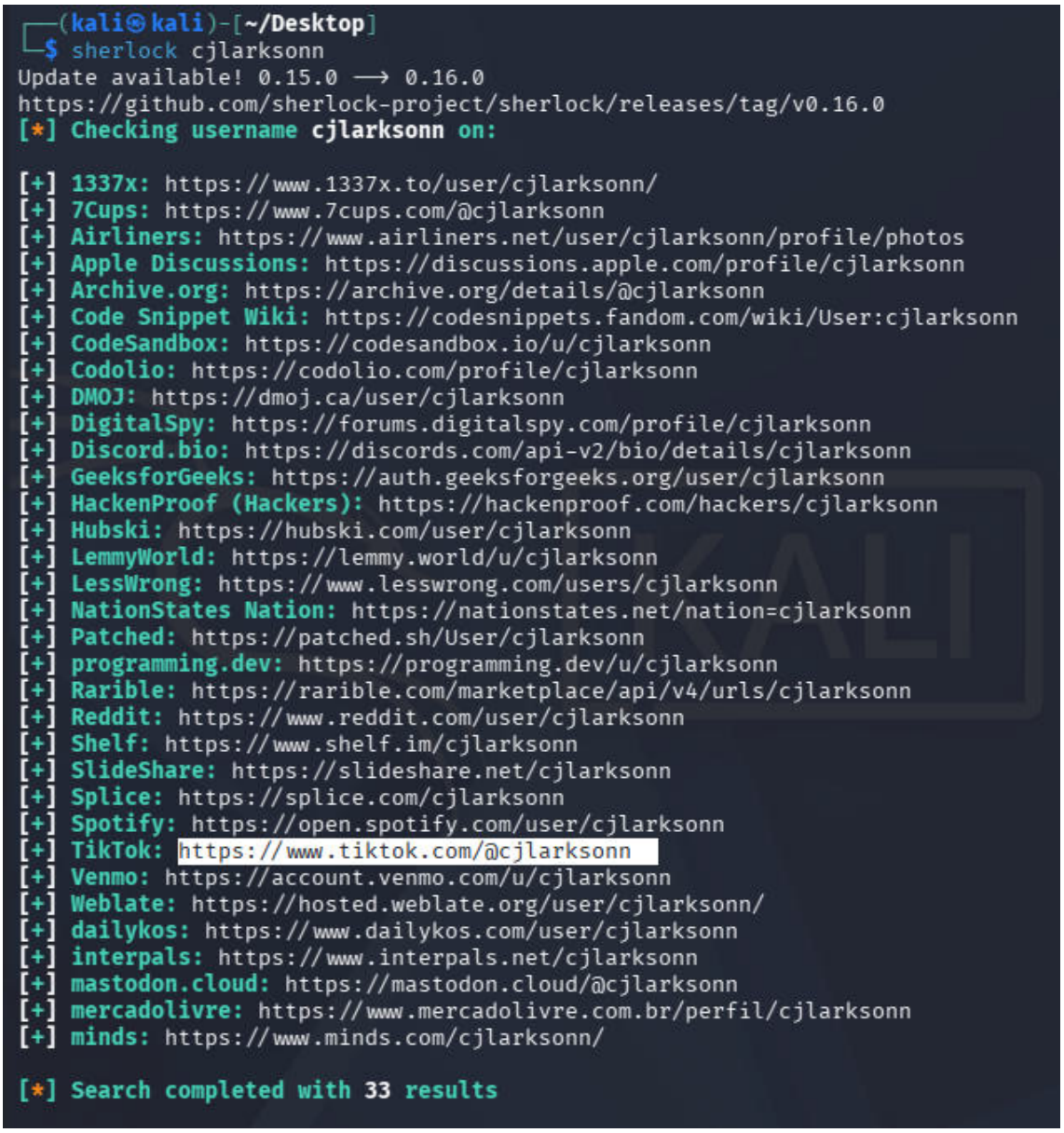

Рисунок 3.4 - Результати сканування утилітою Sherlock із великою кількістю недійсних посилань

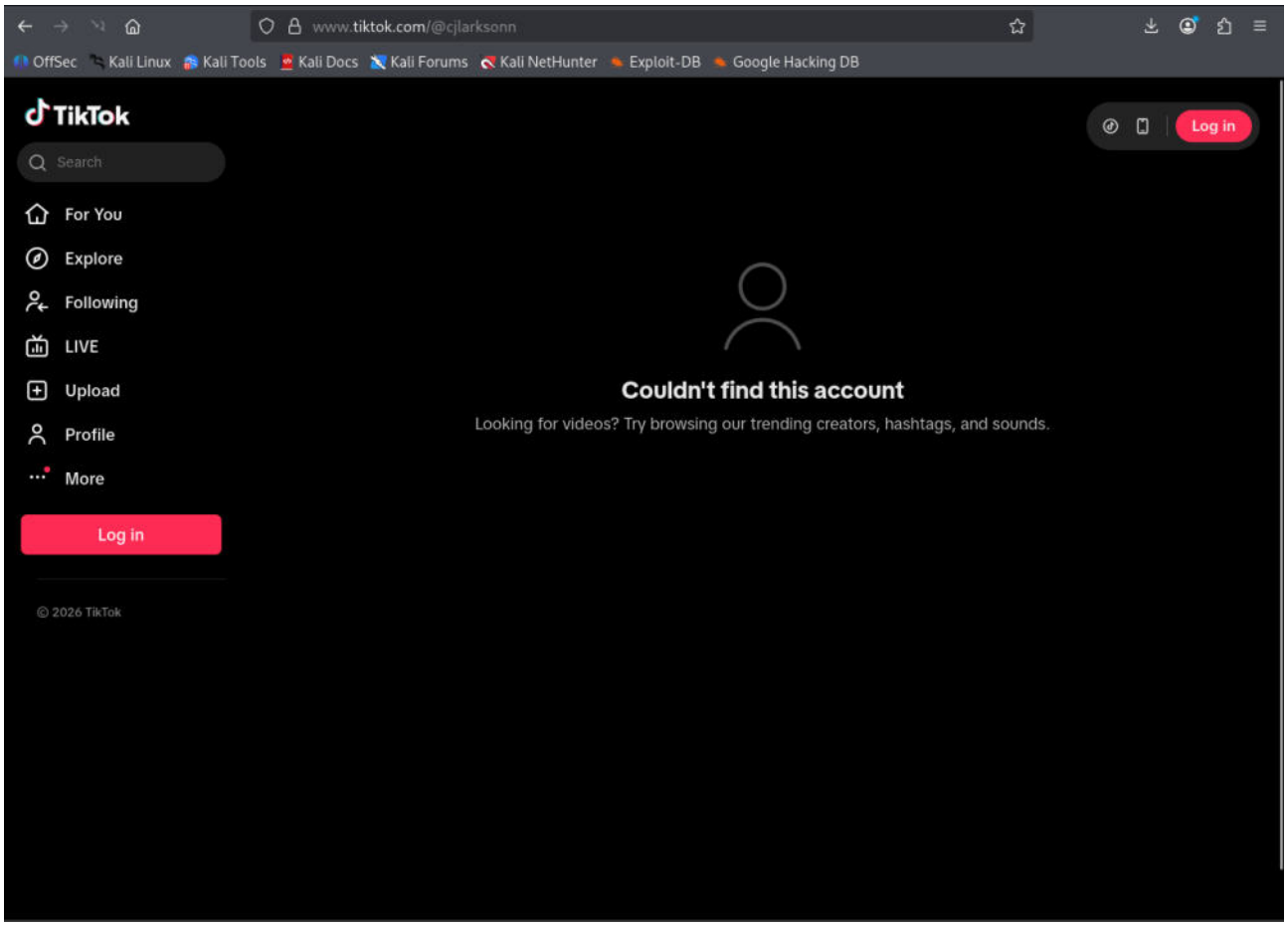

Рисунок 3.5 - Демонстрація перевірки недійсного акаунта після роботи Sherlock

Через низьку ефективність та високий рівень інформаційного шуму переходимо до використання утиліти maigret. Ця програма використовує складніші алгоритми валідації знайдених ресурсів. Вона аналізує не лише коди відповідей, а й проводить контентний аналіз сторінок на наявність специфічних тегів та метаданих профілю. Процес встановлення потребує налаштування ізольованого середовища через pipx:

maigret --version

sudo apt install pipx

pipx install maigret

sudo apt install pkg-config libcairo2-dev build-essential python3-dev -y

Виконується пошук із застосуванням фільтрації, обмежується список перевірки десятьма найбільш популярними світовими ресурсами, що дозволяє уникнути блокувань з боку систем захисту від роботів та прискорює

отримання результатів:

maigret cjlarksonn --top-sites 10

Інструмент maigret демонструє високу точність та швидкість ідентифікації (дивитися рисунок 3.6). Отримується підтвердження присутності користувача в мережах Instagram та X (Twitter). Програма автоматично витягує опис сторінок та виводить їх у термінал. Знаходимо реальне ім’я James Clarkson. Так, з попереднього завдання з назви файлу (J.Clarkson.png) можна було дізнатися фамілію і першу літеру ім'я. Ця невелика деталь підкреслює важливість уважної аналітики і лише підтверджує причетність особи з фото до цих акаунтів. Даний рядок є прапором для другого завдання. Було успішно пов’язано технічний нікнейм із реальною особистістю працівника, що дозволяє перейти до етапу візуальної розвідки профілів.

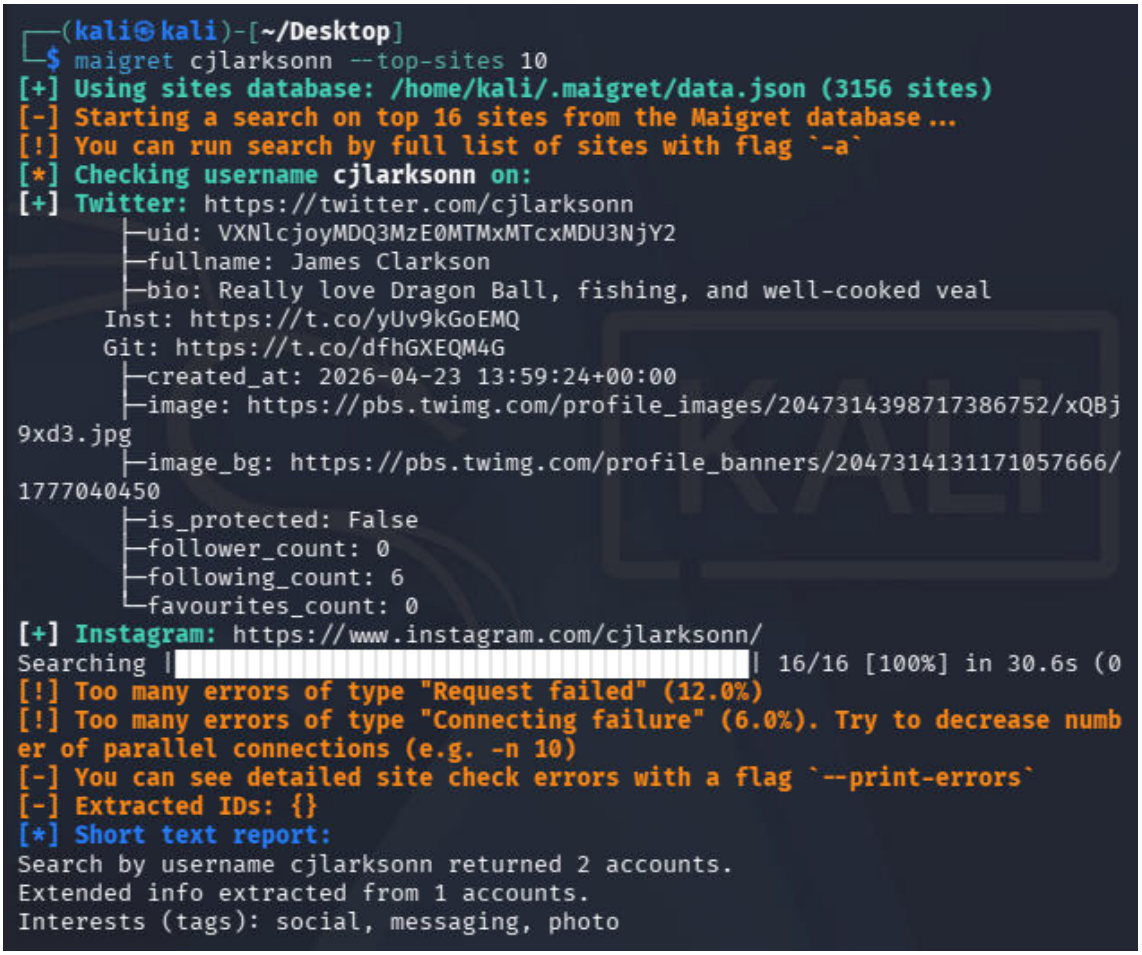

Рисунок 3.6 - Звіт maigret із посиланнями на активні соціальні профілі

Етап 3. Візуальний аналіз та витягування артефактів. Третє завдання сценарію під назвою Extracting Artifacts from Imagery вимагає від аналітика максимальної концентрації на деталях візуального контенту. Проводимо комплексне вивчення знайдених профілів у мережах Instagram та X. На цьому етапі встановлюються технічні та логічні зв'язки між акаунтами. Описи профілів містять перехресні посилання, що дозволяє підтвердити приналежність усіх знайдених ресурсів одній цифровій особистості. Підтверджується, що James Clarkson використовує ідентичний нікнейм для професійної та приватної комунікації.

Проводимо детальний огляд публікацій у стрічці Instagram. Основна увага зосереджена на фотографіях робочого середовища. Серед численних постів виявляється зображення, де користувач зафіксував своє робоче місце. На задньому фоні знімка виділяєтья паперова наліпка поруч із монітором. Стікер містить рукописні записи, можливо, технічного характеру. Головною перешкодою стає алгоритм стиснення зображень соціальної платформи, який робить текст дрібного масштабу майже нечитабельним при стандартному перегляді через веб інтерфейс.

Для отримання графічного файлу в оригінальній якості та обходу обмежень перегляду застосовується сторонній сервіс dumpor.io.

Посилання на платформу dumpor.io: https://dumpor.io/.

Даний інструмент дозволяє анонімно вивантажувати медіафайли з відкритих профілів без втрати роздільної здатності. Вводимо посилання на аккаунт об'єкта в пошуковий рядок сервісу (дивитися рисунок 3.7).

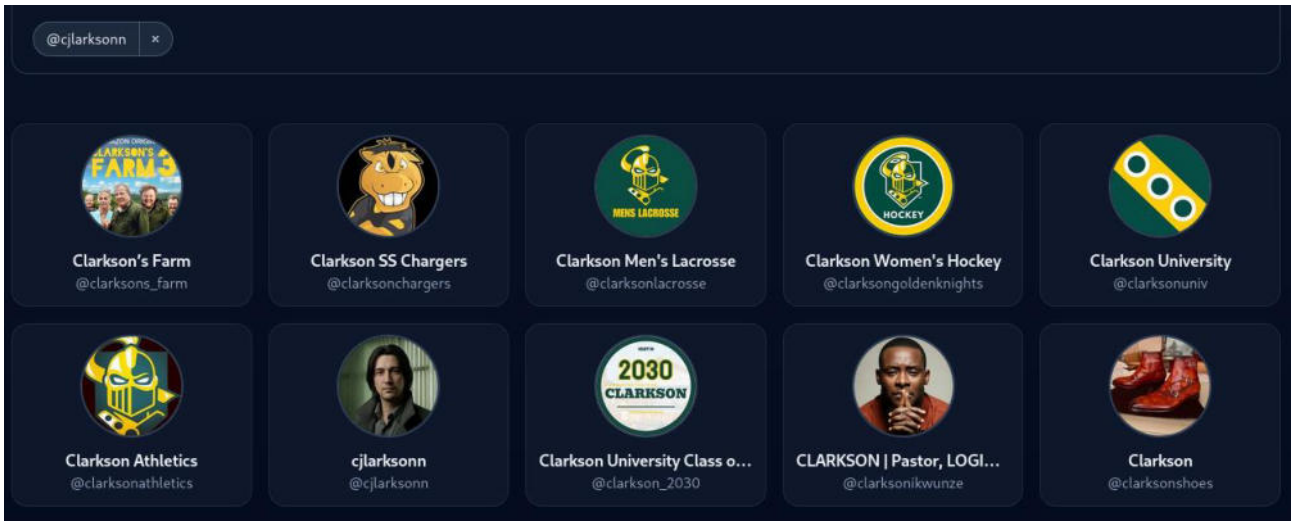

Рисунок 3.7 - Пошук цільового акаунта через сервіс dumpor.io

Знаходимо необхідну фотографію у списку доступних медіафайлів. Проводимо завантаження файлу на локальну робочу станцію. Після отримання зображення в максимальній якості використовуються цифрові методи збільшення та корекції чіткості і проводимо масштабування області з паперовою наліпкою. Виявляється рядок символів svh34x884e, який ідентифікується як пароль. Вводимо отримане значення як прапор у систему CTFd, це завдання наочно демонструє ризики витоку конфіденційних даних через фізичні предмети, які потрапляють у кадр під час випадкової зйомки.

Етап 4. Стеганографічний та криптографічний аналіз. Четверте завдання Steganography and Cryptographic Analysis фокусується на вивченні GitHub репозиторію об’єкта. Знаходимо проект під назвою BestPGPUsage. В описі репозиторію вказано дві кодові фрази: одна фраза слугує ключем для стеганографії, друга фраза є паролем для криптографічного розшифрування. Завантажується зображення з репозиторію. Для роботи зі стеганографією використовується утиліту steghide:

steghide -ver

sudo apt install steghide

Виконується команда для вилучення вмісту (дивитися рисунок 3.8). На цьому етапі проводимо підбір ключа із двох фраз знайдених на GitHub. Одна з фраз успішно відкриває стеганографічний контейнер:

steghide extract -sf image.jpg

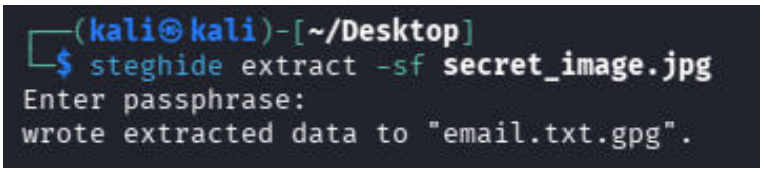

Рисунок 3.8 - Процес вилучення прихованого файлу за допомогою steghide

У результаті роботи програми отримується файл email.txt.gpg. Цей об’єкт є криптографічним контейнером із PGP шифром. Для його дешифрування задіється утиліта gnupg, яка зазвичай попередньо встановлена в дистрибутиві Kali. Перевіряється версія (завантажується утиліта, якщо необхідно) та запускається процес розшифрування (дивитися рисунок 3.9). Використовується друга кодова фраза як пароль до симетричного шифру:

gpg --version

sudo apt install gnupg

gpg --output result.txt --decrypt secret.gpg

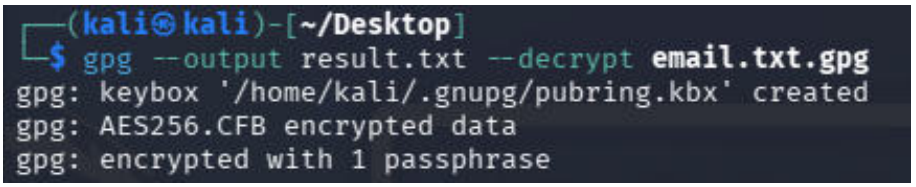

Рисунок 3.9 - Процес розшифрування PGP повідомлення в терміналі

У результаті виконання криптографічної операції отримується текстовий документ result.txt. Усередині документа знаходиться реальна поштова адреса користувача cjlarkson@protonmail.com. Дана адреса стає прапором четвертого етапу. Цим демонструється методика багатоступеневого захисту та ідентифікується прихований контактний канал об’єкта.

Етап 5. Аналіз інфраструктури та геолокація. Фінальний етап розслідування Network Infrastructure Attribution присвячено пошуку витоків технічних параметрів у вихідному коді. Продовжується аудит GitHub акаунта.

Перевіряється репозиторій NetDiagSuite, який позиціонується автором як набір інструментів для діагностики мережі. Проводимо ручний огляд файлової структури проекту. Знаходимо скрипт на мові Python із назвою ping_module.py (дивитися рисунок 3.10).

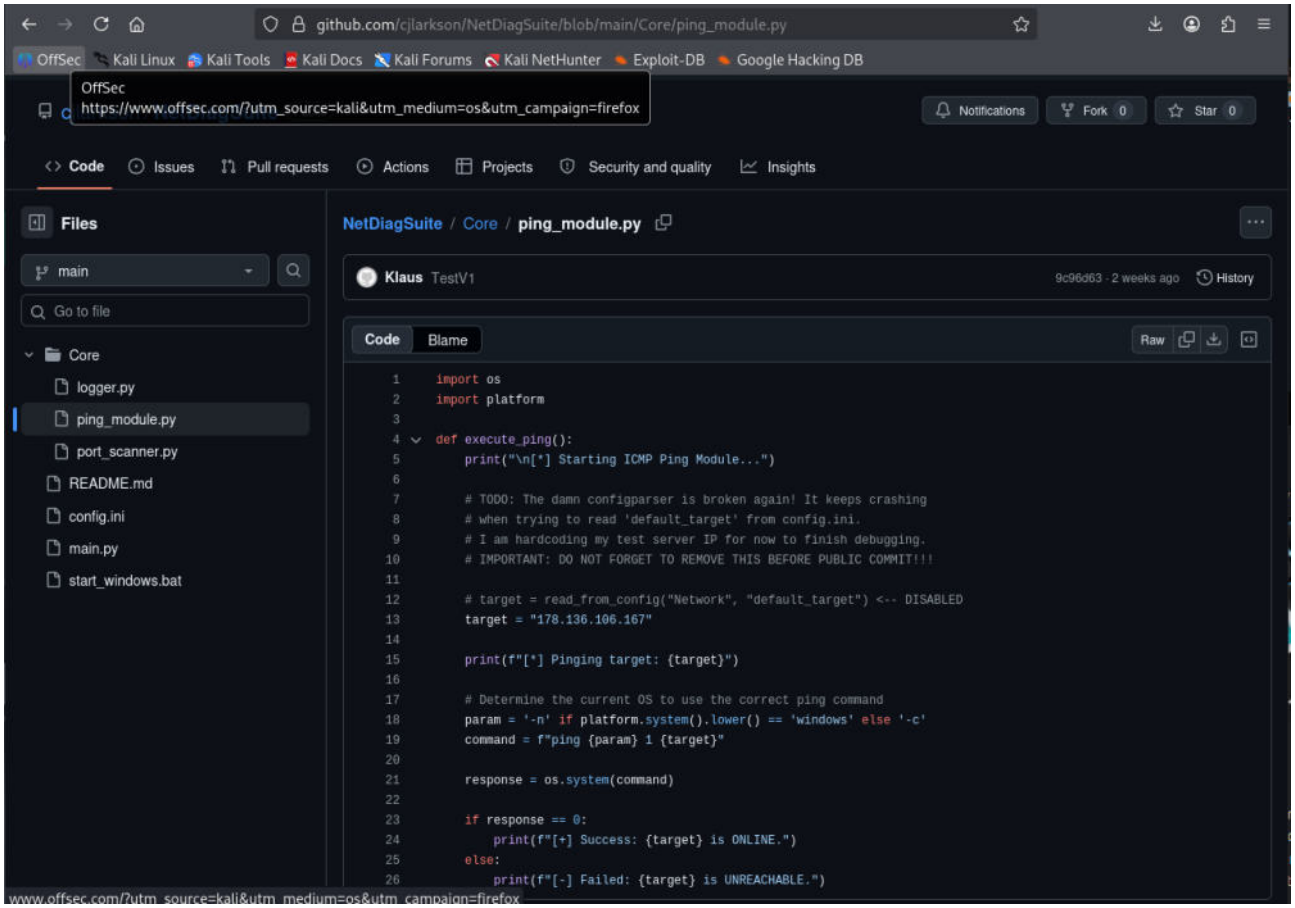

Рисунок 3.10 - Структура репозиторію NetDiagSuite на GitHub

Аналізується код модуля на наявність жорстко закодованих значень. У тілі програми виявляється IP адреса 178.136.106.167. Ця адреса була використана розробником для тестування функцій пінгування та випадково залишена в коді перед публікацією. Наявність реальної IP адреси дозволяє провести ідентифікацію географічного розташування мережевого обладнання об’єкта. Застосовується термінальна команда для звернення до API сервісу ipinfo.io [26]:

curl ipinfo.io/178.136.106.167

Програма здійснює запит до глобальних баз даних реєстрації мережевих

ресурсів. Отримується структурована відповідь у форматі JSON і аналізуються вихідні дані (дивитися рисунок 3.11). Знаходимо поле city, яке містить назву міста Одеса. Отримана назва стає фінальним прапором для завершення проходження всього сценарію. Таким чином довелося довелести, що недбалість при написанні коду призводить до розкриття фізичного місцезнаходження розробника.

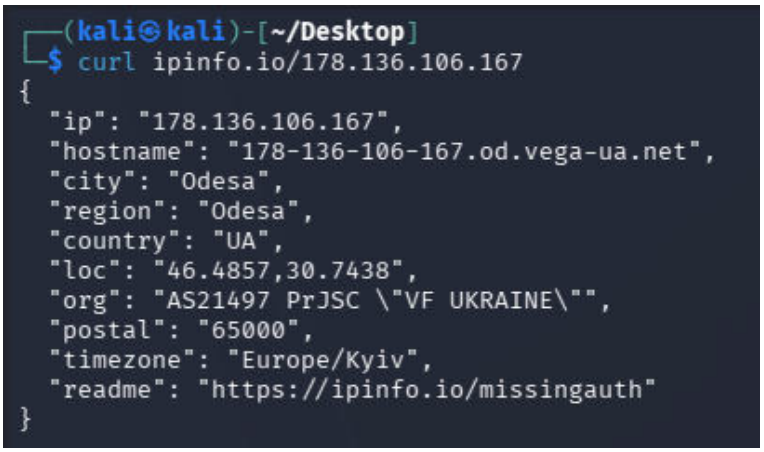

Рисунок 3.11 - Результат запиту до сервісу ipinfo з даними геолокації

Після успішного введення останнього прапора платформа CTFd фіксує повне проходження івенту. Реалізовано повний цикл деанонімізації особи - починаючи від метаданих випадкової фотографії до встановлення точного міста проживання через аналіз соціальних профілів та програмного коду.

3.2 Аналіз результатів ідентифікації та моделювання векторів атак на основі виявлених даних

Успішне проходження п’яти етапів сценарію дозволяє сформувати повний інформаційний портрет об’єкта. Кожен отриманий прапор не є просто текстовим рядком для системи CTFd, а це критичний фрагмент конфіденційної інформації, який зловмисник використовує для підготовки реальної кібератаки. Проводимо детальний технічний аналіз цінності знайдених даних та моделюються можливі сценарії [5] компрометації інфраструктури компанії.

Оцінка критичності технічного ідентифікатора (username). Виявлення

імені користувача cjlarksonn через метадані зображення є фундаментальним витоком. У корпоративному середовищі нікнейми часто збігаються з логінами до внутрішніх систем, таких як Active Directory, VPN або хмарні сховища. Отримання цього ідентифікатора дозволяє зловмиснику почати атаку методом перебору паролів (brute-force) або підбору за словником (dictionary attack). Знання структури логіна нівелює 50 відсотків зусиль, необхідних для несанкціонованого входу в систему. Також цей ідентифікатор стає ключем для пошуку в базах даних попередніх витоків (dumped databases), що дозволяє знайти застарілі паролі користувача, які він міг використати повторно.

Моделювання атак на основі соціальних профілів. Встановлення реального імені James Clarkson та знаходження його акаунтів у Instagram та X відкриває шлях до проведення атак із застосуванням соціальної інженерії. Зловмисник аналізує список друзів, колег та коло інтересів об’єкта. На основі цих даних розробляється сценарій атаки типу Business Email Compromise (BEC). Правопорушник створює фейковий профіль керівника або партнера компанії, використовуючи професійну термінологію та факти з публікацій об’єкта. Високий рівень деталізації цифрового сліду в соціальних мережах дозволяє зловмиснику маніпулювати довірою працівника, що призводить до передачі конфіденційних документів або виконання шкідливих інструкцій.

Аналіз ризиків компрометації паролів та облікових даних. Знахідка пароля svh34x884e на паперовій наліпці є найбільш критичним моментом сценарію - це пряме свідчення порушення політики фізичної безпеки. Наявність пароля поруч із робочим місцем дозволяє отримати миттєвий доступ до робочої станції, якщо зловмисник має фізичний доступ до офісу. В умовах дистанційної розвідки цей пароль перевіряється на збіг із доступами до інших сервісів користувача (credential stuffing) [34]. Працівники часто використовують схожі комбінації для корпоративної пошти та особистих кабінетів. Наявність User ID та пароля дозволяє імітувати сесію легітимного користувача, що робить атаку непомітною для систем виявлення вторгнень (IDS).

Криптографічні виклики та компрометація комунікацій. Отримання

email адреси cjlarkson@protonmail.com через розшифрування PGP шифру вказує на компрометацію каналів конфіденційного зв'язку. Використання сервісу ProtonMail свідчить про наміри об'єкта приховати листування, проте виявлення пошти дає зловмиснику ціль для проведення цілеспрямованого фішингу (spear-phishing). Використовується знайдений у репозиторії PGP ключ для перевірки цифрових підписів інших файлів компанії - це дозволяє ідентифікувати обсяг напрацювань розробника та структуру його проектів. Володіння прихованою поштою працівника технічного підрозділу дає змогу розсилати шкідливі оновлення коду від його імені, що ставить під загрозу цілісність усіх продуктів організації.

Геолокація та встановлення точки присутності. Виявлення IP адреси 178.136.106.167 у вихідному коді скрипта та подальша ідентифікація міста Одеса завершує процес деанонімізації. Знання IP адреси дозволяє зловмиснику почати технічне сканування мережевого периметра за вказаним вузлом. Виконується пошук відкритих портів та вразливих сервісів на цьому пристрої. Географічна прив'язка до міста Одеса допомагає визначити місцевого інтернет провайдера. На основі чого моделюється атака типу Man-in-the-Middle (MITM) через вразливості в обладнанні провайдера або публічні точки доступу Wi-Fi у цьому регіоні. Дані про геолокацію також використовується для проведення фізичного спостереження за об'єктом або координації атак у часових межах його активності. Матрицю взаємозв'язку знайдених даних та потенційних загроз представлено в таблиці 3.1.

Таблиця 3.1 - Матриця взаємозв'язку знайдених даних та потенційних загроз

Тип виявлених даних	**Отриманий прапор**	**Вектор можливої атаки**	**Рівень ризику**
Технічний логін	cjlarksonn	Перебір паролів. Пошук у базах витоків.	Середній

Продовження таблиці 3.1

Персональні дані	James Clarkson	Соціальна інженерія. Крадіжка особистості.	Високий
Текстовий пароль	svh34x884e	Credential stuffing. Несанкціонований доступ.	Критичний
Поштова адреса	cjlarkson@protonmail.com	Спрямований фішинг. Злам листування.	Високий
Мережевий вузол	178.136.106.167 (Одеса)	Сканування портів. MITM атаки.	Середній

Комплексний аналіз показує, що кожен крок розвідки посилює дієвість наступного етапу. Інформація з соціальних мереж робить фішинг більш переконливим, а знайдений пароль надає технічну можливість реалізації атаки. Моделювання цих сценаріїв доводить, що цифровий слід компанії є сукупністю вразливостей, які потребують негайної нейтралізації. Таким чином демонструється, як за допомогою лише відкритих джерел можливо підготувати повномасштабну операцію з проникнення у внутрішню мережу організації.

3.3 Технічні виклики автоматизованого збору даних: обмеження запитів та механізми захисту

Процес ідентифікації цифрового сліду стикається з активною протидією з боку сучасних веб ресурсів. Соціальні платформи впроваджують складні системи захисту від автоматизованого збору інформації (anti-scraping). Усі ці заходи впливають на стабільність роботи утиліт для пошуку профілів. Аналізуються основні технічні чинники, які ускладнюють отримання даних у

межах сценарію розвідки.

Основним методом захисту є обмеження частоти запитів (Rate Limiting). Сервери соціальних мереж відстежують кількість звернень з однієї IP адреси за одиницю часу. При перевищенні встановленого ліміту сайт тимчасово блокує доступ або видає код помилки 429 Too Many Requests. Саме цей фактор зумовлює потребу обмеження пошуку утилітою maigret списком топ 10 найбільш популярних ресурсів. Висока інтенсивність запитів програми Sherlock призводить до отримання пустих відповідей, що програма часто інтерпретує як наявність профілю, в свою чергу - це створює інформаційний шум та потребує ручної перевірки кожного посилання.

Механізми валідації браузера та ідентифікація ботів складають другий рівень захисту. Системи типу Cloudflare [35] аналізують технічні заголовки HTTP запитів (User-Agent), якщо інструмент розвідки використовує стандартні заголовки бібліотек Python або Go. Сервер ідентифікує активність як роботу скрипта. У відповідь сайт може вимагати проходження капчі або надавати неправдивий контент. Використання ротації User-Agent дозволяє зменшити кількість відмов під час сканування глобальних мереж.

Динамічна генерація контенту (Single Page Applications) створює труднощі для класичних парсерів. Багато сучасних сайтів завантажують дані профілю лише після виконання JavaScript сценаріїв у браузері. Прості утиліти OSINT розвідки аналізують лише початковий HTML код сторінки, де потрібна інформація може бути відсутня -це спричиняє ситуації. Коли аккаунт існує, але автоматизований засіб його не знаходить. Основні технічні бар'єри розвідки та методи їх подолання узагальнено в таблиці 3.2.

Таблиця 3.2 - Технічні бар'єри OSINT розвідки та методи їх подолання

Тип перешкоди	**Опис механізму впливу**	**Технічне рішення для обходу**
Rate Limiting	Тимчасове блокування IP при масових запитах	Впровадження затримок та використання проксі.

Продовження таблиці 3.2

Browser Fingerprinting	Ідентифікація автоматизованих скриптів за заголовками	Ротація User-Agent та використання легітимних заголовків.
CAPTCHA	Вимога підтвердження людської діяльності	Застосування сервісів автоматичного розв'язання або API ключів.
Dynamic Content	Завантаження даних через JS сценарії	Використання браузерних рушіїв типу Selenium або Puppeteer.

Розуміння цих технічних обмежень є обов’язковим для фахівця з кібербезпеки. Враховуються механізми захисту сайтів під час планування етапів розвідки. Коректне налаштування інструментарію дозволяє мінімізувати кількість технічних помилок, що забезпечує отримання валідних прапорів та точну ідентифікацію об’єкта в умовах реального інтернет простору.

3.4 Дослідження помилок та надійності роботи обраних програмних засобів

Ефективність ідентифікації цифрового сліду залежить від точності застосованого інструментарію. Практична апробація сценарію виявила низку технічних особливостей та обмежень обраних утиліт. Проводимо аналіз надійності роботи програмних засобів та оцінюється якість отриманих даних.

Аналіз хибних спрацювань (false positive). Найбільша кількість помилок зафіксована під час роботи з утилітою Sherlock. Програма виявила 33 профілі за нікнеймом cjlarksonn. Подальша ручна перевірка показала нульову валідність цих результатів. Жоден із знайдених акаунтів не належав цільовому об’єкту.

Причиною виникнення хибних спрацювань є недосконаліть методу перевірки HTTP-статусів. Sherlock надсилає запит на веб-сторінку профілю.

Програма вважає аккаунт існуючим при отриманні коду 200 OK. Багато сучасних сайтів використовують універсальні сторінки-заглушки для будь-яких запитів. Сервери видають успішну відповідь навіть для неіснуючих користувачів - це створює інформаційний шум та спотворює результати розвідки. Спеціаліст витрачає значний час на відсіювання нерелевантних посилань.

Утиліта maigret демонструє вищу надійність порівняно із Sherlock. Програма застосовує складніші алгоритми валідації вмісту сторінок. maigret аналізує не лише коди відповідей. Програма шукає специфічні текстові рядки та ідентифікатори в коді сайту -це дозволяє уникнути більшості хибних спрацювань, проте ризик помилки залишається при зміні структури веб-ресурсів власниками платформ.

Обмеження безкоштовних ресурсів та баз даних. Використання безкоштовних API для геолокації за IP-адресою має суттєві обмеження щодо точності. Сервіс ipinfo.io надає дані про місто реєстрації мережевого вузла, ці відомості базуються на реєстраційних записах інтернет-провайдерів. Безкоштовні версії баз даних часто мають затримку в оновленні інформації. Отримане місто Одеса вказує на регіональну приналежність обладнання провайдера, але це не гарантує фізичну присутність користувача в конкретній точці міста. Точність геолокації знижується при використанні провайдерами технологій динамічного розподілу адрес.

Додаткові обмеження стосуються безкоштовних інструментів візуального аналізу. Сервіси типу dumpor.io залежать від доступності Instagram API. Соціальна мережа постійно впроваджує нові методи захисту від автоматизованого збору даних, що призводить до тимчасової непрацездатності безкоштовних утиліт та сервісів для скачування контенту. Користувач змушений шукати альтернативні джерела для отримання зображень в оригінальній якості. Оцінку надійності та обмежень обраного інструментарію наведено в таблиці 3.3.

Таблиця 3.3 - Оцінка надійності та обмежень інструментарію

Інструмент	**Тип основної помилки**	**Причина виникнення**	**Рівень точності**
Sherlock	Хибні спрацювання	Особливості HTTP-відповідей сайтів	Низький
maigret	Залежність від парсерів	Зміни в коді веб-сторінок	Високий
ipinfo.io	Неточна локація	Затримки в оновленні GeoIP баз	Середній
exiftool	Відсутність даних	Автоматичне очищення тегів серверами	Максимальний

Результати дослідження підтверджують необхідність комплексного підходу. Фахівець не повинен довіряти результатам однієї утиліти. Кожен отриманий фрагмент цифрового сліду потребує перехресної перевірки іншими методами. Розуміння природи помилок дозволяє критично оцінювати надійність побудованого профілю об’єкта.

3.5 Складання переліку заходів для мінімізації цифрової присутності персоналу

Проведене OSINT дослідження доводить критичну небезпеку неконтрольованого накопичення цифрових слідів. Компанії мають впроваджувати системні заходи для зменшення обсягу доступної ззовні інформації. Розробляється стратегія захисту на трьох рівнях:

- Організаційному
- Технічному

- Персональному

Мета полягає у створенні умов, за яких збирання даних з відкритих джерел стане неефективним для зловмисників.

Стратегічні заходи на рівні організації. Впроваджується політика «Чистого столу» як обов'язковий стандарт роботи. Забороняється розміщення паролів та ідентифікаторів на паперових носіях у межах офісу. Проводимо регулярні аудити робочих місць.

Перевіряється відсутність наліпок на моніторах, перевіряється відсутність записаних логінів у блокнотах. Пояснюється працівникам, що будь яка випадкова фотографія робочого простору стає інструментом зламу системи.

Організовується циклічне навчання персоналу основам кібербезпеки, проводимо симуляції атак із застосуванням соціальної інженерії, демонструється працівникам реальні приклади деанонімізації осіб через соціальні мережі. Прищеплюються навички критичного оцінювання контенту перед його публікацією. Тренінги мають охоплювати всіх співробітників, від адміністративного персоналу до керівництва. Створюється культура відповідальності за розкриття корпоративної інформації.

Здійснюється постійний моніторинг зовнішнього інформаційного периметра. Використовуються методи OSINT для проведення самостійного аудиту компанії. Потрібно шукати витоки технічних даних на форумах, в репозиторіях, ідентифікувати профілі працівників із надмірним рівнем відкритості, розробляти регламенти реагування на виявлені факти публікації конфіденційної інформації та встановити обмеження на використання робочої техніки для особистих потреб.

Технічні регламенти для іт та технічних підрозділів. Встановлюються суворі правила роботи з метаданими. Вимагається обов'язкового очищення технічних тегів з усіх медіафайлів перед завантаженням у мережу. Використовується утиліта ExifTool для автоматизації процесу в межах корпоративних скриптів, видаляються дані про шлях до файлів, версії програм, геомітки. Забезпечується неможливість отримання нікнеймів користувачів через властивості зображень.

Впроваджуються автоматичні фільтри на поштових серверах для видалення метаданих із вкладень.

Впроваджуються стандарти безпечного програмування. Забороняється використання жорстко закодованих IP адрес у вихідному коді. Переходимо на використання змінних середовища для конфігурації підключень. Застосовуються автоматизовані сканери секретів у CI/CD процесах. Налаштовуються файли .gitignore [36] для запобігання потраплянню технічних логів у публічні репозиторії GitHub. Проводимо регулярний аналіз коду на наявність витоків конфіденційної інформації.

Вимагається регулярна перевірка історії комітів у хмарних сховищах коду. Видаляються конфіденційні дані з усіх попередніх версій файлів. Використовуються інструменти для повного затирання історії при випадкових витоках. Розділяється особиста активність розробників від робочих проектів. Забороняється використання робочих поштових адрес для реєстрації особистих профілів на платформах для розробників. Контролюється доступ до корпоративних репозиторіїв через систему аутентифікації.

Персональна цифрова гігієна користувачів. Налаштовуються максимальні параметри приватності в соціальних мережах Instagram та X. Обмежується видимість профілів лише для перевірених контактів. Відключається автоматичне додавання геоміток у налаштуваннях камер смартфонів, перевіряється задній план кожної фотографії перед завантаженням, потрібно переконатися у відсутності документів, у відсутності перепусток, у відсутності ввімкнених екранів комп’ютерів у кадрі.

Використовуються унікальні нікнейми для кожного окремого ресурсу. Уникаються повторення технічних ідентифікаторів облікових записів. Ускладнюється для аналітика процес зв’язування акаунтів у єдиний цифровий профіль, застосовуються різні аватари для професійних та особистих сторінок. Мінімізується обсяг особистої інформації в розділах біографії акаунтів. Потрібно відмовитися від поширення планів про відпустки та робочі поїздки в режимі реального часу.

Впроваджується використання менеджерів паролів для зберігання всіх доступів. Створюються унікальні складні паролі для кожної системи. Потрібно відмовитися від практики використання однакових логінів для робочої пошти та соціальних мереж. Застосовується багатофакторня автентифікацію всюди (де це технічно можливо). Використовуються складні парольні фрази для захисту PGP ключів. Ніколи не публікуються підказки до паролів у відкритому доступі та регулярно перевіряються власні акаунти на наявність підозрілої активності.

Впровадження цих заходів створює надійний бар’єр для розвідки на основі відкритих джерел. Потрібно перетворити кібербезпеку на безперервний процес контролю власної цифрової присутності і підвищити ціну проведення атаки для зловмисника до неприйнятного рівня. Робота забезпечує стійкість компанії до сучасних загроз інформаційному простору.

Висновок

Результати проведеного дослідження дозволяють зробити підсумки щодо ефективності методів OSINT для виявлення цифрового сліду компанії. Головною метою роботи була розробка та тестування практичного сценарію в умовах навчального кіберполігона. Було виконано всі поставлені технічні завдання та обґрунтування доцільність застосування обраних методів ідентифікації об’єктів.

Аналіз предметної галузі показав, що неконтрольоване накопичення публічних даних персоналу створює критичні вразливості для сучасних організацій. Встановлено, що людський фактор залишається головним джерелом витоків конфіденційної інформації. Цифровий слід працівників дозволяє зловмисникам проводити успішні атаки через методи соціальної інженерії та технічну розвідку. Дослідження підтвердило актуальність розробки методів виявлення таких витоків на ранніх стадіях.

У межах роботи розроблено алгоритм із п’яти послідовних етапів ідентифікації об’єкта. Побудовано логічний ланцюжок від аналізу технічних метаданих до встановлення географічного розташування розробника. Для створення реалістичного середовища було використано методи генерації синтетичних особистостей за допомогою штучного інтелекту на платформі Higgsfield, що забезпечило дотримання етичних норм та надало можливість повного контролю над усіма артефактами дослідження. Обґрунтувано вибір технічного стеку на основі утиліт ExifTool. Maigret. Sherlock. Steghide та GnuPG.

Практична частина реалізована через розгортання локальної інфраструктури на базі Docker та платформи CTFd. Використання засобів віртуалізації Kali Linux дозволило обійти обмеження хмарних сервісів та забезпечити стабільність мережевих запитів до соціальних платформ. Створена кімната змагань імітує реальні умови проведення OSINT розслідування. Система автоматичної валідації прапорів забезпечує об’єктивність оцінювання результатів проходження сценарію.

Тестування розробленого рішення підтвердило можливість повної деанонімізації об’єкта на основі лише відкритої інформації. Успішно пройдено шлях від ідентифікації імені користувача в метаданих однієї фотографії до знаходження конфіденційної поштової адреси та IP вузла. Процес виявив технічні недоліки окремих утиліт, таких як Sherlock, через велику кількість хибних спрацювань. Це зумовило перехід до використання більш точних засобів валідації контенту типу maigret. Розшифрування PGP шифрів та аналіз вихідного коду в репозиторіях GitHub довели небезпеку залишення технічних параметрів у публічному доступі.

На основі отриманих даних складено детальний перелік заходів для мінімізації цифрової присутності персоналу. Впровадження політики чистого столу. Регулярне навчання працівників цифрової гігієни та автоматизоване очищення метаданих файлів є необхідними елементами стратегії захисту. Технічні регламенти для IT підрозділів мають включати обов’язковий аудит публічних репозиторіїв на наявність жорстко закодованих даних.

Розроблений сценарій має високу практичну цінність для підготовки персоналу та підвищення кваліфікації фахівців. Проект дозволяє спеціалістам здобути навички роботи з професійними інструментами розвідки в ізольованому середовищі. Робота демонструє аналітичний підхід до ідентифікації прихованих загроз у цифровому просторі. П’ять завдань формують навички пошуку та аналізу витоків конфіденційних відомостей. Комплекс підходить для тренування користувачів із різним рівнем технічної підготовки.

Список використаних джерел

1. OSINT Framework [Електронний ресурс]. - URL: https:// osintframework.com (дата звернення: 01.06.2026).

2. ExifTool Tag Names [Електронний ресурс]. - URL: https://exiftool.org/ TagNames/EXIF.html (дата звернення: 01.06.2026).

3. GitHub Documentation [Електронний ресурс]. - URL: https:// docs.github.com (дата звернення: 01.06.2026).

4. Mosaic theory in intelligence [Електронний ресурс]. - URL: https:// en.wikipedia.org/wiki/Mosaic_theory_of_the_Fourth_Amendment (дата звернення: 01.06.2026).

5. MITRE ATT&CK [Електронний ресурс]. - URL: https://attack.mitre.org (дата звернення: 01.06.2026).

6. Avoiding Social Engineering and Phishing Attacks [Електронний ресурс]. - URL: https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks (дата звернення: 01.06.2026).

7. Guide for Conducting Risk Assessments, NIST Special Publication 800-30 Revision 1 [Електронний ресурс]. - URL: https://nvlpubs.nist.gov/nistpubs/ Legacy/SP/nistspecialpublication800-30r1.pdf (дата звернення: 01.06.2026).

8. ExifTool by Phil Harvey [Електронний ресурс]. - URL: https://exiftool.org (дата звернення: 01.06.2026).

9. Sherlock Project [Електронний ресурс]. - URL: https://github.com/sherlock-project/sherlock (дата звернення: 01.06.2026).

10. Maigret [Електронний ресурс]. - URL: https://github.com/soxoj/maigret (дата звернення: 01.06.2026).

11. Steghide [Електронний ресурс]. - URL: https://steghide.com/ (дата звернення: 01.06.2026).

12. The GNU Privacy Guard [Електронний ресурс]. - URL: https://gnupg.org/ documentation/ (дата звернення: 01.06.2026).

13. FOCA [Електронний ресурс]. - URL: https://github.com/ ElevenPaths/

FOCA (дата звернення: 01.06.2026).

14. Exiv2 - Image metadata library and tools [Електронний ресурс].- URL: https://exiv2.org/ (дата звернення: 01.06.2026).

15. Social Analyzer [Електронний ресурс]. - URL: https://github.com/qeeqbox/social-analyzer (дата звернення: 01.06.2026).

16. OpenStego - Free Steganography solution [Електронний ресурс]. - URL: https://www.openstego.com/ (дата звернення: 01.06.2026).

17. Stegsolve [Електронний ресурс]. - URL: https://github.com/zardus/ctf-tools/tree/master/stegsolve (дата звернення: 01.06.2026).

18. OpenSSL Documentation [Електронний ресурс]. - URL: https://www.openssl.org/ docs/ (дата звернення: 01.06.2026).

19. CTFd Documentation [Електронний ресурс]. - URL: https://docs.ctfd.io (дата звернення: 02.06.2026).

20. Oracle VM VirtualBox Documentation [Електронний ресурс]. - URL: https://www.virtualbox.org/wiki/Documentation (дата звернення: 02.06.2026).

21. Kali Linux Documentation [Електронний ресурс]. - URL: https://www.kali.org/docs/ (дата звернення: 02.06.2026).

22. Docker Documentation [Електронний ресурс]. - URL: https://docs.docker.com/ (дата звернення: 02.06.2026).

23. CTFd Deployment Installation [Електронний ресурс]. - URL: https://docs.ctfd.io/docs/deployment/installation (дата звернення: 02.06.2026).

24. Guide to Integrating Forensic Techniques into Incident Response [Електронний ресурс]. - URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf (дата звернення: 02.06.2026).

25. Social Engineering [Електронний ресурс]. - URL: https://www.crowdstrike.com/cybersecurity-101/social-engineering/ (дата звернення: 02.06.2026).

26. IPinfo API Documentation [Електронний ресурс]. - URL: https://ipinfo.io/developers (дата звернення: 02.06.2026).

27. What is PGP encryption and how does it work? [Електронний ресурс. - URL: https://proton.me/blog/what-is-pgp-encryption (дата звернення: 02.06.2026).

28. Prompting guide for Nano Banana Pro [Електронний ресурс]. - URL: https://dev.to/googleai/nano-banana-pro-prompting-guide-strategies-1h9n (дата звернення: 02.06.2026).

29. What is ByteDance Seedream? [Електронний ресурс]. - URL: https://www.mindstudio.ai/blog/what-is-bytedance-seedream-4-5 (дата звернення: 02.06.2026).

30. ChatGPT Images 2 Review & Use Cases [Електронний ресурс]. - URL: https://www.mindstudio.ai/blog/chatgpt-images-2-review-use-cases (дата звернення: 02.06.2026).

31. Wan 2.2 [Електронний ресурс]. - URL: https://github.com/Wan-Video/Wan2.2 (дата звернення: 02.06.2026).

32. Adobe Express User Guide [Електронний ресурс]. - URL: https://helpx.adobe.com/express/user-guide.html (дата звернення: 02.06.2026).

33. Tampermonkey [Електронний ресурс]. - URL: https://www.tampermonkey.net/ (дата звернення: 02.06.2026).

34. Credential Stuffing [Електронний ресурс]. - URL: https://owasp.org/www-community/attacks/Credential_stuffing (дата звернення: 02.06.2026).

35. What is rate limiting? [Електронний ресурс]. - URL: https://www.cloudflare.com/learning/bots/what-is-rate-limiting/ (дата звернення: 02.06.2026).

36. Gitignore Documentation [Електронний ресурс]. - URL: https://git-scm.com/docs/gitignore (дата звернення: 02.06.2026).

37. Symantec Encryption Desktop (PGP Desktop) [Електронний ресурс] - URL: https://knowledge.broadcom.com/external/article/180244/downloading-the-pgp-encryption-desktop-s.html (дата звернення: 02.06.2026).

ДОДАТКИ

ДОДАТОК А

Побудова завдань на платформі CTFd

Завдання 1

Name: Initial Metadata Reconnaissance

Category: Open Source Intelligence

Message:

Introduction

****Introduction****

In the world of OSINT, metadata is a goldmine. Every photo contains hidden technical data (EXIF/XMP). Often, users accidentally share sensitive information like local file paths, which reveal their username or directory structure.

****The Challenge****

1. Download the file: Download the provided image from Proton Drive: [https://drive.proton.me/urls/623G57W1JC#9xy89zUcmJZD](https://)

2. Analyze: Use some kind of tool to extract all metadata from the file.

3. Identify: Find the Windows file path and extract the username associated with the system.

****Why this matters****

Leaving metadata in shared files is a common security oversight. Always clean your files before distribution!

****Question****

What is the username identified in the metadata path of the image?

Value: 1

Flag: cjlarksonn

Hint: Check the "Source" or "Preserved Filename" tag in the exiftool output. It follows the standard C:\Users\<username> pattern.

Завдання 2

Name: Social Media Footprinting

Category: Open Source Intelligence

Message:

****The Intelligence Cycle****

Now that you have successfully identified the target's username from the initial metadata analysis, the investigation moves into the phase of Active Reconnaissance. In the digital age, a single username often leaves footprints across multiple platforms.

****The Objective****

Your goal is to correlate the username discovered in Task 1 across various social media platforms. Your objective is to uncover the Full Name of the target.

****Guidelines for Investigation****

- Use the identified username to search across common social media networks.
- You are free to choose your own methodology. Whether you prefer automated OSINT frameworks, specialized repository-based tools, or manual Google Dorking techniques, the choice is yours.
- Consider how user patterns, profile descriptions, and public posts might contain the information you need. You do not need to exploit any systems; focus on analyzing publicly available data.

****Ethical Note****

This CTF is for educational purposes only. Always conduct your OSINT activities within legal and ethical boundaries, respecting the privacy and terms of service of the platforms you are researching.

****Question****

What is the full name (First Name and Last Name) of the target identified through social media?

Flag: James Clarkson

Hint: Check the profile "About" sections on the social media platforms. Both the X and Instagram profiles contain the same full name.

Завдання 3

Name: Extracting Artifacts from Imagery

Category: Open Source Intelligence

Message:

****The Hidden Detail****

Visual reconnaissance often reveals sensitive information that users leave exposed in their physical workspace. A common mistake is capturing sensitive documents, sticky notes, or screen content in photographs shared on social media.

****The Challenge****

Your investigation has led you to a specific post on the target's social media profile. The image shows the user's workspace. Your task is to identify and extract the sensitive information (a password) clearly visible in the photo.

****Critical Considerations****

- Social media platforms frequently apply aggressive compression to images, which can degrade quality.
- You must decide how to handle these artifacts. You might need to retrieve the original-resolution image, apply image enhancement techniques, or use specific tools to view the media without quality loss.
- The password is small and potentially blurred, but it is readable. Focus on the physical environment depicted in the photo.

****Question****

What is the password found on the note in the workspace photo?

Flag: svh34x884e

Accepted flag: svh34x884c

Hint: Check Instagram account. The password is written on a sticky note near the monitor. You might need to use an external tool or a browser extension to download the image in its best possible resolution

Завдання 4

Name: Steganography and Cryptographic Analysis

Category: Open Source Intelligence

Message:

****The Developer's Playground****

Public source code repositories are frequently used by developers to showcase their work, but they are also a common source of data leakage. In this phase of the investigation, you are required to analyze the target's GitHub profile.

****The Objective****

Within the repositories, you will find a project related to PGP (Pretty Good Privacy) implementation. Your task is to:

1. Identify the correct repository.
2. Recover the hidden PGP-encrypted message embedded within an image found in the repository.
3. Use the provided keys (found in the repository description) to decrypt the PGP message and reveal the target's private email address.

****Technical Methodology****

- You will encounter various file formats. Think about where information can be hidden within an image file without altering its visual appearance.
- Once the encrypted payload is extracted, you must apply the correct cryptographic procedure using the provided keys.
- Proper identification of the cipher type and key application is crucial for successful decryption.

****Ethical Note****

This task simulates a real-world scenario of sensitive information leakage through insecure storage practices. Never use these techniques to compromise systems without explicit authorization.

****Question****

What is the target's private email address found after decryption?

Answer: cjlarkson@protonmail.com

Hint: First, extract the hidden data from the image using the appropriate steganographic tool. Then, use the remaining phrase as a passphrase for GnuPG to decrypt the extracted file.

Завдання 5

Name: Network Infrastructure Attribution

Category: Open Source Intelligence

Message:

****The Developer's Oversight****

In software development, "hardcoding" configuration data - such as IP addresses, API keys, or credentials - into source code is a critical vulnerability. Developers often use test configurations for internal diagnostics, but failing to remove them before pushing code to a public repository creates a significant security risk.

****The Objective****

Your final task is to perform a comprehensive audit of the target's GitHub repositories. You need to investigate the source code to find any evidence of testing configurations.

****Your Investigation Steps****

1. Review the codebase for diagnostic or networking-related tools.

2. Locate the specific file containing network diagnostic code. Analyze the script to find a leaked IP address used for testing.

3. Once you have obtained the IP address, your task is to correlate it with physical geographic data. Use public tools to determine the registered location (city) of the target's infrastructure.

****Why It Matters****

This exercise demonstrates the importance of "Security by Design" and the necessity of rigorous code reviews. Even a small piece of diagnostic code can lead to complete exposure of an individual's location.

****Question****

What is the city associated with the leaked test IP address**?**

Answer: Odessa

Hint: Use an IP geolocation tool or a CLI utility that queries IP registry databases. Remember: the city name is what we are looking for.

ДОДАТОК Б

Процес створення візуального образу персонажа

Фото №1

Початкове фото:

Рисунок Б.1 - Вихідне зображення персонажа Кендзо Тенма

Промпт:

Transform this image into an ultra-realistic, cinematic photograph of a real person who looks exactly like the man in the reference. Preserve 100% identical identity: exact facial structure, facial features, eye shape and color, hair color and hairstyle with realistic individual strands, exact expression, head tilt and body pose, clothing (dark high-collared jacket with the same texture and details), and the entire background.

Convert the image to photorealistic quality with extreme high detailization and cinematic look. Restore and enhance micro-details: natural skin texture with visible pores and subtle imperfections, realistic hair strands, clear expressive eyes with natural catchlights, sharp and clean edges.

Maintain the exact same composition, framing, and cropping. Do not change, add,

remove, or redesign anything — only enhance quality and realism based on the original.

Apply high contrast sharpness, deep volumetric depth, and balanced cinematic lighting. Professional poster-level realism with studio-grade sharpness. Use only photorealistic textures for skin, hair, fabric, and environment.

Output: 8K resolution, ProRes quality, extremely sharp and detailed, filmic color grading.

Сгенероване фото (без водяного знаку):

Рисунок Б.2 - Згенероване зображення персонажа Джеймс Кларксон

Фото №2

Початкове фото:

В якості референсу для наступного етапу використовувалось попередньо згенероване зображення (дивитися рисунок Д.2.2).

Промпт:

Create a professional LinkedIn-style headshot portrait of the exact same young man from the reference photo.

He is wearing a dark blue over a light grey T-shirt. The outfit should look modern, clean, and professional.

Pose: classic professional headshot pose — shoulders slightly angled, head turned straight towards the camera with a confident, approachable, and neutral expression (subtle friendly smile, direct eye contact).

Lighting: soft, even studio lighting with gentle shadows, creating a polished and flattering look typical of corporate headshots. Clean, minimalist light gray or soft gradient background (professional studio backdrop, no distractions).

Maintain 100% identical facial features, eye color, hair color and hairstyle from the reference. Keep the same face structure, skin details, and overall likeness.

Ultra-realistic photorealistic quality, 8K resolution, extremely sharp details, natural skin texture with visible pores, realistic hair strands, clear expressive eyes. Cinematic yet professional color grading, high sharpness, studio quality.

Professional corporate LinkedIn portrait style, similar to high-end business headshots.

Exact same person with wide shouldres, only change clothing to dark blue over a light grey T-shirt and use a clean studio background.

Сгенероване фото (без водяного знаку):

Рисунок Б.3 - Згенероване «корпоративне» зображення персонажа Джеймс Кларксон

Фото № 3

Початкові фото:

В якості референсу для наступного етапу використовувалось попередньо згенероване зображення (дивитися рисунок Д.2.3), а також:

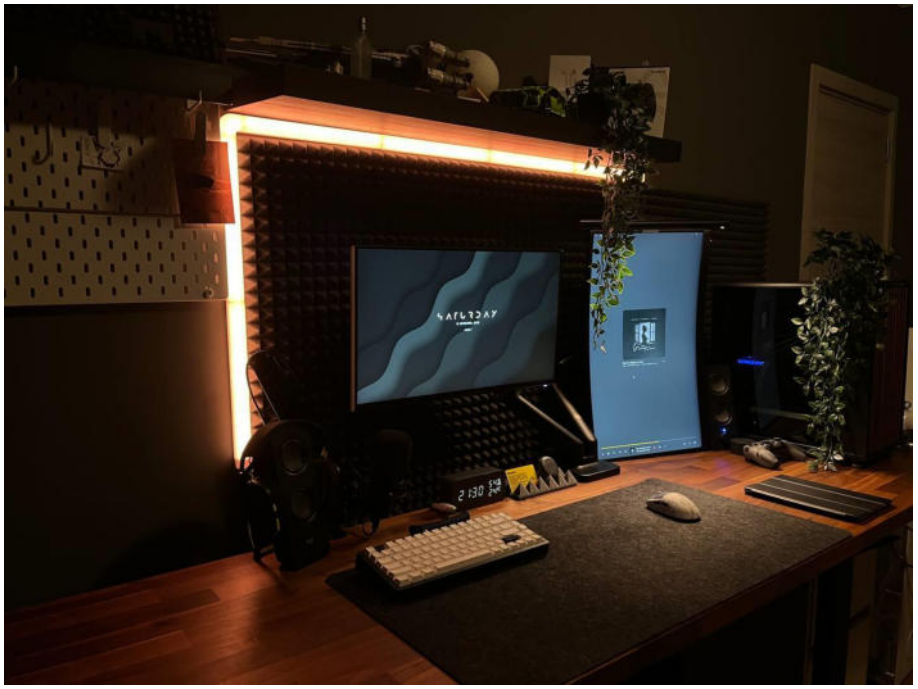

Рисунок Б.4 - Фотореференс робочого місця

Промпт:

Create a highly realistic, natural photograph of the exact same young man from the reference images, standing casually next to his desk in this gaming/workspace setup. Clothing: He is wearing a loose white oversized t-shirt and black shorts (the shorts can be partially or mostly out of frame). The outfit should look comfortable and casual, like home wear.

Pose and expression: Natural relaxed pose, standing slightly to the side of the desk, body gently angled toward the camera. He has a warm, genuine smile with teeth slightly visible, friendly and approachable expression, looking directly at the camera. Position him naturally on the left or right side of the desk so that the workspace remains clearly visible and well-composed. Make sure the lighting on the man blends perfectly with the room — warm ambient light from the LED strips, soft glow from

the monitors, and gentle overall illumination so he looks like he naturally belongs in the scene.

Maintain 100% identical facial features, hair, eye color, skin texture, and overall likeness from the reference photos.

The background must be this exact workspace: wooden desk, dual monitors (one horizontal with blue wallpaper, one vertical), white mechanical keyboard, mouse, headphones, acoustic foam panels, warm orange LED strip lighting along the shelf, hanging plants, pegboard, and all other details exactly as shown.

Significantly enhance the overall image quality: sharper details, better dynamic range, richer but natural colors, improved lighting balance, and cinematic atmosphere while preserving the cozy, dimly lit evening vibe of the room.

Ultra-photorealistic quality, 8K resolution, studio-grade sharpness, natural skin texture with visible pores, realistic hair strands, depth of field with the man in sharp focus. Professional photography style, natural composition.

Exact same room and desk setup, only add the young man in white oversized t-shirt, naturally standing beside the desk with a warm smile. Nothing else added or changed.

Сгенероване фото (без водяного знаку):

Рисунок Б.5 - Згенероване зображення персонажа Джеймс Кларксон біля робочого місця

Фото № 4

Початкове фото:

В якості референсу для наступного етапу використовувалось попередньо згенероване зображення (дивитися рисунок Д.2.3), а також:

Рисунок Б.6 - Mitsubishi Lancer Evolution 6

Рисунок Б.7 - Фотореференс фону з припаркованим автомобілем і роміщення людини у відношенні до автомобіля. На фотореференсі зображений Джеймс Мей - відомий телеведучий програм про автомобілі

Промпт:

A hyper-realistic, cinematic automotive editorial photograph.

The Subject: A dark-haired man standing confidently next to the car. CRITICAL: He must have the EXACT 100% facial likeness, eye shape, olive skin tone, jawline, and subtle facial hair of the provided reference man. His medium-length dark hair is naturally styled. He has a highly athletic, muscular physique. He is wearing a casual white t-shirt and dark cargo pants. His face is clearly visible, looking naturally toward the camera.

The Car: Parked on the dirt road is a silver Mitsubishi Lancer Evolution VI. The car features its iconic large rear spoiler, front bumper vents, and white alloy wheels. The metallic silver paint reflects the surrounding nature.

The Environment & Lighting: The scene is a dirt road shaded by large trees. CRITICAL LIGHTING: Strong, irregular dappled sunlight and cast shadows from the tree leaves must fall naturally across BOTH the man's face/body and the metallic surface of the Mitsubishi. This lighting grounds them perfectly into the scene.

Camera Details: Shot on 35mm lens, perfect depth of field, 8K resolution, photorealistic, ultra-detailed skin pores and fabric texture. Seamless integration with the original background

Сгенероване фото (без водяного знаку):

Рисунок Б.8 - Згенероване зображення персонажа Джеймс Кларксон біля автівки