Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту
інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 Кібербезпека
(код і назва спеціальності)
освітній ступень бакалавр
освітня програма Кібербезпека
(назва освітньо-професійної програми)
на тему: Метод виявлення прихованої інформації на основі технології OSINT

Виконавець: студент IV курсу, групи КБ-41
_____ **Артур ШИШКАНОВ**
(підпис) (ім'я, прізвище)

	Ім'я, прізвище	**Підпис**
Керівник	Олександр ЛАПТЄВ	

Нормоконтроль	Олександр ТОРОШАНКО	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студента **КБ-41** **Шишканова Артура Геннадійовича**
(група) (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Метод виявлення прихованої інформації на основі технології OSINT

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Інтернет-застосунок Tinfoleak для сканування відкритих даних з Twitter акаунтів, застосунок Recon-ng в середовищі Linux для веб-розвідки у відкритих джерелах, програмне забезпечення Maltego для розвідки з відкритим вихідним кодом.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Дослідження методів виявлення прихованої інформації з використанням OSINT, аналіз існуючих методик та інструментів збору та обробки відкритої інформації, їх практичне втілення для виявлення різноманітних видів прихованих даних.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Оцінка методик застосування технологій OSINT, виявлення найефективніших підходів для виявлення інформації

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

Завдання видав _____ Олександр ЛАПТЄВ
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Артур ШИШКАНОВ
(підпис) (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 22.01.2023	*виконано*
2	Аналіз літератури	29.01.2023 – 20.02.2023	*виконано*
3	Дослідження методів пошуку прихованої інформації за допомогою технологій OSINT	24.02.2023 – 04.03.2023	*виконано*
4	Дослідження характеристик тексту та доцільності їх використання	05.03.2023 – 24.03.2023	*виконано*
5	Вивчення методик, пошук текстових джерел	25.03.2023 – 07.04.2023	*виконано*
6	Вибір OSINT-застосунків для розгляду	07.04.2023 – 16.04.2023	*виконано*
7	Проведення практичних досліджень роботи обраних програм	16.04.2023 – 20.04.2023	*виконано*
8	Формування висновків	20.04.2023 – 10.05.2023	*виконано*
9	Оформлення пояснювальної записки	11.05.2023 – 27.05.2023	*виконано*

Завдання видав _____ Олександр ЛАПТЄВ
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Артур ШИШКАНОВ
(підпис) (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 86 сторінок основного тексту, 52 рисунки та 4 таблиці. Список використаних джерел містить 31 найменувань і займає 3 сторінки.

Методи дослідження кваліфікаційної роботи:

- аналіз літератури;
- аналіз документів;
- порівняння.

Об’єктом дослідження в даній роботі є процес виявлення прихованої інформації.

Предметом дослідження в даній роботі є методи, засоби і методики використання OSINT-технологій.

Розглянуті в роботі OSINT-застосунки можна використовувати для пошуку та моніторингу соціальних мереж, аналізу веб-сайтів та форумів, моніторингу новин та медіа, аналізу географічних даних, візуалізації та відображення зв’язків та показників.

ЗМІСТ

ВСТУП

Актуальність даної роботи визначається тією обставиною, що OSINT-технології є одними з найпотужніших інструментів для виявлення прихованої інформації, оскільки вони поєднують доступність, широкий спектр охоплення джерел, аналіз великого обсягу даних, контекстуальний аналіз, широкий спектр застосувань та економію часу і ресурсів.

У сучасному цифровому суспільстві, де доступ до величезної кількості інформації є миттєвим і широко поширеним, проблема виявлення прихованої інформації набуває все більшої актуальності і значущості. Зростаюча кількість загроз безпеці, шпигунської діяльності, дезінформації та кіберзлочинності ставить перед суспільством завдання ефективної інформаційної розвідки та аналізу.

В цьому контексті методи виявлення прихованої інформації на основі технології OSINT (Open Source Intelligence) набувають особливого значення. OSINT є процесом збирання, аналізу та використання інформації, яка доступна відкритим шляхом, таких як соціальні мережі, публічні бази даних, веб-сайти, форуми та інші джерела.

Метою роботи є підвищення ефективності методів виявлення прихованої інформації з використанням технології OSINT. Робота спрямована на аналіз існуючих методик та інструментів збору та обробки відкритої інформації, а також їх практичне втілення для виявлення різноманітних видів прихованої інформації.

Для досягнення поставленої мети необхідно вирішити такі *завдання*:

- Розглянути основні особливості OSINT-технологій та їх використання
- Дослідити існуючі методології та на їх базі окреслити, що необхідно для грамотного використання OSINT-технологій для нашої мети
- Практично розглянути існуючі OSINT-застосунки, механіку їх роботи, інформацію, яку вони можуть надати, порівняти їх особливості

Об’єктом дослідження є процес виявлення прихованої інформації.

Предметом дослідження є методи, використання OSINT-технологій.

Методи дослідження кваліфікаційної роботи бакалавра:

- аналіз літератури та аналіз документів;
- вивчення та узагальнення вітчизняної і зарубіжної практики.

РОЗДІЛ 1. ОСНОВНА ІНФОРМАЦІЯ ПРО OSINT-ТЕХНОЛОГІЇ ТА ЇХ ВИКОРИСТАННЯ

Сьогодні ми стаємо свідками безпрецедентного явища, коли мільярди користувачів по всьому світу активно діляться, спілкуються та обмінюються цифровими даними. Такий спалах доступності даних призвів до появи «інформаційної ери», яка характеризується великою кількістю загальнодоступної інформації. Однак, разом зі своєю трансформаційною силою, інформаційна ера також породжує нові виклики. Досягнення цієї епохи спричинили різноманітні ризики, зокрема злочинність, тероризм та іншу зловмисну діяльність, що зумовило необхідність розробки контрзаходів військовими організаціями, службами безпеки та правоохоронними органами.

Існує поширена помилкова думка про те, що розвідувальна інформація, яка використовується для боротьби зі злочинністю, походить зі здебільшого закритих джерел. Насправді загадані вище організації все більше інвестують у відкритий інтелект (OSINT), використовуючи Інтернет як основне джерело інформації для розробки нових методів. OSINT охоплює всю інформацію та знання, зібрані з загальнодоступних джерел, становлячись визначною силою в зборі розвідданих. Протягом історії суспільства визнавали цінність доступної інформації для отримання кращих висновків, незалежно від того, чи це стосується розкриття злочинів, перемоги в битвах або досягнення успіху в бізнесі.

Що змінилося з часом, так це кількість доступних громадськості даних і методи, які використовуються для їх збору. У той час як традиційний OSINT покладався на такі джерела, як газети, публічні виступи та інтерв'ю, дані сьогодення здебільшого зберігаються в Інтернеті, а методології їх отримання стали більш складними, технологічно просунутими та доступними для всіх.

Використання OSINT розповсюджується серед різноманітних груп користувачів, включаючи міжнародні організації та корпоративні підприємства. Це зростання OSINT можна пояснити кількома ключовими факторами:

- Інтернет став глобальною платформою для спільного використання та обміну інформацією у всесвітньому масштабі.

- Експоненційне зростання цінної інформації, доступної в Інтернеті, забезпечило доступ до раніше недоступних областей.
- Ландшафт загроз громадській безпеці, що розвивається, змістився в бік нетрадиційних цифрових ризиків.

OSINT стала розвиваючою сферою в галузі безпеки та за її межами, що робить її надзвичайно актуальною областю досліджень. Майбутні прогнози вказують на подальше зростання популярності OSINT, при цьому оцінки свідчать про те, що 80% розвідданих уже надходить із відкритих джерел. Отже, слід приділяти більшу увагу визначенню найкращих джерел даних і найефективніших методів розуміння та отримання з цієї інформації корисних даних.

Таким чином, ця дипломна робота спрямована на демонстрацію та оцінку трьох інструментів OSINT, проливаючи світло на їх придатність для цієї мети. Мета полягає в тому, щоб забезпечити всебічне розуміння можливостей і обмежень сучасних OSINT-рішень, вважаючи це значним внеском у цю сферу.

1.1 Визначення Open Source Intelligence

Термін Open Source Intelligence (інформація з відкритих джерел) бере свій початок у військових, правоохоронних та секторах безпеки. Було надано різні описи та визначення, щоб пояснити розвідку з відкритим кодом, але вони, як правило, є широкими та позбавленими конкретики. Деякі розглядають OSINT як “процес” збору та обробки інформації з загальнодоступних джерел, тоді як інші більше зосереджуються на “результаті” збору та аналізу даних, яким є фактична розвідувальна інформація, отримана в результаті цієї діяльності. Визначення OSINT пропонують як науковці, так і різні організації, які використовують інформацію з відкритих джерел. Наприклад, Hassan & Hijazi наводять приклад, заснований на визначенні OSINT Міністерством оборони США:

“Open-source intelligence (OSINT) refers to intelligence that is derived from publicly available information, collected, exploited, and disseminated promptly to an appropriate audience to address a specific intelligence requirement.”

(“Open source intelligence (OSINT) — це розвідувальні дані, отримані на основі загальнодоступної інформації, зібрані, використані та негайно

розповсюджені серед відповідної аудиторії для задоволення певної вимоги до розвідувальних даних”).

Що залишається незмінним у всіх визначеннях OSINT, так це очікування, що воно генерує цінну інформацію та знання, пов’язані з предметом, і що інформація надходить із загальнодоступних каналів, а не із закритих чи секретних джерел.

Зазвичай розвідку з відкритим кодом і рух із відкритим кодом у розробці програмного забезпечення не змішують і вважають окремими областями. Ця відмінність зберігається і в цій роботі. Однак відомо, що деякі OSINT-рішення розробляються як проекти програмного забезпечення з відкритим кодом, дотримуючись відповідних принципів.

1.2 Джерела OSINT

Джерела розвідувальних даних можна розділити на три основні типи (Рисунок 1.1):

- Signal intelligence (SIGINT): Це відноситься до розвідувальної інформації, отриманої в результаті перехоплення сигналів, прослуховування та подібних методів.
- Human intelligence (HUMINT): Цей тип інформації отримується з конфіденційних джерел, які надають інформацію.
- Open source intelligence (OSINT): Ця категорія охоплює дані, зібрані з загальнодоступних джерел інформації.

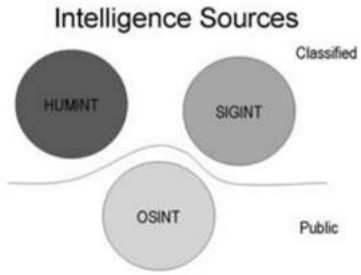


Рисунок 1.1 – Джерела інформації

Серед трьох згаданих розвідувальних джерел OSINT – єдине, яке спирається на загальнодоступну інформацію. Джерела та методи, які

використовуються для збору розвідданих SIGINT або HUMINT, часто є конфіденційними. За останнє десятиліття відбулося значне зростання у сфері OSINT, і вважається, що завдяки більш ефективному використанню OSINT можна зменшити залежність від інших джерел розвідки, зосередившись лише на питаннях, на які неможливо відповісти за допомогою відкритих джерел.

Відповідно до Посібника НАТО з відкритих джерел розвідки, відкриту інформацію та розвідку можна розділити на чотири групи:

Дані з відкритих джерел (OSD): це стосується необроблених даних, отриманих безпосередньо з первинних джерел, таких як фотографії, супутникові зображення або особисті листи.

Open Source Information (Інформація з відкритих джерел) (OSINF): OSINF складається з даних, які пройшли певний рівень фільтрації, що робить їх вторинним джерелом. Приклади включають газети, книги та щоденні звіти. OSINF також може включати комерційні послуги підписки та комерційні супутникові зображення. Такі популярні пошукові системи, як Google, зазвичай використовуються для збору OSINF, а спеціальні веб-сканери розроблені для моніторингу конкретних веб-сайтів і отримання оновлень. Багато блогів пропонують канали RSS, що робить їх доступними для моніторингу.

Open Source Intelligence (OSINT): OSINT стоїть окремо від попередніх двох категорій, оскільки представляє результат циклу розвідки та може безпосередньо відповідати на конкретні запитання. Це результат виявлення, фільтрації та обробки матеріалів з відкритим кодом, що робить його готовим до використання в контексті розвідки.

Validated OSINT (Перевірений OSINT) (OSINT-V): OSINT-V йде ще далі, перевіряючи та підтверджуючи результати циклу розвідки за допомогою додаткових джерел, які можуть включати джерела, що не є OSINT. Така перевірка має вирішальне значення для забезпечення надійності відкритих джерел, які використовуються в процесі розвідки. Це може бути досягнуто шляхом підтвердження висновків із конфіденційних джерел розвідки або шляхом ідентифікації кількох екземплярів тих самих загальнодоступних даних (наприклад, ідентичні зображення, знайдені в Інтернеті).

Важливо зауважити, що хоча OSINT базується на даних з відкритих джерел, Інтернет також може містити секретну або неавторизовану інформацію, відому як NOSINT. Така інформація, яку називають сірою літературою, входить до OSINT-джерел, незважаючи на її легальний доступ. Однак для використання цієї інформації в процесі розвідки потрібен дозвіл.

Інформація з відкритих джерел охоплює різні категорії, включно з традиційними медіа-ресурсами (телебачення, радіо, газети, книги, журнали), комерційними преміум-джерелами в Інтернеті, нішевими комерційними онлайн-джерелами, Інтернетом і Всесвітньою павутиною (форуми, блоги, сайти соціальних мереж, відео - платформи обміну, як-от YouTube, вікі, записи Whois, метадані та цифрові файли, ресурси темної мережі, IP-адреси, системи пошуку людей), сіра література, явні експерти-люди, комерційні зображення та геопросторова інформація (включно з метаданими).

Хоча надати вичерпний список усіх можливих джерел OSINT сьогодні є складним завданням, OSINT Framework пропонує доволі детальний огляд (Рисунок 1.2)

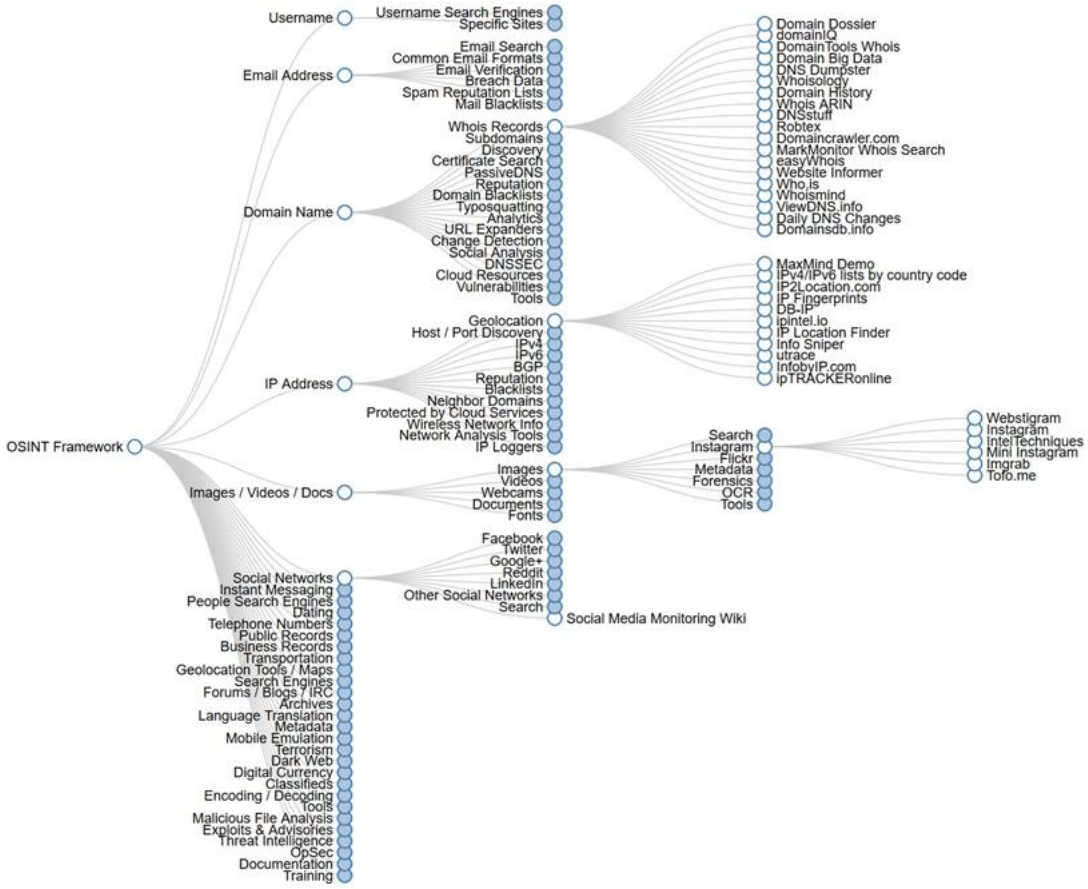


Рисунок 1.2 – Зображення можливих джерел OSINT інформації

Оскільки доступність даних продовжує розширюватися, компанії все більше покладаються на OSINT для збору ринкової інформації. На додаток до джерел, згаданих раніше, компанії також використовують свої внутрішні основні дані для цілей OSINT. Це стосується внутрішніх баз даних, систем (таких як ERP і CRM) і документів, таких як протоколи нарад, бізнес-плани та звіти. Поєднання цих внутрішніх даних із зовнішніми джерелами підвищує цінність аналізу.

Хоча онлайн-джерела становлять найбільший сегмент OSINT, важливо зазначити, що OSINT-джерела не обмежуються лише онлайн-платформами. Однак оцифрування інформації в сучасну інформаційну епоху в поєднанні з культурою обміну інформацією між користувачами Інтернету, призвело до того, що значна частина OSINT-джерел доступна онлайн. Платформи соціальних мереж, зокрема, зазнали значного збільшення кількості користувачів, що сприяло зростанню кількості доступних даних.

Розширення Інтернету речей (IoT) ще більше збільшує обсяг даних в OSINT. Завдяки пристроям і датчикам IoT, які генерують і передають дані через Інтернет, за оцінками, до 2024 року буде використовуватися 22,4 мільярда пристроїв IoT. Ця тенденція призвела до переміщення багатьох джерел OSINT у бік онлайн-платформ.

Загалом існують три типи методів збору інформації: пасивні, напівпасивні та активні.

Пасивний збір є найбільш часто використовуваним методом в OSINT. Він покладається виключно на відкриті джерела інформації, і ціль, за якою спостерігають, не знає про діяльність зі збору розвідданих, оскільки пошуки проводяться анонімно з технічної точки зору. Технічні методи, які використовуються для пасивного збору, не надсилають трафік або пакети на цільові сервери, що може призвести до обмеження інформації про ціль.

Напівпасивні методи збору передбачають надсилання деякого обмеженого трафіку до цілі для збору інформації, намагаючись нагадувати типовий інтернет-трафік, щоб уникнути зайвої уваги, хоча вони не є повністю непомітними. *Активне збирання*, з іншого боку, передбачає прямий контакт із системою, від якої шукають розвідувальну інформацію, з використанням передових методів збору технічних даних. Однак напівпасивні та активні методи збору зазвичай не

використовуються в OSINT, оскільки вони вважаються такими, що порушують суть розвідки відкритих джерел.

Збір даних OSINT може варіюватися від невеликих цільових запитів до великомасштабних операцій, які потребують значних ресурсів і можливостей, як правило, виконуються більшими організаціями, такими як ЦРУ.

Ключовим аспектом OSINT є розуміння різниці між даними, інформацією та знаннями. Дані представляють набір фактів (наприклад, ціна за кілограм картоплі становить 5 доларів США), інформація передбачає належне тлумачення даних у певному контексті (наприклад, ціна на картоплю зросла з 5 до 7 доларів США за кілограм), а знання охоплюють поєднання інформації, розуміння та досвіду, які можна застосувати в подібних контекстах (наприклад, коли ціна на картоплю зростає, ціна на м’ясо також зростатиме).

1.3 Хто використовує OSINT

Інформація з відкритих джерел (OSINT) зазвичай асоціюється з військовою розвідкою та організаціями, але база її користувачів виходить далеко за межі цього. Великі транснаціональні компанії, банки та різні індустрії все більше покладаються на OSINT для збору інформації та бізнес-аналітики для прийняття рішень, отримання конкурентної переваги та захисту свого бізнесу.

Основні групи користувачів OSINT можна класифікувати наступним чином:

- Державні органи, в тому числі військові, служби безпеки та правоохоронні органи.
- Міжнародні організації.
- Бізнес-корпорації.
- Тестери проникнення та хакери.
- Злочинні організації та терористичні групи.
- Особи, які піклуються про конфіденційність.

Серед цих груп державні органи вважаються найбільшими споживачами OSINT. Вони використовують OSINT для національної безпеки, боротьби з тероризмом, запобігання злочинності, профілювання злочинців та аналізу

внутрішніх і зовнішніх перспектив і подій. OSINT також підтримує процеси формування політики, надаючи додаткову інформацію.

Державні органи відрізняються від інших груп користувачів здатністю поєднувати OSINT з конфіденційною розвідувальною інформацією, зібраною іншими способами. Вони часто мають більше можливостей і ресурсів для збору й аналізу даних порівняно з іншими групами, і очікується, що ця тенденція продовжуватиметься із збільшенням уваги та ресурсів, виділених на OSINT. Урядові організації вважаються цінними джерелами OSINT завдяки їхнім можливостям і досвіду в проведенні змістовного аналізу.

Міжнародні організації покладаються на OSINT, щоб отримати неупереджену та прозору точку зору з питань, що їх цікавить, а не покладатися виключно на звіти могутніх держав або інших потенційно упереджених джерел. Організація Об'єднаних Націй (ООН) є прикладом міжнародної організації, яка використовує OSINT для підтримки миротворчих операцій по всьому світу.

Бізнес-корпорації також визнали силу OSINT і все більше використовують її. Розвиток OSINT серед бізнесу можна пояснити Інтернетом, який зробив доступними величезні обсяги інформації, вирівнюючи умови гри для малих підприємств, які раніше не мали ресурсів для участі в діяльності OSINT.

Компанії використовують OSINT для дослідження ринку, моніторингу конкурентів, оцінки робочого середовища та визначення тенденцій і змін. OSINT також цінний для виявлення витоку даних, моніторингу поведінки мережі та захисту від кіберзагроз. Багато приватних корпорацій розробили передові програми та методи збору даних із відкритих джерел для комерційної вигоди.

Тестери проникнення та хакери з чорним капелюхом використовують OSINT цілеспрямовано. Їх метою часто є збір інформації про конкретні цілі в Інтернеті для підготовки до тестування на проникнення або атак соціальної інженерії.

На жаль, злочинні організації та терористичні групи також використовують джерела OSINT для планування атак, збору інформації про цілі, вербування нових членів за допомогою аналізу соціальних мереж, збору військової інформації, розкритої урядами, та розробки ефективних каналів для поширення своєї пропаганди.

Люди, які піклуються про конфіденційність, все частіше звертаються до OSINT, щоб контролювати свою цифрову ідентифікацію та захистити свою конфіденційність. Вони використовують OSINT-інструменти, щоб бути в курсі свого онлайн-виявлення та безпеки своїх особистих даних.

Типовий цикл OSINT-збирання починається з визначення потреби в додатковому розумінні, після чого йде планування діяльності та визначення потенційних джерел інформації. Далі процес включає пошук інформації, вилучення, аналіз тенденцій, аналіз посилань, візуалізацію даних і співпрацю. Кваліфіковані аналітики відіграють вирішальну роль у отриманні значущих ідей із зібраної інформації, оскільки пошук, організація та диференціація інформації вважаються критично важливими навичками в OSINT. Зростання попиту призвело до збільшення кількості постачальників OSINT-послуг у комерційному секторі, які пропонують інструменти та досвід у цій галузі.

1.4 Переваги та проблеми OSINT

В епоху великої кількості інформації вкрай важливо визнати та визнати значні переваги та потенційні перешкоди розвідки з відкритими джерелами (OSINT). Як і будь-яка інша розвідувальна дисципліна, OSINT охоплює як позитивні, так і негативні аспекти. Переваги та виклики, пов’язані з OSINT, загалом схожі, але вони мають різні перспективи. Наприклад, величезна кількість доступних даних є основою переваг OSINT, оскільки вся концепція базується на цій кількості. Однак цей самий обсяг даних створює проблему для OSINT, оскільки величезна кількість інформації створює значні труднощі в її просіюванні, щоб знайти значущі ідеї, навіть для професіоналів.

Враховуючи, що переваги OSINT є багатогранними, наведена нижче стисла колекція елементів OSINT, представлена в таблиці 1, висвітлює позитивні аспекти, які вона забезпечує, а також визнає проблеми, які супроводжують ці елементи.

Таблиця 1.1

Переваги та проблеми OSINT

Переваги OSINT	**Проблеми OSINT**
Обсяг даних	
Обсяг доступних даних перетворюється у світі OSINT на здатність бачити, чути, знати, розуміти, приймати рішення та діяти на основі «всієї інформації, усіх мов, постійно.	Величезний обсяг лякає, а виділення значущої інформації вимагає справжніх зусиль, щоб вважатися цінним інтелектом
Доступність даних для мас	
Джерела OSINT завжди доступні, доступні та актуальні, і можуть бути використані різними сторонами для отримання висновків. Інформація завжди прозора, завжди відкритий доступ, завжди легкодоступна та розглядається більше як ресурс спільноти, ніж окремий товар. Відкриті джерела інформації не є виключною сферою розвідувальних служб.	Використання терміну «загальнодоступний» є оманливим і відкритим для тлумачення, оскільки різні групи користувачів не мають однакового дозволу на всі дані (наприклад, військові чи бізнес). Багато служб даних і баз даних відкриті лише для платних клієнтів і для обмежених користувачів і недоступні для широкої громадськості. Можна також поставити під сумнів, чи є «чесною грою» збирати особисті дані з платформи, де користувачі ділилися своїми даними за «паролем» — захистом від Інтернету. Практично неможливо підтримувати життєздатну колекцію відкритих вихідних матеріалів, які миттєво задовольняють усі інформаційні потреби

продовження табл. 1.1

Надійність	
OSINT має одну перевагу перед іншими джерелами: його вплив на мільйони пар очних яблук. Як прийнято розуміти у світі програмного забезпечення з відкритим кодом, придивіться до нього достатньо, і жодна помилка не буде невидимою. OSINT також пропонує аналітичні системи відліку, які витримали перевірку часом. Це відрізняє OSINT від інших джерел розвідки	OSINT-джерела, особливо коли вони використовуються в контексті розвідки, мають бути ретельно перевірені секретними джерелами, перш ніж їм можна довіряти Джерелами OSINT також можна маніпулювати для трансляції недостовірної інформації, що вводить в оману результати OSINT Сторінки та сайти часто мають короткий термін служби, вміст може постійно змінюватися, і організаціям може бути важко встигати за змінами
Ціна	
Збір даних OSINT, як правило, дешевший порівняно з іншими джерелами розвідки. Наприклад, використання людських джерел або шпигунських супутників для збору даних коштує дорого. Малі підприємства з обмеженим бюджетом на розвідку можуть використовувати джерела OSINT з мінімальними витратами Продукти OSINT можуть зменшити вимоги до секретних ресурсів збору розвідданих, обмежуючи запити на інформацію лише тими питаннями, на які не можна відповісти з відкритих джерел	Людям потрібно переглядати результати автоматизованих інструментів, щоб знати, чи надійні та надійні зібрані дані; їм також потрібно порівняти його з деякими секретними даними (це стосується деякої військової та комерційної інформації), щоб переконатися в його надійності та актуальності. Це фактично поглине час і дорогоцінні людські ресурси. Постійні зміни в джерелах і вмісті джерел вимагають можливості архівувати цільові дані для подальшої обробки, що вимагає додатків, часу та зусиль аналітиків, а також вартості додаткових ресурсів пам’яті.

продовження табл. 1.1

Простота використання OSINT	
На відміну від інших розвідувальних джерел, які можуть вимагати використання шпигунських супутникових знімків або таємних агентів для збору інформації, усе, що вам потрібно для збору онлайн-ресурсів OSINT, це комп'ютер і підключення до Інтернету	Немає жодної пропозиції, яка б задовольнила потребу в повністю інтегрованому інструментарії аналітика OSINT. Частково це пов'язано з відсутністю згоди щодо стандартів у частині, а частково через відсутність узгодженості в державних і корпоративних контрактах, де наголос робився на апаратному забезпеченні та пропрієтарному програмному забезпеченні замість загальної функціональності та простоті інтеграції даних. Не всі дані в Інтернеті індексуються, і аналітики даних повинні мати можливість глибоко занурюватися в «невидиму мережу», знаючи, як отримати доступ до необхідної інформації.
Легальна та етична сторона	
Ресурсами OSINT можна ділитися між різними сторонами, не турбуючись про порушення ліцензії на авторське право, оскільки ці ресурси вже опубліковані для всіх.	OSINT має свої юридичні проблеми, наприклад, у випадку, коли хтось отримує джерела OSINT незаконним шляхом, щоб виправдати чесну справу, або коли зразок OSINT мінімізується або вибирається відповідно до потреб збирача, фактично відкидаючи важливі джерела навмисно на користь досягнення конкретного результату.

OSINT все ще стикається з проблемою досягнення рівного визнання поряд з іншими формами розвідки. Незалежно від того, надається йому заслужена серйозність чи ні, OSINT підтримує взаємні стосунки з іншими розвідувальними дисциплінами, слугуючи для них міцною основою. Він пропонує альтернативний спосіб перевірки результатів, отриманих іншими методами. Подібним чином інші розвідувальні дисципліни також перевіряють висновки, отримані за допомогою відкритих джерел. Мова відіграє вирішальну роль в OSINT. Щоб ефективно використовувати глобальні дані з різних джерел різними мовами, необхідні можливості перекладу. Переклади також мають відповідати певним стандартам якості, щоб полегшити отримання значущих висновків. Таке середовище підкреслює важливість навичок перекладу та розуміння культурних нюансів.

1.5 Майбутнє OSINT

Незважаючи на те, що розвідка з відкритим кодом (OSINT) є усталеним підходом, за останні роки вона зазнала значних змін через такі чинники, як розвиток Інтернету, велика кількість цифрових джерел даних, а також прогрес у технології та техніці. OSINT все ще знаходиться на ранніх стадіях і продовжує розвиватися. Прогрес, досягнутий на цей час, свідчить про те, що OSINT поступово утверджується як окреме явище, переходячи від окремої практики до практики, яка існує сама по собі.

Оскільки OSINT є відносно молодою як окрема дисципліна, вона стикається з кількома проблемами. По-перше, це проблема масштабу. OSINT-проекти все ще набагато менші порівняно з традиційними медіа, і для багатьох проектів може бути складно досягти зростання. По-друге, є економічна проблема. Більшість OSINT-проектів базується на зусиллях волонтерів і пожертвуваних ресурсів. Однак залучення коштів може бути складним в Інтернет-економіці, особливо коли проекти розширюються та потребують більшої інфраструктури та пропускної здатності. Пошук альтернативних шляхів фінансування OSINT-проектів стає вирішальним, оскільки вони діють поза традиційними економічними моделями виробництва та публікації. Цілком ймовірно, що OSINT-проекти досліджуватимуть моделі, що включають прямі доходи (наприклад,

підписки, рекламу), доброзичливі пожертви та зусилля волонтерів. Незважаючи на ці виклики, є сильні прихильники, які вірять у майбутнє OSINT. Обробляти величезні масиви даних і вивчати їх стало основним напрямком, а інструменти та методи OSINT отримують все більш широке визнання, з меншими бар'єрами для входу.

Очікується, що військовий сектор все більше використовуватиме OSINT. Збройні сили не можуть ігнорувати велику кількість інформації, доступної в Інтернеті, і продовжуватимуть підтримувати доступність таких джерел. OSINT також вважається важливим компонентом майбутнього бачення НАТО і цінується за його здатність розробляти та обмінюватися розвідданими на основі відкритої, несекретної інформації між державами-членами та міжнародними операціями. Покладаючись на OSINT, немає ризику розкриття конфіденційних методологій збору розвідувальних даних. OSINT також продовжуватиме відігравати вирішальну роль у підтримці виробництва секретної інформації. Було визнано, що «Інтернет тепер є стандартною архітектурою командування та контролю, зв'язку, обчислення та інтелекту (C4I) практично для всього світу».

У той час як військові організації, такі як НАТО, визнають важливість використання відкритих джерел, OSINT розвиває власне незалежне існування поза урядовими сферами, як заявив Стіл. Отже, багатообіцяюче майбутнє OSINT поширюється і на бізнес. Флейшер прогнозує, що зростання OSINT створить нові можливості на ринку для постачальників послуг OSINT. Сталдер і Гірш також передбачають зростання OSINT-технологій, розглядаючи їх як важливий елемент підтримки когнітивного навчання людини в майбутньому. Вони передбачають, що технологічна культура все більше зливається з культурою навчання.

Зважаючи на це, фокус, здається, зміщується в бік використання доступних технологій для отримання інформації з відкритих джерел. Стіл пропонує перейти від простого збереження колекції матеріалів з відкритими джерелами до створення життєздатної колекції OSINT-джерел — визначення найкращих джерел для відповідей на конкретні запитання та використання відповідних інструментів для оптимальних методів пошуку.

Постійно зростаючий обсяг даних вимагає передових програмних інструментів для керування величезною кількістю інформації. Однак діяльність із

розробки OSINT-сфери є розпорошеною через її зароджуючий характер, що включає численні незалежні проекти. Крім того, зростає кількість розробників і маркетологів у комерційному секторі. Існують також нові ініціативи, такі як Форум EUROSINT, заснований у 2016 році для координації діяльності з розробки OSINT на рівні ЄС між державними установами та бізнесом. Дослідницьке співтовариство також приділяє більше уваги розробці інструментів і методів для підтримки процесу OSINT. Бест прогнозує, що майбутні тенденції досліджень будуть зосереджені на техніках візуалізації зведень текстової інформації, забезпечуючи покращене розуміння з відкритих вихідних даних.

Виходячи з вищезазначених подій, можна передбачити, що сфера розвідки з відкритим кодом продовжить розвиватися, що призведе до більш точних визначень, встановлених правил, передових методів і більшої бази користувачів. Цитуючи CIA, «організація, яка сьогодні інвестує у відкритий код, схожа на людину, яка інвестувала в Google у перший рік існування. Організація, яка цінує цінність і потенціал OSINT, буде найефективнішою в майбутньому».

Висновки до розділу 1

У цьому розділі ми детально розглянули основну інформацію про OSINT-технології та їх використання. OSINT, або відкрите джерело інформації, є потужним інструментом для збору, аналізу та використання відкритої інформації з різних джерел.

Ми розглянули основні принципи, на яких ґрунтується OSINT, включаючи відкритий доступ до інформації, використання веб-джерел, соціальних мереж, публічних баз даних та інших джерел. Також було розглянуто різноманітні методи та інструменти, які можна використовувати для збору та аналізу інформації, включаючи пошукові системи, соціальний інжиніринг, аналіз відкритих джерел та інше.

Ми висвітлили значення OSINT-технологій для різних сфер, включаючи безпеку, розвідку, розслідування, бізнес-аналітику та громадську безпеку. Використання OSINT дозволяє здійснювати ефективні інформаційні дослідження, отримувати значну кількість даних та аналізувати їх для прийняття обґрунтованих рішень.

Основна перевага OSINT-технологій полягає в доступності та широкому спектрі інформації, яку можна отримати з відкритих джерел. Вони допомагають збирати дані з різних джерел, знаходити зв'язки та шаблони, розуміти тренди та події, що відбуваються у реальному часі.

Проте, слід зазначити, що використання OSINT-технологій повинно відбуватися в рамках законодавства та етичних принципів. Дотримання приватності та захисту персональних даних є важливими аспектами при зборі та використанні відкритої інформації.

Загалом, OSINT-технології відіграють важливу роль у сучасному інформаційному світі. Вони надають можливість отримувати цінну інформацію для прийняття обґрунтованих рішень та розв'язання складних завдань. Розуміння основних принципів та використання методів OSINT може стати суттєвим фактором успіху в різних сферах діяльності.

РОЗДІЛ 2. МЕТОДОЛОГІЯ OSINT

Щоб забезпечити ретельну і ефективну роботу, вкрай важливо мати добре структурований і цілеспрямований підхід. Це особливо стосується розслідувань відкритих джерел (OSINT). Надійний процес повинен гарантувати, що слідчі виконують усі необхідні кроки та підтримують належний ланцюжок контролю. Щоб налагодити якісний процес, основою є методологія. Методологія окреслює етапи, які необхідно переглянути, і визначає, що має бути включено до кожного етапу, надаючи вказівки протягом усього розслідування.

Методологія стосується вивчення методів у межах певної дисципліни, тоді як метод — це системний підхід до вирішення проблеми або виконання завдання. Інструмент, з іншого боку, - це техніка або допомога, яка допомагає у виконанні завдання. Методологія охоплює комплексний підхід, який може включати кілька методів, технік та інструментів (Bjerknes & Fasing, 2018).

Метою методології є визначення структурованого розслідування, яке залишається криміналістично обґрунтованим. Розслідування вважається криміналістично обґрунтованим, якщо воно дотримується встановлених принципів, стандартів і процесів цифрового розслідування (Flaglien, 2018). Методологія дослідження цифрових доказів має ґрунтуватися на принципах цифрової криміналістики, а також на загальноприйнятих практиках, яких дотримуються правоохоронні органи та галузь.

Інформація, отримана з відкритих джерел, може слугувати основою як для звичайних розслідувань, так і для розслідувань спецслужбами. Якщо інформація використовується для проведення розслідувань, вона не обов’язково може бути представлена як доказ у суді. Проте вкрай важливо проводити записи аудитів, щоб гарантувати, що особи, які приймають рішення, можуть покладатися на точність інформації, на якій базуються їхні рішення. Коли інформація призначена як доказ для звинувачення, важливо зберегти її автентичність і цілісність, не залишаючи жодних сумнівів щодо її цінності.

Надійна методологія також допомагає уникнути юридичних проблем під час процесу збору інформації. Крім того, це зосереджує увагу дослідників і

забезпечує дотримання основних гіпотез і вимог до інформації Open Source Intelligence. Надійна методологія, заснована на принципах і стандартах дослідження цифрових доказів, гарантує, що докази будуть законно захищені та перевірені відповідно до найкращих практик. Це допомагає з'ясувати його походження, визначити, чи було воно підроблено, і запобігти оманливій інформації, яка може скерувати розслідування в неправильному напрямку або кинути підозру на невинну особу.

Методологія повинна окреслювати мету завдання, процес, різні етапи, використовувані методи та інструменти, а також спосіб представлення та розподілу результатів. Кілька моделей представляють систематичні процеси для роботи з цифровими доказами. Такі стандарти, як ISO/IEC 27037 і NIST SP 800-86, містять вказівки щодо дослідження цифрових доказів (Dilijonaite, 2018). Крім того, існують опубліковані рекомендації, які містять поради щодо поводження з цифровими доказами. І стандарти, і настанови мають рекомендаційний характер. Вони не роблять докази автоматично недійсними, якщо їх не дотримуються точно, але забезпечують криміналістичне дослідження цифрових доказів. Метою розслідування є отримання достовірних доказів для обвинувачення в суді. Керівні принципи можна розглядати як опис ланцюга зберігання, який зберігає докази таким чином, що гарантує автентичність, цілісність і надійність. Хоча стандарти та рекомендації можуть відрізнятися, вони доповнюють один одного, а не суперечать один одному. Під час роботи з розслідуванням цифрових доказів корисно використовувати кілька стандартів і рекомендацій.

Методологія отримання інформації з відкритих джерел також має відповідати принципам, що застосовуються при дослідженні цифрових доказів. Навіть якщо інформація є загальнодоступною, збереження даних має відповідати стандартам і вказівкам щодо збереження цифрових доказів, особливо якщо інформація призначена для використання як доказ у суді. Оскільки методологія Open Source Intelligence повинна охоплювати процес отримання інформації з відкритих джерел як для реактивних, так і для проактивних розслідувань, натхнення та знання слід черпати з процесу розвідки, вказівок щодо дослідження цифрових доказів і основних принципів розслідування.

2.1 Процес OSINT

2.1.1 Вимоги (Requirements)

Існує кілька моделей розвідувального кола або інформаційного кола, деякі з яких віддають перевагу напрямку як відправній точці, тоді як інші наголошують на вимогах. Незважаючи на відмінності, ці моделі мають спільну суть. Усі вони починаються з потреби в інформації, яка керує подальшим процесом. У цій структурі представлено шестифазову модель, першою фазою якої є Requirements (Вимоги).

Розслідування можна класифікувати як реактивні та проактивні. Реактивне розслідування передбачає перевірку одного або кількох кримінальних правопорушень з метою збору необхідних доказів для обвинувачення. Ці докази можуть включати ідентифікацію невідомого підозрюваного, розуміння способу дії злочину або визначення мотиву, що стоїть за ним. З іншого боку, проактивні розслідування, відбуваються, коли розвідувальні дані вказують на планування кримінального злочину або появу кримінальної тенденції, якій правоохоронні органи намагаються протидіяти. Ці розслідування мають на меті змінити хід подій і не допустити розвитку таких тенденцій. Слід зазначити, що розвідка та докази мають різні цілі. Розвідка служить для широкого кола застосувань, включаючи розслідування, рятувальні операції та управління кризовими ситуаціями, тоді як докази особливо допомагають у судових справах, щоб пролити світло на справу.

Незалежно від типу розслідування інформацію потрібно отримувати з різних джерел. На основі аналізованої поліцією інформації формуються гіпотези, які потрібно підтвердити або спростувати. Для цього потрібна релевантна інформація, а інформаційні потреби визначаються на основі гіпотези та конкретної інформації, необхідної для її підтвердження або відхилення.

Часто проблему можна сформулювати у вигляді запитання. Із запитання можна висунути одну або декілька гіпотез. *Гіпотеза* — це можливе пояснення, «ідея або пояснення чогось, що може бути істинним, але ще не повністю доведено».

Для всіх досліджень гіпотеза як пропозиція, зроблена як основа для міркувань без припущення її істинності, і припущення, зроблене як відправна точка для подальшого дослідження відомих фактів (Staniforth, 2016)

Ідея гіпотез полягає в тому, що фокус того, що потрібно дослідити, звужується і забезпечує напрямок для майбутньої роботи. Розробка гіпотез важлива для планування, управління та управління завданням. Гіпотези є орієнтиром для визначення вимог і джерел даних. Це структурує роботу та сприяє створенню спільної платформи та розуміння для всіх учасників. (POD, 2014)

Під час розслідування, реактивного чи проактивного, буде необхідно розробити альтернативні гіпотези, оскільки це пропонує більше можливостей для роз'яснення, підвищення об'єктивності та висвітлює різні шляхи розвитку. Альтернативні гіпотези мають суттєво відрізнятися від гіпотез, які передбачає робота, але водночас бути ймовірними (POD, 2014). Альтернативні гіпотези мають бути альтернативними поясненнями, які можуть бути ймовірними, якщо основна гіпотеза нежиттєздатна.

Створення та використання гіпотез є широко визнаною технікою серед слідчих, яка може бути використана для припущення найбільш логічного чи вірогідного пояснення того, як і чому було вчинено кримінальну дію. Так само його можна використовувати для припущення найбільш логічного або ймовірного пояснення того, хто виконав таку дію. (Staniforth, 2016)

На основі встановлених гіпотез досліджуються різні пояснення, пов'язані з ними. Подальша *вимога* щодо інформації допоможе перевірити або фальсифікувати ці гіпотези.

Приклад: Поліція зафіксувала неодноразові випадки, коли молоді люди підстерігали та билися групами з п'яти-десяти молодих людей. Гіпотеза може полягати в тому, що існує група молодих людей, які шукають самотніх молодих чоловіків у певній місцевості, і вони б'ють їх, щоб позначити себе як групу, юридичну особу, виділити територію тощо. Альтернативна гіпотеза може полягати в тому, що в одному районі діють дві або більше банди, які нападають на окремих членів банди, коли вони натрапляють на них, і що це означає боротьбу за територію. Потім поліція повинна шукати інформацію, щоб перевірити або фальсифікувати гіпотезу, доки вона не залишиться з найбільш

ймовірною або підтвердженою гіпотезою. Лише тоді, коли буде підтверджено, що одна з гіпотез перевірена, можна буде спрямувати ефективні відповіді на проблему.

Незалежно від того, чи має поліція визначити тенденцію для запобігання правопорушенням чи розслідувати кримінальне правопорушення, ми можемо розділити необхідну інформацію на дві частини: те, що ми знаємо, і те, що ми не знаємо. Інформація, якої ми не маємо, яка може скласти повну картину, є необхідною інформацією. Відображення та уточнення того, чого ми не знаємо, - це те, що колишній директор ФБР Роберт Мюллер називає управлінням вимогами (Мюллер, 2004).

Управління вимогами можна описати наступним чином: уточніть інформацію, необхідну для перевірки або фальсифікації гіпотези, потім віднімiть уже отриману інформацію, і залишиться інформаційна вимога.

Щоб забезпечити напрямок подальших етапів процесу, вимоги мають бути консолідовані та окреслені. Опис вимог за допомогою «все, що може підтвердити (або спростувати), що це так» стає надто абстрактним. У наведеному вище прикладі конкретні вимоги можуть бути такими: «Відображення осіб, пов’язаних з бандою А та В», «інформація про будь-які конфлікти між бандою А та В», «Інформація про конфлікти між людьми, пов’язаними з бандою А та В» та «інформація про те, чи зареєстровані особи з угруповання А і Б як потерпілі від нападів».

Ретельний аналіз інформації спочатку буде центральною частиною OSINT. Перша частина, як уже згадувалося вище, буде призначена для огляду того, що ми вже знаємо. У великих випадках ця фаза може включати структурування та аналіз інформації, якою вже володіє поліція, з поліцейських баз даних, поліцейських записів (допитів, звітів тощо) та систем поліцейської розвідки.

Визначення або уточнення терміну «інформація» не буде необхідним як частина відображення, але опис того, яка інформація потрібна для розслідування, має велике значення.

Вимоги відрізнятимуться від випадку до випадку, і вони можуть відрізнятися, чи стосуються вони *відображення* (mapping) кримінальної тенденції чи розслідування справи. У разі розслідування вимоги в основному

стосуватимуться пошуку підозрюваного, виявлення доказів, які можуть довести, що він вчинив злочин, визначення мотивів, основних причин, передачі обставин тощо. Отримання інформації з відкритих джерел матиме відношення до всі частини розслідування.

Центр досліджень безпеки (2008) оцінює, що інформація з відкритих джерел становить від 80 до 95 % усієї інформації, яка використовується розвідувальною спільнотою.

Під час фази вимог будуть встановлені гіпотези та нанесені на карту вимоги до інформації. Це відкриє шлях до наступних етапів роботи. Після визначення вимог до інформації формується стратегія збору інформації з відкритих джерел.

2.1.2 Стратегія та планування (Strategy and planning)

Важливим етапом процесу Open Source Intelligence є стратегія та планування. Є багато причин, чому поліції потрібно збирати інформацію з відкритих джерел. У багатьох контекстах це буде пов’язано з розслідуванням одного чи кількох кримінальних правопорушень або запобіганням кримінальним злочинам (Gibson, 2016). Інтелект з відкритим кодом має керуватися певною метою. Мета визначається випадком, гіпотезами та вимогами. Мета також може базуватися на проекті. Це може бути проект, заснований на загальній стратегії, яка визначає пріоритети поліції на національному чи місцевому рівнях. У методологічному контексті стратегія є специфічною і забезпечує основу для планування та підготовки, які керуватимуть роботою з надання необхідної інформації.

Стратегія тісно пов'язана з плануванням і тому може розглядатися разом. Стратегія та планування формують основу для наступних етапів збору, обробки та аналізу.

Різні моделі включають або описують стратегію на етапі «Напрямок», якщо стратегія та планування взагалі включені в модель. Стратегія повинна визначити напрямок для майбутньої роботи, але вона повинна спиратися на попередню роботу зі встановлення гіпотез і управління вимогами. Стратегія буде

відрізнятися від випадку до випадку, хоча методи, які використовуються, однакові.

Open Source Intelligence стане одним із кількох способів надання інформації широкому колу інформації. Стратегія розвідки з відкритими джерелами має ґрунтуватися на перевірці або фальсифікації гіпотез, охоплюючи інформаційні вимоги, визначені в той час, коли весь процес OSINT будується на меті розслідування. Таким чином, стратегія описуватиме мету збору інформації, яка інформація потрібна, з яких джерел найбільш доречно шукати інформацію та як інформацію можна зберегти, задокументувати та підтвердити.

Стратегія має бути конкретною за формою та змістом, щоб усі залучені сторони розуміли мету та напрямок місії.

Планування буде тісно пов'язане зі стратегією. Якщо стратегія визначає напрямок розслідування, планування сприятиме рухам у правильному напрямку. У багатьох ситуаціях буде інформація, яка змінює фокус, потрібно шукати в інших місцях або слідувати іншим потокам, ніж ви думали спочатку. Тим не менш, планування є ключовою частиною Open Source Intelligence, оскільки йдеться не лише про планування, де думати про пошук інформації, а й про підготовку всього процесу збору, обробки та аналізу інформації, враховуючи обладнання, облікові записи, легенди, безпеку роботи тощо.

Ретельне планування того, як ідентифікувати релевантну інформацію, необхідну для відповідей на запитання, а також процес пошуку та збереження цих даних є важливим першим кроком для отримання інформації, яка має необхідну якість і точність (Gibson, 2016).

Той факт, що інформацію можна знайти у відкритих джерелах, не означає, що її легко знайти або отримати до неї доступ. Необхідно розглянути, яка інформація може сприяти розслідуванню, де цю інформацію можна знайти та як її можна отримати. Інформація буде доступна в багатьох форматах, і те, як працювати з усіма різними форматами, також має бути включено до планування.

У рамках планування важливо описати концепції групування інформації, перевірити інформацію та цінність інформації. Це буде корисно для переходу до етапів збору, обробки та аналізу.

У моделі, де інтелект виводиться з інформації, інформація повинна мати можливість систематично класифікуватися. У стандартизації даних вам потрібно визначити кілька звичайних загальних «об'єктів» даних, з якими буде пов'язане дослідження. Їх можна класифікувати як об'єкти подій (наприклад, пограбування, напад тощо) і статичні об'єкти (наприклад, люди, транспортні засоби, будівлі тощо). Ідентифікуючи кожен унікальний об'єкт, можна створити повний список усіх зв'язків між різними об'єктами.

Щоб групувати інформацію, необхідно розглянути, яке групування може бути доречним. Стандартизація групування інформації буде корисною для подальшого аналізу. TechUK визначає чотири пункти дослідження, які необхідно перевірити, які можна застосувати до всіх розслідувань.

Ці чотири точки дослідження: особа, об'єкт, місце розташування та подія, скорочено *POLE (People, Object, Location, Event)* (TechUK, 2014). Принаймні один із них має бути присутнім, щоб отримати запит. Інтелектуальні дані, отримані з будь-якого джерела, можна буде віднести в рамках моделі даних POLE. У Великій Британії це відповідає посібнику для авторизованої професійної практики Британського поліцейського коледжу, і обговорюється, чи має це бути загальним стандартом для поліції Великої Британії (Ramwell et.al., 2016).

Чотири точки дослідження, описані вище в моделі POLE, можна використовувати для групування сутностей. Сутності – це такі об'єкти, як люди, організації, місця тощо, які з'являються в матеріалі.

Об'єктами також можуть бути особи, адреси електронної пошти, псевдоніми, IP-адреси6 тощо (Gibson, 2016). Усі ці сутності можна згрупувати за людьми, об'єктами, місцями та подіями. Іншими словами, суб'єкт – це особа, об'єкт, місце або подія, описані в розслідуванні.

У більшості випадків *люди* часто є найповнішою сутністю. За злочином завжди стоїть людина, незалежно від того, чи він скоєний, чи на стадії планування. У багатьох випадках як у злочині, так і в завчасній підготовці беруть участь декілька осіб. Це робить людину в будь-якому розслідуванні, реактивному чи проактивному, найважливішим об'єктом дослідження.

Розвідувальна інформація щодо осіб, які беруть участь у розслідуванні, міститиме як інформацію про окрему особу у справі, так і стосунки різних людей з іншими суб’єктами.

Люди як інформаційні об’єкти можуть бути як ідентифікованими, так і неідентифікованими. Особи відомого підозрюваного, свідка чи потерпілого встановлюються. Неідентифікована особа може бути невідомим підозрюваним або свідком, який описаний у справі без знання того, хто є свідком. Цю особу можна назвати свідком у справі на основі інформації від інших осіб, відеоспостереження тощо.

Об’єкти – це сутності, які не належать до інших категорій, наприклад «Люди», «Розташування» або «Події». Іншими словами, об'єктами може бути майже все. Об’єктами такої класифікації будуть транспортний засіб, тварина, зброя, гроші тощо. Будівлі можуть бути об’єктами, оскільки будівля та місце не пов’язані між собою. Сутність розташування може бути місцем без будівель, а по-друге, будівля може бути об’єктом, не прив’язаним до місця розташування, тобто будівлю можна детально описати без ідентифікації її розташування.

Об’єкти не обов’язково мають мати фізичні розміри. Зокрема, Інтернет ідентифікує багато об’єктів, які не існують фізично, а існують лише цифрово. IP-адреса, адреса електронної пошти, доменне ім’я, ім’я користувача та ідентифікатор Facebook – усе це елементи, які існують лише в цифровому вигляді, але вони все ще є важливими об’єктами розслідування.

Локації – це сутності, які можуть описувати територію, місце тощо... Найбільш центральне місце часто є місцем кримінального правопорушення. Деякі злочинні дії відбуваються на кількох місцях злочину, наприклад викрадення гаманця (місце 1), який містить кредитну картку, яка використовується для зняття грошей (місце 2), можливо, кілька разів (місця 3, 4 тощо).

Це також може бути явище, яке відбувається в кількох місцях протягом певного періоду часу, як-от серійні пограбування або серійні зґвалтування, де характер справи змушує їх розглядати в контексті.

Іншими місцями розслідування можуть бути місця проживання фігурантів (підозрюваних і потерпілих), місця планування та підготовки, шляхи прибуття та евакуації, спостережні пости тощо.

Розташування, пов’язані з цифровими доказами, також будуть об’єктами розташування в розслідуванні. Можуть бути розміщені базові станції, до яких активно чи пасивно підключені мобільні телефони, або базові станції, що охоплюють місце злочину чи інші центральні місця. Також можуть бути місцезнаходження, отримані з даних EXIF7 із зображень у мобільних телефонах тощо.

Події займають таке ж центральне місце в розслідуванні, як і люди. Це стосується проактивного розслідування, коли історичні події можуть розкрити щось про очікувані події, яких хочеться запобігти.

Подібно до того, як місце злочину є центральною сутністю Місцезнаходження, кримінальні злочини будуть найбільш центральною сутністю Події. Тим не менш, кримінальний злочин рідко є імпульсивною дією. Подія, швидше за все, буде спланована заздалегідь, а потім плани шляхів евакуації та інші дії. Це теж ключові події в розслідуванні.

Події стосуватимуться і цифрового світу. Майже будь-яке використання цифрових технологій можна визначити як події. Трафік між різними службами в Інтернеті є подіями, надісланий електронний лист є подією, вхід до служби є подією та завантаження матеріалів про насильство над дітьми є подіями.

Люди, які роблять щось шахрайське, хотіли б спробувати приховати свої сліди. Однією з причин, чому злочинці діють в Інтернеті або через нього, є можливість анонімності (Bryant, 2014). Як і інші люди, вони все одно будуть робити помилки та залишати сліди, за якими може стежити поліція. Одним із джерел, яке часто надає інформацію, є, наприклад, коли інші люди публікують зображення когось у соціальних мережах і, можливо, навіть позначають цю особу тегом на ім’я без відома цієї людини. Відвертість інших людей дозволить отримати доступ до інформації про об’єкт розслідування через бекдор. (Ramwell, 2016).

Рамвелл вказує на дві сфери, які відкривають можливості в розслідуванні. Їх називають Лінь та Его і називають їх *експлуатаційними (exploitables)*.

Лінь і Его є двома причинами того, що інформація стає доступною для поліції, коли вона має знання та навички, щоб знайти її. Лінь пов’язана з тим фактом, що люди не можуть робити все, що потрібно, щоб зберегти інформацію

про себе в Інтернеті прихованою, або вони не усвідомлюють, скільки інформації залишається відкритим і що їм потрібно зробити, щоб запобігти цьому (Ramwell 2016). Приховування слідів, зроблених в Інтернеті, включатиме не лише ті, які вони зробили самі, але й ті, які залишили інші. Як згадувалося вище, інші зможуть публікувати фотографії та інформацію про людину, яка намагається залишатися анонімною в Інтернеті, і це вимагає багато зусиль, щоб переконатися, що ніхто інший не публікує інформацію про вас.

Его — ще одна поширена пастка в соціальних мережах. Люди свідомо чи підсвідомо використовують соціальні медіа, щоб публікувати свої емоції, думки та фотографії себе. Крім того, вони відзначатимуться в різних місцях або подіях, на яких вони присутні, і їм сподобатимуться сторінки, які відповідають їхнім інтересам і вподобанням. Більшість людей, також злочинців, хочуть публікувати речі про своє життя, особливо те, що вони якимось чином засвоїли, можливо, щоб похвалитися чи похизуватися. Це також може включати вихваляння злочинною діяльністю, яку вони здійснюють (Ramwell et.al. 2016). У 2017 році Norwegian Broadcasting (NRK) зробив репортаж про мандрівників, які керували торгівлею людьми та проституцією в Бергені. Вони стежили, зокрема, за відкритими профілями підозрюваних у Facebook, де показували великі суми грошей, дорогі машини та фотографії з дорогих вечірок, хоча не мали роботи та доходу. Інформація з різних облікових записів Facebook була невід'ємною частиною матеріалу, який журналіст використовував для обґрунтування та документування справи (NRK, 2017).

2.1.3 Збір (Collection): пошук, отримання, підтвердження

Сьогодні кожен так чи інакше присутній в Інтернеті. Більшість людей також певною мірою використовують соціальні мережі як частину взаємодії з іншими людьми. Усі дії з використанням Інтернету залишають цифрові сліди. Це ці сліди, за якими ми хочемо стежити та збирати дані. Треба починати з тієї інформації, яку ми вже маємо. У нас може бути псевдонім, IP-адреса, назва форуму, школи, адреса електронної пошти тощо. Нам є з чого почати, щоб отримати нову інформацію. Етап збору буде значною мірою зосереджений на

пошуку фрагментів інформації, які можуть привести до нової інформації, яка, у свою чергу, веде до нової інформації. Це можна назвати наступними сухарями.

Визначення того, які дані необхідні для задоволення інформаційних вимог, є першим кроком у процесі визначення найкращого джерела та методу отримання цих даних. Те, що дані існують, не означає, що вони легко доступні. Потрібні дані може бути важко знайти та представлені в незвичному форматі. Звичайні обшуки за допомогою пошукових систем — це завдання, з яким справляються більшість поліцейських, але проведення повного обшуку буде поза компетенцією більшості звичайних слідчих. Крім того, багато інформації може міститися на різних форумах тощо, і будь-хто, хто працюватиме з Open Source Intelligence, повинен навчитися шукати інформацію в більш незнайомих місцях, таких як, серед іншого, онлайнові чат-сервіси та мережі обміну файлами (Ferraro). і Кейсі, 2005)

Процес пошуку інформації можна виконувати як вручну, так і за допомогою програмного забезпечення, яке виконує пошук за різними критеріями пошуку в багатьох місцях автоматично. На основі визначених вимог і планування дослідник шукатиме інформацію там, де її найімовірніше можна знайти. При використанні інструментів для автоматичного пошуку велика частина роботи буде пов’язана з обробкою та перевіркою даних, оскільки автоматизовані інструменти, ймовірно, автоматично зберігають інформацію. Важливою частиною колекції є те, що вона постійно відкриватиме нову інформацію для пошуку, а також з’являтимуться речі, які не були враховані під час планування. Потрібно також бути креативним у пошуку нових місць для пошуку та нових способів отримання інформації.

Список усієї потенційно доступної інформації про когось може бути таким же вичерпним, як книга. Ми маємо звузити його до інформації, яка нам потрібна для досягнення результату, який ми прагнемо. Для цього потрібен системний підхід. Завжди буде деяка загальна інформація, яка потрібна незалежно від випадку, а також буде багато інформації, яка є доречною в одному випадку, але не в іншому.

При зборі даних з відкритих джерел в Інтернеті, кількість інформації може бути надзвичайною. Те, що має бути пріоритетним під час збору інформації, може відрізнятися. Збір даних може бути ручним пошуком в Інтернеті, пошуком

на платформах соціальних медіа, форумах, групах новин тощо для пошуку фрагментів інформації, як-от номер телефону, ім’я користувача, ідентифікатор тощо, які можна використовувати далі. Офіцер, який збирає інформацію, завжди повинен порівнювати використання ручного пошуку з ефектом автоматизованих інструментів. Природно, буде велика різниця між офіцерами, які збирають інформацію з відкритих джерел у рідкісних випадках у випадках на роботі, і тими, чия розвідка з відкритих джерел є основним завданням у своїй роботі. В останній групі, ймовірно, буде значно більше використання автоматизованих інструментів, оскільки вони роблять це так часто, що вони знаходять ці інструменти та навчаються, як ними користуватися, а в деяких випадках створюють їх самі.

Збираючи інформацію, необхідно враховувати, за якими напрямками слідувати, а які слід відкласти або визначити пріоритет пізніше. Важливо відстежувати потенційні потенційні клієнти, за якими в даний момент не слідкують, оскільки вони можуть стати актуальними на пізнішому етапі.

Хороша практика збереження та документування всієї отриманої інформації є дуже важливою. Необхідно дотримуватись принципу ланцюга контролю через контрольний слід. З точки зору цифрових доказів, вони зможуть швидко змінюватися, і якщо контрольний слід не буде дотриманий, ланцюжок контролю незабаром може бути порушено. Чим більш мінливі дані, тим важливіше ретельно їх документувати, оскільки це може виявитися важко перевірити пізніше на більш пізньому етапі

Зберігання даних, які будуть використовуватися як докази для обвинувачення, має відповідати принципам, стандартам і методам комп’ютерної криміналістики. «Комп’ютерна криміналістика — це науковий збір, експертиза, автентифікація, збереження та аналіз даних, що зберігаються на комп’ютерних носіях інформації або витягуються з них таким чином, щоб інформація могла бути використана як доказ у суді» (Gottschalk, 2010). Під час збору не завжди можна знати, чи буде інформація використана як доказ, тому весь збір має здійснюватися відповідно до цих принципів і стандартів.

Також важливо подумати про порядок волатильності. Багато джерел часто шукаються одночасно або в одному процесі. Наскільки мінливими є різні дані,

навіть в Інтернеті, це буде різним. Принцип порядку мінливості описує наступне: «Визначення пріоритетів потенційного джерела доказів, яке потрібно зібрати, відповідно до мінливості даних» (Flaglien, 2018). Тому важливо в першу чергу визначити пріоритети збереження найбільш мінливих даних, якщо вони ідентифіковані. У комп'ютерній криміналістиці це стосується того, що дані, що зберігаються на диску, менш мінливі, ніж дані, що зберігаються в пам'яті (Nist, 2006). В Інтернеті дані, що зберігаються в новинах разом із картами та супутниками, будуть менш мінливими, ніж дані, що зберігаються на форумах, у соціальних мережах і групах новин.

Зберігати інформацію з відкритих джерел в Інтернеті можна багатьма способами за допомогою різних інструментів. Немає необхідності мати доступ до дорогих або передових інструментів для захисту інформації, але вони можуть бути корисними, коли потрібно зібрати багато інформації з різних джерел. Спосіб збору даних залежить від інформації, яку ви шукаєте. Якщо доречно захистити всю інформацію з веб-сайту організації, яку ви досліджуєте, було б корисно зберегти весь сайт як у формі «Print Screen», яка показує, як виглядають веб-сторінки, так і весь веб-сайт із джерелом код. В інших випадках може бути достатньо задокументувати лише одну публікацію на форумі з іменем користувача, вмістом і міткою часу. У деяких ситуаціях його можна зберегти за допомогою «Print Screen» і URL-адреси в адресному рядку браузера. Важливо зберегти дані таким чином, щоб дотримуватись принципів судово обґрунтованого розслідування та щоб докази витримали в суді.

Під час збору буде зібрано деяку інформацію, яка не має відношення до конкретного випадку. Там може бути інформація, яка може мати відношення до інших поточних розслідувань, можуть бути докази кримінальних справ, про які не повідомляється, або може бути інформація про можливі кримінальні злочини, які ще не були вчинені. Це може бути як особиста інформація, так і інша інформація, і така інформація повинна оброблятися належним чином і відповідно до юрисдикції різних країн. По суті, слідчий повинен переконатися, що зібрана особиста інформація пов'язана зі справою таким чином, щоб її можна було використовувати надалі в розслідуванні (Ramwell, 2016).

2.1.4 Обробка (Processing)

Під час обробки зібрані дані будуть перевірені та підготовлені для подальшого аналізу. Важливо документувати кожен крок під час процесу, щоб зберегти ланцюжок відповідальності. Експертиза цифрових доказів часто передбачає реструктуризацію, аналіз і повторну обробку даних, щоб зробити їх зрозумілими для подальшого аналізу.

У разі збору інформації з відкритих джерел в Інтернеті цей етап передбачатиме перегляд зібраних даних для підготовки до аналізу. Це може бути обробка даних у загальному форматі, щоб можна було порівнювати дані з різних джерел. Також може знадобитися пройти через збережену веб-сторінку, щоб зібрати дані для подальшого використання на етапі аналізу.

В загалому обробка полягає в перетворенні даних у необхідний формат для аналізу, об’єднанні з іншими джерелами даних, ідентифікації відповідних даних і початку процесу вилучення та агрегації. (Gibson, 2016)

Дані будуть отримані як у структурованому, так і в неструктурованому вигляді. Структуровані дані – це дані, які легко містяться в базах даних із поясненнями для різних таблиць і комірок і зв’язків між ними. Неструктуровані дані є протилежністю, коли дані не виникають у структурі з моделлю, яка описує вміст і зв’язки. Неструктуровані дані, як правило, можуть бути веб-сторінками, зображеннями, відео та іншими файлами, які зазвичай вимагають перевірки вручну.

Обробка природної мови — це метод обробки тексту з відкритих джерел. Значна частина даних, захищених Open Source Intelligence, буде в текстовому форматі, тому вони будуть доступні для індексування та пошуку. Проблемою може бути те, що користувачі можуть писати, використовуючи регіональні розмовні лексики або діалекти, які не розпізнаються в письмовій формі, особливо із захистом даних із форумів, соціальних медіа та еквівалентів; він може бути пронизаний друкарськими помилками, крім того, потрібно враховувати імена користувачів і псевдоніми. Тут також досліднику буде корисно навчитися використовувати автоматизовані інструменти, щоб полегшити роботу.

Ідентифікація сутностей є важливою частиною обробки. Сутності важливі в процесі аналізу, а отже, вирішальні для вилучення. Аналіз може виявити, що кілька сутностей можуть бути об'єднані, оскільки ім'я користувача та псевдонім можуть бути пов'язані з конкретною особою, або він може виявити, що інші, здавалося б, самотні сутності в матеріалі виглядають однаковими.

Моделювання – ще один метод обробки. Часто текстові дані поміщаються в контекст. Може існувати ланцюжок чату чи форуму, де повідомлення в контексті є важливим для надання будь-якого значення. У соціальних мережах публікація часто є відповіддю на іншу публікацію. Потім різні записи потрібно помістити в контекст, щоб можна було встановити зв'язки.

Перевірка – це постійний процес від збору до обробки та аналізу. Перевірка повинна проводитися як невід'ємна частина пошуку, тому що під час пошуку та захисту інформації найбільш природним є оцінка джерела інформації, перевірка інформації, яка може підтвердити достовірність джерела, і пошук для перевірки інформації з інших джерел. Однак перевірити всю інформацію під час збору неможливо, тому процес перевірки продовжується під час обробки. Гібсон (2016) розглядає перевірку інформації виключно як частину обробки.

Перевірка інформації, отриманої за допомогою Open Source Intelligence, може бути проблемою. Це значною мірою залежатиме від джерела інформації, тому оцінка джерела є центральною частиною перевірки інформації з відкритих джерел.

Як згадувалося вище, важливою частиною Open Source Intelligence є переміщення інформації з OSINT у V-OSINT. Встановлюючи та впроваджуючи методи визначення пріоритетів, оцінки достовірності та підтвердження джерел, інформації та розвідувальних даних, ми збільшуємо ймовірність того, що представлене має високу надійність, точність і цінність. Це створює кращу основу для прийняття рішень на основі інтелекту (Gibson, 2016).

Оцінка достовірності може бути важким завданням, тому оцінка джерела має першочергове значення. НАТО використовує наступні рекомендації для оцінки достовірності джерела:

1. Авторитетність джерела,

2. Точність джерела,

3. Об'єктивність джерела,

4. Вживаність джерела

5. Охоплюваність джерела

(Gibson, 2016)

Інформація від відомих ЗМІ матиме значно вищу довіру, ніж прості записи в соціальних мережах, таких як Facebook, Twitter, Instagram тощо. Точність і об’єктивність часто будуть вищими у тих, хто вважається надійними джерелами. Якщо джерело не вказує автора та дату публікації інформації, це не викликає довіри. Тоді інформацію важко перевірити. Інформацію з соціальних медіа, форумів тощо може бути набагато складніше перевірити, оскільки вміст було створено користувачами без певної форми контролю якості чи редакційного контролю. Окрема особа може публікувати на цих форумах, але опублікований елемент може мати значення лише через його існування. Однак, порівнюючи та перехресно посилаючись на іншу інформацію, опублікований елемент потенційно може бути перевірений або спростований. Інформація про місцезнаходження людей у соціальних мережах може бути підтверджена з інших джерел, напр. туристичні компанії або органи інших країн через паспортний контроль. Об’єднання даних OSINT і не-OSINT також можна використовувати для перевірки інформації, але така перевірка зазвичай виконується на етапі аналізу.

Різні спецслужби часто використовують різні методи для класифікації достовірності за шкалами від чотирьох, п’яти, шести і більше значень. НАТО має свій метод, армія США має свій метод, а поліція Великобританії має свій метод (Gibson, 2016). Хоча різні агентства використовують різні методи оцінки достовірності інформації, цікаве питання з точки зору методології: наскільки різноманітні критерії, що використовуються для розміщення інформації за шкалою від чотирьох до шести і так далі? Це не повинно ґрунтуватися на суб’єктивних міркуваннях. Важливо, наскільки це можливо, використовувати об'єктивні критерії для оцінки достовірності інформації. Якщо модель не надає чітких вказівок щодо того, як слід проводити валідацію та які об’єктивні критерії повинні лежати в основі оцінки, такі моделі будуть малоцінними.

Об'єктивною оцінкою інформації буде перевірка з інших, незалежних джерел. Усі джерела також повинні відповідати тим самим критеріям оцінки, що

й вихідна інформація. Інакше проблема може полягати в тому, що та сама помилка в інформації поширюється багатьма через її природу. Подія, про яку багато хто розповідає в соціальних мережах, не отримає автоматично високої довіри, навіть якщо її поширюють багато. Інформація про смерть актора Едді Мерфі охопила значну частину світу, хоча й була неправдивою.

Статті новин можна легше перевірити, оскільки часто інші ЗМІ повідомляють про те саме. Важливим контрольним пунктом є переконатися, що не всі посилаються на те саме джерело. Тоді ймовірність того, що вона є невірною, буде такою ж високою, якби про це повідомила лише одна медіа-компанія, але більшість серйозних медіа-компаній намагатимуться перевірити інформацію з багатьох джерел або висловлять застереження, якщо це неможливо.

Перевірити зібрану з відкритих джерел інформацію не завжди можливо. У випадках, коли перевірити інформацію неможливо, важливо, щоб вона була задокументована таким чином, щоб відсутність перевірки була чіткою та легкою для перегляду. Інформація, яку неможливо перевірити, не буде прийнята як надійний доказ, але вона є непрямою і тому може підтримувати гіпотезу. У проактивному розслідуванні вимоги до перевірки часто будуть нижчими, оскільки інформація використовуватиметься як основа для реагування поліції, а не як доказ для обвинувачення.

2.1.5 Аналіз (Analysis)

Інформація не стане розвідкою без аналізу. Здатність аналізувати інформацію – це те, що відрізняє базовий OSINT від чудового OSINT (Hribar, 2014, як згадується в Gibson, 2016). У Open Source Intelligence можна проводити багато форм аналізу, а також різні інструменти, які можуть бути корисними.

Аналіз полягає в оцінці та збиранні інформації для підтримки або відхилення гіпотез. Важливою частиною аналізу є перегляд інформації в контексті. Важливо структурувати інформацію, щоб забезпечити більш чітке уявлення про інформацію, яку інакше було б важко побачити. Стандартизація інформації за фіксованими категоріями полегшує аналіз. Використовуючи модель даних POLE (TechUK, 2014) як відправну точку, аналіз визначає різні сутності в

отриманому матеріалі. Ключовою цінністю для розслідування є виявлення стосунків між різними людьми, об’єктами, місцями та подіями у справі.

Сутності в справі будуть пов’язані з однією або кількома іншими сутностями. Коли ми збираємо інформацію, зв’язок між цими суб’єктами часто є однією з найважливіших відомостей. Це не означає, що інформація про зв'язки відома, але зв'язок має бути. Відносини дадуть підказки про зв’язки між різними частинами інформації. Це можна проаналізувати, вставивши в матрицю для подальшого експорту в інструмент візуалізації, такий як наприклад Maltego. Таку матрицю можна постійно заповнювати під час аналізу, а також відображати поля, де інформація відсутня.

Таблиця 2.1

Матриця відношень

Сутність	Тип сутності	Опис	Відношення	Підтверджено	Сутність	Тип сутності	Опис
Іван	Людина	121265-3452	Власник	Так	Машина	Об’єкт	ABC1234DE
Крадіжка	Подія	Справа: 12345678	Досліджується	Ні	Машина	Об’єкт	ABC1234DE
Іван	Людина	121265-3452	Підозрюваний	Ні	Крадіжка	Подія	Справа: 12345678

Під час експорту до інструменту візуалізації, такого як Блокнот аналітика, можна вибрати перевірені посилання цілою лінією, а неперевірені – пунктирними лініями.

Зібрані дані можуть бути додатково проаналізовані, серед іншого, за допомогою аналізу тексту, аналізу мережі, аналізу розташування та аналізу часу. Зазвичай кілька форм аналізу виконуються одночасно, але представлені по-різному. На карті мережі можна візуалізувати, хто з ким має стосунки та наскільки ці стосунки підтверджені, а також силу (наприклад, кількість контактів) стосунків. Мережеву карту або мережевий аналіз часто використовують для пошуку зв’язків між різними особами, визначення типу зв’язків у них, перегляду та підтвердження зв’язків. Карту мережі також можна використовувати для візуалізації зв’язків між людьми, організаціями, транспортними засобами та

іншими об’єктами. На карті мережі також можна вибрати центральні зв’язки, щоб побачити співвідношення різних типів зв’язків між об’єктами. I Analyst's Notebook, і Maltego можуть автоматизувати аналіз мережі.

Хронологічна шкала може візуалізувати інформацію таким чином, щоб було легше побачити послідовність, у якій відбувалися події та з яким інтервалом. Він може надавати інформацію, яка не була виявлена під час надходження інформації, а також може відображати області, де даних бракує, напр. що для підтвердження гіпотези відсутня подія. Пошук інформації про цю подію стане новим завданням.

Дані також можуть бути представлені на картах, щоб вказати, де відбулися різні події або розташування різних об’єктів. Це може бути місце, де живуть або зупиняються різні люди, можуть бути місця для різних подій і може бути зіставлення різної інформації з різних джерел.

Під час збору інформації компіляція та аналіз інформації з багатьох джерел є частиною завдання. У розвідувальній доктрині норвезької поліції це описується як аналіз із багатьох джерел (Pod, 2014). У цій частині аналізу йдеться про збирання інформації з різних джерел і перегляд кореляцій, які не виявляються шляхом аналізу кожного окремого джерела окремо. Різні сутності в зібраному матеріалі часто з’являються в кількох типах даних, і дані можуть мати різну валідність. Проблема може полягати в тому, щоб об’єднати різні ідентифікаційні дані сутності в унікальну ідентичність. Може бути профіль Facebook, який підтверджено належить конкретній особі (наприклад, підозрюваному), а потім кілька ідентифікацій з різних форумів, і всі вони можуть належати одній особі. Як їх можна об’єднати, якщо немає впевненості, що це одна і та ж сутність? Тут виникає нова гіпотеза, яку необхідно перевірити або сфальсифікувати. Якщо перевірка або фальсифікація гіпотези є невдалою, невизначеність повинна виникнути в представленні аналізу. З іншого боку, це злиття ідентифікаторів буде хорошим інструментом, якщо можна перевірити, що ідентифікатори належать одній сутності. Раптом з’являється набагато більше інформації про сутність.

Дей, Гібсон і Рамвелл (2016) представляють подібний процес злиття даних OSINT і не-OSINT. Процес описує злиття інформації, що надходить з OSINT, з інформацією із закритих джерел. Закритими джерелами може бути інформація,

напр. Поліцейські записи, записи телекомунікацій, реєстри населення, фінансові записи, медичні записи та інша інформація, яка не є загальнодоступною. Традиційно поліція в основному використовує ці закриті джерела та інформаторів для надання розвідувальної інформації. Донедавна використання інформації з відкритих джерел не розглядалося як потенціал. Коли поліцейські побачать потенціал OSINT-даних і не-OSINT-даних, вони матимуть ширший спектр джерел для отримання інформації. Крім того, можна отримати більше знань, об'єднавши кілька різних ідентифікацій в одну з інформацією, що міститься в OSINT-даних і не-OSINT-даних.

Аналіз часто є повторюваним процесом, який генерує нову інформацію, яка, у свою чергу, породжує нові завдання. Нові завдання створять збір нових даних для обробки, які потім будуть проаналізовані. Таким чином, це можна розглядати як циклічний процес від збору до обробки до аналізу і далі до нового збору, нової обробки та нового аналізу. Цей циркулярний процес триває до тих пір, поки необхідна інформація не буде зібрана та проаналізована, а результат може бути поширений.

2.1.6 Поширення та Оцінка (Dissemination and Evaluation)

Онлайн-розслідування або збір інформації з відкритих джерел передбачає збір мінливих даних. Не всю знайдену інформацію можна відтворити, і в багатьох випадках буде важко відтворити процес і результати просто тому, що даних більше немає. Тому під час роботи з мінливими даними, незалежно від того, чи йдеться про криміналістику даних у реальному часі, онлайн-розслідування чи розвідку з відкритим джерелом, важливо постійно документувати те, як інформація знаходилася, отримувалася, оброблялася й аналізувалася. Це можна зробити вручну або автоматично. Деякі інструменти, такі як Fireshot, забезпечать позначку часу під час створення знімка екрана веб-сторінки.

Важливість документації та перевірки повторюється в багатьох стандартах і рекомендаціях щодо дослідження цифрових доказів. У RFC 3227 вказується на важливість «документування кожного кроку» під час збереження цифрових доказів, а також на важливість збереження «ланцюга контролю» (The Internet

Society, 2002). Керівні принципи ACPO також наголошують на важливості аудиторського сліду та документації, де принцип 3 описується так: «Потрібно створювати та зберігати аудиторський слід або інший запис усіх процесів, застосованих до цифрових доказів. Незалежна третя сторона повинна мати можливість перевірити ці процеси та досягти того самого результату» (ACPO, 2012). Крім того, NIST SP 800-86 пояснює важливість документації: «Документація дозволяє іншим аналітикам повторити процес пізніше, якщо це необхідно» (NIST, 2006).

Документування є послідовним процесом. Навіть перед тим, як розпочати пошук інформації, слід задокументувати час, місцезнаходження, апаратне та програмне забезпечення, що використовувалося, і це повинно бути послідовним протягом усього процесу. Зрештою, це має призвести до звіту.

Важливо враховувати, що звіт має бути прозорим і зрозумілим для читача. В першу чергу варто подумати про те, хто є аудиторією (реципієнтом) доповіді. Якщо звіт має бути зачитаний адвокатом обвинувачення або використаний як доказ у суді, слід уникати технічних термінів, наскільки це можливо. Необхідно описати основні технічні терміни та надати короткий виклад суті процесу.

Флаглін представляє типові моменти для звіту під час дослідження цифрових доказів:

• Ролі та завдання для розслідування,

• Резюме всіх джерел інформації та доказів,

• Судово-медична експертиза та аналіз, які відображають ланцюжок зберігання та цілісність доказів,

• Візуалізація та діаграми,

• Зображення та знімки екрана,

• Інформація, яка підтримує повторюваність і відтворюваність аналізу.

• Використовувані інструменти та

• Висновки. (Flaglien, 2018, стор. 46)

Баззел рекомендує, щоб результати та висновки були представлені в резюме, а інформація про джерела, процес і докази була представлена пізніше у звіті (Bazzel, 2018).

Баззел описує, що його звіти зазвичай містять такі моменти:

• Резюме: односторінковий синопсис життєво важливих доказів

• Деталі підозрюваного; Конкретні дані, такі як усі персональні ідентифікатори, імена користувачів тощо

• Описовий звіт: детальні висновки з посиланнями на цифрові докази та резюме

• Підсумковий звіт: короткий виклад фактів на одній сторінці та необхідність подальшої роботи.

• Цифрові докази: DVD або флеш-накопичувач, який містить усі знімки екрана та файли. (Bazzel, 2018, стор. 456).

Під час презентації етапу аналізу було описано різні форми аналізу, які можуть візуалізувати інформацію дуже прозорим способом, як-от карти мережі, часові шкали тощо. Було б корисно включити їх у звіт. Читачеві звіту буде набагато легше зрозуміти результат, побачивши візуальні представлення, а не покладаючись виключно на текст. Як пише Флаглін, «стіна з тексту нікому не годиться» (Флаглін, 2018). Прозоро написаний звіт із хорошими візуальними ефектами, які відображають ключові докази, буде набагато кориснішим для того, хто отримає звіт і використовуватиме інформацію далі, наприклад. як підставу для звинувального акту.

Більш детальний процес, який виконується вручну або за допомогою інструментів, може бути представлений у вигляді вкладення або в окремому розділі звіту. Ця частина може показати, які пошуки та знахідки були зроблені. Тут можна включити весь детальний процес пошуку, операторів, відвіданих URL-адрес тощо. Ця інформація в основному буде цікава тому, хто перевірятиме процес. Багато інструментів, які можна використовувати в цифровому розслідуванні, створюють власні звіти. Їх також буде природно додати як вкладення до звіту, включаючи важливі питання в резюме

Задокументований ланцюжок поставок — це сполучна ланка, яка з’єднує методологію та процеси. Звіт захищатиме принцип ланцюга контролю, щоб жодна помилкова документація щодо завдань або відкриттів не давала можливості поставити питання щодо достовірності та цілісності доказів у суді.

Існує багато прикладів і шаблонів структурування таких звітів, але немає однозначної відповіді, який із них найкращий. Головне, щоб звіт містив прозоре

та зрозуміле резюме, яке стосується найважливіших висновків, і щоб усі завдання були добре задокументовані.

Важливою частиною такого звіту часто є рекомендації щодо подальших дій або інших розслідувальних завдань. Тут природно розрізняти доповіді, які є частиною доказів для висунення обвинувачення у кримінальній справі, і доповіді, які будуть використовуватися керівництвом органу для прийняття рішень.

У звіті про кримінальну справу рекомендації та заходи будуть зарезервовані для тимчасових або внутрішніх звітів. Остаточний звіт, який використовується як частина обвинувального висновку, буде остаточним звітом, у якому містяться всі рекомендації. Короткий виклад процесу та результатів буде центральною частиною протоколу кримінальної справи.

У процесі розвідки для отримання необхідної інформації для прийняття рішення щодо реагування на запобігання злочинам рекомендації та заходи будуть центральним розділом звіту.

Результат, описаний у *звіті* або поданий іншим чином, повинен бути розповсюджений серед тих, хто потребує інформації. У кримінальному провадженні буде слідче керівництво та прокурор. Крім того, готові доповіді у кримінальній справі розсилаються захисникам та іншим сторонам.

Розвідувальний продукт має бути доступним для тих, хто потребує інформації. Це можуть бути офіцери, які патрулюють у районі, де існує проблема, це може бути будь-хто в проекті, який працює над певним типом злочину, часто буде керівництво, також можуть бути зовнішні співробітники, як-от служба захисту дітей, соціальна служба тощо. Це відповідальність керівника представляти правильний і належний розподіл знань.

Оцінка процесу важлива для оцінки досягнення мети. Результат слід порівняти з гіпотезами та місією. Чи отримано необхідну інформацію? Якщо ні, то чому? Чи були проведені належні обшуки? Чи були використані правильні інструменти та чи була забезпечена анонімність? Це ключові питання, які потрібно поставити під час оцінювання. Про оцінку легко забути, особливо коли мета досягнута і місія вирішена. Тим не менш, важливо розглядати процеси в світлі вимог.

Оцінку можна проводити різними способами. Найважливіше оцінити результат у порівнянні з початковими вимогами. Чи отримали відповіді на початкові запитання? Крім того, було б важливо розглянути, чи результат породить нові запитання, на які потрібно знайти відповідь. Також важливо вивчити з процесу для подальшого використання як те, що було успішним, так і те, що пішло не так. Нарешті, було б корисно оцінити використання ресурсів. Чи витрачається час на правильні питання? Можливо, було витрачено непропорційно багато ресурсів на те, що не вело вперед? Чи варто було закінчити кілька пошуків раніше?

2.2 Модель для методології OSINT

Представлена методологія складається з шести етапів. Розслідування починається з виявлення явища, організації або відкритої кримінальної справи. На основі цього формуються гіпотези щодо конкретних вимог. З вимог розробляється стратегія, яка є основою для планування процесу розслідування. Потім інформація збирається та обробляється для подальшого аналізу. Кінцевий результат представляється у формі звіту або схожого звіту.

Процес OSINT проходить круговий шлях від “Requirements” (Вимоги) до “ Dissemination and evaluation” (Поширення та оцінка). У цьому циклічному процесі продукт не тільки розповсюджується, але й оцінюється відповідно до початкових гіпотез. На основі результатів формуються нові гіпотези, що ведуть до нового напрямку, і процес починається спочатку. Рисунок 3 ілюструє цей циклічний процес.

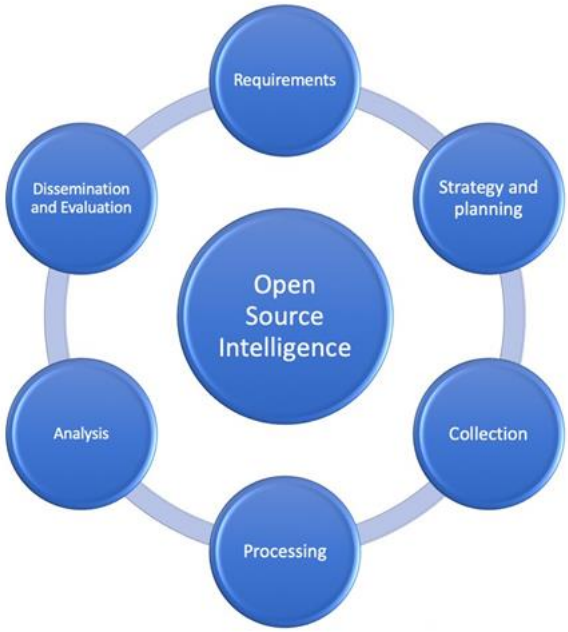


Рисунок 2.1 – Перший спосіб представлення моделі процесу OSINT, круговий шлях

Метою Open Source Intelligence є перевірка або спростування початкових гіпотез. Під час процесу може з’явитися нова інформація, що потребуватиме формулювання нових гіпотез. На завершальному етапі звіт містить рекомендації та заходи, які можуть свідчити про необхідність ініціювати новий процес.

На практиці поліцейські, які займаються розвідкою з відкритих джерел, як спеціалісти, так і в рамках своєї слідчої роботи, можуть не суворо дотримуватися представленої моделі. Однак чітке розуміння того, на якому етапі процесу виконуються завдання, допомагає прийняти рішення і визначитися із діями. Після того, як керівництво призначає завдання на основі реалізованих гіпотез, вимог і стратегії, роль оператора полягає в тому, щоб постачати продукт на основі цього завдання. Якщо презентація оператора та результати виправдовують це, керівництво може встановити нові гіпотези.

Практична реалізація Open Source Intelligence часто передбачає циклічний процес, оскільки результати певних процесів можуть призвести до нових завдань в інших процесах. Інтелектуальні дані, отримані в результаті аналізу, можуть породити потребу в новій інформації, яку потім необхідно обробити й проаналізувати. Це створює циклічний процес у моделі OSINT, який переходить від збору даних до обробки, аналізу та назад до нового збору.

Модель Open Source Intelligence Methodology можна представити двома способами. Перший – це круговий потік від вимог до розповсюдження, який є найбільш корисним для керівництва, оскільки він ілюструє послідовні фази. Однак для тих, хто виконує розвідку з відкритим вихідним кодом, процес починається з вимог, стратегії та планування, які визначають напрямок. Після планування та підготовки фактичний процес проходить круговий шлях, що включає збір даних, обробку та аналіз до представлення та розповсюдження кінцевого результату.

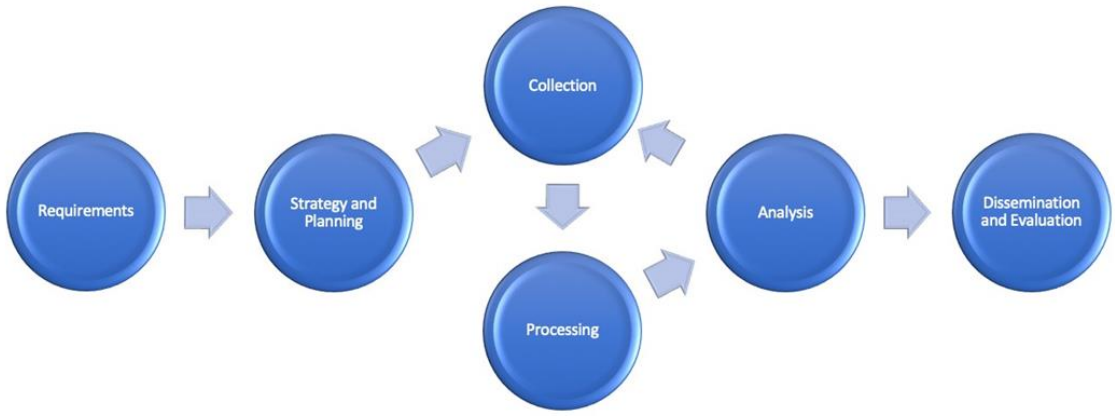


Рисунок 2.2 – Другий спосіб представлення моделі процесу OSINT

У таблиці 2.3 показано різні етапи процесу OSINT з відповідним рівнем проведення та відповідальності від процесу розвідки.

Таблиця 2.3

Етапи процесів OSINT у відповідності з етапами інформаційної розвідки

Фаза в процесі інформаційної розвідки	**Фаза в процесі OSINT**	**Хто виконує**	**Хто відповідає**
Prepare, Lead and Prioritize (Підготовка та пріоритезація)	Requirements (Вимоги)	Виконавчий директор	Виконавчий директор
Planning (Планування)	Strategy and planning (Стратегія та планування)	Голова розвідки Оператор	Голова розвідки
Collection (Збір)	Collection (Збір)	Оператор	Голова розвідки
Processing (Обробка)	Processing (Обробка)	Оператор	Керівник відділу операцій

продовження табл. 2.3

Analysis (Аналіз)	Analysis (Аналіз)	Оператор чи Аналітик	Керівник відділу аналізу
Dissemination (Поширення)	Dissemination and Evaluation (Поширення та оцінка)	Оператор та Голова розвідки	Голова розвідки

Дивлячись на те, який рівень несе відповідальність і який рівень виконує різні фази процесу, природно, що це стане колом серед завдань на рівні оператора, перш ніж результат буде передано керівництву. На рисунку 2.3 показана схожа модель, що й на рисунку 2.2, але з описом рівня виконання:

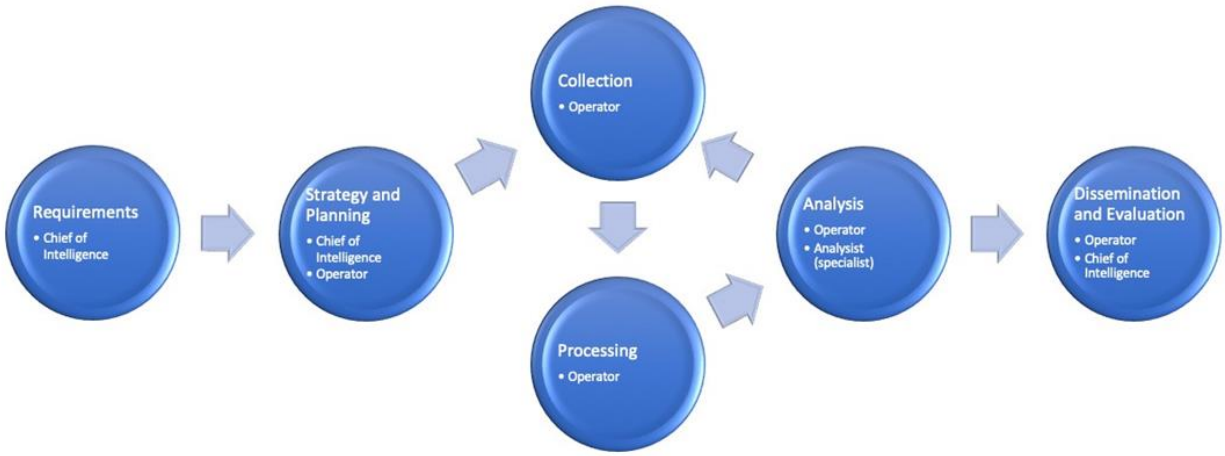


Рисунок 2.3 – Модель з описом рівня виконання

2.2Порівняння моделей

Існують різні моделі, які описують процес дослідження цифрових доказів. Вони можуть виглядати по-різному і можуть бути адаптовані до різних форм цифрового дослідження, але по суті вони містять багато однакових елементів. Процес, описаний у цій дисертації, компілюється тут із кількома іншими моделями, щоб побачити спільні знаменники та відмінності.

Flaglien (2018) представляє криміналістичний процес як процес дослідження цифрових доказів. Криміналістичний процес визначає структуроване дослідження цифрових доказів з будь-якого джерела, яке може зберігати дані. Процес, представлений Флаглієном, має бути універсальним з точки зору того, що його можна використовувати для дослідження будь-яких цифрових доказів,

незалежно від справи, про яку йдеться. Процес складається з п'яти етапів:

• Ідентифікація

Першим кроком у процесі є ідентифікація цифрових доказів і місця їх зберігання.

• Збір

Збереження інформації має відповідати принципам і стандартам, застосовним до збереження цифрових доказів, щоб гарантувати автентичність, цілісність і надійність.

• Обстеження

Під час процесу експертизи зібрані дані слід перевірити та підготувати для подальшого аналізу. Перевірка цифрових доказів часто передбачає реструктуризацію, синтаксичний аналіз і повторну обробку необроблених даних, щоб зробити їх зрозумілими для подальшого аналізу.

• Аналіз

Зібрані дані необхідно проаналізувати, щоб зробити вміст значущим і переконатися, що цифрова інформація може бути використана як доказ

• Презентація

Результат відображається у звіті, де задокументовано ланцюжок поставок і описано всі процеси, інструменти та результати.

Hassan & Hijazi (2018) представляють свою модель п’ятиетапного процесу OSINT:

• Визначення джерел (Identifying the sources) для збору даних

• Збір даних (Harvest the data)

Використання інструментів і методів для збору даних

• Обробка та перевірка даних (Process and verify data)

Оброблення зібраних даних та перевірка невизначених даних з інших джерел

• Аналіз даних (Analyze the data), щоб знайти зв’язки для завершення картини

• Представлення результату (Deliver the results).

Якщо різні моделі вставити в матрицю, на рисунку 2.7 можна побачити значні подібності.

Таблиця 2.2

Порівняння моделей

Процес OSINT	**Криміналістичний процес (Flaglien)**	**Модель OSINT (Hassan&Hijazi)**
Вимоги		
Стратегія та планування		
Збір	Ідентифікація Збір	Визначення джерел Збір даних
Обробка	Обстеження	Обробка та перевірка даних
Аналіз	Аналіз	Аналіз даних
Поширення та оцінка	Презентація	Представлення результату

Висновки до розділу 2

У цьому розділі ми детально розглянули і порівняли різні методології OSINT, що використовуються для збору та аналізу відкритої інформації. Ми ознайомилися з основними принципами і підходами до використання OSINT, а також порівняли методи підвищення ефективності збору, аналізу та використання відкритої інформації для різних цілей, включаючи розвідку, розслідування, моніторинг та прийняття рішень.

Можна побачити, що в двох інших моделях відсутні вхідні значення, які описують те, що шукається. Їхнім моделям також бракує стратегії та планування. Наявність плану перед початком пошуку та забезпечення цифрових доказів дуже важлива, цим не можна нехтувати. Їхні моделі більшою мірою розраховані на виконавця, який буде виконувати практичну частину процесу. Можна зауважити, що як модель процесу дослідження цифрових доказів вони не такі ефективні, оскільки їм бракує вимог, стратегій та планування.

РОЗДІЛ 3. ВИВЧЕННЯ ЗАСТОСУНКІВ OSINT ТА МЕТОДІВ ЇХ РОБОТИ

В цьому розділі ми показуємо та пояснюємо три інструменти OSINT, які використовуються для збору розвідувальних даних з відкритих джерел. Набір інструментів, який ми представляємо тут, є прикладом різних особливостей інструментів OSINT. Ці рішення представляють різні типи OSINT-додатків і дають ширший огляд доступних можливостей OSINT. Діапазон таких рішень зазвичай дуже широкий, від рішень, спрямованих на окремі запити, до потужних OSINT-рішень, що здатні виконувати запити значно більшого масштабу.

Багато широкомасштабних OSINT-рішень створюються на замовлення з великими бюджетами для урядових організацій і великих компаній, і доступ до них обмежений лише власникам цих рішень. Такі рішення використовують автоматизовані процеси, штучний інтелект і передову технологію фільтрації.

Отже, доступ до таких рішень є обмеженим. Проте існує значна кількість загальнодоступних інструментів і ресурсів, які дозволяють здійснювати потужний пошук.

Однак, для майбутнього розвитку OSINT критично важливими є можливості інструментів для процесів пошуку та аналізу даних. Тому важливо вивчати та оцінювати доступні рішення.

Продемонстровані в цій дипломній роботі інструменти доступні будь-якому користувачеві Інтернету. В наступних параграфах ми надаємо окремий опис кожного з інструментів. Кожен інструмент супроводжується фактичною демонстрацією його можливостей. Після цього в розділах 3.4 та 3.5 ми підсумовуємо результати та порівнюємо ці рішення між собою.

3.1 Tinfloleak.com

Найпростішим із рішень, представлених у цій дипломній роботі, є Tinfoleak.com. Tinfoleak.com — це веб-сайт, де можна отримати детальну інформацію про будь-якого користувача Twitter. Це веб-інтерфейс (Рисунок 3.1) для інструменту OSINT «Tinfoleak», автором якого є Вісенте Агілера Діас.

Tinfoleak.com являє собою веб-інтерфейс і не потребує встановлення від користувача. Tinfoleak.com є гарним прикладом веб-рішення OSINT для нашої роботи, демонструючи, як легко можна отримати доступ до запитів OSINT.

Рисунок 3.1 – Веб інтерфейс Tinfoleak

Для отримання пов'язаних з користувачем даних з Twitter за допомогою Tinfoleak, потрібно лише ввести ім'я користувача Twitter, який нас цікавить. Tinfoleak видає детальний звіт про цього користувача на основі запиту. В звіті міститься основна інформація про користувача Twitter, така як його ім'я, зображення, місцезнаходження, кількість підписників, а також інформація про пристрої, операційні системи, програми та соціальні мережі, які він використовує. Звіт також включає місця, які він відвідував, та їх геолокаційні координати, а також надає можливість завантаження всіх зображень, які він опублікував у своєму звіті.

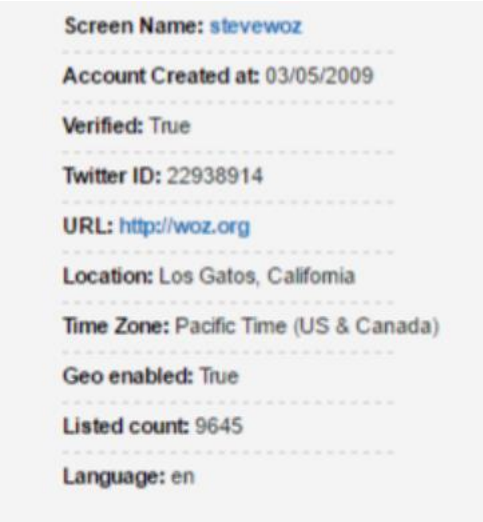


Рисунок 3.2 – Приклад інформації, що знаходить Tinfoleak

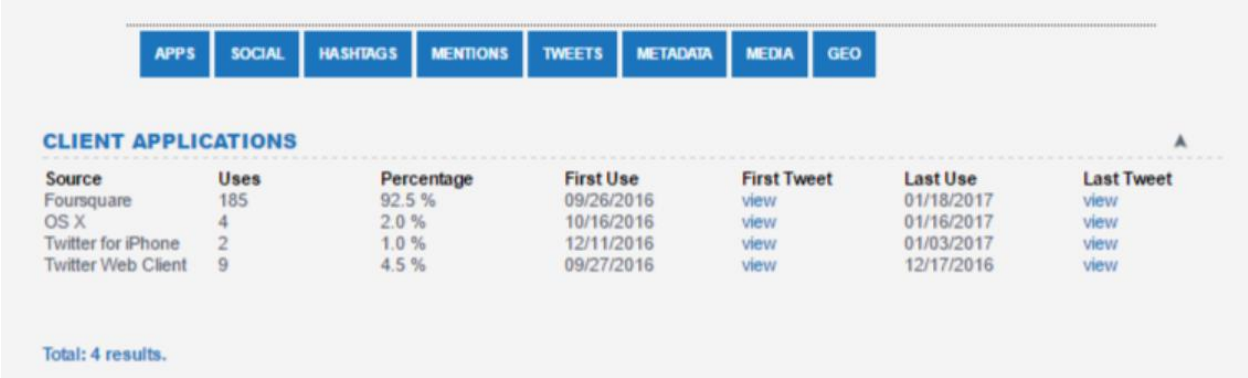


Рисунок 3.3 - Приклад інформації, що знаходить Tinfoleak

Для подальшого дослідження оберемо ціль:

Рисунок 3.4 – Чому б і ні?

Обов’язковою умовою є необхідність вказати власну електронну пошту:

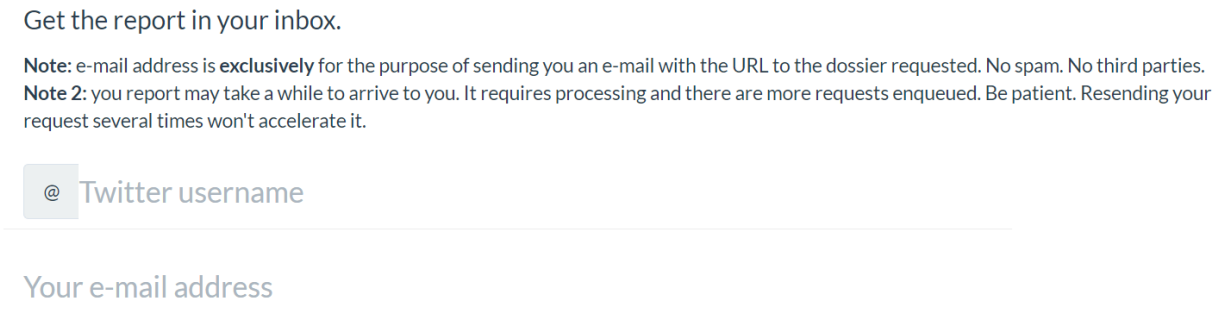


Рисунок 3.5 – Відправка звіту

Ми отримаємо повідомлення, що результат дослідження буде відправлено на нашу пошту:

Довжина звіту Tinfoleak.com залежить від користувача та його активності в Twitter. У нашому випадку обсяг звіту становить приблизно 23 сторінки (формат A4).

Звіт про користувача Twitter, який надає Tinfoleak.com, є досить обширним. У звіті міститься перелік основної інформації (наприклад, ідентифікатор Twitter, дата створення, місцезнаходження, мова) (Рисунок 3.6) разом із клієнтськими програмами, які використовуються для твітів, і соціальними мережами, до яких підключено обліковий запис Twitter:

Рисунок 3.6 – Базова інформація про акаунт

У звіті перераховуються хештеги, які використовувалися в твітах (із зазначенням дати, часу, “вподобайок” та інших подробиць), деталі хештегів, що містять статистику для кожного використаного хештегу, список користувачів, згаданих у твітах, і детальну інформацію про згадування користувачів, у тому числі найпопулярніші згадки користувачів у твітах. Якщо розглянути декілька акаунтів, то можна побачити, що застосунок погано працює з акаунтами, які давно не були активними. Наприклад, при аналізі акаунту @KyivUniversity, в якому останній твіт був 2019 року, в звіті була записана лише основна інформація, в той час як деталі щодо згадуваних користувачів, пристроїв, зображень, тощо повністю відсутня.

На основі звіту можна дізнатися про користувальницьке обладнання та інтерфейси користувача, які використовуються для твітів. Згідно звіту, твіти створюються за допомогою iPhone (Рисунок 3.7).

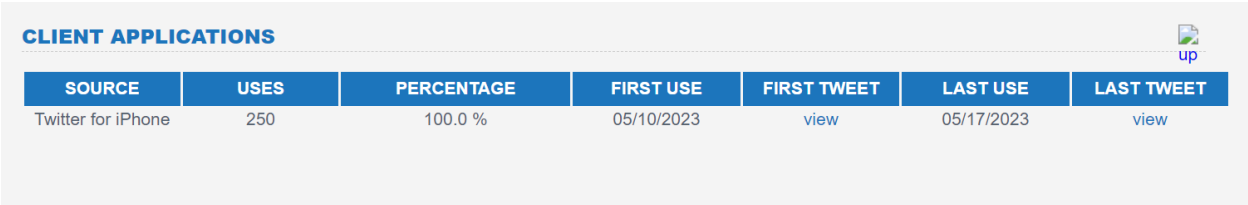


Рисунок 3.7 – Застосунки користувача

Також можна побачити, кого користувач Twitter згадує у своїх твітах. У нашому випадку у твітах згадується приблизно 220 користувачів (Рисунок 3.8).

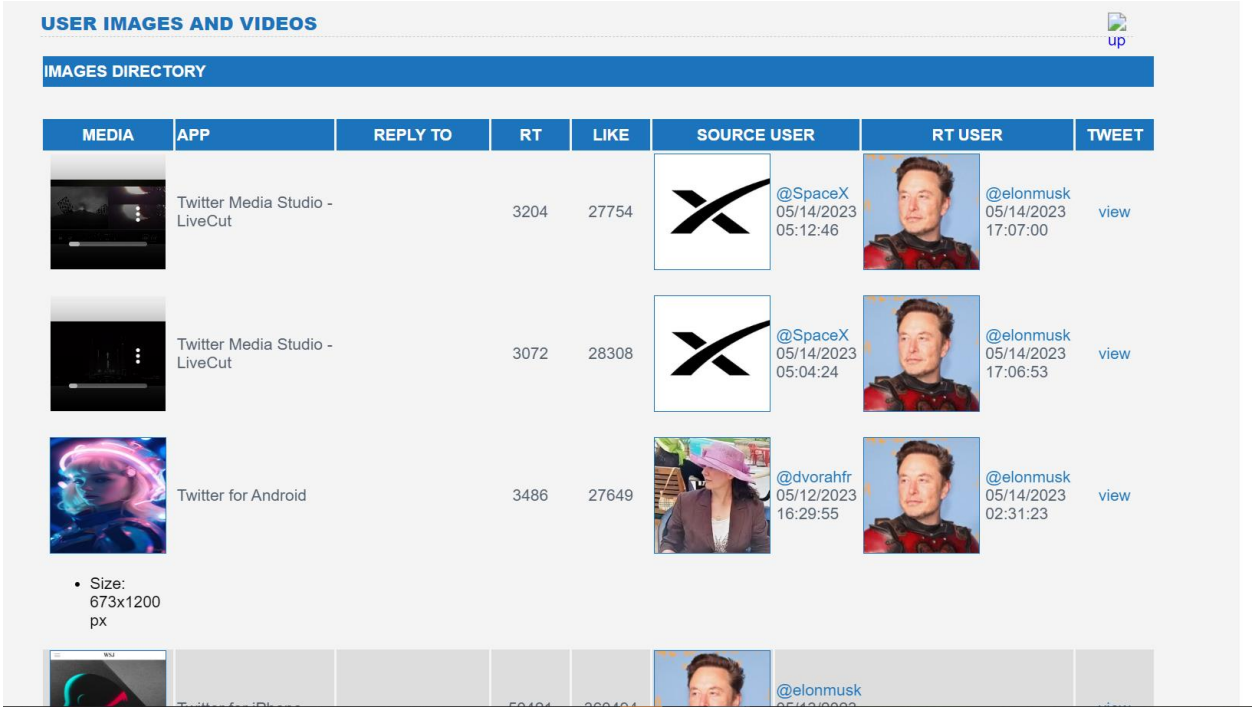
05/10/2023	04:44:01	694	13242	view	@elonmusk			@RubinReport
05/10/2023	04:40:01	1215	8786	view	@TwitterMktg		Twitter HQ	@TwitterMktg
05/10/2023	04:24:04	613	17796	view	@elonmusk			@TheBabylonBee
05/10/2023	04:20:15	199	3567	view	@elonmusk			@DavidSacks
05/10/2023	04:17:47	305	4508	view	@elonmusk			@donlemon

Рисунок 3.8 - Список згадуваних користувачів

USER MENTION DETAIL

DATE (SINCE)	DATE (UNTIL)	RT	LIKE	COUNT	NAME	@MENTION
05/17/2023	05/17/2023	309	4020	1	Andrea Stroppa Claudius Nero's Legion	@andst7
05/17/2023	05/17/2023	135	1216	1	Wittgenstein	@backtolife_2023
05/17/2023	05/17/2023	92	1139	1	Genevieve Roch-Decter, CFA	@GRDecter
05/12/2023	05/17/2023	639	9752	3	Austen Allred	@Austen
05/17/2023	05/17/2023	159	1987	1	Chris Bakke	@ChrisJBakke
05/12/2023	05/17/2023	1698	25538	2	Mike Solana	@micsolana
05/17/2023	05/17/2023	2300	31962	1	Endrina Pavlić	@EPavlic
05/10/2023	05/17/2023	10435	160031	7	Shibetoshi Nakamoto	@BillyM2k
05/13/2023	05/17/2023	3659	68615	3	Sir Doge of the Coin	@dogeofficialceo
05/17/2023	05/17/2023	2300	31962	1	Alex Lewis	@MyDogeCTO
05/17/2023	05/17/2023	2300	31962	1	Jordan Jefferson	@MyDogeCEO
05/17/2023	05/17/2023	2300	31962	1	Aliens	@big3aliens
05/17/2023	05/17/2023	2300	31962	1	Own The Doge	@ownthedoge
05/11/2023	05/17/2023	3080	42237	3	Tesla Owners Silicon Valley	@teslaownersSV
05/17/2023	05/17/2023	2300	31962	1	Earl of FrunkPuppy	@28delayslater
05/11/2023	05/17/2023	156	2974	2	Not Jerome Powell	@alifarhat79
05/10/2023	05/17/2023	1599	14628	3	The Rabbit Hole	@TheRabbitHole84
05/10/2023	05/17/2023	21629	203378	6	KanekoaTheGreat	@KanekoaTheGreat
05/11/2023	05/17/2023	666	10267	3	@goth	@goth600
05/16/2023	05/17/2023	2284	20555	2	CNBC	@CNBC
05/12/2023	05/17/2023	25164	175483	8	Brian Krassenstein	@krassenstein
05/10/2023	05/17/2023	295	4870	2	Paul Graham	@paulg
05/17/2023	05/17/2023	560	9064	2	ShitpostGateway	@ShitpostGate
05/10/2023	05/17/2023	12053	87119	4	David Sacks	@DavidSacks
05/17/2023	05/17/2023	480	4860	1	Aaron Maté	@aaronjmate
05/11/2023	05/16/2023	6366	37296	2	Elon Musk	@elonmusk

Рисунок 3.9 – Більш детальна інформація стосовно згадуваних користувачів



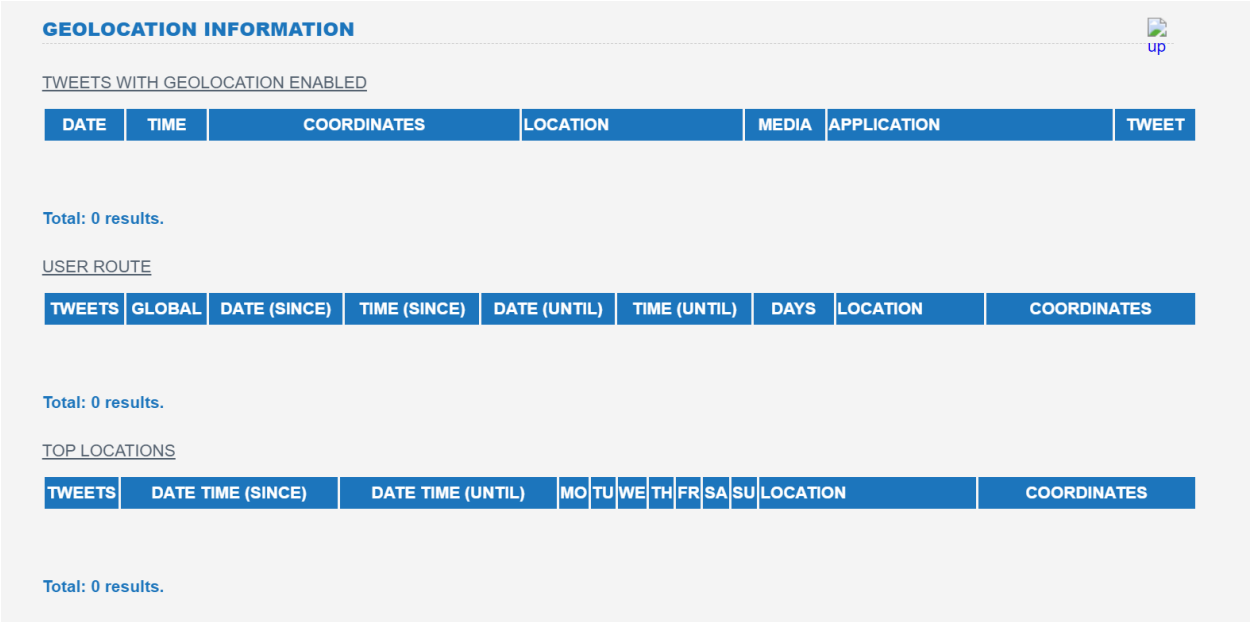
USER IMAGES AND VIDEOS

IMAGES DIRECTORY

MEDIA	APP	REPLY TO	RT	LIKE	SOURCE USER	RT USER	TWEET
	Twitter Media Studio - LiveCut		3204	27754	@SpaceX 05/14/2023 05:12:46	@elonmusk 05/14/2023 17:07:00	view
	Twitter Media Studio - LiveCut		3072	28308	@SpaceX 05/14/2023 05:04:24	@elonmusk 05/14/2023 17:06:53	view
	Twitter for Android		3486	27649	@dvorahfr 05/12/2023 16:29:55	@elonmusk 05/14/2023 02:31:23	view

- Size: 673x1200 px

Рисунок 3.10 – Відео та зображення користувача



GEOLOCATION INFORMATION

TWEETS WITH GEOLOCATION ENABLED

DATE	TIME	COORDINATES	LOCATION	MEDIA	APPLICATION	TWEET

Total: 0 results.

USER ROUTE

TWEETS	GLOBAL	DATE (SINCE)	TIME (SINCE)	DATE (UNTIL)	TIME (UNTIL)	DAYS	LOCATION	COORDINATES

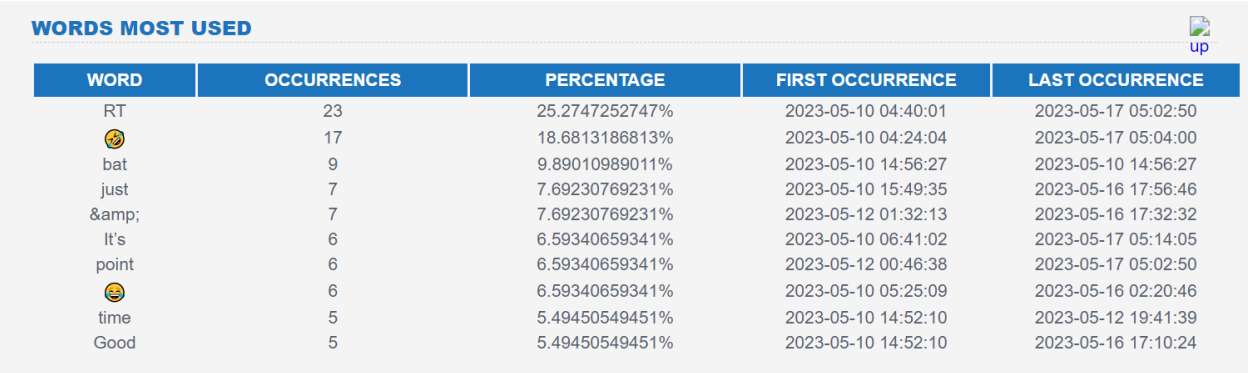
Total: 0 results.

TOP LOCATIONS

TWEETS	DATE TIME (SINCE)	DATE TIME (UNTIL)	MO	TU	WE	TH	FR	SA	SU	LOCATION	COORDINATES

Total: 0 results.

Рисунок 3.11 – Інформація стосовно розташування відсутня, оскільки користувач ні разу не використовував застосунок із ввімкненою геолокацією



WORDS MOST USED

WORD	OCCURRENCES	PERCENTAGE	FIRST OCCURRENCE	LAST OCCURRENCE
RT	23	25.2747252747%	2023-05-10 04:40:01	2023-05-17 05:02:50
🤣	17	18.6813186813%	2023-05-10 04:24:04	2023-05-17 05:04:00
bat	9	9.89010989011%	2023-05-10 14:56:27	2023-05-10 14:56:27
just	7	7.69230769231%	2023-05-10 15:49:35	2023-05-16 17:56:46
&	7	7.69230769231%	2023-05-12 01:32:13	2023-05-16 17:32:32
It's	6	6.59340659341%	2023-05-10 06:41:02	2023-05-17 05:14:05
point	6	6.59340659341%	2023-05-12 00:46:38	2023-05-17 05:02:50
😂	6	6.59340659341%	2023-05-10 05:25:09	2023-05-16 02:20:46
time	5	5.49450549451%	2023-05-10 14:52:10	2023-05-12 19:41:39
Good	5	5.49450549451%	2023-05-10 14:52:10	2023-05-16 17:10:24

Рисунок 3.12 – Слова, що використовуються найчастіше

Таким чином, Tinfoleak дозволяє досить легко ознайомитися із активністю одного середньостатистичного користувача.

3.2 Recon-ng

Recon-ng представляє інший тип інструменту OSINT, ніж Tinfoleak, представлений у попередньому розділі. Порівняно з Tinfoleak, Recon-ng є платформою для більш широкомасштабної розвідки. Recon-ng дозволяє, напр. пошук доменів і соціальних веб-сайтів у пошуках компаній, сховищ, імен користувачів, контактів. Це досить потужне середовище для збору інформації з відкритих веб-джерел.

Recon-ng був розроблений Тімом Томсом (LaNMaSterR53) і дозволяє швидко й ретельно проводити пошуки для збору розвідувальних даних. Інструмент містить вбудовані функції відновлення, взаємодію з базою даних, незалежні модулі, інтерактивну довідку та завершення команд. Це також дозволяє легко керувати ключами API, надаючи доступ до більшої кількості даних. Наприклад, Recon-ng може використовувати Bing, Google, Facebook, Instagram, LinkedIn та інші онлайн-додатки після того, як ключі API подано в інструмент. Завдяки ключам API інструмент надає майже необмежений доступ до відповідних програм. Recon-ng зазвичай називають інструментом для тестувальників на проникнення та хакерів.

Recon-ng включено в Kali Linux і керується через термінал у Linux. Ми запустимо застосунок в Ubuntu (Рисунок 3.13)

Рисунок 3.13 – Користувацький інтерфейс Recon-ng

Наступним кроком ми встановлюємо користувацькі модулі (Рисунок 3.14):

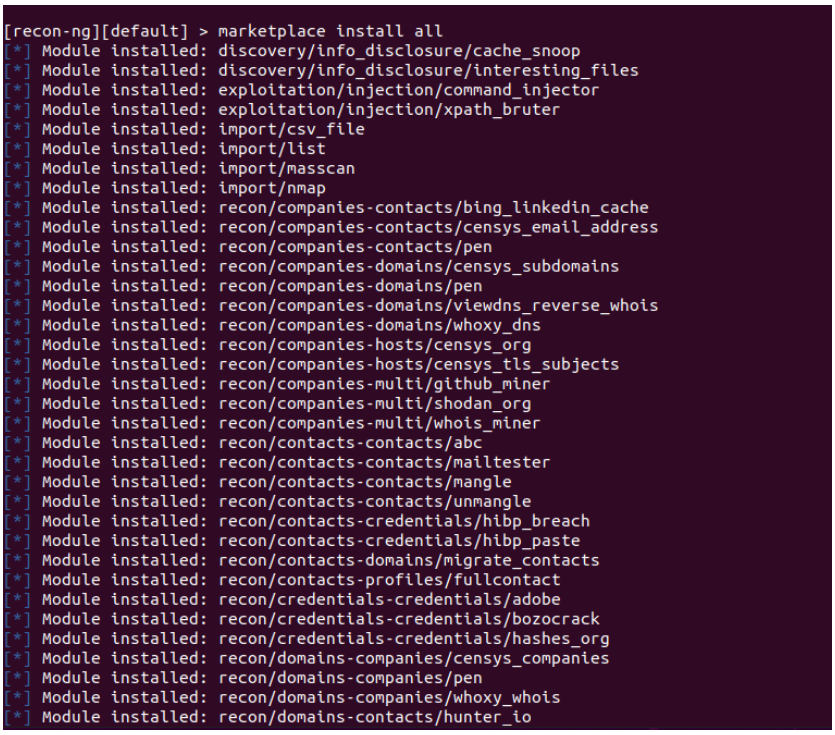


Рисунок 3.14 –Установка модулів

Рисунок 3.15 – Інтерфейс із встановленими модулями

Список вбудованих інструментів розвідки Recon-ng є доволі довгим і містить 79 модулів розвідки (recon), 8 модулів звітності (report), 4 модулі імпорту (import), 2 модулі експлуатації (exploitation) та 2 модулі виявлення (discovery)(Рисунок 3.16, 3.17, 3.18).

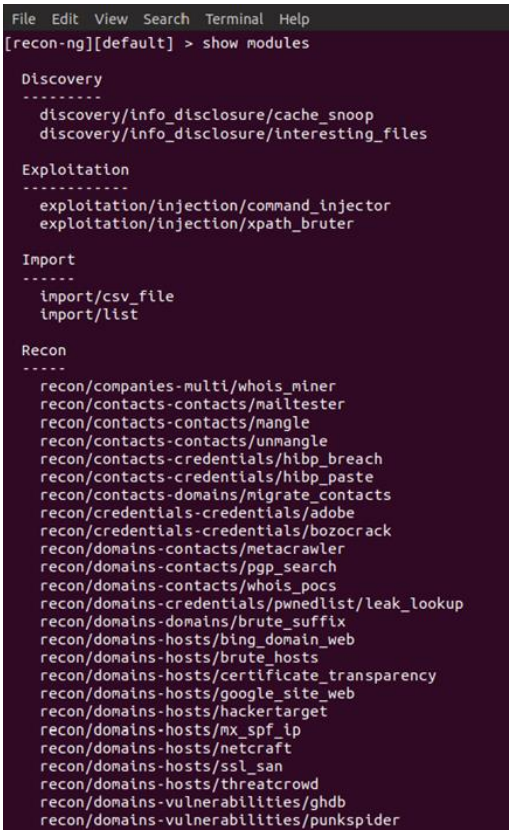


Рисунок 3.16 – Модулі доступні у Recon-ng

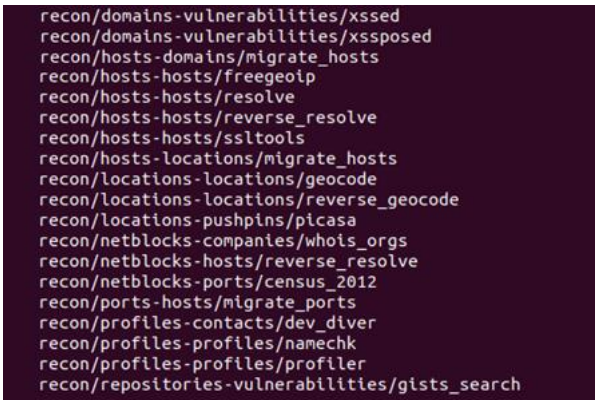


Рисунок 3.17 – Модулі доступні у Recon-ng

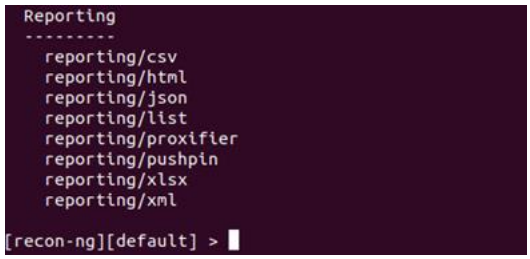


Рисунок 3.18 – Модулі доступні у Recon-ng

Слід зазначити, що Recon-ng є проектом з відкритим кодом. Завдяки мові програмування Python і модульній структурі з незалежними модулями розробникам було легко зробити внесок у проект, але оригінальний розробник Тім Томес все ще підтримує структуру.

Якщо хтось хоче виконати розширену розвідку за допомогою Recon-ng, для цього інструменту знадобляться ключі API. Ключі API дозволять перераховувати всі серверні технології, виявляти вразливості та реалізовані технології з конфігураціями, визначати слабкі місця у фізичній безпеці та шукати облікові дані.

Створюємо workspace (Рисунок 3.19, 3.20):

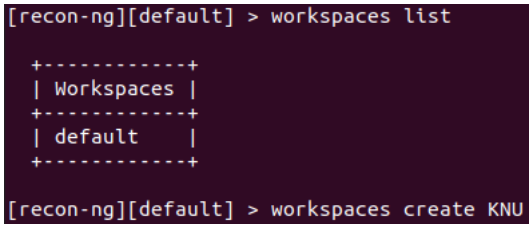


Рисунок 3.19 – Створення workspace

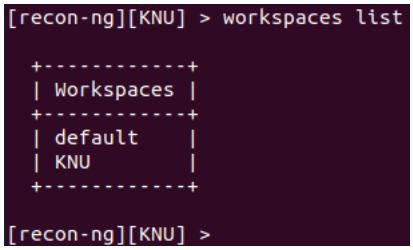


Рисунок 3.20 – Створений workspace

Наступним кроком ми додаємо домейн (Рисунок 3.21):

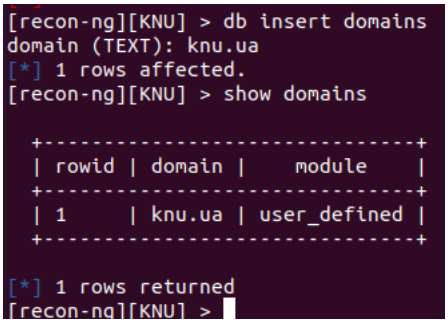


Рисунок 3.21 – Доданий домейн

Як було зазначено раніше, інструмент містить кілька різних модулів для виконання пошуку даних. Демонстрація використання кожного модуля виходить за рамки цієї дипломної роботи, і, як і було сказано, ця демонстрація зосереджена на показі функціонування та результатів наступних модулів, щоб показати приклади використання Recon-ng:

- recon/domains-contacts/whois_pocs
- recon/domains-hosts/bing_domain_web
- recon/domains-hosts/brute_hosts
- recon/domains-hosts/google_site_web
- recon/hosts-hosts/resolve
- recon/hosts-hosts/reverse_resolve
- discovery/info_disclosure/interesting_files

1) Recon/domains-contacts/whois_pocs

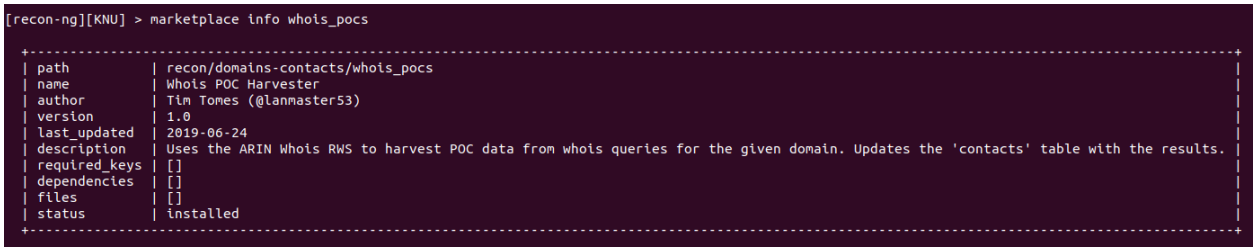


Рисунок 3.21 – Whois_pocs

Перевірка контактної інформації для кожного домену за допомогою whois_pocs. Whois_pocs використовує ARIN Whois RWS для збору даних POC із запитів whois для даного домену. Це оновить таблицю recon-ng «контакти» з результатами. Запуск Whois_pocs для пошуку на knu.ua не знаходить жодного контакту (Рисунок 3.22), тому ми переходимо до наступного запиту.

Рисунок 3.22 – Інформація про whois_pocs та його робота

2) Recon/domains-contacts/bing_domain_web

Рисунок 3.23 – Bing_domain_web

Використовуємо bing_domain_web для збирання хостів із Bing.com за допомогою оператора пошуку site. Це оновить таблицю “hosts” Recon-ng із результатами. У результаті Recon-ng знаходить 60 нових хостів з knu.ua (Рисунок 3.24, 3.25, 3.26).

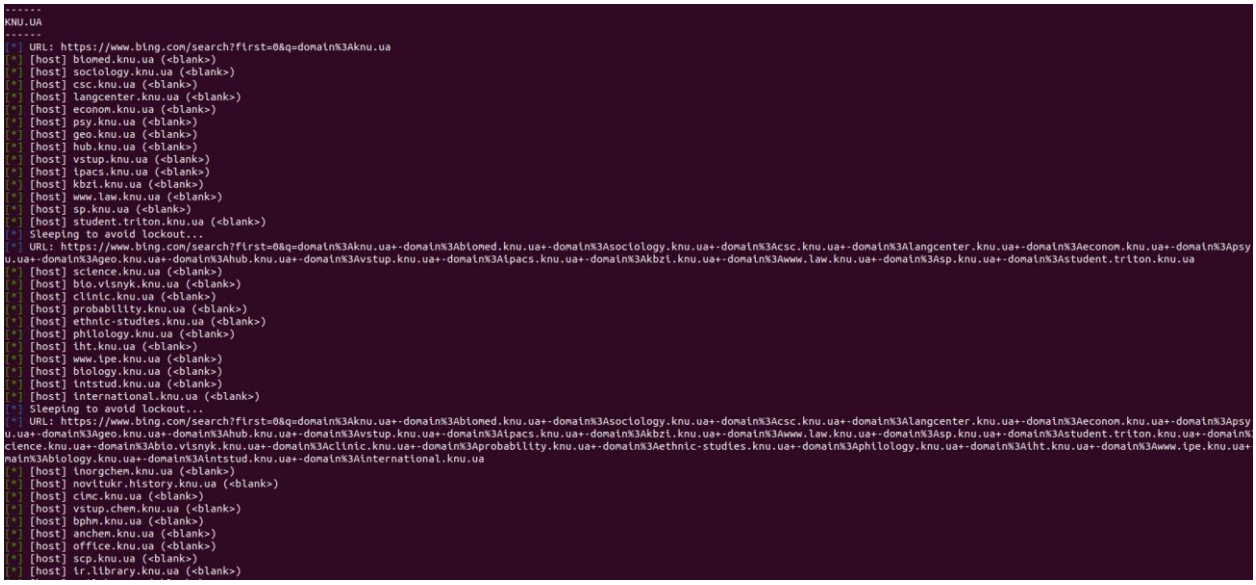


Рисунок 3.24 – Нові хости

Рисунок 3.25 – Нові хости, їх загальна кількість

```
[recon-ng][KNU][bing_domain_web] > back
[recon-ng][KNU] > show hosts

  +-----------------------------------------------------------------------------------------------------------------+
  | rowid |             host             | ip_address | region | country | latitude | longitude |      module     |
  +-----------------------------------------------------------------------------------------------------------------+
  | 1     | biomed.knu.ua                |            |        |         |          |           | bing_domain_web |
  | 2     | sociology.knu.ua             |            |        |         |          |           | bing_domain_web |
  | 3     | csc.knu.ua                   |            |        |         |          |           | bing_domain_web |
  | 4     | langcenter.knu.ua            |            |        |         |          |           | bing_domain_web |
  | 5     | econom.knu.ua                |            |        |         |          |           | bing_domain_web |
  | 6     | psy.knu.ua                   |            |        |         |          |           | bing_domain_web |
  | 7     | geo.knu.ua                   |            |        |         |          |           | bing_domain_web |
  | 8     | hub.knu.ua                   |            |        |         |          |           | bing_domain_web |
  | 9     | vstup.knu.ua                 |            |        |         |          |           | bing_domain_web |
  | 10    | ipacs.knu.ua                 |            |        |         |          |           | bing_domain_web |
  | 11    | kbzi.knu.ua                  |            |        |         |          |           | bing_domain_web |
  | 12    | www.law.knu.ua               |            |        |         |          |           | bing_domain_web |
  | 13    | sp.knu.ua                    |            |        |         |          |           | bing_domain_web |
  | 14    | student.triton.knu.ua        |            |        |         |          |           | bing_domain_web |
  | 15    | science.knu.ua               |            |        |         |          |           | bing_domain_web |
  | 16    | bio.visnyk.knu.ua            |            |        |         |          |           | bing_domain_web |
  | 17    | clinic.knu.ua                |            |        |         |          |           | bing_domain_web |
  | 18    | probability.knu.ua           |            |        |         |          |           | bing_domain_web |
  | 19    | ethnic-studies.knu.ua        |            |        |         |          |           | bing_domain_web |
  | 20    | philology.knu.ua             |            |        |         |          |           | bing_domain_web |
  | 21    | iht.knu.ua                   |            |        |         |          |           | bing_domain_web |
  | 22    | www.ipe.knu.ua               |            |        |         |          |           | bing_domain_web |
  | 23    | biology.knu.ua               |            |        |         |          |           | bing_domain_web |
  | 24    | intstud.knu.ua               |            |        |         |          |           | bing_domain_web |
  | 25    | international.knu.ua         |            |        |         |          |           | bing_domain_web |
  | 26    | inorgchem.knu.ua             |            |        |         |          |           | bing_domain_web |
  | 27    | novitukr.history.knu.ua      |            |        |         |          |           | bing_domain_web |
  | 28    | cimc.knu.ua                  |            |        |         |          |           | bing_domain_web |
```

Рисунок 3.26 – Нові хости у таблиці “hosts”

3) Recon/domain-hosts/brute_hosts

```
[recon-ng][KNU] > modules load brute_hosts
[recon-ng][KNU][brute_hosts] > info

      Name: DNS Hostname Brute Forcer
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Brute forces host names using DNS. Updates the 'hosts' table with the results.

Options:
  Name      Current Value                            Required  Description
  --------  -------------                            --------  -----------
  SOURCE    default                                  yes       source of input (see 'show info' for details)
  WORDLIST  /home/arthur/.recon-ng/data/hostnames.txt  yes       path to hostname wordlist

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][KNU][brute_hosts] >
```

Рисунок 3.27 – Brute_hosts

Brute_hosts можна використовувати для примусового пошуку імен хостів за допомогою DNS. Це оновить таблицю «hosts» Recon-ng із результатами. У результаті він знаходить 44 нових хоста, загальний результат тепер становить 104 знайдені хости (Рисунок 3.28, 3.29).

```
[*] xmail.knu.ua => Request timed out.
[*] xmail.knu.ua => No record found.
[*] wwwdev.knu.ua => No record found.
[*] x-ray.knu.ua => No record found.
[*] wyoming.knu.ua => No record found.
[*] xi.knu.ua => No record found.
[*] wwwchat.knu.ua => No record found.
[*] wwwmail.knu.ua => No record found.
[*] xlogan.knu.ua => No record found.
[*] xml.knu.ua => No record found.
[*] yellow.knu.ua => No record found.
[*] x.knu.ua => No record found.
[*] y.knu.ua => No record found.
[*] wy.knu.ua => No record found.
[*] ye.knu.ua => No record found.
[*] yankee.knu.ua => No record found.
[*] young.knu.ua => No record found.
[*] yt.knu.ua => No record found.
[*] yu.knu.ua => No record found.
[*] xp.knu.ua => No record found.
[*] z-log.knu.ua => No record found.
[*] za.knu.ua => No record found.
[*] zera.knu.ua => No record found.
[*] z.knu.ua => No record found.
[*] zm.knu.ua => No record found.
[*] zeus.knu.ua => No record found.
[*] zebra.knu.ua => No record found.
[*] zw.knu.ua => No record found.
[*] zulu.knu.ua => No record found.
[*] zlog.knu.ua => No record found.

-------
SUMMARY
-------
[*] 60 total (44 new) hosts found.
```

Рисунок 3.28 – Результат пошуку через brute_hosts

```
| 73  | http.knu.ua                | 91.202.128.122 |  |  |  |  | brute_hosts |
| 74  | noc.knu.ua                 |                |  |  |  |  | brute_hosts |
| 75  | in.knu.ua                  |                |  |  |  |  | brute_hosts |
| 76  | in.knu.ua                  | 91.202.128.111 |  |  |  |  | brute_hosts |
| 77  | international.knu.ua       | 91.202.128.71  |  |  |  |  | brute_hosts |
| 78  | jobs.knu.ua                |                |  |  |  |  | brute_hosts |
| 79  | jobs.knu.ua                | 91.202.128.71  |  |  |  |  | brute_hosts |
| 80  | mail.knu.ua                | 91.202.128.59  |  |  |  |  | brute_hosts |
| 81  | new.knu.ua                 |                |  |  |  |  | brute_hosts |
| 82  | new.knu.ua                 | 91.202.128.71  |  |  |  |  | brute_hosts |
| 83  | nms.knu.ua                 | 91.202.128.111 |  |  |  |  | brute_hosts |
| 84  | ns.knu.ua                  | 91.202.128.100 |  |  |  |  | brute_hosts |
| 85  | ns1.knu.ua                 | 91.202.129.100 |  |  |  |  | brute_hosts |
| 86  | ns3.knu.ua                 | 91.202.128.53  |  |  |  |  | brute_hosts |
| 87  | ns2.knu.ua                 | 3.72.133.105   |  |  |  |  | brute_hosts |
| 88  | office.knu.ua              | 91.202.128.59  |  |  |  |  | brute_hosts |
| 89  | online.knu.ua              | 91.202.128.139 |  |  |  |  | brute_hosts |
| 90  | ideas.knu.ua               |                |  |  |  |  | brute_hosts |
| 91  | radio.knu.ua               |                |  |  |  |  | brute_hosts |
| 92  | radio.knu.ua               | 91.202.128.102 |  |  |  |  | brute_hosts |
| 93  | rd.knu.ua                  | 91.202.128.62  |  |  |  |  | brute_hosts |
| 94  | ss.knu.ua                  |                |  |  |  |  | brute_hosts |
| 95  | ss.knu.ua                  | 91.202.128.71  |  |  |  |  | brute_hosts |
| 96  | ssl.knu.ua                 |                |  |  |  |  | brute_hosts |
| 97  | ssl.knu.ua                 | 91.202.128.71  |  |  |  |  | brute_hosts |
| 98  | staff.knu.ua               |                |  |  |  |  | brute_hosts |
| 99  | staff.knu.ua               | 91.202.128.71  |  |  |  |  | brute_hosts |
| 100 | hp.esoc.knu.ua             |                |  |  |  |  | brute_hosts |
| 101 | store.knu.ua               |                |  |  |  |  | brute_hosts |
| 102 | hpo.esoc.knu.ua            |                |  |  |  |  | brute_hosts |
| 103 | haproxy-omega.esoc.knu.ua  |                |  |  |  |  | brute_hosts |
| 104 | store.knu.ua               | 91.202.128.62  |  |  |  |  | brute_hosts |
+-----+----------------------------+----------------+--+--+--+--+-------------+

[*] 104 rows returned
```

Рисунок 3.29 – Результат пошуку у таблиці “hosts”

4) Recon/domain-hosts/google_site_web

```
[recon-ng][KNU] > modules load google_site_web
[recon-ng][KNU][google_site_web] > info

      Name: Google Hostname Enumerator
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with
  the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'show info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs
```

Рисунок 3.30 – Google_site_web

Google_site_web дозволяє перевіряти більше хостів за допомогою Google.com за допомогою оператора пошуку «site». Він оновлює таблицю Recon-ng “hosts” результатами. Google_site_web знаходить 116 результатів, серед них 74 - нові хости, які не були враховані попередніми запитами (Рисунок 3.31).

```
.knu.ua -site:navigator.knu.ua -site:philology.knu.ua -site:metphys.knu.ua -site:studia-linguistica.knu.ua -site:psy.knu.ua -site:law.knu.ua -site:visnyk.law
.knu.ua -site:clinic.knu.ua -site:conf.chem.knu.ua -site:pst.knu.ua -site:www.csc.knu.ua -site:langcenter.knu.ua -site:geo.knu.ua -site:intstud.knu.ua -site:
inorgchem.knu.ua -site:ce.knu.ua -site:omc.knu.ua -site:theory.phys.knu.ua -site:bill.knu.ua -site:txim.history.knu.ua -site:milstand.knu.ua -site:rex.knu.ua
 -site:psyservice.knu.ua -site:sociology.knu.ua -site:shz-st.knu.ua -site:fkgrt.knu.ua -site:www.americanstudies.history.knu.ua -site:pedvisnyk.knu.ua -site:
mol.phys.knu.ua -site:mil.knu.ua -site:phys.knu.ua -site:miljournals.knu.ua -site:dole.fit.knu.ua -site:eustudies.history.knu.ua -site:www.journ.knu.ua -site
:ais.knu.ua -site:mova.knu.ua -site:www.ist.fit.knu.ua -site:mobility.knu.ua -site:material.phys.knu.ua -site:semantics.knu.ua -site:chasopys.history.knu.ua
-site:theory.law.knu.ua -site:orgchem.knu.ua -site:nitd.knu.ua -site:ce-europe.knu.ua -site:visnyk.soch.robota.knu.ua -site:help-rectorat.knu.ua -site:vkslaw
.knu.ua -site:elphys.rex.knu.ua -site:student.triton.knu.ua -site:novitukr.history.knu.ua -site:international.knu.ua -site:ecoimpact.knu.ua -site:archives.kn
u.ua -site:ir.library.knu.ua -site:visnyk.history.knu.ua -site:ukr.movoznavstvo.knu.ua -site:gl.vlabs.knu.ua -site:www.ipe.knu.ua -site:scp.knu.ua -site:hydr
o-chemistry-ecology.knu.ua -site:vybory2020.knu.ua -site:rebuild.knu.ua -site:www.law.knu.ua -site:ktm.journ.knu.ua -site:justice.law.knu.ua -site:ip.law.knu
.ua -site:economic.law.knu.ua -site:art.history.knu.ua -site:gen.phys.knu.ua
[*] No New Subdomains Found on the Current Page. Jumping to Result 9401.
[*] Searching Google for: site:knu.ua -site:mechmat.knu.ua -site:spo.knu.ua -site:infopacket.knu.ua -site:www.phys.knu.ua -site:bphm.knu.ua -site:kiis.knu.ua
 -site:pcsits.knu.ua -site:scc.knu.ua -site:csc.knu.ua -site:econom.knu.ua -site:zvo.knu.ua -site:naukaprosto.knu.ua -site:labs.journ.knu.ua -site:chem.knu.u
a -site:ritm.knu.ua -site:geophys.knu.ua -site:ipsycho.knu.ua -site:staff.knu.ua -site:microbimconf.knu.ua -site:physgeo.knu.ua -site:upml.knu.ua -site:anche
m.knu.ua -site:vstup.knu.ua -site:ists.knu.ua -site:jobs.knu.ua -site:sp.knu.ua -site:science.knu.ua -site:hub.knu.ua -site:biomed.knu.ua -site:kbzi.knu.ua -
site:applaw.knu.ua -site:fit.knu.ua -site:generalmath.knu.ua -site:www.space.knu.ua -site:journ.knu.ua -site:zpv.knu.ua -site:iss.csc.knu.ua -site:bpsy.knu.u
a -site:physchem.knu.ua -site:visnyk-geo.knu.ua -site:studmisto.knu.ua -site:alumni.law.knu.ua -site:probability.knu.ua -site:iht.knu.ua -site:visnykknuskhid
.knu.ua -site:navigator.knu.ua -site:philology.knu.ua -site:metphys.knu.ua -site:studia-linguistica.knu.ua -site:psy.knu.ua -site:law.knu.ua -site:visnyk.law
.knu.ua -site:clinic.knu.ua -site:conf.chem.knu.ua -site:pst.knu.ua -site:www.csc.knu.ua -site:langcenter.knu.ua -site:geo.knu.ua -site:intstud.knu.ua -site:
inorgchem.knu.ua -site:ce.knu.ua -site:omc.knu.ua -site:theory.phys.knu.ua -site:bill.knu.ua -site:txim.history.knu.ua -site:milstand.knu.ua -site:rex.knu.ua
 -site:psyservice.knu.ua -site:sociology.knu.ua -site:shz-st.knu.ua -site:fkgrt.knu.ua -site:www.americanstudies.history.knu.ua -site:pedvisnyk.knu.ua -site:
mol.phys.knu.ua -site:mil.knu.ua -site:phys.knu.ua -site:miljournals.knu.ua -site:dole.fit.knu.ua -site:eustudies.history.knu.ua -site:www.journ.knu.ua -site
:ais.knu.ua -site:mova.knu.ua -site:www.ist.fit.knu.ua -site:mobility.knu.ua -site:material.phys.knu.ua -site:semantics.knu.ua -site:chasopys.history.knu.ua
-site:theory.law.knu.ua -site:orgchem.knu.ua -site:nitd.knu.ua -site:ce-europe.knu.ua -site:visnyk.soch.robota.knu.ua -site:help-rectorat.knu.ua -site:vkslaw
.knu.ua -site:elphys.rex.knu.ua -site:student.triton.knu.ua -site:novitukr.history.knu.ua -site:international.knu.ua -site:ecoimpact.knu.ua -site:archives.kn
u.ua -site:ir.library.knu.ua -site:visnyk.history.knu.ua -site:ukr.movoznavstvo.knu.ua -site:gl.vlabs.knu.ua -site:www.ipe.knu.ua -site:scp.knu.ua -site:hydr
o-chemistry-ecology.knu.ua -site:vybory2020.knu.ua -site:rebuild.knu.ua -site:www.law.knu.ua -site:ktm.journ.knu.ua -site:justice.law.knu.ua -site:ip.law.knu
.ua -site:economic.law.knu.ua -site:art.history.knu.ua -site:gen.phys.knu.ua
[!] Google CAPTCHA triggered. No bypass available.

-------
SUMMARY
-------
[*] 116 total (74 new) hosts found.
```

Рисунок 3.31 – 74 нові хости в результаті пошуку

5) Recon/domain-hosts/resolve and reverse_resolve

```
[recon-ng][KNU] > modules load recon/hosts-hosts/resolve
[recon-ng][KNU][resolve] > info

      Name: Hostname Resolver
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Resolves the IP address for a host. Updates the 'hosts' table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'show info' for details)

Source Options:
  default        SELECT DISTINCT host FROM hosts WHERE host IS NOT NULL AND ip_address IS NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

Comments:
  * Note: Nameserver must be in IP form.
```

Рисунок 3.32 – Resolve

Recon/hosts-hosts/resolve знаходить IP-адреси для хостів і оновлює таблицю Reconng «hosts» результатами. Запуск Recon/hosts-hosts/resolve з доменом knu.ua не знаходить нових хостів, але видає інформацію про IP (Рисунок 3.33).

```
[recon-ng][KNU][resolve] > run
[*] biomed.knu.ua => 185.104.45.66
[*] sociology.knu.ua => 91.202.128.71
[*] csc.knu.ua => 91.202.128.71
[*] langcenter.knu.ua => 91.202.128.71
[*] econom.knu.ua => 91.202.128.71
[*] psy.knu.ua => 91.202.128.71
[*] geo.knu.ua => 91.202.128.71
[*] hub.knu.ua => 91.202.128.59
[*] vstup.knu.ua => 91.202.128.71
[*] ipacs.knu.ua => 91.202.128.62
[*] kbzi.knu.ua => 91.202.128.71
[*] www.law.knu.ua => 91.202.128.71
[*] sp.knu.ua => 91.202.128.71
[*] student.triton.knu.ua => 91.202.128.59
[*] science.knu.ua => 91.202.128.71
[*] bio.visnyk.knu.ua => 91.202.128.71
[*] clinic.knu.ua => 91.202.128.71
[*] probability.knu.ua => 91.202.128.71
[*] ethnic-studies.knu.ua => 91.202.128.71
[*] philology.knu.ua => 91.202.128.71
[*] iht.knu.ua => 91.202.128.71
[*] www.ipe.knu.ua => 91.202.128.71
[*] biology.knu.ua => 185.104.45.66
[*] intstud.knu.ua => 91.202.128.71
[*] international.knu.ua => 91.202.128.71
[*] inorgchem.knu.ua => 91.202.129.108
[*] novitukr.history.knu.ua => 91.202.128.71
[*] cimc.knu.ua => 91.202.128.71
[*] vstup.chem.knu.ua => 91.202.129.108
[*] bphm.knu.ua => 91.202.128.71
[*] anchem.knu.ua => 91.202.129.108
[*] office.knu.ua => 91.202.128.59
```

Рисунок 3.33 – Результати пошуку з resolve

Recon/hosts-hosts/reverse_resolve (Рисунок 3.34) можна використовувати для здійснення зворотного пошуку IP-адрес для кожної IP-адреси для визначення імені хоста. Запит оновлює таблицю «hosts» Recon-ng результатами. Функція reverse_resolve у цій демонстрації дозволила 17 нових імен хостів (Рисунок 3.35)

```
[recon-ng][KNU] > modules load recon/hosts-hosts/reverse_resolve
[recon-ng][KNU][reverse_resolve] > info

      Name: Reverse Resolver
    Author: John Babio (@3vi1john), @vulp1n3, and Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Conducts a reverse lookup for each IP address to resolve the hostname. Updates the 'hosts' table
  with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'show info' for details)

Source Options:
  default        SELECT DISTINCT ip_address FROM hosts WHERE ip_address IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs
```

Рисунок 3.34 – Reverse_resolve

```
[recon-ng][KNU][reverse_resolve] > run
[*] [host] web108.ukraine.com.ua (185.104.45.66)
[*] [host] nuke.univ.kiev.ua (91.202.128.71)
[*] [host] spark.knu.ua (91.202.128.59)
[*] [host] evs.knu.ua (91.202.128.62)
[*] [host] chem.univ.kiev.ua (91.202.129.108)
[*] [host] waw07s06-in-f19.1e100.net (142.250.203.147)
[*] [host] ns.univ.kiev.ua (91.202.128.100)
[*] 91.202.128.155 => No record found.
[*] [host] esoc.knu.ua (91.202.128.40)
[*] [host] http2.univ.kiev.ua (91.202.128.122)
[*] [host] noc.univ.kiev.ua (91.202.128.111)
[*] [host] ns2.univ.kiev.ua (91.202.129.100)
[*] [host] library.univ.kiev.ua (91.202.128.53)
[*] [host] ec2-3-72-133-105.eu-central-1.compute.amazonaws.com (3.72.133.105)
[*] 91.202.128.139 => No record found.
[*] [host] ce.univ.kiev.ua (91.202.128.102)
[*] [host] web400.default-host.net (185.68.16.180)
[*] [host] bill.univ.kiev.ua (91.202.129.216)
[*] [host] 233.168.117.34.bc.googleusercontent.com (34.117.168.233)
[*] [host] virgo.univ.kiev.ua (91.202.128.58)

-------
SUMMARY
-------
[*] 18 total (17 new) hosts found.
```

Рисунок 3.35 – Результат пошуку через reverse_resolve

Загальний результат після цих п’яти запитів на хости knu.ua та IP-адреси становить 195 об’єктів (Рисунок 3.36). Щоб просунутися вперед, щоб знайти, наприклад, інформацію про геолокацію для зібраних хостів, знадобляться деякі ключі API, тому ми завершимо демонстрацію застосунку тут. Ця демонстрація є достатньою, щоб показати, як керувати Recon-ng і використовувати його для збору інформації.

```
  | 165 | elphys.rex.knu.ua                                | 91.202.128.71   |  |  |  |  | google_site_web |
  | 166 | ecoimpact.knu.ua                                 | 91.202.128.71   |  |  |  |  | google_site_web |
  | 167 | archives.knu.ua                                  | 91.202.128.71   |  |  |  |  | google_site_web |
  | 168 | visnyk.history.knu.ua                            | 142.250.203.147 |  |  |  |  | google_site_web |
  | 169 | ukr.movoznavstvo.knu.ua                          | 91.202.128.71   |  |  |  |  | google_site_web |
  | 170 | gl.vlabs.knu.ua                                  | 91.202.128.58   |  |  |  |  | google_site_web |
  | 171 | vybory2020.knu.ua                                | 91.202.128.71   |  |  |  |  | google_site_web |
  | 172 | rebuild.knu.ua                                   | 91.202.128.71   |  |  |  |  | google_site_web |
  | 173 | ktm.journ.knu.ua                                 | 91.202.128.71   |  |  |  |  | google_site_web |
  | 174 | justice.law.knu.ua                               | 142.250.203.147 |  |  |  |  | google_site_web |
  | 175 | ip.law.knu.ua                                    | 142.250.203.147 |  |  |  |  | google_site_web |
  | 176 | economic.law.knu.ua                              | 142.250.203.147 |  |  |  |  | google_site_web |
  | 177 | art.history.knu.ua                               | 91.202.128.71   |  |  |  |  | google_site_web |
  | 178 | gen.phys.knu.ua                                  | 91.202.128.71   |  |  |  |  | google_site_web |
  | 179 | web108.ukraine.com.ua                            | 185.104.45.66   |  |  |  |  | reverse_resolve |
  | 180 | nuke.univ.kiev.ua                                | 91.202.128.71   |  |  |  |  | reverse_resolve |
  | 181 | evs.knu.ua                                       | 91.202.128.62   |  |  |  |  | reverse_resolve |
  | 182 | chem.univ.kiev.ua                                | 91.202.129.108  |  |  |  |  | reverse_resolve |
  | 183 | waw07s06-in-f19.1e100.net                        | 142.250.203.147 |  |  |  |  | reverse_resolve |
  | 184 | ns.univ.kiev.ua                                  | 91.202.128.100  |  |  |  |  | reverse_resolve |
  | 185 | esoc.knu.ua                                      | 91.202.128.40   |  |  |  |  | reverse_resolve |
  | 186 | http2.univ.kiev.ua                               | 91.202.128.122  |  |  |  |  | reverse_resolve |
  | 187 | noc.univ.kiev.ua                                 | 91.202.128.111  |  |  |  |  | reverse_resolve |
  | 188 | ns2.univ.kiev.ua                                 | 91.202.129.100  |  |  |  |  | reverse_resolve |
  | 189 | library.univ.kiev.ua                             | 91.202.128.53   |  |  |  |  | reverse_resolve |
  | 190 | ec2-3-72-133-105.eu-central-1.compute.amazonaws.com | 3.72.133.105 |  |  |  |  | reverse_resolve |
  | 191 | ce.univ.kiev.ua                                  | 91.202.128.102  |  |  |  |  | reverse_resolve |
  | 192 | web400.default-host.net                          | 185.68.16.180   |  |  |  |  | reverse_resolve |
  | 193 | bill.univ.kiev.ua                                | 91.202.129.216  |  |  |  |  | reverse_resolve |
  | 194 | 233.168.117.34.bc.googleusercontent.com          | 34.117.168.233  |  |  |  |  | reverse_resolve |
  | 195 | virgo.univ.kiev.ua                               | 91.202.128.58   |  |  |  |  | reverse_resolve |
  +-----+--------------------------------------------------+-----------------+--+--+--+--+-----------------+

[*] 195 rows returned
[recon-ng][KNU] >
```

Рисунок 3.36 – Фінальний результат пошуків

6) Recon/domain-hosts/interesting_files

```
[recon-ng][KNU] > modules load interesting_files
[recon-ng][KNU][interesting_files] > info

      Name: Interesting File Finder
    Author: Tim Tomes (@lanmaster53), thrapt (thrapt@gmail.com), Jay Turla (@shipcod3), and Mark Jeffery
   Version: 1.2

Description:
  Checks hosts for interesting files in predictable locations.

Options:
  Name      Current Value                                          Required  Description
  --------  -------------                                          --------  -----------
  CSV_FILE  /home/arthur/.recon-ng/data/interesting_files_verify.csv  yes       custom filename map
  DOWNLOAD  True                                                   yes       download discovered files
  PORT      80                                                     yes       request port
  PROTOCOL  http                                                   yes       request protocol
  SOURCE    default                                                yes       source of input (see 'show info' for details)

Source Options:
  default       SELECT DISTINCT host FROM hosts WHERE host IS NOT NULL
  <string>      string representing a single input
  <path>        path to a file containing a list of inputs
  query <sql>   database query returning one column of inputs

Comments:
  * Files: robots.txt, sitemap.xml, sitemap.xml.gz, crossdomain.xml, phpinfo.php, test.php, elmah.axd,
  server-status, jmx-console/, admin-console/, web-console/
  * CSV Default: /home/arthur/.recon-ng/data/interesting_files_verify.csv
  * Google Dorks:
    - inurl:robots.txt ext:txt
    - inurl:elmah.axd ext:axd intitle:"Error log for"
    - inurl:server-status "Apache Status"
```

Рисунок 3.37 – Interesting_files

Щоб навести ще один останній приклад Recon-ng, ця демонстрація також показує, як перевірити будь-які пов’язані “цікаві” файли. Модуль «interesting_files» із Recon-ng перевіряє хости на наявність “цікавих” файлів у передбачуваних місцях (Рисунок 3.38). Файли можуть бути у форматі robots.txt, sitemap.xml, sitemap.xml.gz, crossdomain.xml, phpinfo.php, test.php, elmah.axd. стан сервера, консоль jmx/, консоль адміністратора/, веб-консоль/. У результаті Recon-ng знаходить 156 “цікавих” файлів.

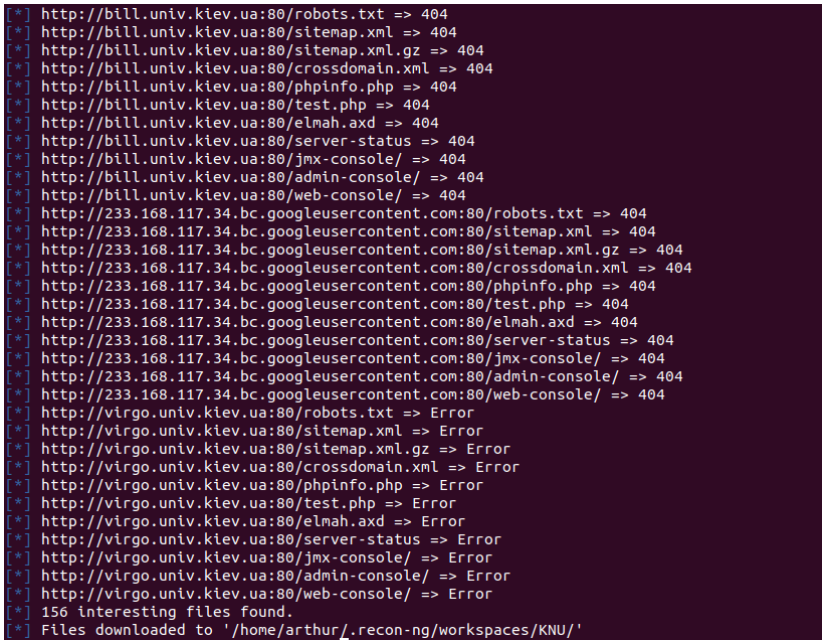


Рисунок 3.38 – Пошук “цікавих” файлів

3.3 Maltego CE

Maltego CE є найдосконалішим рішенням із цих трьох OSINT-додатків, принаймні для представлення результатів. Maltego CE забезпечує найбільш наочну інтерпретацію результатів і показує зв’язки між будь-якими знайденими примірниками. Це також найдосконаліший із цих трьох інструментів у тому сенсі, що він виконує кілька запитів за один пошук.

Встановлення Maltego CE також просте. Все, що потрібно, це зареєструватися у версії спільноти Maltego, завантажити відповідний пакет програмного забезпечення та запустити інсталяцію. Реєстрація та програмні пакети доступні на домашніх сторінках Paterva Maltego CE (20). Maltego CE можна завантажити практично на будь-який комп’ютер, оскільки він працює на Windows, Mac або Linux.

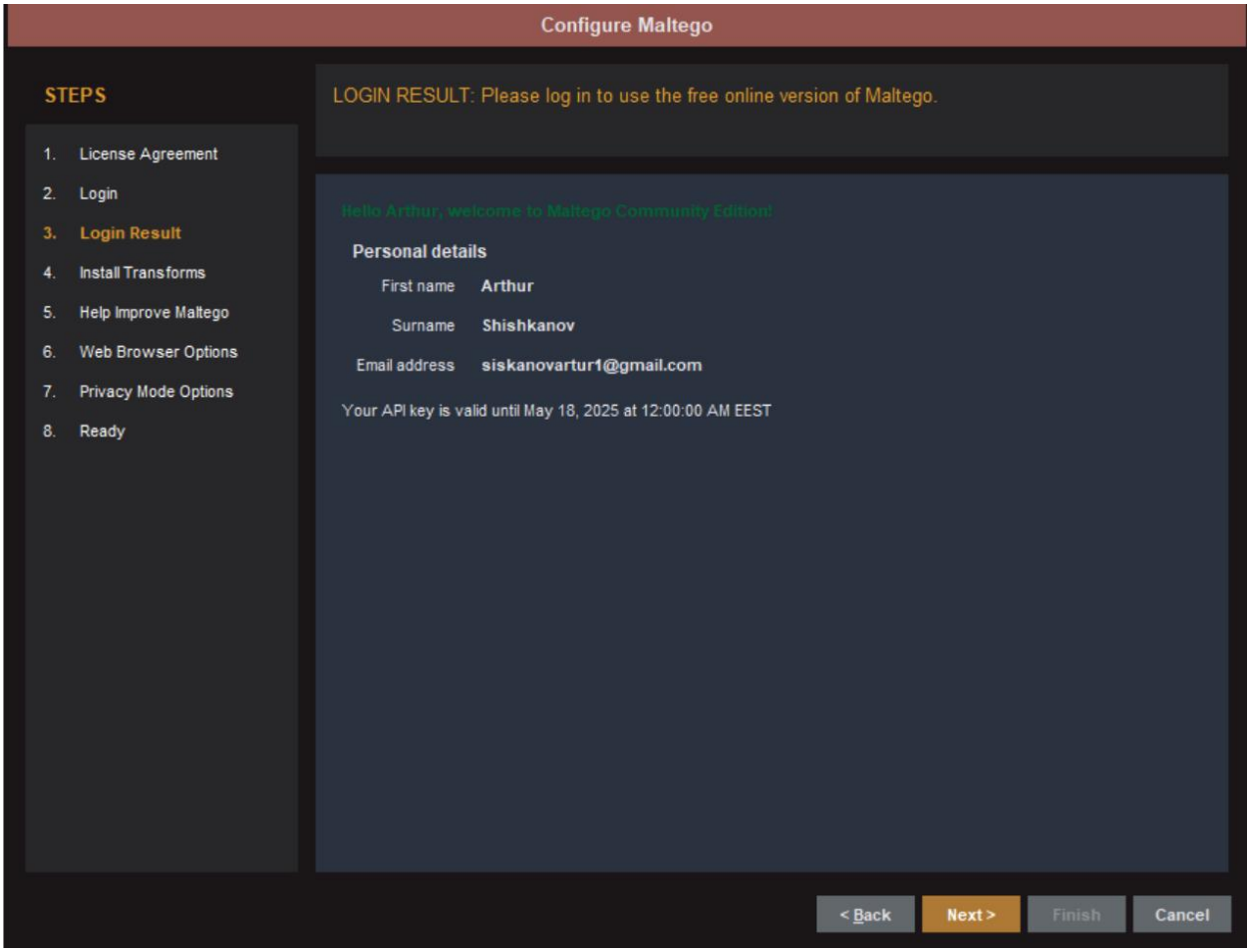


Рисунок 3.39 – Перший запуск Maltego

Також дозволяється обрати режим приватності (Рисунок 3.40):

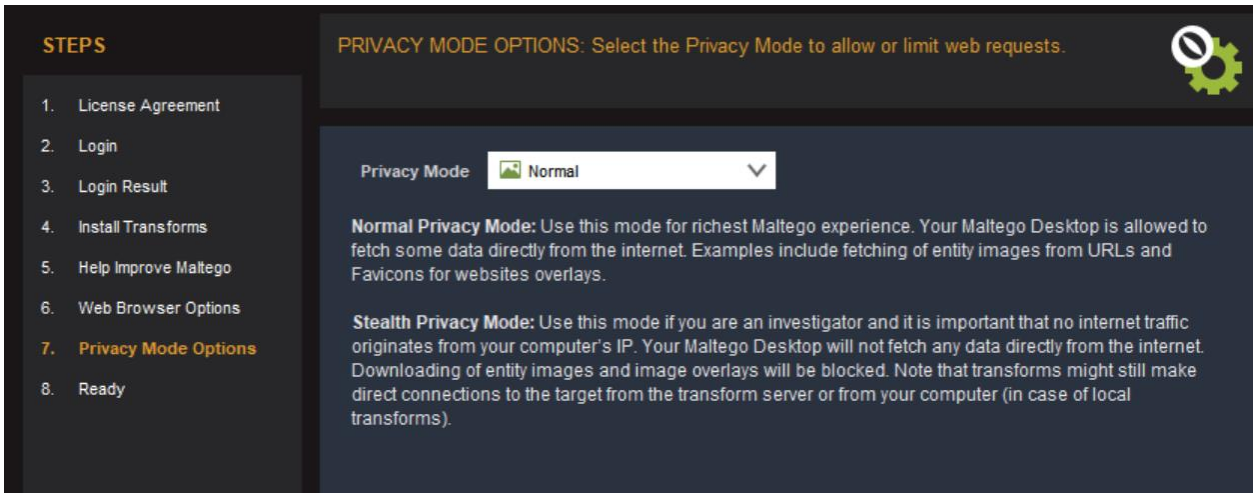


Рисунок 3.40 – Режим приватності

Після встановлення Maltego програма готова до використання. Так само, як і Recon-ng, Maltego може виконувати більш потужні запити, якщо користувач може надати ключі API. Однак в цій роботі ключі API ми не використовуємо, а

запити виконуються з базовими налаштуваннями.

Керувати Maltego CE легко. Візуальні запити викликаються шляхом створення нового графіка (який краще можна було б описати як полотно) і вибору шуканого об’єкта, що вивчається. У цій роботі відправною точкою для будь-якого запиту був knu.ua, і, отже, це також стосується Maltego CE. Тим не менш, запит knu.ua починається з вибору домену як об’єкта пошуку та введення на ньому knu.ua.

Наступним кроком користувач може вибрати окремо, які “перетворення” запускати для виконання запиту, або вибрати всі “перетворення” для запуску одночасно. “Трансформація” (або перетворення) — це термін, який використовується в Maltego для логіки запиту та діяльності.

Після виконання вибраних перетворень (у цій демонстрації ми робимо все, що було можливо без ключів), Maltego CE відображає результати на графіку/полотні як ілюстрацію. Деталі кожного запису можна переглянути на бічній панелі інтерфейсу користувача Maltego, активувавши відповідний запис. Перетворення, які були запущені, разом із їхніми результатами також надаються у форматі письмового списку в одному з підвікон інтерфейсу користувача.

Пошук показаний на рисунку нижче (Рисунок 3.41-45). Кожна піктограма на графіку ілюструє різний тип знайдених даних, будь то зв’язаний домен, IP-адреса, ім’я DNS, мережеві блоки, запис NS, запис MX (запис поштового обмінника), адреса електронної пошти, особа, номер телефону, веб-сторінка або пов'язана організація або компанія.

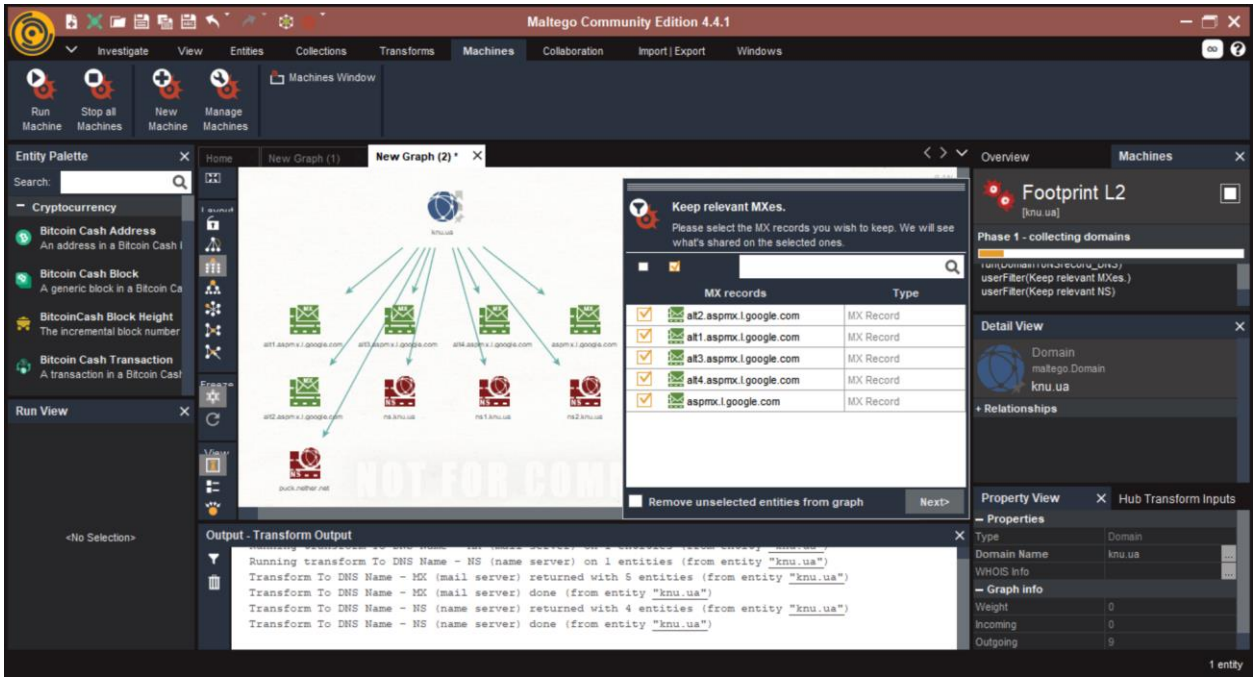


Рисунок 3.41 – Процес пошуку з машиною Footprint L2

Задля демонстрації роботи ми будемо шукати через усі знайдені записи

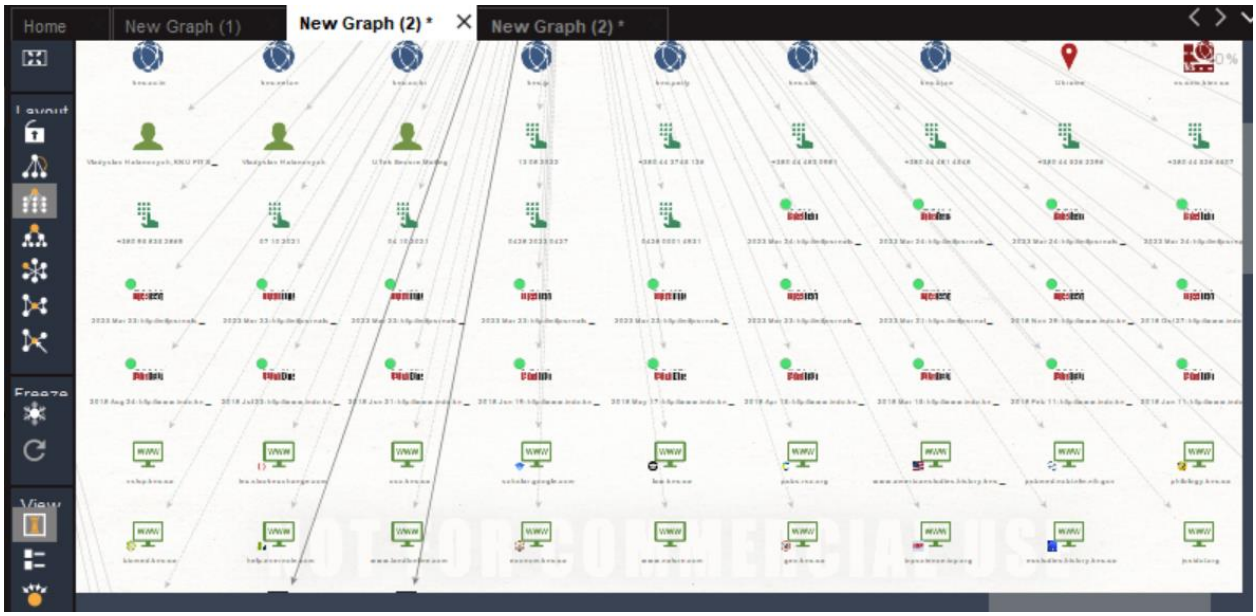


Рисунок 3.42 – Після застосування доступних нам перетворень нам відобразилася інформація стосовно пов’язаних з домейном користувачів, телефонних номерів, веб-сайтів, електронних адрес, DNS, тощо

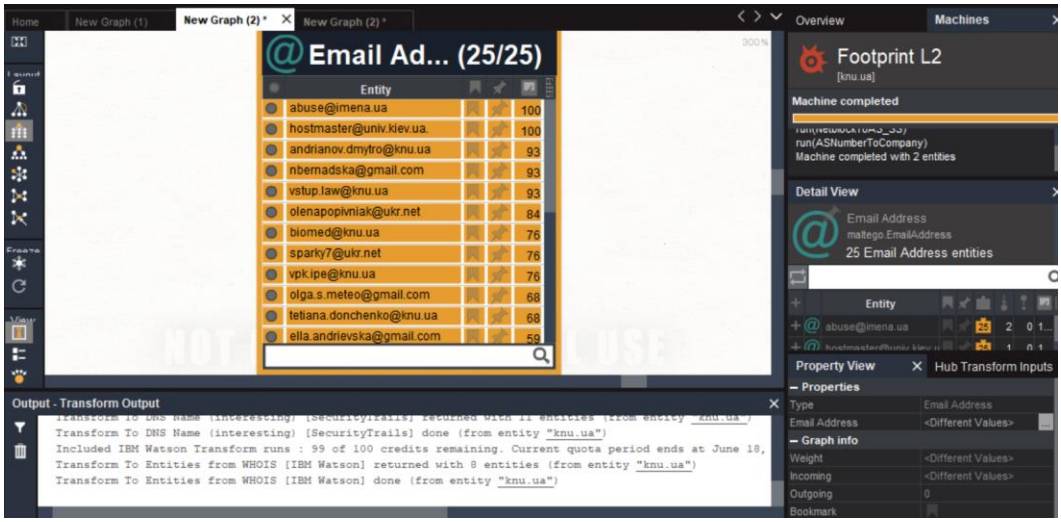


Рисунок 3.43 – Знайдені електронні адреси

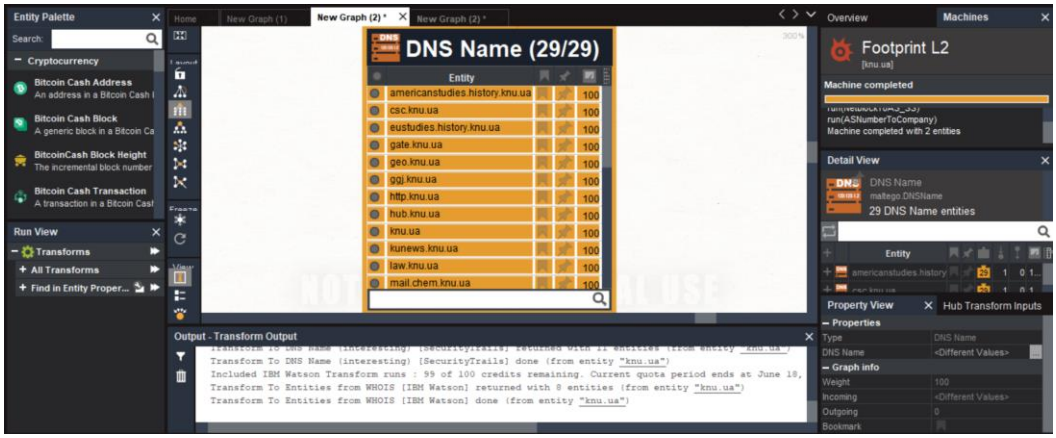


Рисунок 3.44 – Знайдені DNS

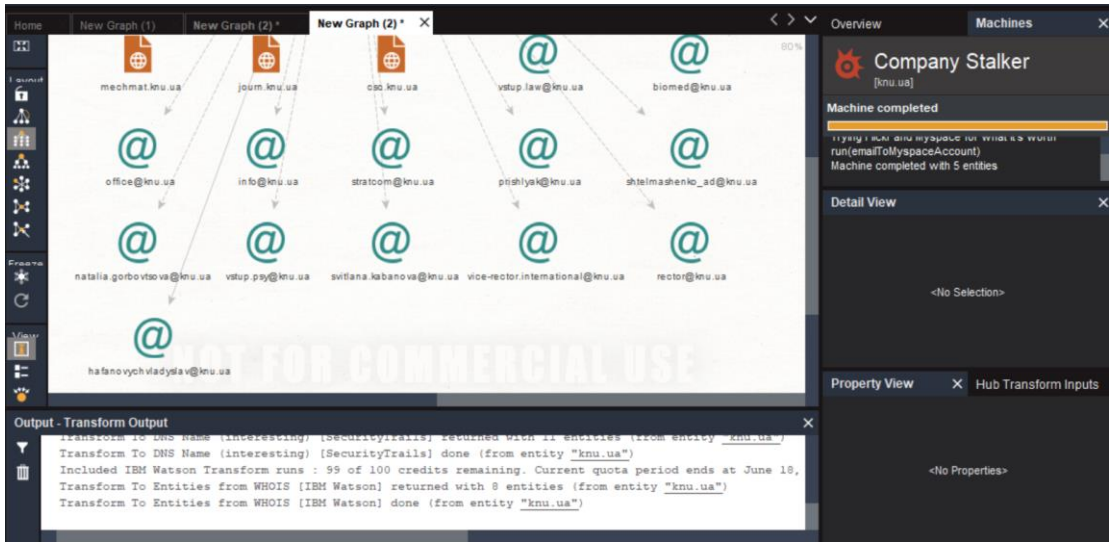


Рисунок 3.45 – Результати пошуку через машину Company Stalker (пошук електронних адрес).

Електронні адреси співпадають з тими, щ обули знайдені після застосування перетворень у Footprint L2

Варто зауважити, що Maltego також може виконувати більш розширені пошуки, коли всі ключі API та всі можливі перетворення будуть увімкнені. Інструмент Maltego містить хаб для перегляду та додавання додаткових можливостей перетворення в рішення (Рисунок 3.46, 3.47). Як вже було зазначено раніше, ми працювали тільки з тим, що в нас було.

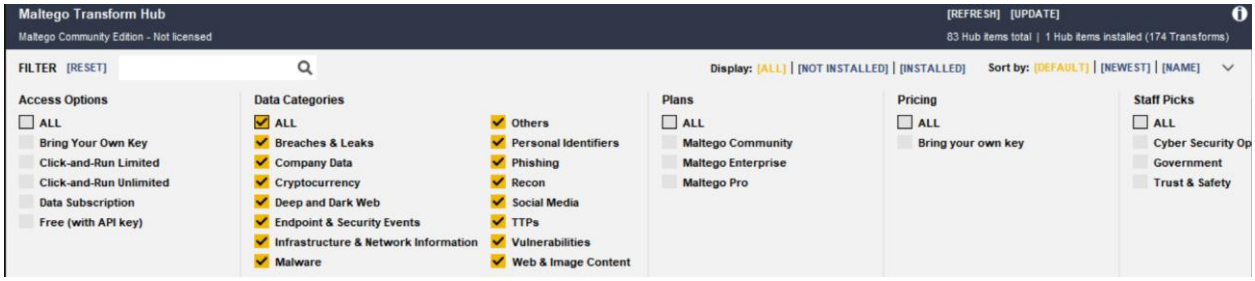


Рисунок 3.46 – Фільтр для пошуку перетворень

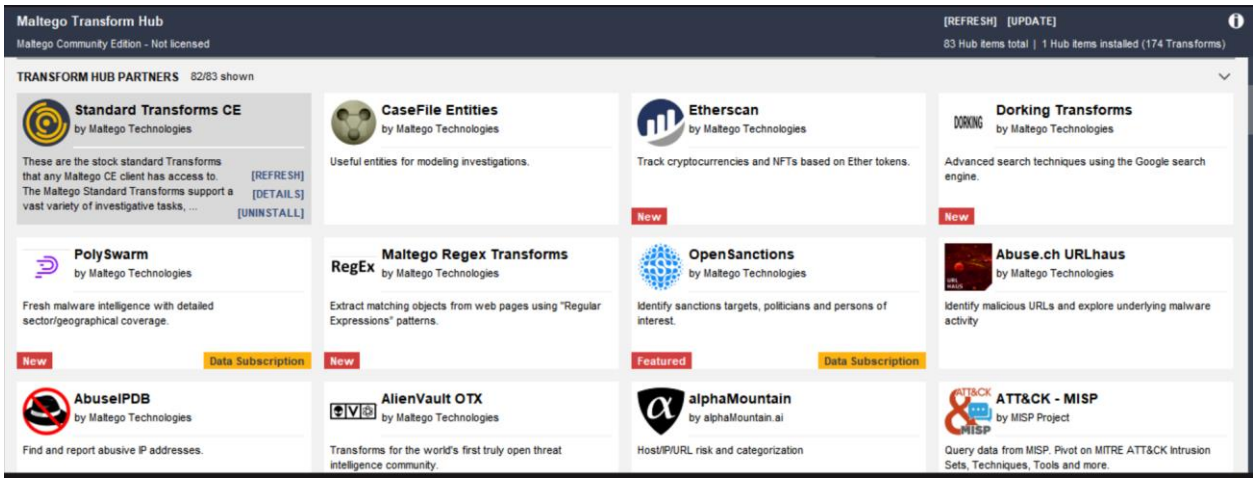


Рисунок 3.47 – Transform Hub

3.4 Порівняння застосунків

У даному розділі ми підсумовуємо демонстрації вибраних інструментів OSINT шляхом порівняння рішень одне з одним для остаточного огляду рішень. Як було вказано на початку цього розділу, вибрані інструменти представляють різні підходи до додатків OSINT і є гарними прикладами того, як по-різному можна збирати дані OSINT. Кожен із них також надає результати збору даних у різних форматах.

У наведеній нижче таблиці (таблиця 3.1) порівнюються рішення з вибраними атрибутами, які були визнані значущими для порівняння, і описуються відмінності рішень.

Таблиця 3.1

Порівняльна таблиця трьох застосунків

	Tinfoleak.com	**Recon-ng**	**Maltego CE**
Складність установки	Не потребує установки	Низька-середня	Низька
Операційна система	Веб застосунок	Linux	Windows, Mac, Linux
Тип запитів	Автоматичний	Командна строка	Автоматичний
Метод відправки запитів	Пасивний	Активний, користувач обирає які модулі використовувати	Активний, користувач обирає машину та перетворення, що працюють з інформацією
Кількість запитів за раз	Один запит на одного користувача за раз	Середній, збирає результати з кількох запитів разом, але кожен запит має виконуватися окремо.	Широкомасштабні автоматизовані запити, що збирають інформацію із багатьох джерел
Дані, що збираються	Вузьке коло даних, отримується інформація стосовно конкретно користувача Twitter	Велике коло, можна отримувати дані з кількох різних джерел, використовуючі різні пошукові методи	Велике коло, можна отримувати дані з кількох різних джерел, використовуючі різні пошукові методи
Формат отриманих результатів	HTML-звіт із переліком деталей	Текстовий перегляд із підсумковуванням усіх результатів за категорією (можливо експортувати у CSV та HTML)	Візуальний графік з усіма знайденими записами та їх зв'язками з іншими знайденими записами
Переваги	Застосунок швидкий і простий у використанні, надає хороший огляд окремого користувача	Широкий діапазон для пошуку, відкритий код, безкоштовний для використання, міцна користувацька спільнота	Наочна ілюстрація результатів, ілюстрація зв'язків між записами, можливість опрацьовувати декілька пошукових запитів одночасно
Недоліки	Обмеження до одного користувача за раз	Потребує ознайомлення та базових навичок роботи із терміналом Linux, працює лише на одній операційній системі	Комерційна версія потребує оплати, деякі перетворення потребують наявності підписки.

Висновки до розділу 3

У результаті порівняння трьох застосунків OSINT - Tinfoleak, Recon-ng та Maltego - було виявлено, що кожен з них має свої унікальні переваги та функціонал, які можуть бути корисними в різних ситуаціях дослідження та аналізу відкритої інформації.

Tinfoleak відзначається своєю простотою використання та інтуїтивним інтерфейсом. Він надає широкий спектр аналітичних інструментів для вивчення аккаунтів в Twitter та дозволяє отримати детальну інформацію про профілі, активність та зв'язки.

Recon-ng дозволяє використовувати різноманітні модулі та сканери для збору інформації з різних джерел, включаючи соціальні мережі, веб-сайти та бази даних. Він надає можливість налаштування та адаптації для задоволення специфічних потреб користувача.

Maltego відзначається своїм великим спектром функціоналу та здатністю до візуалізації даних. Цей застосунок забезпечує розширені можливості для аналізу графів зв'язків, включаючи пошук інформації про особи, організації, домени та багато іншого. Він дозволяє відстежувати зв'язки між сутностями та виявляти складні залежності.

Як показано в наведеній вище таблиці, характеристики продемонстрованих інструментів досить помітно відрізнялися, але кожен із інструментів виконував свої власні завдання. Користувач має дуже мало можливостей, якщо взагалі має, побачити або вплинути на те, як працює логіка пошуку даних у цих інструментах.

Серед переглянутих нами застосунків, Tinfoleak є найбільш простим і доступним, в той же час надаючи найменше інформації. Два інших застосунки теж можуть збирати ті ж самі дані, але той же Maltego дозволяє її устаткувати та візуалізувати в більш сприйнятному вигляді. Recon-ng та Maltego йдуть майже нога в ногу, але врешті-решт Maltego перемагає, пропонуючи більш досконалу та розгорнуту інформацію. Наприклад, лише в Maltego мені вдалося знайти контактні електронні адреси та телефонні номери, а в Recon-ng доступні модулі з цим завданням не впоралися.

ВИСНОВОК

Метою цієї дипломної роботи було вивчити, що таке розвідка з відкритим кодом, розглянути окремі методи пошуку прихованої інформації за допомогою OSINT та дослідити їх ефективність. У теоретичних розділах ця стаття розглядала поточний стан OSINT і оцінювала його майбутнє. Основне дослідницьке питання цієї роботи було сформульовано таким чином, щоб охопити загальну мету дослідження, і воно було поділено на піддослідницькі питання для охоплення основного змісту кожного з них. Нарешті всі вони були доведені до висновків. Отже, у цьому розділі висновки робляться, переходячи від піддослідницьких питань до головних.

Перше запитання було спрямоване на розуміння OSINT як концепції, спочатку запитуючи, які характеристики специфікують розвідку з відкритим кодом.

Характеристики, що визначають розвідку з відкритим кодом на основі теорії, можна підсумувати таким чином:

– Інформація, яка використовується в розвідці з відкритих джерел, надходить з різних джерел

– Теоретично відкриті джерела мають бути доступними для всіх, але на практиці деякі з них знаходяться за платними екранами та окремими авторизаціями

– Група користувачів коливається від урядів до звичайних громадян

– Популярність OSINT постійно зростає, а використання OSINT розширюється на нові сфери

– Головним завданням OSINT є обсяги даних і, таким чином, пошук значущих бітів із доступної інформації

Друге питання було сформовано із необхідності забезпечення найбільш ефективного процесу аналізу та збору інформації з відкритих джерел. Дослідження методології OSINT вносить значну користь для забезпечення ефективності збору та аналізу інформації наступними способами:

– Розробка структурованого підходу: Дослідження методології OSINT допомагає в розробці структурованого підходу до збору та аналізу інформації.

Воно включає в себе вивчення кращих практик, розробку процедур, методів та інструментів, що сприяють ефективному виконанню завдань OSINT. Це допомагає встановити чіткий план дій, оптимальні критерії пошуку та оцінки інформації, що сприяє ефективному процесу збору та аналізу.

– Використання розширених пошукових методів: Дослідження OSINT дозволяє ознайомитися з різноманітними пошуковими методами та інструментами, які сприяють більш точному та повному збору інформації. Це включає в себе використання розширених пошукових операторів, пошук за ключовими словами, моніторинг соціальних мереж, автоматизовані засоби збору даних та інші техніки, які дозволяють отримати більше цінних даних за короткий проміжок часу.

– Аналіз та фільтрація даних: Дослідження методології OSINT надає інструменти та підходи до ефективного аналізу та фільтрації отриманих даних. Це допомагає виокремити важливу інформацію, відсіяти шум та неперевірені джерела, ідентифікувати зв'язки та шаблони, що полегшує роботу з великим обсягом інформації та дозволяє зосередитися на ключових аспектах.

– Отримання актуальної інформації: Збір і аналіз відкритих даних швидко забезпечують оновлену та актуальну інформацію. Завдяки дослідженню методології OSINT, дослідники можуть виявляти нові джерела інформації, слідкувати за змінами та оновленнями в певних областях і використовувати цю свіжу інформацію для прийняття важливих рішень.

Ця робота представила та продемонструвала три доступні рішення OSINT і певною мірою показала природу та відмінні атрибути доступних рішень. Спектр OSINT-рішень видається досить широким, і немає стандартизованих підходів до створення таких програм.

Представлені OSINT-додатки точно знайшли інформацію з предмета пошуку. Процеси, що виконували пошук, також були автоматизовані. Однак жоден із інструментів не надавав доступу чи видимості для зміни будь-якої логіки пошуку всередині інструментів (Recon-ng може бути винятком), отже оптимізація пошуку відповідно до смаків користувача була неможливою.

Широкий діапазон рішень та їх розрізненість стали досить очевидними на основі цього дослідження. Кожен виконує свої власні завдання, у свій власний

розроблений спосіб, забезпечуючи свої результати у свій спосіб. Поєднання даних із різних OSINT-рішень для комплексного огляду та аналізу є проблемою принаймні до певної міри. Там, де Steel дійшов висновку, що наразі немає рішення, яке б відповідало всім вимогам повністю інтегрованого аналітичного інструментарію (за винятком великих організацій), з чим можна погодитися і в нашому випадку. Glassman і Kang приходять до висновку, що користувачам може знадобитися встановити власні набори інструментів, і це також підтверджується результатами цього дослідження. Слово «набір інструментів» може бути ключовим на арені OSINT через розрізненість окремих рішень.

Цікаво, що Hassan & Hijazi стверджували в розділах теорії, що напівпасивні та активні методи збору даних зазвичай не розглядаються в OSINT, оскільки їх можна вважати такими, що порушують суть розвідки з відкритим кодом. Два інструменти OSINT, використані в цій роботі, були охарактеризовані як напівпасивні або активні, отже, можна стверджувати, що вони взагалі не сумісні з OSINT-рішеннями. Можна припустити, що досить багато OSINT-рішень, доступних на ринку, знаходяться в цій сірій зоні – в чому саме полягає «відкритість» даних, які вони збирають, і чи збираються вони за допомогою використання лише пасивних методологій?

Те, як програми допомогли зрозуміти отриману інформацію, різнилося залежно від рішення – здебільшого знайдені записи просто перераховувалися, а висновки залишалося зробити користувачу, тоді як найдосконаліше рішення для представлення результатів візуально допомагало користувачеві зрозуміти зв’язки між різними записами даних . Візуалізація отриманих результатів має бути місцем, на яке слід звернути увагу при розробці OSINT-рішень у майбутньому. За підтримкою Беста, у центрі уваги майбутніх досліджень у цій OSINT-сфері мають бути методи візуалізації резюме. У майбутньому слід також зосередитися на навичках окремих осіб щодо пошуку та обробки даних, чи то для здатності краще використовувати доступні OSINT-рішення, але більше для здатності розробляти більш складні OSINT-рішення в майбутньому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України "Про інформацію" № 48, прийнятий 13 січня 2011 року. Доступно за посиланням: https://zakon.rada.gov.ua/laws/show/2657-12#Text

2. Роспорядження № 900-р, "Про затвердження плану дій з реалізації принципів Міжнародної хартії відкритих даних", прийняте 21 листопада 2018 року. Доступно за посиланням: https://zakon.rada.gov.ua/laws/show/900-2018-%D1%80#Text

3. Hassan N.A., Hijazi R. 2018. The Evolution of Open Source Intelligence. In:Open Source Intelligence Methods and Tools. Apress, Berkeley, CA

4. Hassan, N.A., Hijazi, R. (2018). Open source intelligence methods and tools: A PracticalGuide to online Intelligence. New York, NY: Apress

5. Steele, R.D. 2007. Open Source Intelligence. Published in Loch Johnson (ed.) Handbook of Intelligence Studies. New York: Routledge, Chapter 10,129-147.

6. Best, C. 2008. Open source intelligence. Published in Fogelman-Soulié, F (ed.) Mining Massive Data Sets for Security: Advances in Data Mining, Search, Social Networks and Text Mining, and Their Applications to Security. NATO Science for Peace and Security Series, Sub-Series D: Information and Communication Security – Vol.19, 331-343.

7. Wells, D., & Gibson, H. 2017. OSINT from a UK perspective: Considerations from the law enforcement and military domains. Proceedings Estonian Academy of Security Sciences, 16: From Research to Security Union, 16, 84-113.

8. Fleisher, C. S. (2008). Using open source data in developing competitive and marketing intelligence. European journal of marketing, 42(7/8), 852-866.

9. Burke, C. 2007. Freeing knowledge, telling secrets: Open source intelligenceand development. CEWCES Research Papers, (11), 18, 1-22.

10. Akhgar, B. (2016). OSINT as an Integral Part of the National Security Apparatus. In Akhgar, B., Bayerl, P. S. & Sampson, F. (Ed.). Open Source Intelligence Investigation: From strategy to implementation. (pp. 3-9). Cham: Springer

11. Association of Chief police officers. (ACPO). (2012). ACPO Good Practice Guide for Digitalevidence.

12. Bazzel, M. (2018). Open Source Intelligence Techniques: Resources for searching and analyzing online information. CreateSpace Independent Publishing Platform

13. Bjerke, O. T. & Fasing, I. A. (2018). Investigation: Principles, methods and practices.[Investigation: Principles, methods and practice] Bergen: Fiction the publisher

14. Bryant, R. (2014). Digital Crime. In Bryant, R., & Bryant, S. (Ed.). Policing Digital Crime.(Pp. 1-42). Farnham: Ashgate.

15. Bryant, R. & Kennedy, I. (2014). Investigating Digital crime. In Bryant, R., & Bryant, S.(Ed.). Police digital crime. (Pp. 123-145). Farnham: Ashgate.

16. Center for Security Studies CSS. (2008). Open Source Intelligence: A Strategic Enabler of National Security. Retrieved from Http://www.css.ethz.ch/content/dam/ethz/special- interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analyses-32.pdf

17. Day, T., Gibson, H. & Ramwell, S. (2016). Fusion of OSINT and non-OSINT Data. In Akhgar, B., Bayerl, P. S. & Sampson, F. (Ed.). Open Source Intelligence Investigation: From strategy to implementation. (pp. 133-152). Cham: Springer

18. Dilijonaite, A. (2018). Digital Forensic readiness. In Årnes, A (Ed.). Digital Forensics. Hoboken, (Pp. 117-146). Nj: Wiley

19. Flaglien, A. O. (2018). The Digital Forensic Process. In Årnes, A (Ed.). Digital Forensics.(pp. 13-49). Hoboken, NJ: Wiley

20. Gibson, H. (2016). Acquisition and preparation of Data for OSINT. In Akhgar, B., Bayerl, P.S. & Sampson, F. (Ed.). Open Source Intelligence Investigation: From strategy to implementation. (pp. 69-93). Cham: Springer

21. Gibson, H., Ramwell, S. & Day, T. (2016). Analysis, Interpretation and validation of Open Source Data. In Akhgar, B., Bayerl, P. S. & Sampson, F. (Ed.). Open Source Intelligence Investigation: From strategy to implementation. (pp. 95-110). Cham: Springer

22. Nhàn, J. & Huey, L. (2012). 'We don't have the laser beams and stuff like that': Police investigations as low-tech work in a high-tech world. In Leman-Langlois, S. (Ed.). Technocrime, police, and surveillance (Routledge frontiers of Criminal Justice). (pp.79-90). New York, NY: Routledge.

23. Norwegian Broadcasting. (2017). Sex, Dope and Beggar Cup. (sex, drugs, and Beggars Cup).

24. RET Rei at from https://www.nrk.no/dokumentar/xl/sex_-dop-og-tiggerkopp-1.13463802

25. Ramwell, S., Day, T. & Gibson, H. (2016). Use cases and Best practice for LEAs. In Akhgar, B., Bayerl, P. S. & Sampson, F. (Ed.). Open Source Intelligence Investigation: From strategy to implementation. (pp. 189-211). Cham: Springer

26. Rogers, C. (2012). Intelligence Gathering and police Systems. In Awan, I., & Blakemore, B. (Ed.). Police the cyber hating, cyber threats and cyber terrorism. (pp. 129-148). Farnham: Ashgate.

27. Sampson, F. (2016). Following the breadcrumbs: Using Open Source Intelligence as evidence in Criminal proceedings. In Akhgar, B., Bayerl, P. S. & Sampson, F. (Ed.). Open Source Intelligence Investigation: From strategy to implementation. (pp. 295-304). Cham: Springer

28. Schaurer, F. & Störger, J. (2013). The Evolution of Open Source Intelligence *(OSINT).* RET Rei at From Https://www.afio.com/publications/Schauer_Storger_Evo_of_OSINT_WINTERSPRING2013.pdf

29. Staniforth, A. (2016). Police Use of Open Source Intelligence: The longer Arm of Law. In Akhgar, B., Bayerl, P. S. & Sampson, F. (Ed.). Open Source Intelligence Investigation: From strategy to implementation. (pp. 21-31). Cham: Springer

30. Sunde, I. M. (2018). Cybercrime Law. In Årnes, A (Ed.). *Digital Forensics*. (pp. 51-75). Hoboken, NJ: Wiley

31. TechUK. (2014). Breaking down barriers. [Report]. Retrieved from Https://www.techuk.org/insights/reports/item/2302-techuk-launches-breaking-down-barriers-report