Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: *Комп'ютерна система аналізу трафіку локальної мережі*

Виконав: студент *IV курсу,* групи *СІ-41*
спеціальності *123 Комп'ютерна інженерія*
(шифр і назва спеціальності)

(підпис) *Лукашук В.О.* (прізвище та ініціали)

Керівник (підпис) *Баран І.О.* (прізвище та ініціали)

Нормоконтроль (підпис) (прізвище та ініціали)

Завідувач кафедри (підпис) *Осухівська Г.М.* (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль -2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет *комп'ютерно-інформаційних систем і програмної інженерії*
(повна назва факультету)

Кафедра *комп'ютерних систем та мереж*
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ *Осухівська Г.М.*
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня *Бакалавр*
(назва освітнього ступеня)

за спеціальністю *123 Комп'ютерна інженерія*
(шифр і назва спеціальності)

Студенту *Лукашуку Владиславу Олеговичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Комп'ютерна система аналізу трафіку локальної мережі*

Керівник роботи *Баран Ігор Олегович., к.т.н., доц.*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від *« 24 » 04 2024 року № 4/7-408*

2. Термін подання студентом завершеної роботи *25.06. 2024 р.*

3. Вихідні дані до роботи *Технічне завдання*

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ.
1. Аналіз технічного завдання.
2. Проектна частина.
3. Практична частина.
4. Безпека життєдіяльності, основи охорони праці.
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Схема локальної мережі. Принцип дзеркалювання трафіку
2. Структурна схема розробки
3. UML діаграма. Блок-схеми роботи
4. Скріншоти роботи програмної частини

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці			

7. Дата видачі завдання *2024 р.*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	*Ознайомлення з завданням до кваліфікаційної роботи*	*24.04 – 25.04*	*Виконано*
2.	*Розробка технічного завдання*	*26.04 – 29.04*	*Виконано*
3.	*Підбір джерел про системи аналізу трафіку мережі*	*30.04 – 06.05*	*Виконано*
4.	*Опрацювання літературних джерел*	*07.05 – 10.05*	*Виконано*
5.	*Виконання дослідження щодо розробки системи*		
	аналізу трафіку комп'ютерної мережі	*11.05 – 18.05*	*Виконано*
6.	*Написання програмного коду*	*19.05 – 25.05*	*Виконано*
7.	*Оформлення розділу «Аналіз технічного завдання»*	*26.05 – 29.05*	*Виконано*
8.	*Оформлення розділу «Проектна частина»*	*30.05 – 02.06*	*Виконано*
9.	*Оформлення розділу «Практична частина»*	*03.06 – 08.06*	*Виконано*
10.	*Виконання завдання до підрозділу «Безпека*		
	життєдіяльності, основи охорони праці»	*20.05 – 04.06*	*Виконано*
11.	*Оформлення кваліфікаційної роботи*	*08.06 – 11.06*	*Виконано*
12.	*Нормоконтроль*	*09.06 – 12.06*	*Виконано*
13.	*Перевірка на плагіат*	*11.06 – 14.06*	*Виконано*
14.	*Попередній захист кваліфікаційної роботи*	*14.06 – 18.06*	*Виконано*
15.	*Захист кваліфікаційної роботи*	*26.06*	

Студент _____ *Лукашук В.О.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Баран І.О.*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Комп'ютерна система аналізу трафіку локальної мережі // Кваліфікаційна робота бакалавра // Лукашук Владислав Олегович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно–інформаційних систем і програмної інженерії, кафедра комп'ютерних систем та мереж, група СІ–41 // Тернопіль, 2024 // с. – 52, рис. – 27, табл. – 2, аркушів А1 – 4, бібліогр. – 21.

Ключові слова: АНАЛІЗАТОР ТРАФІКУ, ДЗЕРКАЛЮВАННЯ ТРАФІКУ, СИНХРОНІЗАЦІЯ ПАКЕТІВ, SHARPPCAP

Кваліфікаційна робота присвячена розробці засобу для захоплення пакетів мережевих даних з метою подальшого аналізу трафіку на всьому маршруті передачі даних.

Після проведеного аналізу існуючих аналогів були сформульовані чіткі вимоги до системи, що розробляється. Основною складовою визначено програмний інструмент аналізу трафіку на усіх мережевих ділянках. Було спроектовано структурну схему розробки та продемонстровано принцип її роботи, показаний спосіб отримання даних мережі за допомогою створеного програмного забезпечення та утиліт, вбудованих у мережеве обладнання.

Забезпечується відкриття пакетів даних мережі та розбиття на параметри для аналізу, синхронізація пакетів даних за часом відправки / прибуття та за адресними параметрами, можливість перегляду даних за допомогою інтерфейсу користувача. Побудована система одержання даних з пристроїв локальної мережі, котра забезпечує попередню підготовку інформації до опрацювання. Створено додаток обробки значного обсягу отриманих даних, де виділяються необхідні параметри даних мережі, що готує їх з різних пристроїв мережі до подальшого аналізу та демонстрації, що дає змогу користувачеві виділяти тимчасові та неявні залежності.

ANNOTATION

Computer system of local network traffic analysis // Bachalor thesis // Lukashuk Vladyslav // Ternopil Ivan Pul'uj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Computer Systems and Nets // Ternopil, 2024 // p.- 52, fig. – 27, table. – 2, Sheets A1 – 4, Ref. – 21.

Keywords: TRAFFIC ANALYZER, TRAFFIC MIRROR, PACKET SYNCHRONIZATION, SHARPPCAP

The qualification work deals with the development of a tool for capturing network data packets in order to further analyze the traffic along the entire data transmission route.

After the analysis of existing analogues, clear requirements for the system under development were formulated. The software tool for traffic analysis on all network sections is defined as the main component. The structure diagram of the development was designed and the principle of its operation was demonstrated, the method of obtaining network data using the created software and utilities built into the network equipment was shown.

Opening of network data packets and splitting into parameters for analysis, synchronization of data packets by time of departure / arrival and by address parameters, possibility of viewing data using the user interface is provided. A system for receiving data from local network devices has been built, which provides preliminary preparation of information for processing. An application for processing a large volume of received data is created, where the necessary network data parameters are highlighted, preparing them from various network devices for further analysis and demonstration, which allows the user to highlight temporary and implicit dependencies.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ СКОРОЧЕНЬ І ТЕРМІНІВ

OSI (Open Systems Interconnection Basic Reference Model) – абстрактна мережева модель для комунікацій і розроблення мережевих протоколів/

HUB (Концентратор) — пристрій фізичного рівня, з'єднувальний компонент, до якого під’єднують усі комп'ютери в мережі за топологією «зірка».

NAT (Network Address Translation) – це механізм у мережах TCP/IP, котрий дозволяє змінювати IP-адресу у заголовку пакету, котрий проходить через пристрій маршрутизації трафіку.

WPF (Windows Presentation Foundation) – графічна (презентаційна) підсистема.

АТ – аналізатор трафіку

Дзеркалювання трафіку (Traffic Mirroring) – це функція комунікаційного пристрою, яка забезпечує пересилання копій повідомлень з одного інтерфейсу пристрою на інший інтерфейс цього ж пристрою.

Міжмережевий екран — програмний чи програмно-апаратний елемент комп'ютерної мережі для контролю та фільтрації мережевої інформації, що проходить через нього, відповідно до заданих правил і протоколів.

НСД – несанкціонований доступ.

ОС – операційна система.

ПЗ – програмне забезпечення.

ВСТУП

В даний час часто виникає необхідність обробки даних мережевого трафіку для зручної оцінки навантаження мережі. Для цього можна застосовувати існуюче ПЗ, яке дозволяє із зручністю керувати пакетами даних мережі та проводити аналіз трафіку.

Актуальністю даної теми є те, що наявні розробки не надають можливість аналізувати трафік на всьому його мережевому шляху.

Необхідно створити комп’ютеризовану систему, яка дасть змогу внести дані, отримані на різних ділянках локальної мережі шляхом запису трафіку за допомогою агентів та здійснити аналіз отриманих даних у створеному ПЗ.

Мета роботи – розробка спеціалізованого засобу для спрощення підготовки даних за рахунок зниження обсягів (зниження розмірності) та виділення тимчасових та неявних залежностей для подальшого аналізу трафіку.

Завдання, необхідні для досягнення даної мети:

– здійснити вибір програмних засобів моделювання та розробки програми;

– виконати моделювання програми, що розробляється;

– виконати програмну реалізацію програми для платформ Windows;

– проаналізувати одержані результати роботи.

РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

1.1 Особливості завдання для виконання

Актуальність даної теми зумовлена тим, що на даний момент часу активно розробляються, застосовуються і використовуються різні методи виявлення вторгнень, що відбулися, і запобіганню майбутніх вторгнень, але вони далеко не завжди є ефективними на практиці. Внаслідок цього всі технології захисту постійно вивчаються і покращуються [1, 2].

У цій роботі необхідно розробити засіб для обробки мережних пакетів даних, які буде отримувати користувач з мережевих пристроїв. Агенти в критичних точках локальної мережі повинні прослуховувати трафік і записувати файли для подальшої передачі та обробки. Розробка повинна буде порівнювати характер, основні параметри та окремі пакети з різних точок локальної мережі та допомагати користувачеві в подальшому проводити аналіз з метою пошуку прихованих залежностей, мережевих втрат, можливих уразливостей та інших.

Першою функцією розробки має бути можливість захоплення пакетів даних з мережевих пристроїв за маршрутом за допомогою створеного ПЗ або іншого схожого з таким функціоналом, шляхом дзеркалювання трафіку з пристрою, на якому встановлені агенти із захоплення даних мережі, яку хочемо аналізувати.

Після отримання необхідної кількості даних агентами користувач збирає цю інформацію і поміщає в основну програму, де ми вже зможемо спростити процес пошуку НСД, застосування, розкриття, недостовірності, змінювання, дослідження, записування чи видалення інформації. Після того як користувач отримає всю необхідну інформацію про те, що відбувалося в мережі, він зможе запобігти майбутнім спробам НСД в мережу шляхом розслідування інцидентів,

котрі відбулися, тим самим зможе захистити дані своєї локальної мережі.

1.2 Потреба створення розробки

Основні потреби:

– створити прототип розподіленої системи для аналізу структури мережевого трафіку та оцінки ефективності використання комп'ютерних мереж;

– розробка методів підготовки даних мережі до подальшого аналізу для визначення структури мережевого трафіку, ефективності використання мережевих ресурсів;

– розробка агентів збору та алгоритмів попередньої обробки мережевого трафіку.

Сучасні компоненти мережевої інфраструктури використовують велику кількість керуючих протоколів та сервісів, повному налаштуванню яких не приділяється належної уваги. Це призводить до неефективного завантаження мережевих ресурсів та зниження інформаційної безпеки [3].

Актуальним є створення системи, яка дозволила б оцінити структуру трафіку, наявність непродуктивної активності та інші параметри в сегментах мережі та виробити рекомендації для підвищення ефективності використання мереж та зниження ризику загроз.

Система буде орієнтована на підприємства, що спеціалізуються на аудиті та віддаленому супроводі інформаційної та телекомунікаційної складової бізнесу, інтернет-сервіс провайдерів, а також підприємства великого та середнього бізнесу, що мають комп'ютерні мережі.

1.3 Аналіз існуючих аналогів

В цьому підрозділі будуть досліджені основі існуючі на ринку АТ.

1.3.1 WireShark

Є порівняно новим АТ у галузі рішень для аналізу та діагностування мережі, проте незважаючи на цей факт це не перешкодило йому стати успішним та визнаним ІТ-фахівцями [4].

Цей АТ успішно дає раду із аналізом мережевого трафіку, прекрасно справляючись із потрібною роботою. Мережеві адмінам вдалося отримати якісний інструмент, котрий є чимось середнім між опрацюванням вихідних даних та їх візуальним представленням у існуючому інтерфейсі. Саме тому у WireShark немає явних перегинів у ту чи іншу сторону, котрі присутні у більшості інших схожих АТ. WireShark достатньо простий і портативний, а також є сумісним із значною кількістю системам. Юзери одержують якраз той потрібний функціонал, котрий вони власне і хочуть, та одержують його миттю (рис. 1.1).

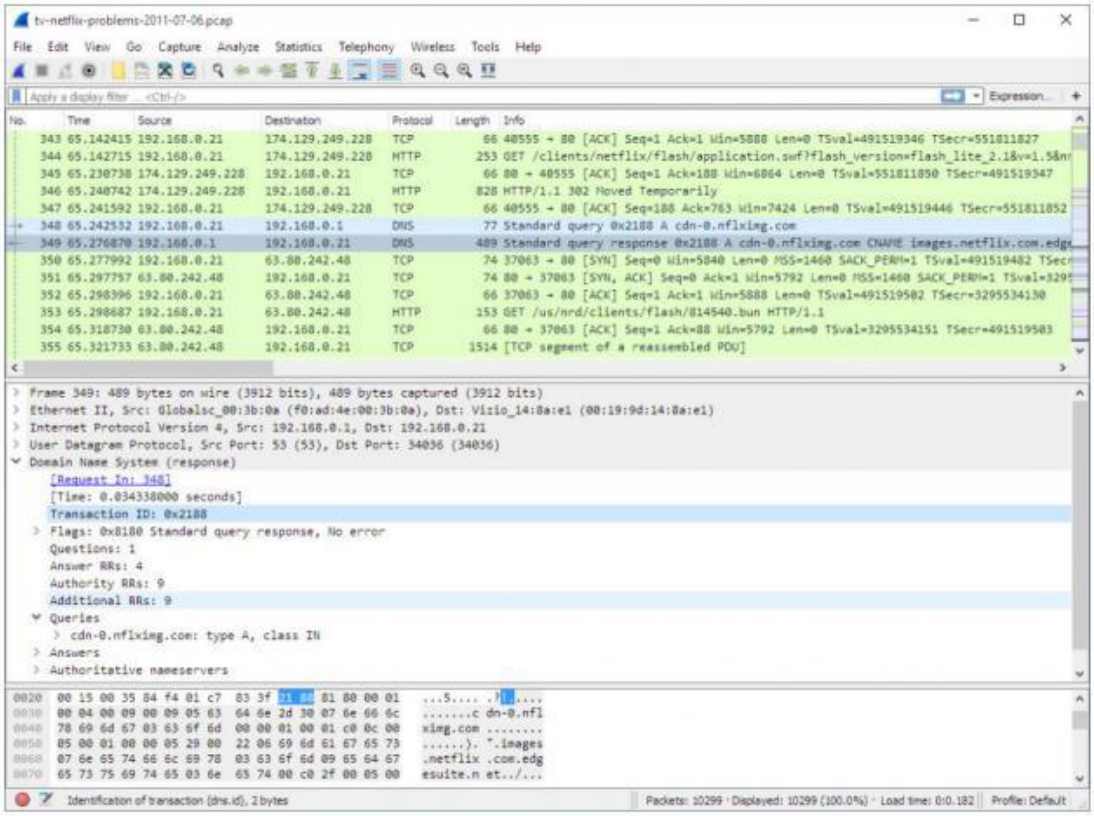

Рисунок 1.1 – Інтерфейс АТ WireShark

Це ПЗ має достатньо зручний користувацький інтерфейс, володіє

множиною опцій і функціями для проведення фільтрації та відсортовування, проте у нього відсутній функціонал для виконання глибокого аналізу мережевого трафіку. АТ WireShark зарекомендував себе з кращої сторони при роботі з найбільш популярнішими ОС, такі як *NIX, Windows та macOS [4].

Різниця даної технології від пропонованого рішення у цьому, що розглянуте ПЗ дозволяє аналізувати мережеву інформацію тільки на якомусь одному визначеному фрагменті мережі, проте не на усьому маршруті передавання даних.

1.3.2 tcpdump

Цей АТ ззовні є якимось інструментом, котрий використовувався десятиліття тому назад, і, насправді, якщо оцінювати його з точки зору функціоналу, то функціонує він також як достатньо давнє ПЗ [5]. Попри те, що із завданнями, які поставлені перед ним, tcpdump справляється успішно, він при цьому застосовує для цього мінімальні ресурси системи, абсолютно мінімізуючи навантаження на системи.

Більшості сучасних юзерів буде надзвичайно складно вникнути у значну кількість таблиць із інформацією про параметри трафіку мережі, котрі містять не всі необхідні дані. Проте все ж таки трапляються випадки, в яких таке ПЗ здатне допомогти у вирішенні будь-якої задачі, застосування полегшених і менш вимогливих інструментів до ресурсів у практиці могло би бути корисним. У окремих середовищах чи на мало потужній машині такий мінімалізм може стати єдино можливим варіантом для роботи.

ПЗ tcpdump створено під *NIX – подібні середовища, проте в даний час цей АТ успішно функціонує і з окремими портами Windows [5]. tcpdump володіє основним функціоналом, який ви можете котрий присутній у будь-якому схожому АТ, тут і захоплення, і записування, і т.п. (рис. 1.2).

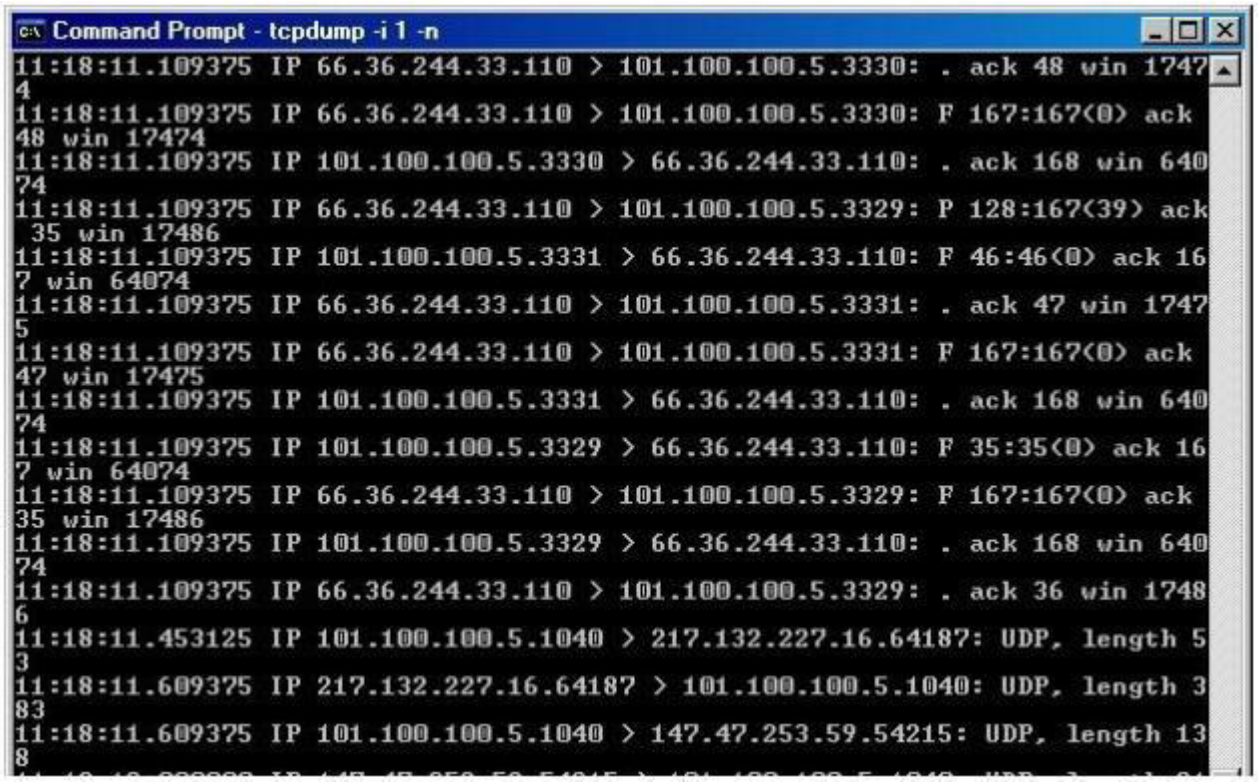

Рисунок 1.2 – Робота tcpdump

Виявлені недоліки полягають в тому, що інтерфейс АТ є незручним, також немає захоплення пакетів в реалі.

1.3.3 Kismet

Є open-source ПЗ, розроблене для вирішення визначених мережевих задач. Цей АТ не є лімітованим тільки аналізом мережного трафіку, він має значно ширший функціонал [6]. Для прикладу, це ПЗ може досліджувати трафік прихованих і бездротових мереж, котрі не передають свої розпізнавальні ідентифікатори. Kismet є корисним та ефективним, якщо у бездротовій мережі наявне щось таке, що здатне спричинити проблеми, проте оперативно визначити їхнє джерело не вдається [6]. Цей АТ дійсно допоможе визначити інуючу мережу чи точку доступу, які неавторизовані, проте володіють неграмотними налаштуваннями (рис. 1.3).

Рисунок 1.3 – AT Kismet

1.3.4 EtherApe

Достатньо сильно схожий за своїм функціоналом цей AT на WireShark, окрім того також має відкритий код та безкоштовно розповсюджується. Проте, є і значні відмінності на тлі іншого ПЗ, головна з них – орієнтація на візуальне представлення даних при допомозі графічних можливостей [7].

У WireShark результати можна переглядати у цифровому форматі та у таблиці, а у EtherApe увесь трафік відображається із застосуванням просунутого графічного інтерфейсу, коли будь-яка вершина графа є окремим пристроєм. Властиво розміри вершин та ребер і відображають розмір власне мережевого трафіку на цьому пристрої, тут кольором показуються різноманітні протоколи, котрі зуміло отримати це ПЗ [7]. Ті юзери, котрі надають перевагу візуальному сприйняттю інформації по статистиці, застосовують AT EtherApe. Він може бути використаним для Unix- та macOS- середовищ.

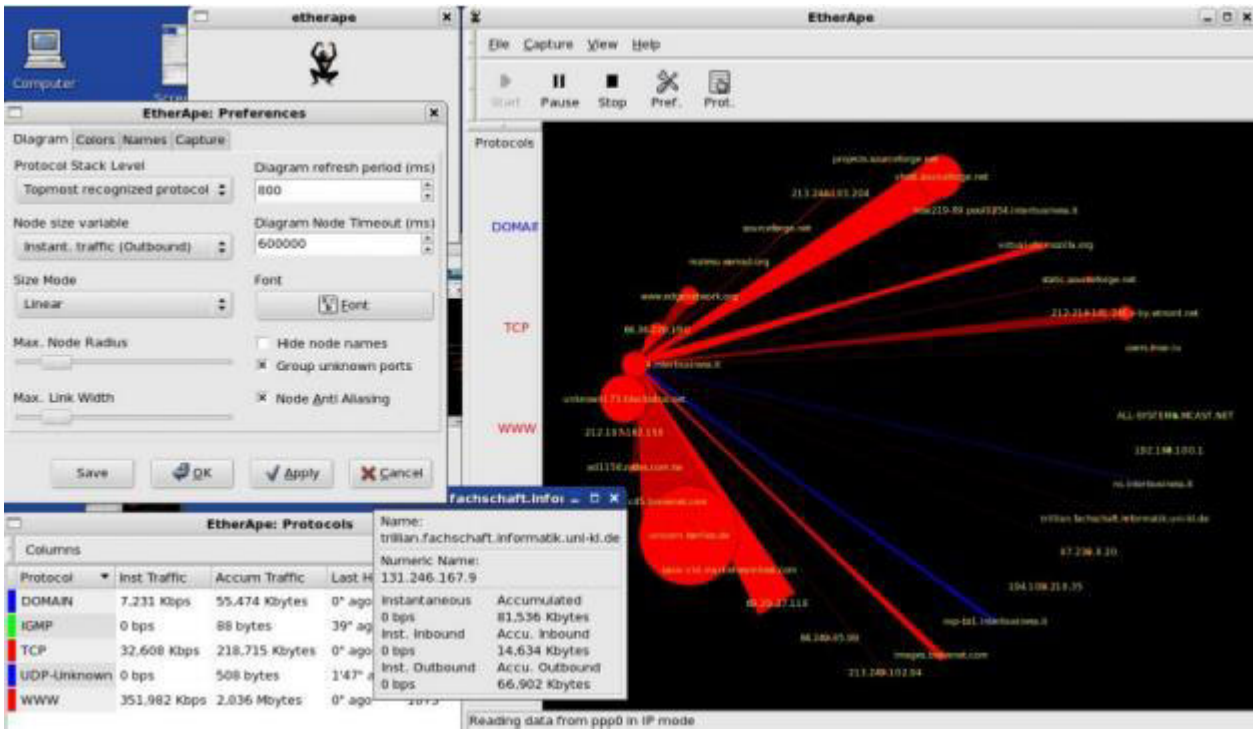

Рисунок 1.4 – Інтерфейс програми EtherApe

1.3.5 Cain and Abel

У цього ПЗ потенціал аналізу трафіку є більш додатковою чи допоміжною складовою, аніж базовою. У випадках , якщо задача юзерів є не просто і не тільки аналіз трафіку, тоді, як правило, потребують саме цього ПЗ [8]. З допомогою цього АТ є можливість відновити забуті паролі під ОС Windows, виконувати «атаки» для віднайдення втрачених облікових даних, одержування даних VoIP у мережі, проводити аналіз та маршрутизацію пакетних даних та еякі інші специфічні дії.

Cain and Abel - це сильний АТ для просунутого адміна із значним числом повноважень (рис. 1.5). Його основна вада – робота можлива тільки під ОС Windows.

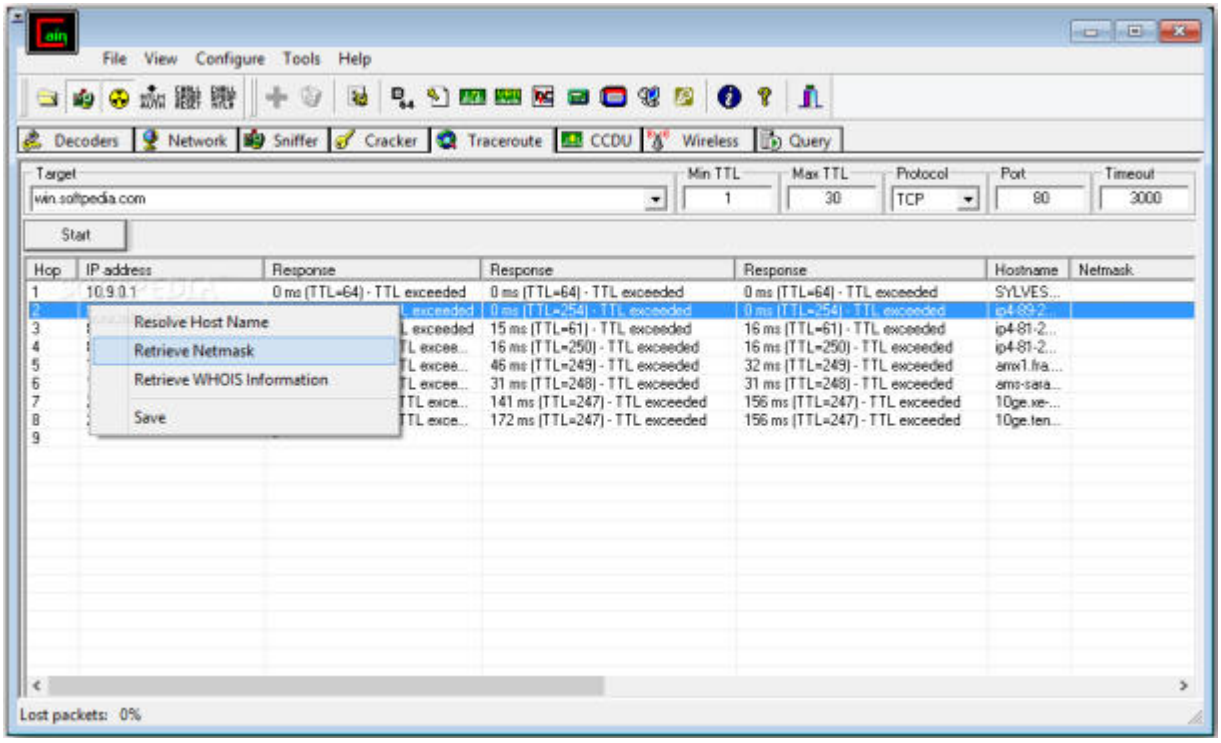

Рисунок 1.5 – Вікно AT Cain and Abel

Цей застосунок володіє функціями відстеження користувацьких даних та уразливостей мережі [8], проте не має змоги абсолютно контролювати усі частини мережі.

1.3.6 NetworkMiner

Дане ПЗ є ще одним інструментом, чий функціонал перевершує межі чистого АТ [9]. Більшість схожого ПЗ опрацьовують параметри відправлення і одержання пакетів, NetworkMiner приділяє увагу тому, хто і як власне виконує ці відправки та одержання (рис. 1.6). Дане ПЗ може бути застосовано для визначення проблемних машин чи користувачів у мережі, проте не для просунутого аналізу даних, спостереження чи діагностики. Як і попередньо розглянутий АТ NetworkMiner функціонує лише під ОС Windows.

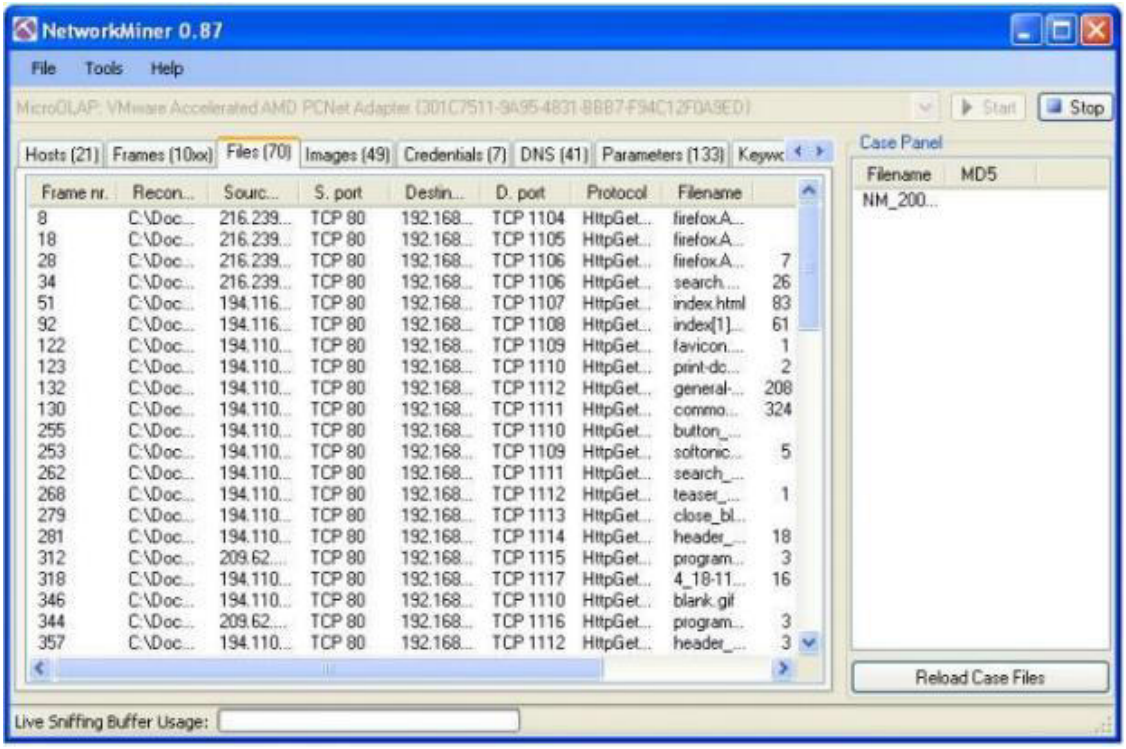

Рисунок 1.6 – Інтерфейс програми NetworkMiner

Цей АТ дає змогу проводити аналіз трафіку і апаратного забезпечення мережі [9], але це не у всіх випадках дозволить виявити мережеву уразливість.

1.3.7 KisMAC

Є описаним раніше Kismet, лише зручніше оформлений для MacOS (рис. 1.7). На даний момент цей АТ працює лише macOS, саме через це складається хибна думка, що фактично KisMAC непотрібний. Проте варто згадати, що це ПЗ володіє своєю кодовою базою і не є явним похідним АТ Kismet. Також треба зуважити, що дане ПЗ надає нам окремі унікальні можливості, зокрема накладання на карту розміщення пристроїв в мережі чи атака аутентифікації на ОС macOS [10].

Kismet такими функціональними можливостями не володіє. Такі спеціалізовані фунції у надзвичайно рідкісних випадках зможуть бути перевагою у виборі саме такого АТ.

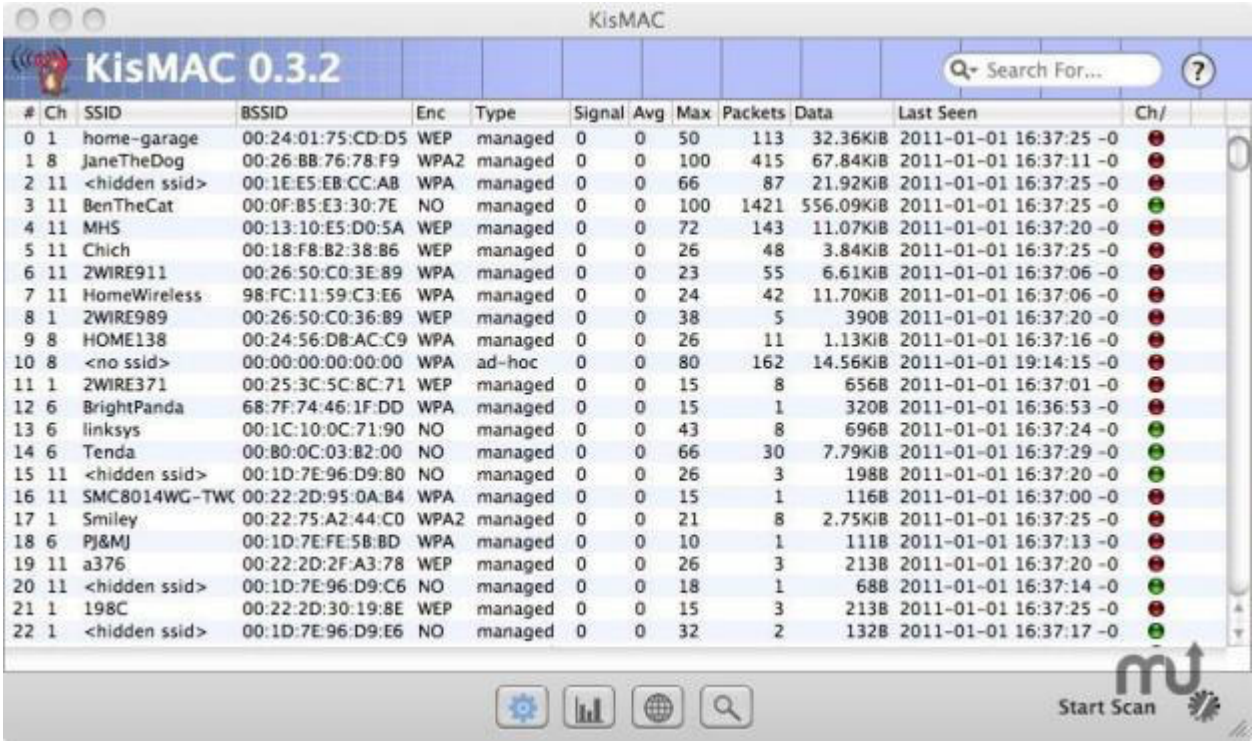

Рисунок 1.7 – AT KisMAC

Цей засіб створений унікально під macOS, саме тому і володіє вельми недостатньою сферою застосування [10]. Цей АТ не може бути використаний на серверах під інші ОС.

1.4 Висновок до розділу

В результаті аналізу завдання на дипломне проектування були сформульовані чіткі вимоги до системи, що розробляється. Було вирішено, що її основною складовою буде програмний інструмент, котрий містить дві складові: перша здійснює захоплення мережевих даних із пристроїв одного мережного маршруту та відповідає за їх збереження у Pcap- форматі, тоді як друга проводить аналіз одержаних даних для виявлення уразливостей мережі, через які може статися НСД у мережу, що розглядається.

Було проаналізовано декілька аналогів програм по роботі з даними мережі і виявлено, що жодна з них не має функціонального наповнення для аналізу трафіку на усіх мережевих ділянках.

РОЗДІЛ 2 ПРОЕКТНА ЧАСТИНА

2.1 Способи отримання файлів даних мережі

На рис. 2.1 представлена структурна схема локальної мережі, в якій встановлено систему зі збору даних трафіку. За допомогою програм прослуховування, розглянутих в п. 1.3 за типом tcpdump і wireshark [4, 5], можливо отримувати трафік, що приходить на комп'ютер користувача.

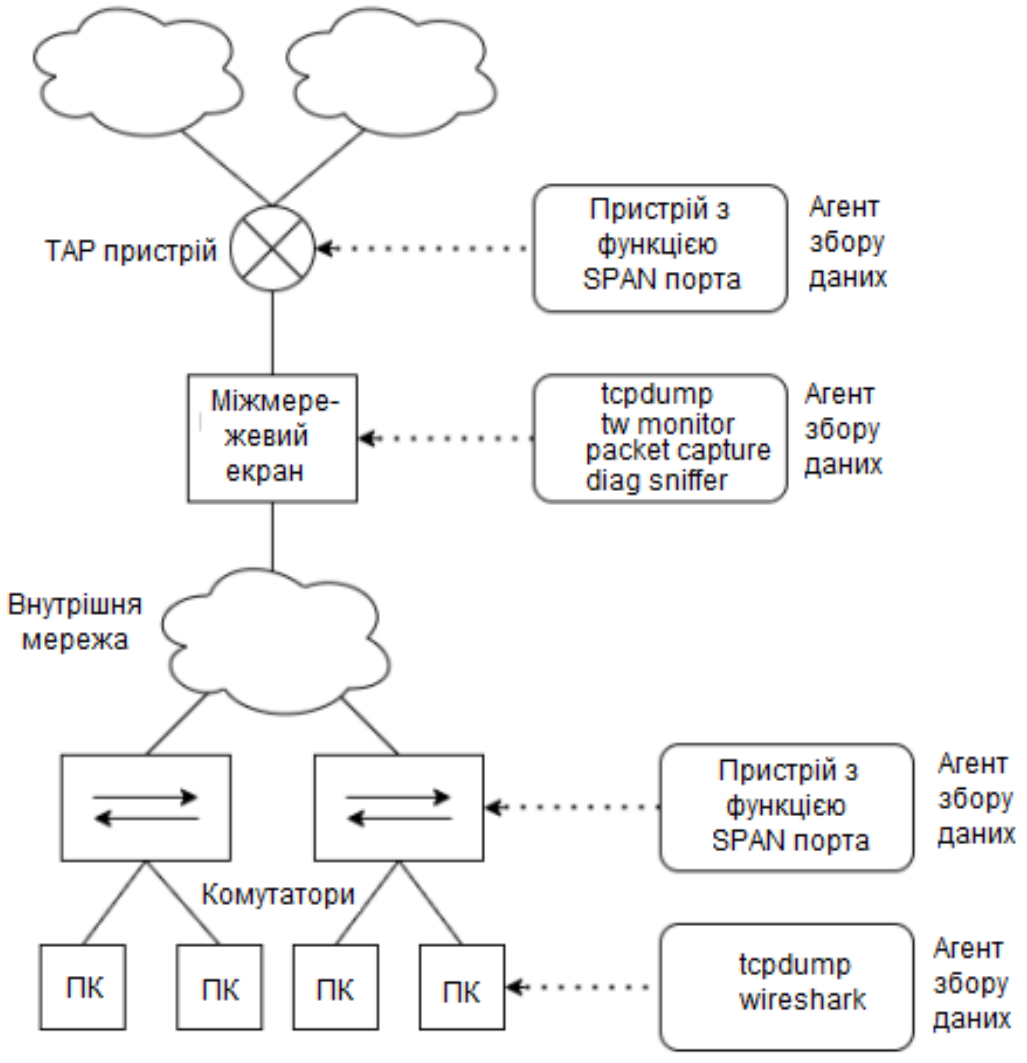

Рисунок 2.1 – Схема локальної мережі

Основними завданнями, які вирішує міжмережевий екран, є застереження елементів мережі чи поодиноких її точок від НСД із застосуванням уразливостей у визначених протоколах стандартної моделі OSI чи у ПЗ нашої локальної мережі та обладнання в ній [11]. Такі засоби дозволяють трафіку проходити чи забороняють йому прохід, шляхом порівняння його параметрів із визначеними шаблонами. Міжмережеві екрани володіють встановленими утилітами по фільтрації даних, такі утиліти залежать від мережевого обладнання [11].

Наприклад:

– Check point - fw monitor;
– Cis - packet capture;
– Fortigate - diag sniffe;
– Nix - tcpdump.

За отримання файлів даних відповідають агенти збирання даних. Агентами є пристрої з встановленим ПЗ, які володіють здатністю захоплювати трафік в певних ділянках мережі і відсилати дані на основний пристрій, де і буде відбуватися подальший аналіз трафіку.

Є кілька таких способів отримання даних, один з таких способів можливо здійснити якщо в мережі, яку ми хочемо аналізувати, встановлений HUB або мережевий концентратор. Завдяки тому, що HUB працює на фізичному рівні мережевої моделі OSI, ретранслюючи вхідний сигнал з одного з портів на всі інші підключені порти ми дуже просто можемо перехоплювати всі дані та сигнали, що проходять через HUB (рис. 2.2).

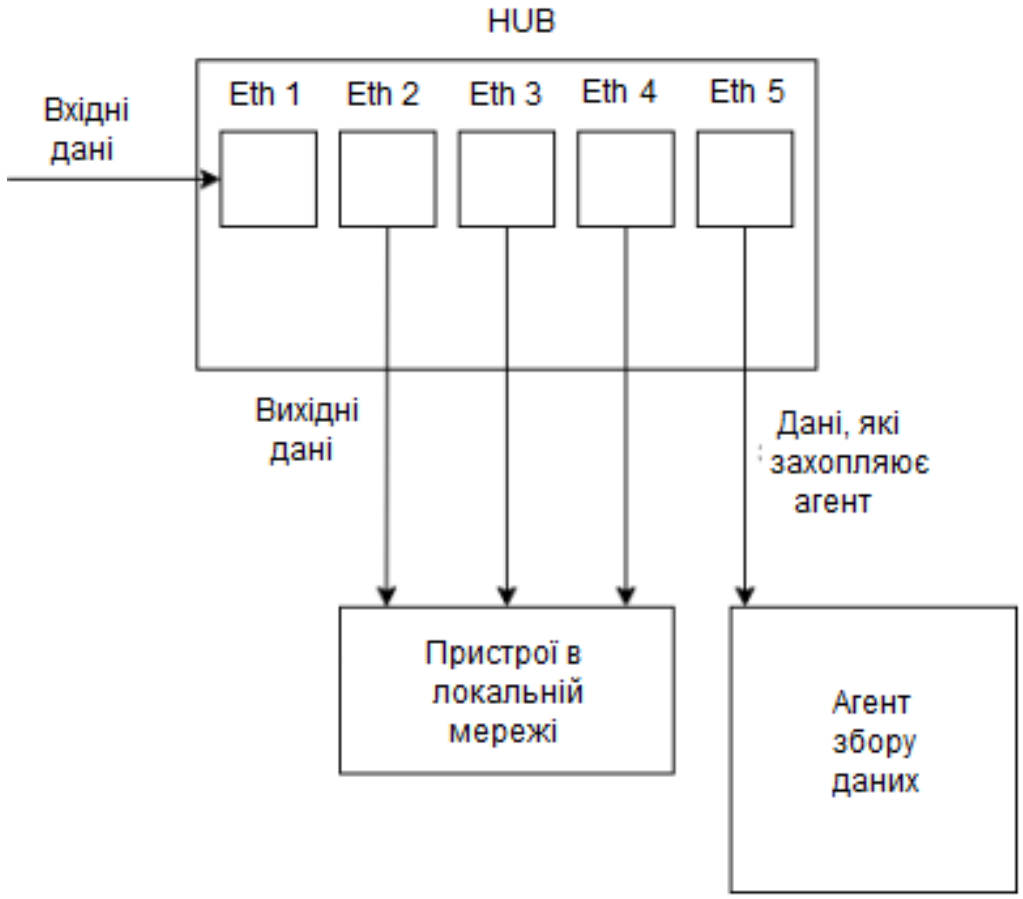

Рисунок 2.2 – Приклад роботи HUB у локальній мережі

Через те, що технологія HUB не актуальна і застаріла в даний момент, ми не завжди можемо використовувати дану можливість і захоплювати трафік просто прослуховуючи наш мережевий пристрій, тому потрібно мати ще один варіант захоплення даних мережі.

Дзеркалювання трафіку і буде таким ще одним варіантом. Ця технологія є здатністю копіювання пакетів одного порту мережного комутатора та окремих VLAN на інший порт [12]. На даний момент велика кількість мережних комутаторів, що налаштовуються, дозволяють віддзеркалити трафік від одного або навіть декількох портів, або VLAN на окремий порт виділений для даної потреби. Метод дзеркалювання використовується на мережних пристроях типу комутатор або маршрутизатор для відправки копій мережевих пакетів з даними, який може бачити користувач на вихідних портах, відправка відбувається на інші зазначені порти призначення. При ввімкненому зеркалюванні портів пакети ми

маємо можливість відстежувати та аналізувати їх.

Є два типи дзеркалювання: локальне та віддалене, відрізняються вони тим, що принцип роботи цих типів заснований на різних діапазонах дзеркалювання. Вони працюють за різними схемами [12].

Локальне зеркалювання портів - це проста форма дзеркалювання. Всі першочергові порти знаходяться на тому мережному пристрої, на якому і порт призначення. Копіювання трафіку локального порту дає можливість мережному пристрою переслати копію пакета даних з порту, звідки була відправлена інформація на порт призначення. Далі пристрій відстеження, встановлений на порт призначення, може отримувати та аналізувати пакет (рис. 2.3).

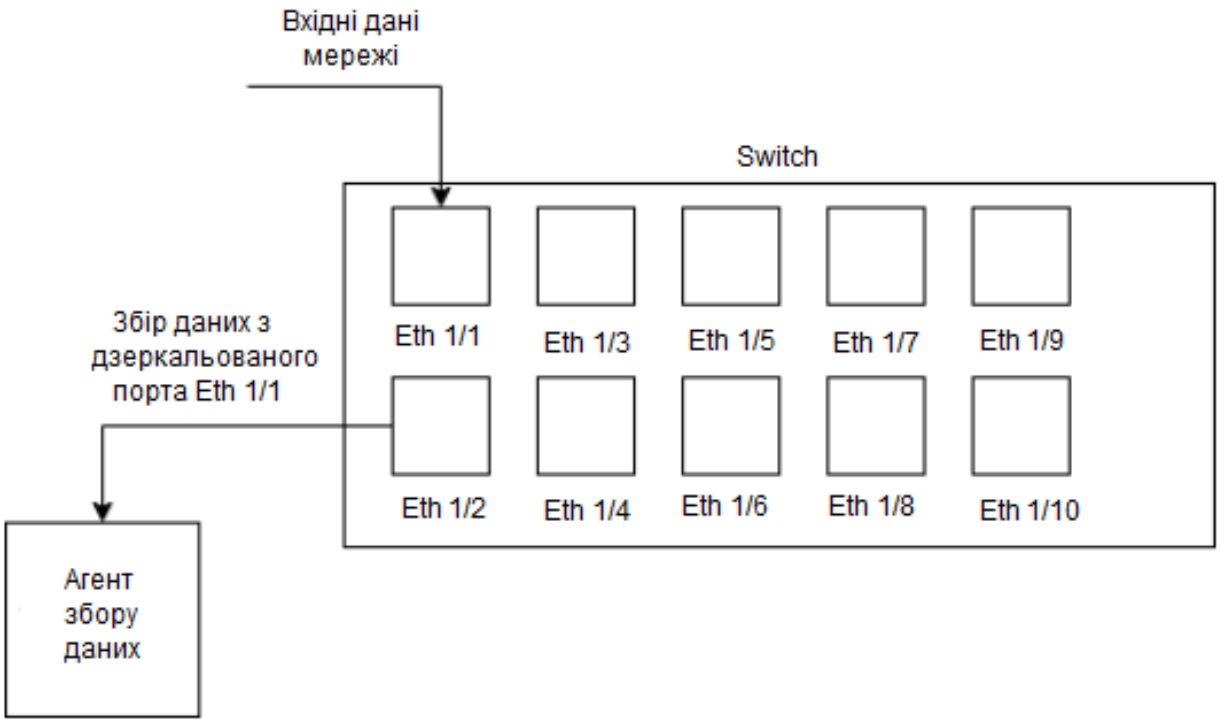

Рисунок 2.3 – Принцип роботи локального дзеркалювання портів

Для віддзеркалення віддалених портів основна відмінність у тому, що порт з вихідними даними та порт призначення знаходяться на різних пристроях (рис. 2.4). Порт з вихідними даними знаходиться першому комутаторі, а порт призначення - другому комутаторі. Вихідний порт відправляє копію віддзеркаленого пакета до порту призначення за допомогою з'єднання висхідної

лінії зв'язку, досягнутого портами на двох даних комутаторах. Надалі копіювання даних локальних портів дозволяє здійснювати моніторинг і аналіз даних на різних пристроях [12].

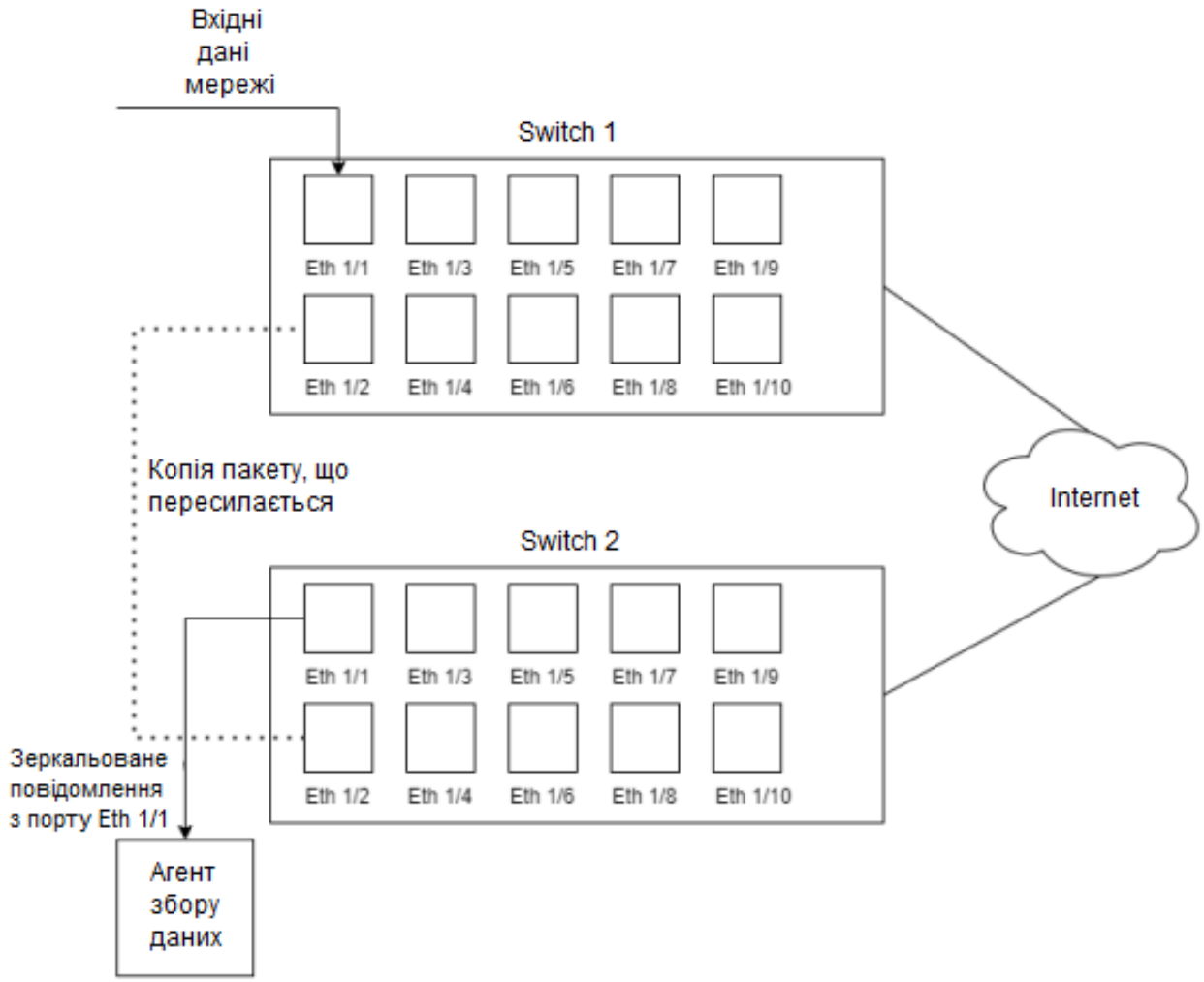

Рисунок 2.4 – Принцип роботи віддаленого дзеркалювання портів

Найбільш універсальним і відповідним варіантом є функція дзеркалювання трафіку. Дана здатність комутатора, створена для перенаправлення потоку даних мережі з одного порту мережного пристрою на інший порт цього ж мережного пристрою або на віддалений порт комутатора чи іншого пристрою з подібним функціоналом. Вихідний порт копіює потік даних, що відповідає за заданими правилами від клієнта до порту призначення, який згодом відправляє скопійований потік даних на пристрій моніторингу . Даний потік даних трафіку може бути налаштований за допомогою ACL (Access Control

List) або команд конфігурації. При дзеркалюванні трафіку на пристрій моніторингу даних мережі надсилаються лише вибраний або узгоджений трафік, а при дзеркалюванні портів копіюється кожен пакет, який проходить через інтерфейс, на пристрій моніторингу (рис. 2.5).

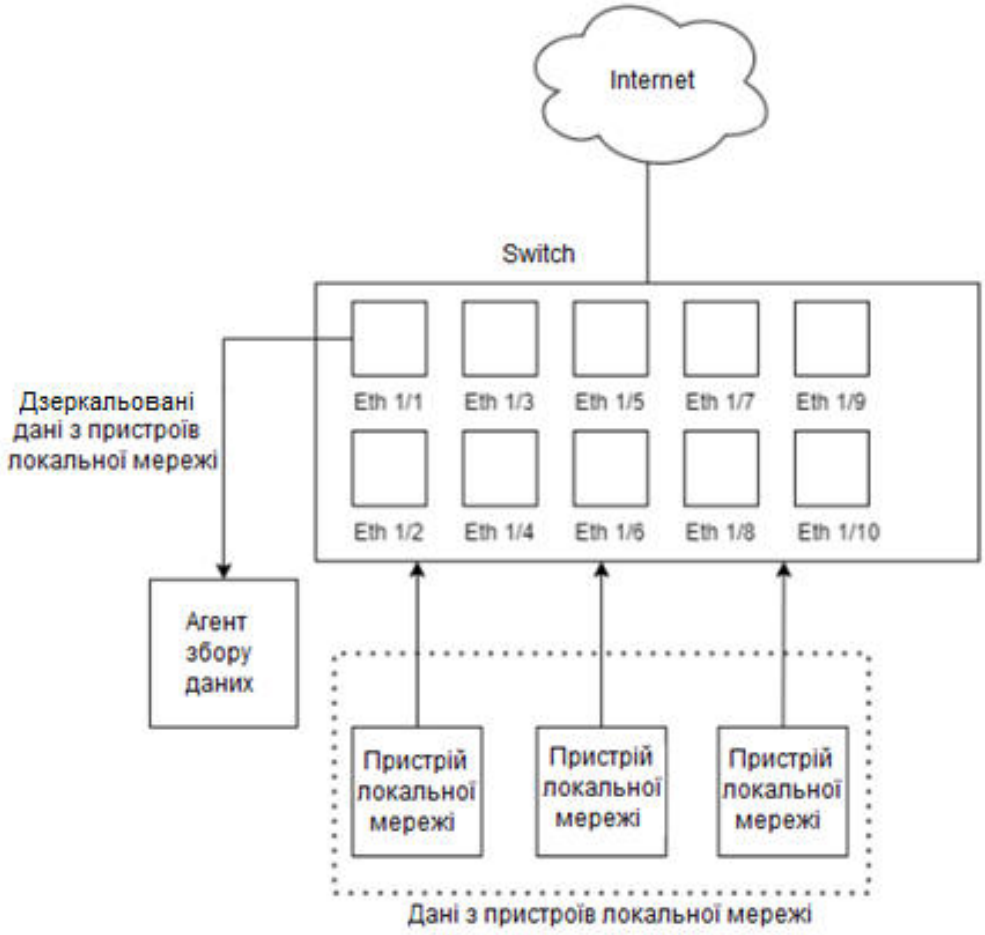

Рисунок 2.5 – Принцип роботи дзеркалювання трафіку

2.2 Функціонал агента зі збору даних

Агент зі збору даних - це додатковий пристрій в мережі, функціонал якого розрахований на отримання даних мережі для подальшого аналізу мережі. Отримання даних відбувається за допомогою сніферів (sniffers) [13].

Сніфери — це ПЗ, котре здатне прослуховувати, перехоплювати та аналізувати мережевий трафік. Сніфери використовуються у разі, коли необхідно отримати з потоку даних трафіку мережі будь-які відомості або

провести діагностику цієї самої мережі. Програму потрібно встановити на пристроях, до яких має доступ користувач, і протягом деякого проміжку часу отримати всі можливі для отримання передані дані.

Так як отримання даних відбувається на різних ділянках мережі, всі сніфери повинні бути синхронізовані між собою для точного відстеження даних мережі для подальшого аналізу трафіку. Дані, які отримує сніфер, перетворюються на пакети даних для подальшого транспортування [13].

Агенти зі збору повинні одночасно вмикатися та починати отримання трафіку упродовж певного часу. Увімкнення відбувається за сигналом користувача. Після того як сніфери виконують своє завдання зі збору трафіку, дані передаються на основний пристрій де вже і буде аналіз з отриманої інформації з мережі. Процес ввімкнення та вимкнення сніферів контролює користувач віддалено з основного пристрою.

2.3 Завдання основного ПЗ

На рис. 2.6 наведена схема локальної мережі, в яку впроваджено систему зі збору інформації та передачу отриманих даних в основну програму .

Першим завданням основної програми буде робота з даними трафіку, отриманими за допомогою агентів зі збору даних мережі. Підготовка отриманих даних до подальшого аналізу шляхом визначення вмісту пакетів даних.

Далі потрібно провести зіставлення даних між собою, отриманих на різних ділянках мережі. Це необхідно для точного визначення та відстеження маршруту даних та подальшого аналізу, що відбувається у нашій локальній мережі.

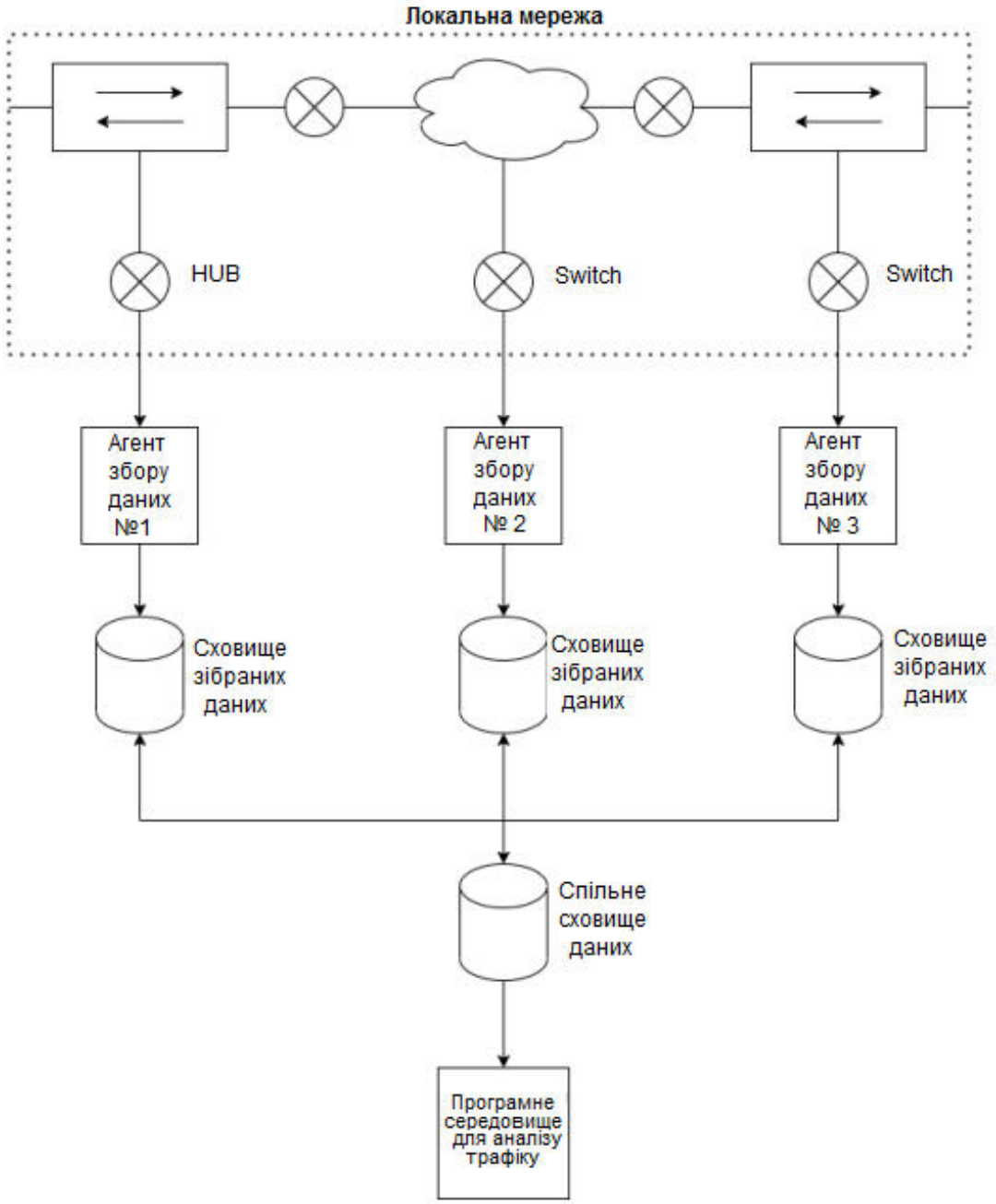

Рисунок 2.6 – Структурна схема розробки

Після завантаження даних у нашу програму підготовки пакетів потрібно перейти до аналізу отриманої інформації (рис. 2.7). Дані можуть аналізуватися користувачем шляхом порівняння параметрів мережі, які будуть демонструватися на екрані.

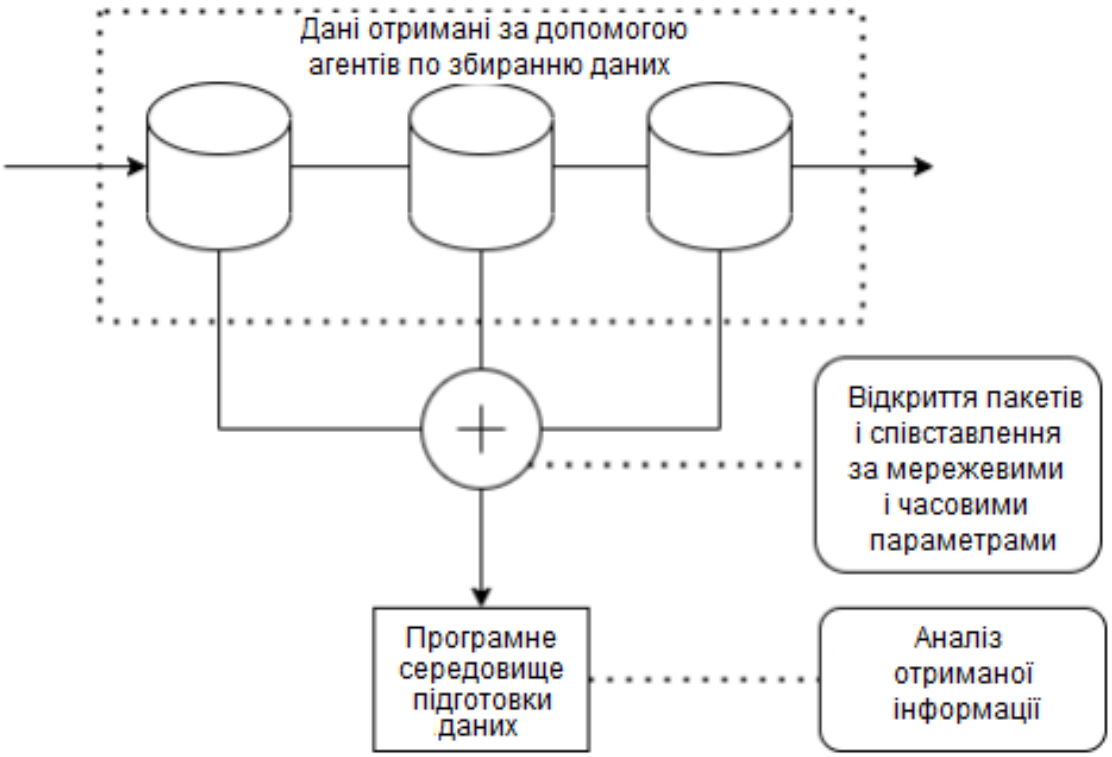

Рисунок 2.7 – Схема завантаження даних у програму

Також необхідно розглянути варіанти якщо в мережі може бути NAT.

2.4 Засоби програмної розробки

2.4.1 Мова програмування

Програма розроблятиметься об'єктно-орієнтованою мовою C# [14]. Вона створена в 1998 році групою фахвцями компанії Microsoft. Основним її завданням є створення програм для платформи Microsoft .NET Framework і .NET Core.

C# має C –подібну граматичну будову, котра дуже близька до C++ чи Java. Володіє статичною типізацією, підтримує такі можливості як: поліморфізм, перевантаження операторів, делегати, атрибути, події, змінні, властивості, узагальнені типи та методи, ітератори, анонімні функції з підтримкою замикань, LINQ, вийнятки, коментарі у форматі XML [14]. Ця мова отримала значний багаж від своїх предків - мов C++, Delphi, Модула, Smalltalk і, найперше, Java.

C#, спирається на досвід їх застосування, виключаючи кілька моделей, що виявили себе як задачі, котрі мають проблематичні ситуації при побудові склданих проєктів [15]. Для прикладу, C# на противагу C++ не має можливості підтримувати множинне успадкування класів.

2.4.2 Бібліотека обробки мережевих пакетів

SharpPcap - це бібліотека для захоплення, відкриття та обробки мережевих пакетів [16]. На даний момент SharpPcap активно розвивається так як є бібліотекою з відкритим вихідним кодом. Код бібліотеки розміщений на майданчику SourceForge. SharpPcap є повністю керованою кросплатформною бібліотекою. Бібліотека працює на тій же збірці, на якій працює під Microsoft .NET також як Моно на 32 або 64-бітових платформах. Даний список демонструє можливості, які зараз підтримуються в SharpPcap [17]:

– одна збірка для Microsoft. NET і Моно платформ на Windows (32 або 64- розрядні), Linux (32 або 64 біт) та Mac;

– висока продуктивність — SharpPcap дозволяє захоплювати дані до > 3MB/s швидкості передачі

– WinPcap частково підтримує віддалене захоплення пакетів, налаштування розміру буфера ядра, ін'єкції пакетів, використовуючи надсилання черг;

– збір мережевої статистики за певним мережевим інтерфейсом;

– підтримка AirPcap;

– перерахування та відображення докладних відомостей про фізичних мережевих інтерфейсів на WindQws – машині;

– захоплення низькорівневих мережевих пакетів, що проходять через певний інтерфейс;

– використання Packet.Net для аналізу пакетів;

– читання та запис у pcap файли.

Packet.Net підтримує для аналізу та аналізу такі протоколи:

– SLL (Linux Cooked-Mode Capture);

– Ethernet;
– ARP (Address Resolution Protocol)
– IP (Internet Protocol);
– IPv4;
– IPv6;
– TCP ;
– UDP (User Datagram Protocol);
– ICMP (Internet Control Message Protocol);
– ICMPv4;
– ICMPv6;
– IGMPv2;
– PPPoE;
– PTP;
– LLDP
– Wake-on-LAN (WOL);
– SharpPcap має багаторівневу архітектуру, на верхньому рівні класи, які працюють з усіма пристроями:;
– CaptureDeviceList — повертає список усіх пристроїв у системі
– ICaptureDevice — усі пристрої захоплення мають інтерфейс ICaptureDevice.

Ієрархія простору імен:

– LibPcap;
– LibPcapLiveDevice – IcaptureDevice;
– LibPcapLiveDeviceList - запитує список пристроїв (він включає pcap/ winpcap та airpcap пристрої);
– CaptureFileReaderDevice - пристрій, який зчитує з Pcap-файлу;
– CaptureFileWriterDevice - пристрій, який створює та записує в Pcap – файл;
– WinPcap;
– WinPcapDeviceList - запитує список WinPcapDevices (він включає

winpcap і airpcap пристрої);

– WinPcapDevice - LibPcapLiveDevice з додатковими WinPcap функціями та інтерфейсами;

– AirPcap;

– AirPcapDeviceList - запитує список AirPcapDevices;

– AirPcapDevice — WinPcapDevice з додатковими AirPcap функціями та інтерфейсами.

CaptureDeviceList повертає список усіх пристроїв. Кожен із ICaptureDevice буде або LibPcapLiveDevice, WinPcapDevice або AirPcapDevice. Це дозволяє отримати всі пристрої та диференціювати їх за типами. Якщо ви хочете отримати конкретний тип пристрою, можна використовувати один із спеціальних класів DeviceList .

2.4.3 Платформа створення інтерфейсу C#

WPF є платформою користувацького інтерфейсу, яка широко застосовується для розробки клієнтських застосунків системах [18]. Вона володіє підтримкою значного числа елементів для створення ПЗ, включно із моделлю програми, ресурсами, компонентами керування, графічними елементами, макетами, засобами прив'язки даних і т.п.

WPF є складовою платформи .NET і застосовує XAML для того, щоб забезпечити декларативну модель для розробки застосунків [19].

2.5 Висновки до розділу

Було спроектовано структурну схему розробки та продемонстровано принцип її роботи.

Описано принцип роботи основної програми з аналізу трафіку, а також показаний спосіб отримання даних мережі за допомогою створеного ПЗ та утиліт, котрі вбудовані у мережеве устаткування.

Також були виділені необхідні функції, які має реалізувати додаток:

– відкриття пакетів даних мережі та розбиття на параметри для аналізу;

– синхронізація пакетів даних за часом відправлення та прибуття;

– синхронізація пакетів даних за параметрами IP та MAC адрес;

– можливість перегляду даних за допомогою користувальницького інтерфейсу;

– необхідно розглянути можливість зіставлення даних у мережі з NAT.

.

РОЗДІЛ 3 ПРАКТИЧНА ЧАСТИНА

3.1 Функції програми

Основною функцією програми є розкриття файлів формату Pcap. Бібліотека SharpPcap має функції, що дозволяють проводити розбір за параметрами, які зберігаються в пакетах даних [17]. Пакети з даними передаватимуться в основну програму з агентів на віддалених пристроях (рис. 3.1).

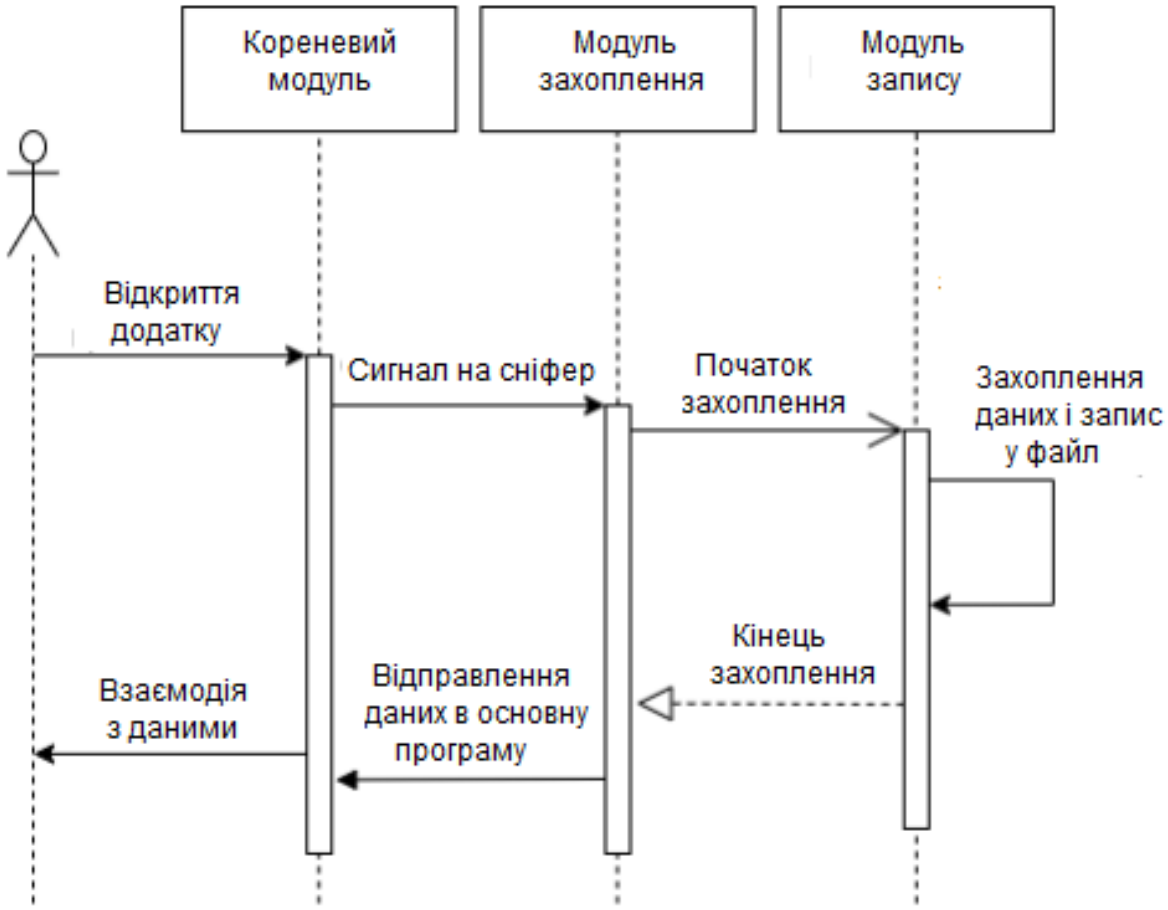

Рисунок 3.1 –UML діаграма

3.1.1 Функціонал ПЗ для захоплення трафіку

ПЗ для захоплення трафіку заздалегідь встановлено і запущено на пристроях в мережі. Агенти синхронізуються між собою та основним ПЗ та очікують сигналу на початок запуску прослуховування трафіку. Користувачеві необхідно переконатися перед початком роботи, що зв'язок з усіма агентами встановлений шляхом надсилання сигналу та отримання відповіді. Далі користувач встановлює часові рамки для початку та закінчення роботи агента. Агент починає захоплення пакетів із даними упродовж встановленого часу. Після закінчення захоплення агенти відсилають пакети з даними в основне сховище. Файли з основного сховища потрапляють основну програму, де і відбувається подальша взаємодія користувача з інформацією.

3.1.2 Функція OpenFileDialog

Пакети завантажуються в програму за допомогою функції WPF OpenFileDialog. Дана функція дозволяє відкривати провідник Windows в попередньо прописаному каталозі і відбирати дані за вказаними критеріями. Вибираючи потрібний файл у провіднику, ми отримуємо та завантажуємо в програму такі параметри, як місцезнаходження файлу в системі та ім'я файлу.

На рис. 3.2 наведено фрагмент коду програми з цією функцією:

```
1.  var filePath = string.Empty;
2.  string capFile;
3.  using (OpenFileDialog openFileDialog = new OpenFileDialog())
4.  {
5.  openFileDialog.InitialDirectory = "c:\\";
6.  openFileDialog.Filter = "pcapng files (*.pcapng)|*.pcapng|All files (*.*)|*.*";
7.  openFileDialog.FilterIndex = 2;
8.  openFileDialog.RestoreDirectory = true;
9.  if (openFileDialog.ShowDialog() == DialogResult.OK)
10. {
11. //Get the path of specified file
12. filePath = openFileDialog.FileName;
13. //Read the contents of the file into a stream
14. }
```

Рисунок 3.2 – Фрагмент коду функції OpenFileDialog

На рис. 3.3 показано алгоритм функції завантаження файла у програму.

Рисунок 3.3 – Порядок дій при завантаженні файла у програму

3.1.3 Функція OpenRead

Після отримання інформації про місцезнаходження файлу в нашій системі, ми передаємо цю інформацію у функцію OpenRead, де відбувається відкриття цього файлу за допомогою функціоналу бібліотеки SharpPcap [17].

Фрагмент коду програми з цією функцією наведено на рис. 3.4.

```
1.  public static void OpenRead(string capFile)
2.  {
3.  packetIndex = 0;
4.  ICaptureDevice device;
5.  device = new CaptureFileReaderDevice(capFile);
6.  device.Open();
7.  device.OnPacketArrival += device  OnPacketArrival;
8.  device.StartCapture();
9.  System.Threading.Thread.Sleep(50);
10. }
```

Рисунок 3.4 – Фрагмент коду функції OpenRead

На рис. 3.5 відображено алгоритм функції OpenRead.

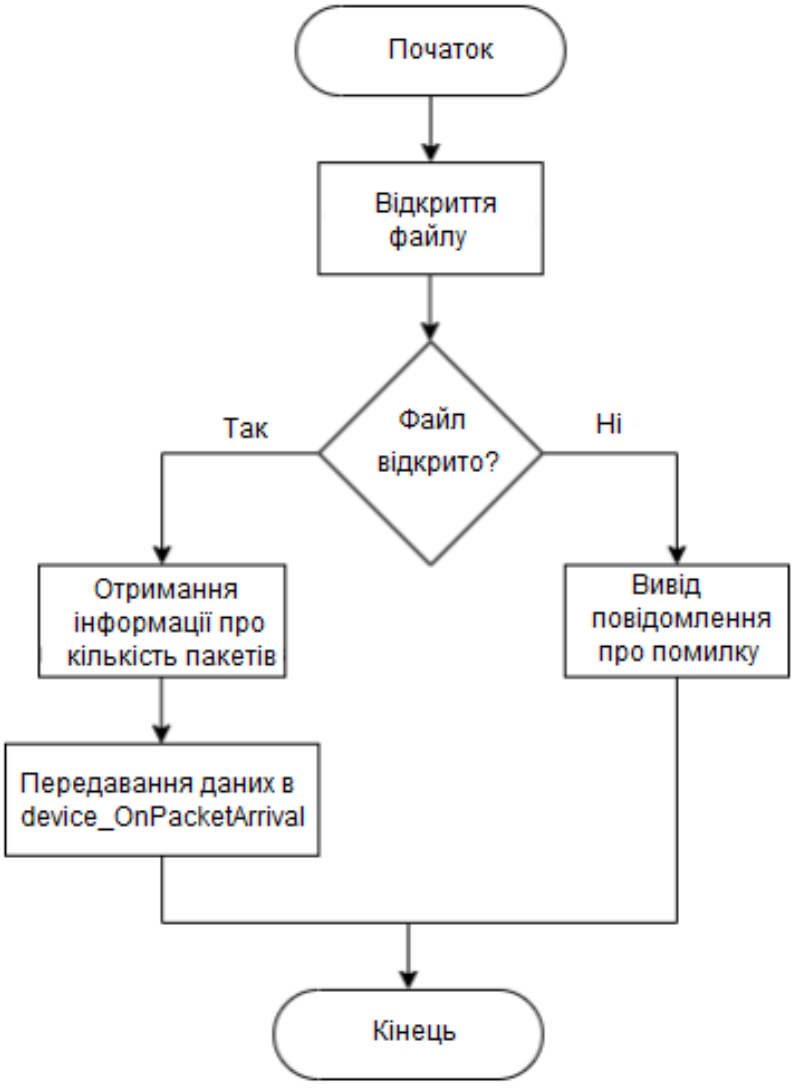

Рисунок 3.5 – Блок-схема алгоритму функції відкриття файлу

3.1.4 Функція device_OnPacketArrival

Далі ми переходимо в подію device_OnPacketArrival, в якій відбувається розбір відкритого нами файлу на параметри, які потрібно буде продемонструвати користувачеві. Отримання параметрів відбувається за допомогою функції бібліотеки SharpPcap.

На рис. 3.6 показано фрагмент коду програми з цією подією.

```
1.  private static void device_OnPacketArrival(object sender, PacketCapture e)
2.  {
3.  var rawPacket = e.GetPacket();
4.  var packet = PacketDotNet.Packet.ParsePacket(rawPacket.LinkLayerType,
rawPacket.Data);
5.  var ethernetPacket = packet.Extract<EthernetPacket>();
6.  index = packetIndex;
7.  if (ethernetPacket != null)
8.  {
9.  var srsadd = new Regex(@"SourceAd-
dress=\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b");
10.  var protocol = new Regex(@"Protocol=\b\d{1,5}\b");
11.  TimevalDate.Add(e.Header.Timeval.Date.ToString());
12.  Millisecond.Add(e.Header.Timeval.Date.Millisecond.ToString());
13.  DestinationMACAddress.Add(ethernetPacket.DestinationHardwareAd-
dress.ToString());
```

Рисунок 3.6 – Фрагмент коду функції device_OnPacketArrival

На рис. 3.7 відображено блок-схему алгоритму функції розпакування даних пакета.

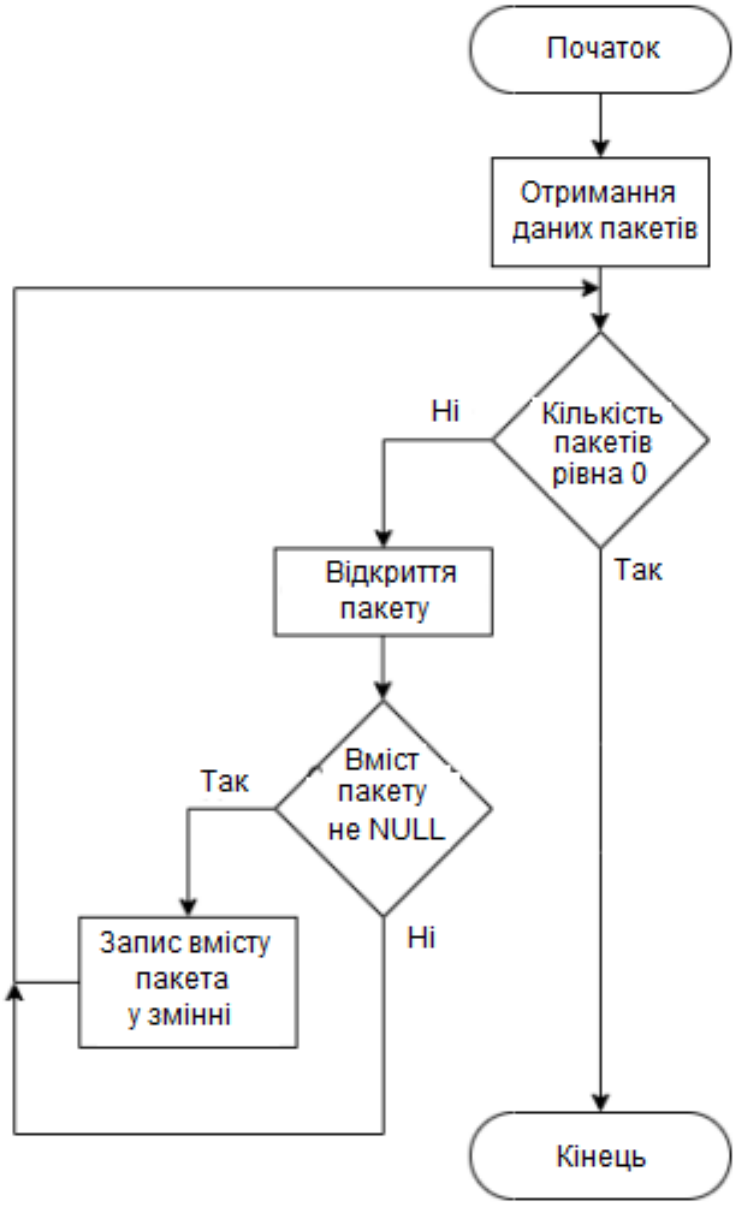

Рисунок 3.7 – Блок-схема алгоритму роботи функції device_OnPacketArrival

3.1.5 Функція treeView

Після зчитування необхідних параметрів необхідно провести демонстрацію отриманих даних із пакета. Інформацію буде виводитися у вигляді деревоподібної структури у вікнах treeView які взяті з функціоналу WPF.

Фрагмент коду даної функції наведено на рис. 3.8.

```
1.  treeView.Nodes.Clear();
2.  for (int i = 0; i < PcapFunck.index; i++)
3.  {
4.  treeView.BeginUpdate();
5.  treeView.Nodes.Add("Packet№" + i);
6.  treeView.Nodes[i].Nodes.Add("Timeval.Date:" + PcapFunck.Timeval-
Date[i]);
7.  treeView.Nodes[i].Nodes.Add("Millisecond:" + PcapFunck.Mil-
lisecond[i]);
8.  treeView.Nodes[i].Nodes.Add("SourceHardwareAddress MAC:" + Pcap-
Funck.SourceMACAddress[i]);
9.  treeView.Nodes[i].Nodes.Add("DestinationHardwareAddress  MAC:" +
PcapFunck.DestinationMACAddress[i]);
```

Рисунок 3.8 – Фрагмент коду функції treeView

Блок-схема функції виводу інформації на екран зображена на рис. 3.9.

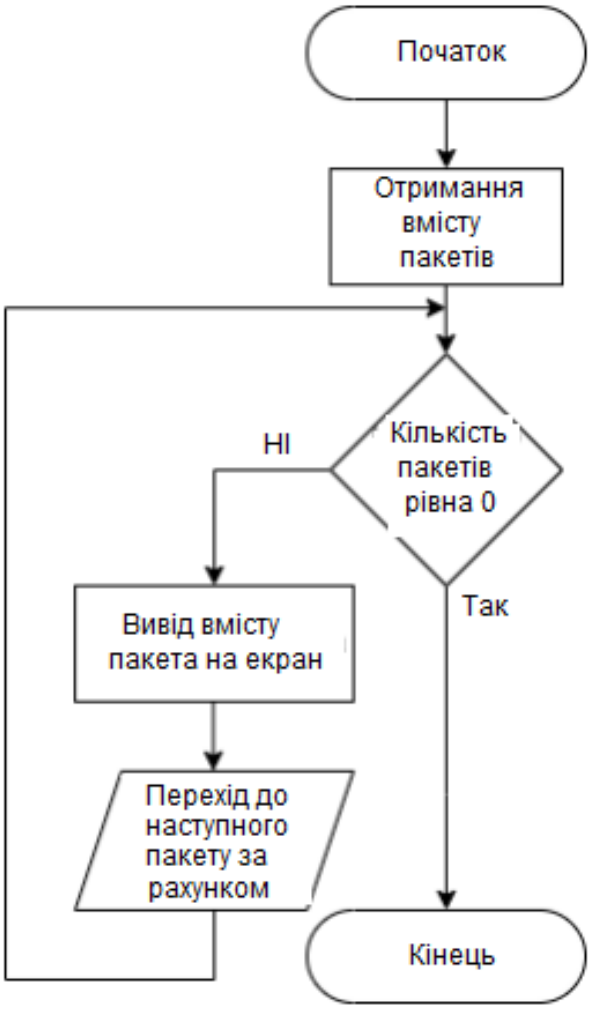

Рисунок 3.9 – Блок-схема алгоритму роботи функції treeView

3.2 Приклад роботи розробки

Розроблене ПЗ складається із декількох полів (рис. 3.10). Першим полем є статична карта пристроїв локальної мережі, з якою може взаємодіяти користувач. У цьому полі знаходяться кнопки, за допомогою яких користувач може завантажувати файли формату Pcap, отримані з пристроїв, на яких було заздалегідь здійснено захоплення трафіку мережі. На даний момент у програму можна завантажити до чотирьох таких файлів.

У другому полі відбувається виведення файлів, завантажених у програму. Користувач отримує інформацію з файлів у вигляді деревоподібної структури. Користувач має можливість отримувати більш докладну інформацію вмісту пакетів даних відкриваючи їх та зчитуючи такі дані як: source ip, destination ip, розмір пакета, часові характеристики.

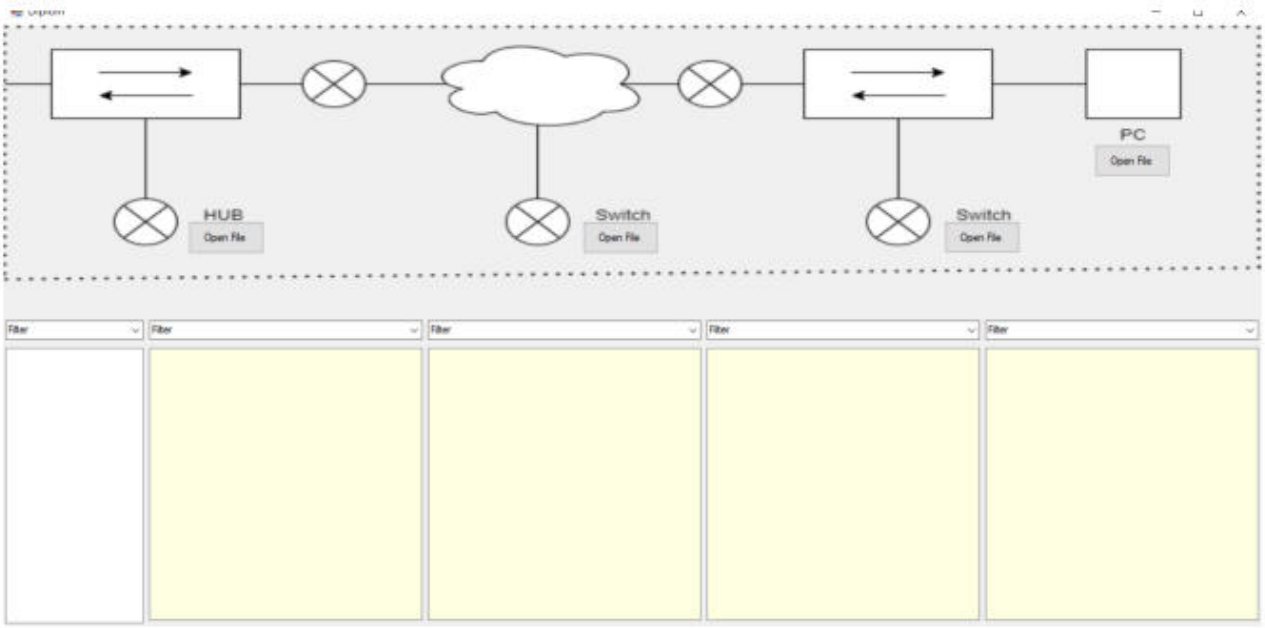

Рисунок 3.10 – Інтерфейс програми

Користувач може встановлювати фільтри, за допомогою яких змінюється вміст вікон виведення інформації за необхідними критеріями пакетів.

Кнопки для завантаження файлів знаходяться на статичній карті локальної мережі поруч із пристроями, з яких повинен братися заздалегідь перехоплені

дані трафіку мережі. Файли завантажуються в ту область на карті локальної мережі з якої вони були отримані (рис. 3.11).

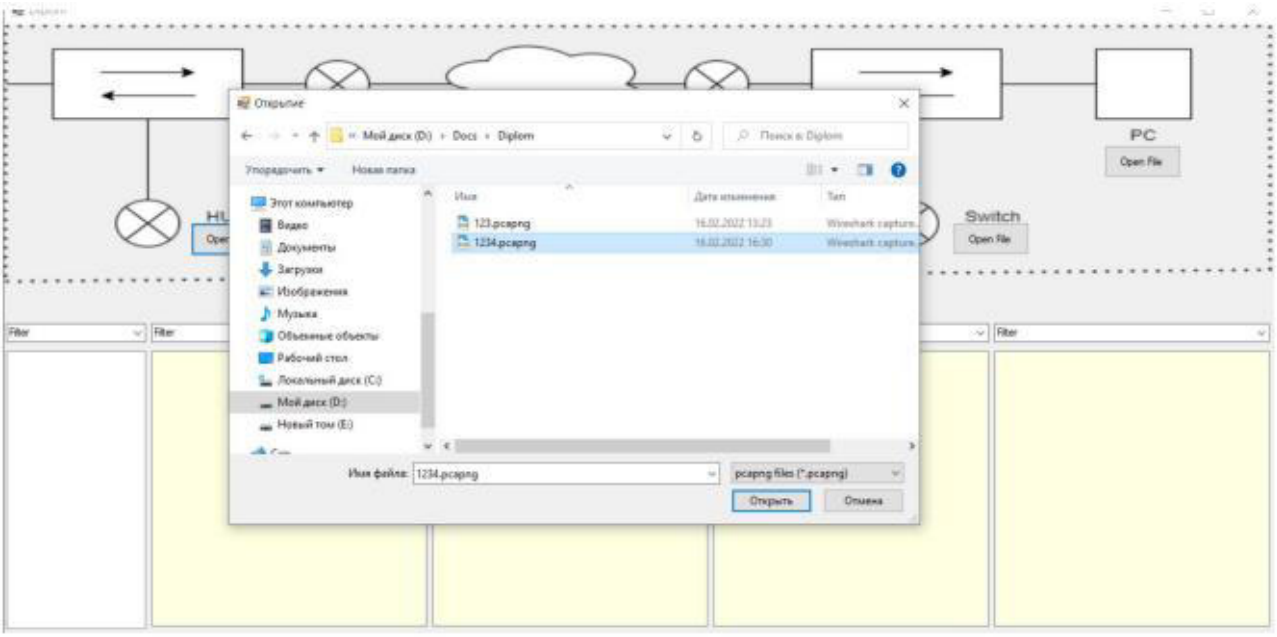

Рисунок 3.11 – Завантаження файлів Pcap

Інформація, що міститься в пакетах, виводиться в 5 різних вікнах. Перше вікно являє собою список тимчасових характеристик пакетів, він є єдиним для наступних чотирьох вікон, початок захоплення даних і закінчення проводилося одночасно.

Вікна з виведенням інформації про дані трафіку мережі заповнюються в міру завантаження файлів (рис. 3.12). Кожне вікно пов'язане з ділянкою на карті і демонстрація інформації відбудеться тоді, коли користувач завантажить файл за допомогою верхнього поля програми.

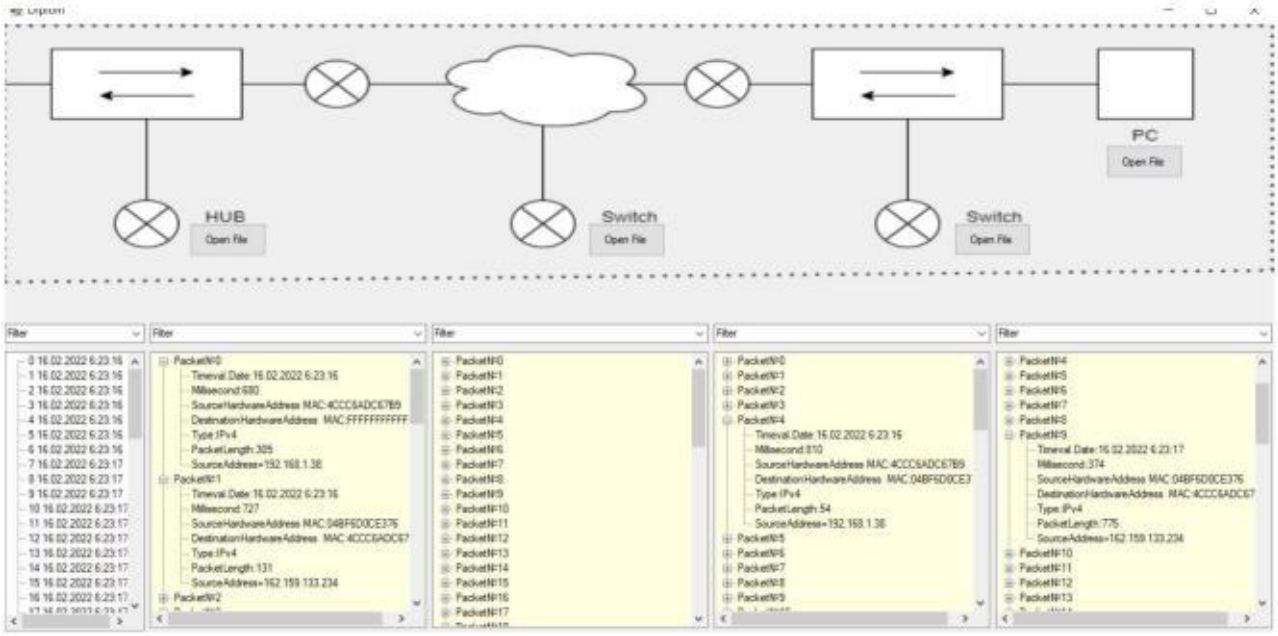

Рисунок 3.12 – Виведення інформації з пакетів

Над вікнами з виведенням інформації з пакетів даних розташовані текстові поля, призначені для зміни вмісту полів для виведення за певними критеріями, які необхідні користувачеві для подальшого аналізу трафіку. Якщо інформація записана в дане поле співпадатиме з інформацією в пакетах даних, то вміст вікна відсортується за наявності збігів (рис. 3.13).

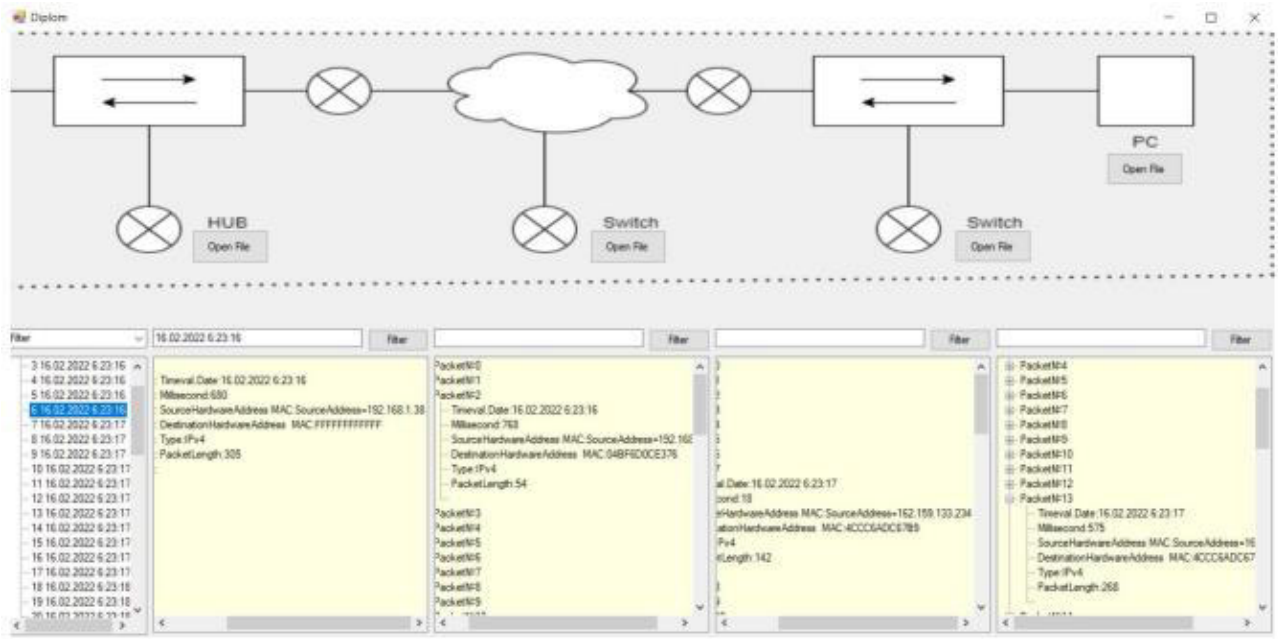

Рисунок 3.13 – Застосування функції фільтрації даних

3.3 Висновки до розділу

На основі сформульованих вимог у розділі 2 були визначені технології розробки. В результаті програмної реалізації було створено додаток мовою програмування C# з використанням платформи для створення інтерфейсу користувача WPF і бібліотеки для збору даних мережі SharpPcap.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Санітарно-гігієнічні вимоги до умов праці з ПК

Санітарні правила і норми влаштування і обладнання кабінетів комп'ютерної техніки в навчальних закладах та режиму праці учнів на персональних комп'ютерах встановлюють нормативи фізичних чинників, що створюються комп'ютерами при їх роботі, та гігієнічні вимоги до проектування, виготовлення і експлуатації вітчизняних та експлуатації імпортних персональних комп'ютерів, що застосовуються в навчально-виховному процесі.

Вимоги до приміщень та розташування робочих місць з ПК: приміщення, призначені для роботи з ПК, повинні мати природне освітлення. Орієнтація вікон повинна бути на північ або північний схід, вікна повинні мати жалюзі, які можна регулювати, або штори; не дозволяється розміщувати кабінети обчислювальної техніки у підвальних приміщеннях будинків; кабінети, обладнані комп'ютерною технікою, в навчальних закладах повинні розміщуватись в окремих приміщеннях з природним освітленням та організованим обміном повітря; стіни, стеля і підлога та обладнання кабінетів комп'ютерної техніки повинні мати покриття із матеріалів з матовою фактурою з коефіцієнтом відбиття: стін — 40- 50 %, стелі — 70 - 80 %, підлоги — 20-30 %, предметів обладнання — 40-60 % (робочого столу — 40-50 %, корпуса дисплею та клавіатури — 30-50 %, стелажів — 40-60 %); поверхня підлоги повинна мати антистатичне покриття та бути зручною для вологого прибирання; забороняється використовувати для оздоблення інтер'єру приміщень комп'ютерних кабінетів полімерні матеріали (дерев'яно-стружкові плити, шпалери, що придатні для миття, плівкові та рулонні синтетичні матеріали, шаровий паперовий пластик та ін.), що виділяють у повітря шкідливі хімічні речовини, які перевищують гранично допустимі концентрації; вміст

шкідливих хімічних речовин в повітрі дошкільних та учбових приміщень з комп'ютерною технікою не повинен перевищувати середньодобові концентрації [20].

Вимоги до освітлення приміщень та робочих місць: приміщення з ПК повинні мати природне та штучне освітлення; штучне освітлення в приміщеннях з ПК повинно здійснюватись системою загального освітлення; як джерела світла при такому освітленні повинні застосовуватись переважно люмінесцентні лампи; яскравість світильників загального освітлення в зоні кутів випромінювання від 50° до 90° з вертикаллю в поздовжній та поперечній площинах повинна складати не більше 200 кд/м^2, захисний кут світильників повинен бути не менше 40; загальне освітлення повинно бути виконано у вигляді суцільних або переривчастих ліній світильників; штучне освітлення повинно забезпечувати на робочих місцях в кабінетах з ПК освітленість не нижчу, а на екранах дисплеїв — не вище приведених в таблиці 4.1; коефіцієнт запасу для освітлювальних установок загального освітлення приймається рівним 1,4; необхідно проводити чищення скла вікон та світильників не менше двох разів на рік, а також заміну перегорілих ламп по мірі їх виходу з ладу; в кабінетах з ПК слід обмежити нерівномірність розподілу яскравості в полі зору учнів [20]. Співвідношення яскравості між робочим екраном та близьким оточенням не повинно перевищувати 5:1, між поверхнями робочого екрану і оточенням (стіл, обладнання) — 10:1; величина коефіцієнту пульсації освітленості не повинна перевищувати 5 %. Газорозрядні лампи повинні застосовуватись в світильниках загального та місцевого освітлення з високочастотними пускорегулюючими апаратами; необхідно передбачити обмеження прямого блиску від джерел природного та штучного освітлення; яскравість великих поверхонь (вікна, світильники і таке інше), що знаходяться у полі зору, не повинна перевищувати 200 кд/м^2, мірою захисту від прямого блиску має бути зниження яскравості видимої частини джерел світла застосуванням спеціальних розсіювачів, відбивачів та інших світлозахисних пристроїв, а також правильне розміщення робочих місць відносно джерел світла; повинні передбачатись заходи щодо

обмеження відбитого блиску на робочих поверхнях (екран, стіл, клавіатура); яскравість полисків на екрані не повинні перевищувати 80 кд/кв. м. Яскравість стелі при застосуванні системи відбитого освітлення не повинна перевищувати 200 кд/кв. м.

Таблиця 4.1 — Норми освітленості в кабінетах з ПК

Характеристика роботи	Робоча поверхня	Площина	Освітленість,лк	Примітка
Робота переважно з екранами дисплеїв ПК (50 % та більше робочого часу)	Екран	вертикальна	200	не вище
	Клавіатура	горизонтальна	400	не нижче
	Стіл	горизонтальна	400	не нижче
Робота переважно з екранами дисплеїв ПК (менше 50 % робочого часу)	Екран	вертикальна	200	не вище
	Клавіатура	горизонтальна	400	не нижче
	Стіл	горизонтальна	500	не нижче
	Дошка	вертикальна	500	не нижче
Проходи основні	Підлога	горизонтальна	100	

Вимоги, що забезпечують захист від впливу іонізуючих та неіонізуючих електромагнітних полів та випромінювань: ВДТ на електронно-променевих трубках можуть бути потенційними джерелами гігієнічно значимих рівнів електромагнітних випромінювань в діапазоні частот 50Гц-300 МГц; інтенсивність ультрафіолетового випромінювання на відстані 0,3м від екрану не повинна перевищувати в діапазоні довжин хвиль 400 - 320 нм — 2 Вт/м^2, 320 - 280 нм — 0,002 Вт/м^2, ультрафіолетового випромінювання в діапазоні 280 - 200 нм — не повинно бути.

4.2 Вимоги до виробничого освітлення та його нормування

Приміщення для роботи з ВДТ повинні мати природне та штучне освітлення відповідно до ДБН В.2.5-28-2006 (на заміну СНиП II-4-79).

Природне освітлення має здійснюватись через світлові прорізи, орієнтовані переважно на північ чи північний схід і забезпечувати коефіцієнт природної освітленості не нижче ніж 1,5%. Розраховується він за методикою, викладеною в ДБН В.2.5-28-2006. За виробничої потреби дозволяється експлуатувати ЕОМ у приміщеннях без природного освітлення за узгодженням з органами державного нагляду за охороною праці та органами і установами санітарно-епідеміологічної служби. Вікна приміщень з ВДТ повинні мати регулювальні пристрої для відкривання, а також жалюзі, штори, зовнішні козирки та ін.

Штучне освітлення приміщення з робочими місцями, обладнаними ВДТ ЕОМ загального та персонального користування, має бути обладнане системою загального рівномірного освітлення. У виробничих та адміністративно-громадських приміщеннях, де переважають роботи з документами, допускається вживати систему комбінованого освітлення (додатково до загального освітлення встановлюються світильники місцевого освітлення).

Загальне освітлення має бути виконане у вигляді суцільних або переривчатих ліній світильників, що розміщуються збоку від робочих місць (переважно зліва) паралельно лінії зору працівників. Допускається застосовувати світильники таких класів світлорозподілу: світильники прямого світла – П; переважно прямого світла – Н; переважно відбитого світла – В. При розташуванні ВДТ за периметром приміщення лінії світильників штучного освітлення повинні розміщуватися локально над робочими місцями. Для загального освітлення необхідно застосовувати світильники із розсіювачами та дзеркальними екранними сітками або віддзеркалювачами, укомплектовані високочастотними пускорегулювальними апаратами (ВЧ ПРА). Застосування світильників без розсіювачів та екранних сіток забороняється [21].

Як джерело світла при штучному освітленні повинні застосовуватися, як правило, люмінесцентні лампи типу ЛБ. При обладнанні відбивного освітлення у виробничих та адміністративно-громадських приміщеннях можуть

застосовуватися металогалогенні лампи потужністю до 250 Вт. Допускається у світильниках місцевого освітлення застосовувати лампи розжарювання.

Яскравість світильників загального освітлення в зоні кутів випромінювання від 50º до 90º відносно вертикалі в подовжній і поперечній площинах повинна складати не більше 200 кд/м2, а захисний кут світильників повинен бути не більшим за 40º. Коефіцієнт запасу відповідно до ДБН В.2.5-28-2006 для освітлювальної установки загального освітлення слід приймати рівним 1,4. Коефіцієнт пульсації повинен не перевищувати 5 % і забезпечуватися застосуванням газорозрядних ламп у світильниках загального і місцевого освітлення. За відсутності світильників з ВЧ ПРА лампи багатолампових світильників або розташовані поруч світильники загального освітлення необхідно підключати до різних фаз трифазної мережі.

Рівень освітленості на робочому столі в зоні розташування документів має бути в межах 300…500 лк. У разі неможливості забезпечити даний рівень освітленості системою загального освітлення допускається застосування світильників місцевого освітлення, але при цьому не повинно бути відблисків на поверхні екрану та збільшення освітленості екрану більше ніж до 300 лк. Світильники місцевого освітлення повинні мати напівпрозорий відбивач світла з захисним кутом не меншим за 40º. Необхідно передбачити обмеження прямої блискості від джерела природного та штучного освітлення, при цьому яскравість поверхонь, що світяться (вікна, джерела штучного світла) і перебувають у полі зору, повинна бути не більшою за 200 кд/м2. Необхідно обмежувати відбиту блискість шляхом правильного вибору типів світильників та розміщенням робочих місць відносно джерел природного та штучного освітлення. При цьому яскравість відблисків на екрані відеотерміналу не повинна перевищувати 40 кд/м2, яскравість стелі при застосуванні системи відбивного освітлення не повинна перевищувати 200 кд/м2 [21].

Необхідно обмежувати нерівномірність розподілу яскравості в полі зору осіб, що працюють з відеотерміналом, при цьому відношення значень яскравості

робочих поверхонь не повинно перевищувати 3:1, а робочих поверхонь і навколишніх предметів (стіни, обладнання) – 5:1.

Необхідно використовувати систему вимикачів, що дозволяє регулювати інтенсивність штучного освітлення залежно від інтенсивності природного, а також дозволяє освітлювати тільки потрібні для роботи зони приміщення.

Для забезпечення нормованих значень освітлення в приміщеннях з відеотерміналами ЕОМ загального та персонального користування необхідно очищати віконне скло та світильники не рідше ніж 2 рази на рік, та своєчасно проводити заміну ламп, що перегоріли.

ВИСНОВКИ

В результаті виконання роботи була вивчена предметна область і існуючі на даний момент аналоги.

Після вивчення аналогів було сформульовано низку вимог, пред'явлених до додатку. Програма була написана мовою C# з використанням платформи для створення інтерфейсу користувача WPF і бібліотеки для збору даних мережі SharpPcap.

Була створена структура програмного середовища, описані принципи роботи основного додатку з підготовки трафіку до аналізу, а також показаний спосіб отримання даних мережі за допомогою створеного ПЗ та утиліт, вбудованих у мережеве обладнання.

В результаті була розроблена система отримання даних з пристроїв локальної мережі, що дозволяє проводити попередню підготовку інформації до обробки.

Було розроблено додаток обробки великої кількості отриманої інформації, в якому визначаються і виділяються необхідні параметри даних мережі, що готує дані з різних пристроїв мережі до подальшого аналізу та демонстрації, що дозволяє користувачеві виділяти тимчасові та неявні залежності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Інформаційна безпека: навчальний посібник / За ред. Ю.Я. Бобала, І.В. Горбатого. Львів: Видавництво Львівської політехніки, 2019. 580 с.

2. "Network Security: Private Communication in a Public World". Charlie Kaufman, Radia Perlman, Mike Speciner (2021).

3. Остапов С.Є, Євсєєв С.П., Король О.Г. Технології захисту інформації. Львів: Новий світ-2000. 2020. 500 с.

4. Wireshark. URL: https://www.wireshark.org/ (дата звертання: 20.04.2024).

5. Tcpdump. URL: https://www.tcpdump.org/manpages/tcpdump.1.html (дата звертання: 20.04.2024).

6. Kismet. URL: https://www.kismetwireless.net (дата звертання: 21.04.2024).

7. Etherape. URL: https://etherape.sourceforge.io/ (дата звертання: 21.04.2024).

8. Cain and Abel. URL: https://en.wikipedia.org/wiki/ Cain_and_Abel_(software) (дата звертання: 21.04.2024).

9. NetworkMiner. URL: https://www.netresec.com/?page=NetworkMiner (дата звертання: 22.04.2024).

10. KisMAC. URL: https://kismacng.org/ (дата звертання: 22.04.2024).

11. Що таке міжмережевий екран і навіщо він ротрібен? URL: https://stack-systems.com.ua/blogs/shtcho-take-mizmerezevyj-ekran-i-navishtcho-vin-potriben (дата звертання: 27.04.2024).

12. CCNA Security 210-260. Official Cert Guide / Omar Santos, John Stuppi. Cisco Press, 2015. 658 p

13. Сніфери, та де вони мешкають. URL: https://qaukraine.online/snifery-ta-de-vony-meshkaiut/ (дата звертання: 29.04.2024).

14. Що таке мова C# (C-Sharp) і навіщо її вивчати? URL: https://w3schoolsua.github.io/cs/index.html#gsc.tab=0 (дата звертання: 30.04.2024).

15. Ерік Фрімен, Елізабет Робсон. Head First. Патерни проєктування. Харків: Фабула, 2020, 672 с.

16. Sharppcap. URL: https://github.com/dotpcap/sharppcap (дата звертання: 30.04.2024).

17. Sharppcap. URL: https://sourceforge.net/projects/sharppcap/ (дата звертання: 02.05.2024).

18. WPF. URL: https://wpf-tutorial.com/uk/1 po-wpf/що-таке-wpf/ (дата звертання: 02.05.2024).

19. Windows Presentation Foundation. URL: https://www.wikidata.uk-ua.nina.az/Windows_Presentation_Foundation.html (дата звертання: 03.05.2024).

20. Основи охорони праці: Підручник.; 3-те видання, доповнене та перероблене / За ред. К. Н Ткачука. К.: Основа, 2011. 480 с.

21. Яремко З. Безпека життєдіяльності: Навч. посіб. Львів., 2005. 301 с.

22. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі. Книга 1 [навчальний посібник]. Львів : «Магнолія 2006», 2013. 256 с.

23. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі. Книга 2. [навчальний посібник]. Львів : "Магнолія 2006", 2014. 312 с.

24. Лупенко С. А., Пасічник В. В., Тиш Є. В. Комп'ютерна логіка. Львів: Видавництво «Магнолія - 2006». 2015. 354 с.

25. Осухівська Г. М., Тиш Є. В., Луцик Н. С., Паламар А. М. Методичні вказівки до виконання кваліфікаційних робіт здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 123 «Комп'ютерна інженерія» усіх форм навчання. Тернопіль, ТНТУ. 2022. 28 с.

Додаток А.

Технічне завдання

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп’ютерно-інформаційних систем і програмної інженерії

Кафедра комп’ютерних систем та мереж

“Затверджую”

Завідувач кафедри КС

_____ Осухівська Г.М.

“___” _____2024 р

КОМП'ЮТЕРНА СИСТЕМА АНАЛІЗУ ТРАФІКУ ЛОКАЛЬНОЇ МЕРЕЖІ

ТЕХНІЧНЕ ЗАВДАННЯ

на _8_ листках

Вид робіт: Кваліфікаційна робота

На здобуття освітнього ступеня «Бакалавр»

Спеціальність 123 «Комп’ютерна інженерія»

«УЗГОДЖЕНО»	«ВИКОНАВЕЦЬ»
Керівник кваліфікаційної роботи	Студент групи СІ-41
_____ к.т.н., доц. Баран І.О.	_____ Лукашук В.О.
«____» _____ 2024 р.	«____» _____ 2024 р.

Тернопіль 2024

1 Загальні відомості

1.1 Повна назва та її умовне позначення

Повна назва теми кваліфікаційної роботи: «Комп'ютерна система аналізу трафіку локальної мережі».

Умовне позначення кваліфікаційної роботи: КС КРБ 123.120.00.00

1.2 Виконавець

Студент групи СІ-41, факультету комп’ютерно-інформаційних систем і програмної інженерії, кафедри комп’ютерної інженерії, Тернопільського національного технічного університету імені Івана Пулюя, Лукашук Владислав Олегович.

1.3 Підстава для виконання роботи

Підставою для виконання кваліфікаційної роботи є наказ по університету (№ 4/7-408 від 24.04.2024 р.)

1.4 Планові терміни початку та завершення роботи

Плановий термін початку виконання кваліфікаційної роботи – 24.04.2024 р.

Плановий термін завершення виконання кваліфікаційної роботи – 25.06.2024 р.

1.5 Порядок оформлення та пред’явлення результатів роботи

Порядок оформлення пояснювальної записки та графічного матеріалу здійснюється у відповідності до чинних норм та правил ІСО, ГОСТ, ЕСКД, ЕСПД та ДСТУ.

Пред’явлення проміжних результатів роботи з виконання кваліфікаційної роботи здійснюється у відповідності до графіку, затвердженого керівником роботи.

Попередній захист кваліфікаційної роботи відбувається при готовності роботи на 90% , наявності пояснювальної записки та графічного матеріалу.

Пред’явлення результатів кваліфікаційної роботи відбувається шляхом захисту на відповідному засіданні ЕК, ілюстрацією основних досягнень за допомогою графічного матеріалу.

2 Призначення і цілі створення системи

2.1 Призначення системи

Комп'ютерна система аналізу трафіку локальної мережі призначена для порівнювання характеру, основних параметрів та окремих пакетів з різних точок локальної мережі та повинна допомагати користувачеві в подальшому проводити аналіз з метою пошуку прихованих залежностей, мережевих втрат, можливих уразливостей та інших.

До складу системи повинні входити як апаратна складова, так і програмна.

Доцільність створення системи зумовлена тим, що на даний момент часу активно розробляються, застосовуються і використовуються різні методи виявлення вторгнень, що відбулися, і запобіганню майбутніх вторгнень, але вони далеко не завжди є ефективними на практиці. Внаслідок цього всі технології захисту постійно вивчаються і покращуються.

2.2 Мета створення системи

Основна метою є розробка спеціалізованого засобу для спрощення підготовки даних за рахунок зниження обсягів (зниження розмірності) та виділення тимчасових та неявних залежностей для подальшого аналізу трафіку.

Для того, щоб досягти поставленої мети роботи, необхідно розв’язати наступні задачі:

- здійснити вибір програмних засобів моделювання та розробки програми;
- виконати моделювання програми, що розробляється;
- виконати програмну реалізацію програми для платформ Windows;

– проаналізувати одержані результати роботи.

Система буде орієнтована на підприємства, що спеціалізуються на аудиті та віддаленому супроводі інформаційної та телекомунікаційної складової бізнесу, інтернет-сервіс провайдерів, а також підприємства великого та середнього бізнесу, що мають комп'ютерні мережі.

2.3 Характеристика системи

2.3.1 Основні задачі та функції системи

Передбачається розробити засіб для обробки мережних пакетів даних, які буде отримувати користувач з мережевих пристроїв. Агенти в критичних точках локальної мережі повинні прослуховувати трафік і записувати файли для подальшої передачі та обробки..

Основні функції, що вимагають реалізації в комп'ютерній системі для аналізу трафіку локальної мережі:

– можливість захоплення пакетів даних з мережевих пристроїв за маршрутом за допомогою створеного ПЗ;

– дзеркалювання трафіку з пристрою, на якому встановлені агенти із захоплення даних мережі;

– спрощення процесу пошуку несанкціонованого доступу (НСД), застосування, розкриття, недостовірності, змінювання, дослідження, записування чи видалення інформації;

– запобігання майбутнім спробам НСД в мережу шляхом розслідування інцидентів, котрі відбулися;

– захист даних локальної мережі.

3 Вимоги до системи

3.1 Вимоги до системи в цілому

Система повинна бути спроектована так, щоб до її складу особливих зусиль можна інтегрувати різні елементи, не порушуючи при цьому структуру системи.

Система міститиме дві складові: перша здійснює захоплення мережевих даних із пристроїв одного мережного маршруту та відповідає за їх збереження у Pcap-форматі, друга проводить аналіз одержаних даних для виявлення уразливостей мережі, через які може статися НСД у мережу, що розглядається.

У проектованій системі повинні бути забезпечені:

– проведення аналіз структури мережевого трафіку;
– можливість оцінювання ефективності використання комп'ютерних мереж;
– ефективність роботи агентів збору та алгоритмів попередньої обробки мережевого трафіку;
– продуктивність роботи програмного забезпечення;
– часова ефективність та ефективність використання ресурсів системи.

3.1.1 Вимоги до структури та функціонування системи

До структури та функціонування комп'ютерної системи для аналізу трафіку локальної мережі входять:

– локальна комп’ютерна мережа;
– HUB;
– Switch;
– міжмережевий екран;
– агенти зі збору даних;
– сховище зібраних даних;
– програмне середовище для аналізу трафіку.

3.1.2 Вимоги до способів та засобів зв’язку між компонентами системи

Отримання даних відбувається за допомогою сніферів. Всі сніфери повинні бути синхронізовані між собою для точного відстеження даних мережі для подальшого аналізу трафіку. Дані, які отримує сніфер, перетворюються на пакети даних для подальшого транспортування. Пакети з даними передаватимуться в основну програму з агентів на віддалених пристроях.

Агенти зі збору повинні одночасно вмикатися та починати отримання трафіку упродовж певного часу. Увімкнення відбувається за сигналом користувача. Після

того як сніфери виконують своє завдання зі збору трафіку, дані передаються на основний пристрій де вже і буде аналіз з отриманої інформації з мережі. Процес ввімкнення та вимкнення сніферів контролює користувач віддалено з основного пристрою.

3.1.3 Вимоги по діагностуванню системи

Діагностика комп'ютерної системи аналізу трафіку локальної мережі відбувається у відповідності до затвердженого розкладу профілактичних заходів.

3.1.4 Перспективи розвитку, модернізація системи

Перспективами розвитку та модернізації комп'ютерної системи аналізу трафіку локальної мережі є розширення функціонального наповнення для аналізу трафіку на усіх мережевих ділянках.

Існуюча апаратна складова системи при цьому не повинна зазнавати значних змін, а програмне забезпечення системи повинно передбачати гнучкість та здатність до масштабування.

3.1.5 Вимоги до надійності системи

Комп'ютерна система аналізу трафіку локальної мережі повинна бути захищена на рівнях моделі OSI.

Фізичний рівень захисту повинен забезпечувати надійність щодо доступу до апаратного забезпечення. Програмний рівень захисту повинен передбачати захист від сторонніх втручань і впливів.

3.1.6 Вимоги до функцій та задач, які виконує система

Функціональні вимоги та задачі, які повинна реалізовувати комп'ютерна система аналізу трафіку локальної мережі полягають в наступному:

- підготовка отриманих даних до подальшого аналізу шляхом визначення вмісту пакетів даних;
- зіставлення даних між собою, отриманих на різних ділянках мережі;
- завантаження даних у програму;
- припинення роботи у разі виявлення несправностей;

– аналіз даних користувачем шляхом порівняння параметрів мережі;

– синхронізація пакетів даних за часом відправлення/прибуття та за параметрами IP та MAC адрес;

– можливість перегляду даних за допомогою користувальницького інтерфейсу;

– забезпечення часової ефективності роботи системи;

– забезпечення зручності використання програмної частини.

3.1.7 Вимоги до апаратного забезпечення

– Hub – 1 шт;

– Switch – 2 in;

– ПК

3.1.8 Вимоги до програмного забезпечення

Мова програмування для розробки - C#

Бібліотека для захоплення, відкриття та обробки мережевих пакетів – SharpPcap.

Платформа користувацького інтерфейсу - Windows Presentation Foundation/

4 Вимоги до документації

Документація повинна відповідати вимогам ЄСКД та ДСТУ

Комплект документації повинен складатись з:

– пояснювальної записки;

– графічного матеріалу:

1 Схема локальної мережі. Принцип дзеркалювання трафіку.

2 Структурна схема розробки.

3 Структурна схема розробки

4 Скріншоти роботи програмної частини.

*Примітка: У комплект документації можуть вноситися міни та доповнення в процесі розробки.

5 Техніко-економічні показники

Планована собівартість комп'ютерної системи аналізу трафіку локальної мережі повинна становити не більше 30 000 грн.

*Примітка: собівартість системи може змінюватись під час розрахунку в процесі розробки.

6 Стадії та етапи проектування

Таблиця 1 – Стадії та етапи виконання кваліфікаційної роботи бакалавра

№ етапу	Назва етапу виконання кваліфікаційної роботи	Термін виконання
1.	Ознайомлення з завданням до кваліфікаційної роботи	24.04 – 25.04
2.	Розробка технічного завдання	26.04 – 29.04
3	Підбір джерел про системи аналізу трафіку мережі	30.04 – 06.05
4.	Опрацювання літературних джерел	07.05 – 10.05
5.	Виконання дослідження щодо розробки системи	
	аналізу трафіку комп’ютерної мережі	11.05 – 18.05
6.	Написання програмного коду	
7.	Оформлення розділу «Аналіз технічного завдання»	19.05 – 25.05
8.	Оформлення розділу «Проектна частина»	26.05 – 29.05
9.	Оформлення розділу «Практична частина»	30.05 – 02.06
10.	Виконання завдання до підрозділу «Безпека	
	життєдіяльності, основи охорони праці»	20.05 – 04.06
11.	Оформлення кваліфікаційної роботи	08.06 – 11.06
12.	Нормоконтроль	09.06 – 12.06
13.	Перевірка на плагіат	11.06 – 14.06
14.	Попередній захист кваліфікаційної роботи	14.06 – 18.06
15.	Захист кваліфікаційної роботи	26.06

7 Додаткові умови виконання кваліфікаційної роботи

Під час виконання кваліфікаційної роботи у дане технічне завдання можуть вноситися зміни та доповнення.