Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Навчально-науковий центр заочної форми навчання*
(повна назва)

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

другий (магістерський)
(рівень вищої освіти)

Дослідження програм з інжинірингу
-
трафіка
(тема)

Виконав:
студент 2 курсу, групи *ІМІзм-19-2*
Кузьмінов Ю.О.
(прізвище, ініціали)

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)

Тип програми *освітньо-наукова програма*

Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)

Керівник *доц. Скорик Ю.В.*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ *Безрук В.М.*
(підпис) (прізвище, ініціали)

2021 р.

Не містить відомостей заборонених до відкритого публікування.

Студент _____ / *Кузьмінов Ю.О.*/

Керівник _____ /*Скорик Ю.В.*/

Харківський національний університет радіоелектроніки
(повна назва вищого навчального закладу)

Навчально-науковий центр заочної форми навчання

Кафедра *Інформаційно-мережної інженерії*

Освітній рівень *другий (магістерський)*

Спеціальність *172 Телекомунікації та радіотехніка*
(код і назва)

Тип програми *освітньо-наукова програма*
(освітньо-професійна або освітньо-наукова)

Освітня програма *Інформаційно-мережна інженерія*
(назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)

«____»_____ 20 ___ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові *Кузьмінову Юрію Олександровичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження програм з інжинірингу трафіка*

затверджена наказом університету від « *25* » *березня* 2021 року № *33 Стз*

2. Термін подання студентом роботи до екзаменаційної комісії *18 травня 2021 р.*

3. Вихідні дані до роботи *дослідити та проаналізувати різні програмні засоби аналізатори трафіку, розглянути теоретичні особливості цих програм, а також застосувати практично*

4. Перелік питань, що потрібно опрацювати в роботі

Вступ

1. Ознайомлення з інжинірингом трафіку

2. Поняття і види програмних засобів, їх призначення, види захоплень

3. Дослідження та порівняльний аналіз програмних засобів інжинірингу трафіку

Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____
Слайди у форматі Power Point (назва та мета роботи, види програмних аналізаторів, дослідження програмних засобів, архітектури програм, порівняльний аналіз аналізаторів трафіку, висновки)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів атестаційної роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	*25.03 – 26.03.21*	
2	*Підбір літератури за темою роботи.*	*27.03 – 30.03.21*	
3	*Виконання розділу 1*	*31.03 – 12.04.21*	
4	*Виконання розділу 2*	*13.04 – 23.04.21*	
5	*Виконання розділу 3*	*24.04 – 07.05.21*	
6	*Оформлення пояснювальної записки*	*08.05 – 12.05.21*	
7	*Оформлення презентаційного матеріалу,*		
	підготовка до захисту у ЕК	*13.05 – 18.05.21*	

Дата видачі завдання *25 березня 2021 р.*

Студент _____ *Кузьмінов Ю.О.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Скорик Ю.В.*
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 76 стор., 37 рис., 12 табл., 16 посилань.

Мета роботи – дослідити та провести порівняльний аналіз програм з інжинірингу трафіку.

Розглянуто та проаналізовано програмне забезпечення аналізу мережного трафіку: Wireshark, Iris Network traffic Analyzer, NetFlow Traffic Analyzer, Bro Network Security Monitor, Snort, ClearSight Analyzer, CommView.

ІНЖИНІРИНГ ТРАФІКУ, МЕРЕЖА, МАРШРУТИЗАЦІЯ, СНІФЕР, ЗАХОПЛЕННЯ ДАНИХ, АНАЛІЗАТОРИ ТРАФІКУ.

THE ABSTRACT

Explanatory note: 76 pp., 37 Fig., 16 reference, 12 tab.

Object of work – research and conduct a comparative analysis of traffic engineering programs.

In the work was reviewed analyzed network traffic analysis software: Wireshark, Iris Network traffic Analyzer, NetFlow Traffic Analyzer, Bro Network Security Monitor, Snort, ClearSight Analyzer, CommView.

TRAFFIC ENGINEERING, NET, ROUTING, SNIFFER, DATA CAPTURE, TRAFFIC ANALYSATOR.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ARP – (address resolution protocol) протокол визначення адрес;

ATM – (asynchronous transfer mode) асинхронний спосіб передачі даних;

HTTP – (hypertext transfer protocol) протокол передачі даних;

ICMP – (internet control message protocol) міжмережний протокол керуючих повідомлень;

IP – (internet protocol) міжмережний протокол;

ISDN – (integrated services digital network) цифрова мережа з інтегрованими службами;

LAN – (local area network) локальна комп'ютерна мережа;

LER – (label switch edge routers) прикордонний пристрій комутуючий по мітках;

LDP – *(* label distribution protocol) протокол розподілу міток;

LSR – маршрутизатор в мережі;

MAC – (media access contro) управління доступом до середовища;

MPLS – (multiprotocol label switching) багатопротокольна комутація по мітках;

NIC – (network interface card) мережева карта, мережевий адаптер;

OSI – (open systems interconnection) діюча модель взаємодії відкритих систем;

OSPF – (open shortest path first) протокол динамічної маршрутизації;

QoS – (quality of service*)* якість обслуговування;

SSL – (secure sockets layer*)* рівень захищених сокетів;

TCP – (transmission control protocol) протокол управління передачею;

TE – (traffic engineering) інжиніринг трафіку;

UDP – (user datagram protocol) протокол датаграм користувача;

VoIP – (voice over IP) технологія передачі медіа-даних у реальному часі за допомогою сімейства протоколів TCP/IP.

VPN – (virtual private network) віртуальна приватна мережа;

WAN – (wide area network) глобальна комп'ютерна мережа;

WLAN – (wireless local area network) безпровідна локальна мережа;

ВСТУП

На сьогодні темп розвитку галузі телекомунікацій є одним з найшвидших. Відбувається зростання трафіка через те, що впроваджуються нові технології і збільшуються потреби у послугах на базі IP-технологій.

На даний час можна побачити багато програм, які призначені, щоб провести аналіз та моніторинг мережного трафіку, кожна з яких має достоїнства та недоліки, тому актуальною є тема кваліфікаційної роботи, яка присвячена програмам аналізаторам.

Захоплення трафіка проводиться аналізаторами трафіку (сніферів). Сніфер – це програмний продукт, який призначено, щоб зробити перехоплення трафіку. Ці програми дають гарні засоби для візуалізації обсягу вхідного та вихідного трафіків, ведення статистики, вимірювання швидкості, мається можливість спостерігати за активністю користувача у мережі. У деяких програм є і додаткові можливості, це й аналіз заголовку мережного протоколу, фільтрація по заданим критеріям, відновлення сесії.

Дана кваліфікаційна робота присвячена дослідженню і порівняльному аналізу програмного забезпечення з інжинірингу трафіка, таких програм як: Wireshark, Iris Network traffic Analyzer, NetFlow Traffic Analyzer, Bro Network Security Monitor, Snort, ClearSight Analyzer, CommView.

1 АНАЛІЗАТОРИ ТРАФІКУ

1.1 Сніфер

Аналізатор трафіку (сніфер) – це програмний засіб, призначення якого у захопленні та детальному аналізу захопленого трафіка чи деякого сегмента мережі. Якщо аналіз захопленого трафіку проведено докладно і інформативно, то відбувається декодування пакету із зашифрованої форми.

Програмний сніфер за допомогою мережної карти проводить захоплення даних. Коли усі пакети з даними поступають через фізичний канал, то далі мережний адаптер перенаправляє їх на обробку до програми.

Така архітектура мережі як IEEE 802.3 Ethernet дає змогу підключити програмні сніфери, щоб прослуховувати.

Реалізується це крізь проектування локальних мереж на основі Ethernet.

Технологія Ethernet базується на двох типах топологій:

– зіркоподібна (рис. 1.1);
– лінійна (рис. 1.2).

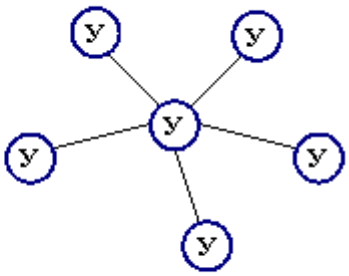


Рисунок 1.1 – Зіркоподібна мережа

Рисунок 1.2 – Лінійна мережа

Сніфер може провести аналіз тільки тих даних, які проходять крізь його мережну карту. Всередині одного сегменту мережі Ethernet усі пакети розсилаються усім комп’ютерам, отже є можливість перехопити чужі дані. Використовуючи комутатори (switch, switch-hub) з їх правильной конфігурацією вже можна захиститися від прослуховувань. Між сегментами дані передаються крізь комутатори. При комутації пакетів дані розділяються на окремі пакети, та пересилаються до пункту призначення окремими маршрутами. Сніфер можна встановлювати як на роутері, а також і на крайовому вузлу мережі [1, 2].

1.2 Принцип роботи аналізаторів трафіку

Спочатку створили сніфери для знаходження неполадок та їх усунення у локальній мережі. Великий набір можливостей, таких як захоплення, декодування, збереження пакетів, що передані, дає можливість повноцінно аналізувати усю комп'ютерну мережу.

Завдяки таким аналізаторам мережі (сніферам) системний адміністратор може контролювати процес переданих даних у мережі і якщо маються неполадки, усунути їх.

Зрозуміло, що за такими можливостями програм сніферів можна здійснювати незаконне заволодіння конфіденційної інформації.

Сніфер це додаткова програма, що має функціонувати на канальному рівні завдяки мережному адаптеру NIC (network interface card).

Робота сніфера проводиться у прихованому режимі, щоб захопити пакети з трафіку, чи у режимі діагностики, щоб усунити проблеми усередині мережі.

Робота програм сніферів проводиться у прихованому режимі, отже сніфер може проходити крізь фільтри адрес та портів, які Ethernet і TCP/IP застосовують, щоб визначити дані. Після перехоплення даних, програма сніфер зберігає їх як окремий формат двійкового значення, та потім застосовує

декодуючі програми розшифровує та робить аналіз пакетів для отримання інформації, яку легко можна считати [3].

Рисунок 1.3 – Принцип роботи пакетного сніферу

Вагомої небезпеки програми сніфери набували, коли дані, що відправлялись по мережі у не зашифрованому вигляді та мережі були спроектовані з використанням концентратів (hub). На даний час наявність сніфера у мережі не дає гарантію оволодіння чужими особистими даними.

Тому, що при проектуванні локальних мереж за допомогою концентратора мається одне середовище передачі даних – мережний кабель.

До кожного вузла комп'ютерної мережі пересилається один до одного пакети даних з інформацією, проте є конкуренція за доступ у середовище. Пакет даних, який відправлено одним із узлів мережі, доставляється на кожен порт концентратору та аналізується усіма вузлами, що входять до комп'ютерної мережі, проте прийом робить конкретний вузол мережі, до якого відправлено пакет з даними [4].

Якщо ж на якомусь вузлі мережі є пакетний сніфер, то він може захопити кожен мережний пакет, який є в мережі, що створена з використанням концентраторів (рис. 1.4).

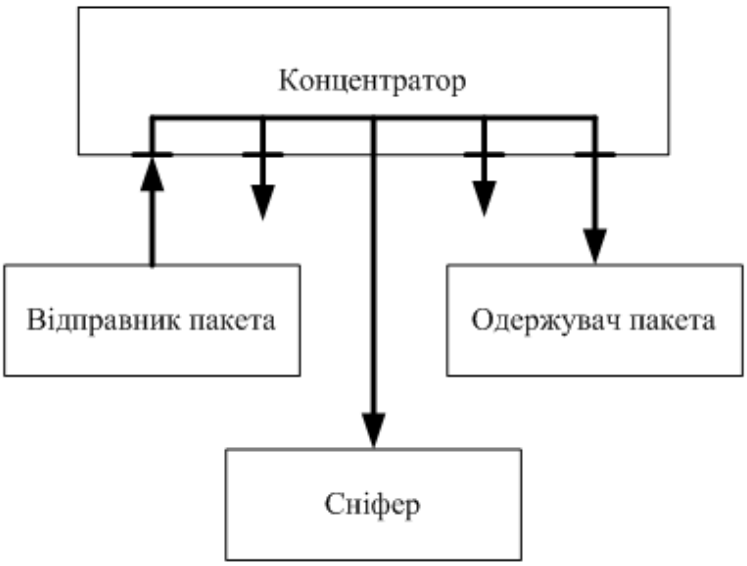


Рисунок 1.4 – При використанні концентраторів сніфер здатний перехоплювати всі пакети мережного сегмента

Комутатор може зберігати адреси кожного пристрою, що підключен до порту мережі та передача даних здійсниться між конкретними портами. Завдяки цьому можна зменшити навантаження на інші порти і при цьому не робити передачу пакетів з інформацією до кожного порту, ніж коли використовують концентратор.

Передача пакету даних з одного вузлу проводиться на призначений порт комутатору, а решта вузлів мережі не має доступа та не може отримати цей пакет (рис. 1.5).

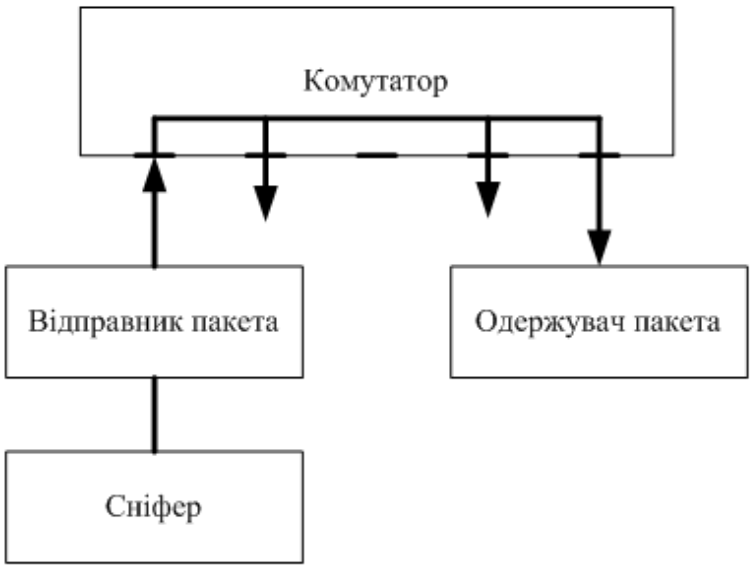


Рисунок 1.5 – При використанні комутаторів сніфер здатний перехоплювати тільки вхідні і вихідні пакети одного вузла мережі

1.3 Атаки за допомогою сніферів

TCP/ IP пакети мають інформацію, необхідну, щоб підтримати зв'язок між двома мережними інтерфейсами, а також мають дані про усі порти, номери, ip адреси, типи протоколів і номери пакетів даних. Ця інформація потрібна для взаємодії у кожному рівні мережного стеку та програм, що належать до прикладного рівня OSI [5].

Якого типу інформацію може перехопити сніфер у моделі OSI наведено на рис. 1.6, рис. 1.7.

Прикладний	захоплення імен користувачів і паролів
Представницький	захоплення трафіку сесій SSL/TLS
Сеансовий	захоплення трафіку Telnet і FTP
Транспортний	захоплення TCP- сесій і UDP- трафіку
Мережний	захоплення IP-адресів і номерів портів
Канальний	захоплення MAC-адресів і ARP-запросів
Фізичний	отримання відомостей про мережу

Рисунок 1.6 – Розподіл рівнів OSI

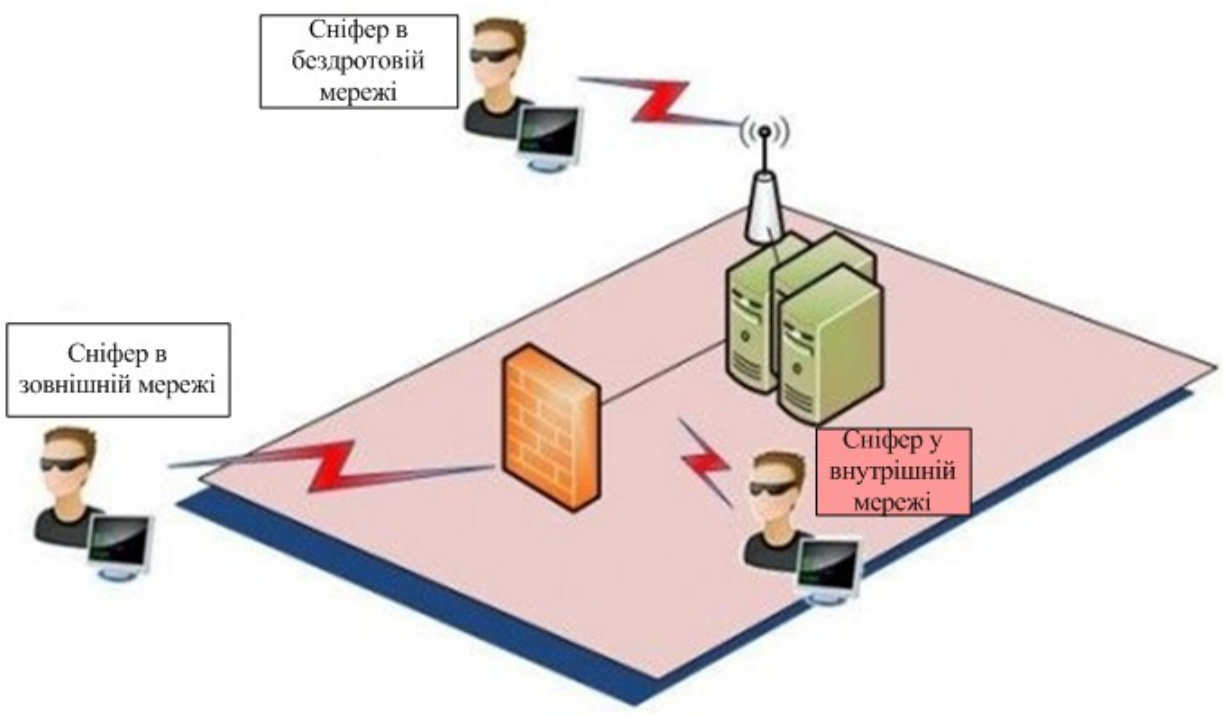


Рисунок 1.7 – Напрямки атак з використанням сніфера

У мережної безпеки часто є поняття спуффінг (spoofing attack) – атака з підміною. При використанні такої атаки, особа, яка призводить атаку, може бути за межами даної мережі, та робити захоплення пакетів з даними на мережному рівні. Тому на сьогодні застосовують таку методику захоплення

даних у бездротових мережах, тому що необхідно знаходитись у зоні дії мережі, щоб зробити підключення до неї та здійснити захват пакетів з даними.

У табл. 1.1 наведені правомірні та не правомірні дії, які можна робити за допомогою сніфірів.

Таблиця 1.1 – Правомірні і не правомірні дії використання сніферів

Приклад правомірного використання сніферу	Приклад не правомірного використання сніферу
Захват пакетів	Викрадення ідентифікаторів і паролів користувачів
Аналіз використання трафіку в мережі	Викрадення даних щодо повідомлень електронної пошти і служб миттєвих повідомлень
Перетворення пакетів для аналізу даних	Викрадення даних із застосуванням спуфінга
Діагностика мереж	Викрадення засобів і заподіяння шкоди репутації

З технічної точки зору процес захоплення пакетів з даними робиться програмою сніфером у режимі promiscuous. Цей режим може здійснити захват та збереження пакетів з даними трафіку мережі.

На сьогодні існує багато засобів, якими можливо зробити захоплення трафіку у мережі. Розглянемо деякі [6,7].

1.4 Захоплення даних у локальній мережі

Коли використовують програму сніфер у внутрішній мережі можливо зробити захоплення інформаціх в усіх діапазонах ip адрес. Тому, зловмисник може отримати усі необхідні відомості про працюючу мережу, це й перелік вузлів, які активні та і відкриті порти. При наявні відомості про відкриті порти, може бути порушена працездатність деяких служб, які працюють на портах.

Цей метод базується на захопленні пакетів даних, які відносяться до протоколів мережі [7].

1.5 Захоплення ARP-трафіку

Захоплення ARP-трафіку – це один з відомих методів, яким користуються зловмисники, щоб захопити дані. У разі такого захоплення робиться крадіжка усіх даних, щоб можна було створити таблицю з ip адресами та mac-адресами. З такою таблицею можна замінити ARP записи (poisoning), знаходити вразливі місця у маршрутизаторів та здійснити спуфінг атаки.

Викрадення TCP-сесій (TCP session stealing) засновано на захопленні трафіка, який передається між відправником та його адресатом. Пакети з даними проходять крізь мережний інтерфейс у promiscous режимі.

Інформацію про усі номери портів, що використовані у службах, номерах TCP/IP є найбільш важливі для здійснення атак у мережі. Якщо є потрібні пакети з даними, то можливо відновлення TCP-сесій, з метою підмінити вузли правильної роботи [8].

1.6 Викрадення паролів

У ході атак робиться перехоплення даних HTTP-сесій та з них виділяють ідентифікатор користувача та паролі, які викрадають. Однак, щоб захистити

HTTP-сесії від такого роду атак і розроблено протокол SSL, також є безліч сайтів у внутрішніх мережах, які користу.ться стандартним менш безпечним шифруванням. Доволі просто зробити перехоплення даних, які зашифровані за алгоритмами Base64 чи Base128 та одержати пароль, застосувавши при цьому спеціалізоване програмне забезпечення. У сучасних сніферах наявна функція захоплення та отримання даних, переданих у рамках SSL-сесій [8].

2 ДОСЛІДЖЕННЯ ПРОГРАМНИХ ЗАСОБІВ

2.1 Wireshark

Wireshark – це програма-аналізатор трафіка для мереж Ethernet та інших. За допомогою цієї програми можна розібрати мережний пакет з відображенням значень у кожному полі протокола будь-якого рівню. Для того, щоб захопити пакети використовують pcap, тому можливе захоплення пакетів з даними тільки тієї мережі, яка підтримує цю бібліотеку. Але, Wireshark може працювати із множиною форматів вхідних даних, отже, є можливість розпаковувати файл даних, що захоплен іншою програмою, це значно розширює можливість захоплення пакетів з даними.

На рис. 2.1 зображено архітектуру програми Wireshark. Ця програма має два компоненти: бібліотека, завдяки якій робиться перехоплення мережного трафіку (WinPcap для ОС Windows, libpcap для ОС Linux); та прикладна програма, яка має функцію розбора протоколу і графічний інтерфейс, щоб візуалізувати результати аналізу та взаємодії з системою. За допомогою WinPcap (libpcap) є зв’язок із драйвером мережного інтерфейса. Цей зв’язок дає можливість перехопити і впровадити мережні пакети, та застосувати критерії фільтрації. Бібліотека libwiretap необхідна для взаємодії із мережними трасами різноматнітних форматів (у тому числі pcap). Компонент Dumpcap робить запис пакетів, що перехоплено у файл, і далі перенаправляє їх до обробки [8].

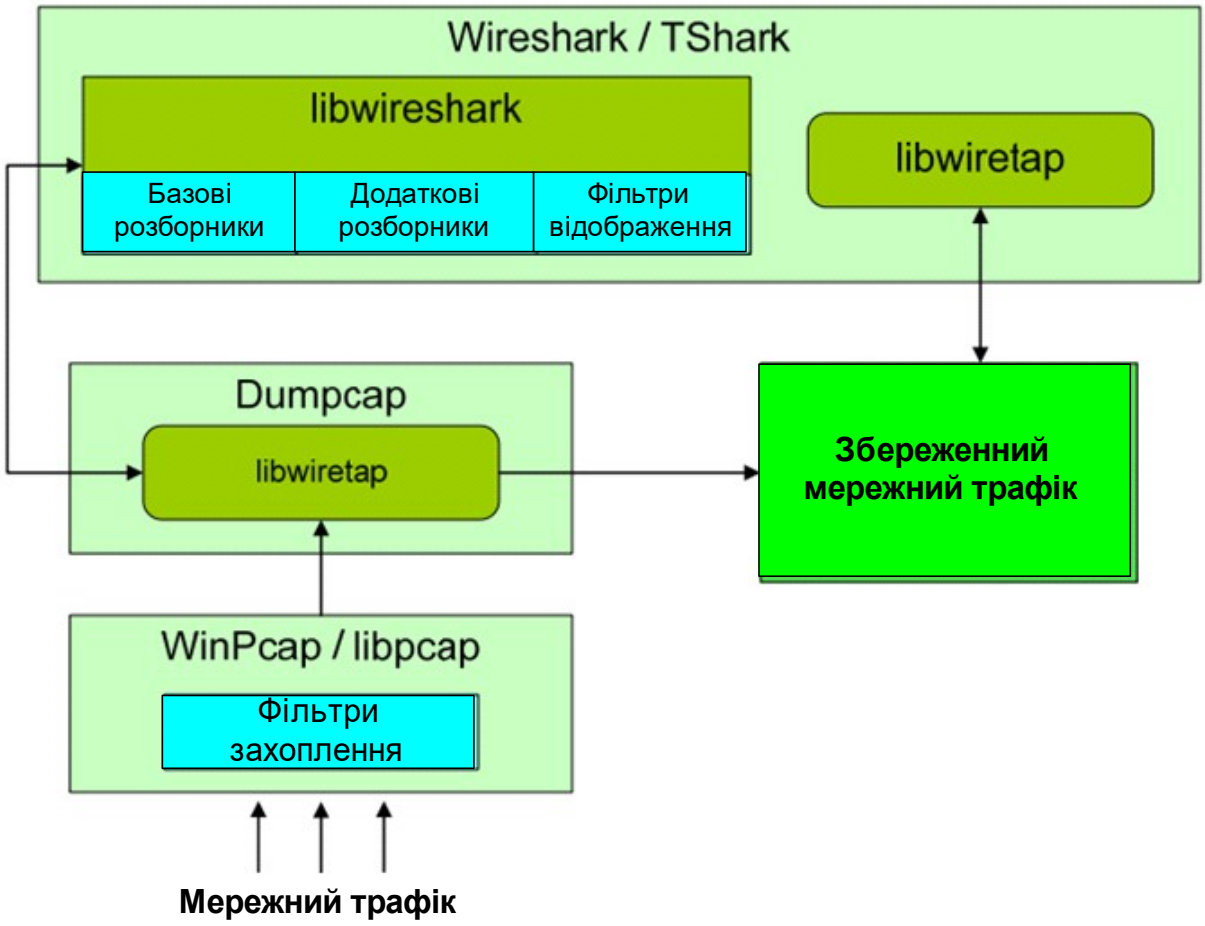


Рисунок 2.1 – Архітектура Wireshark

Основні можливості, а також переваги та недоліки Wireshark наведено у табл. 2.1.

Таблиця 2.1 – Основні можливості, переваги та недоліки програми Wireshark

Можливості Wireshark	– можливість збереження і перегляду раніше збереженого мережного трафіку; – імпорт та експорт даних з інших пакетних аналізаторів. Wireshark уміє зберігати перехоплені пакети в формати інших програм

Продовження табл.2.1

	(libpcap, tcpdump, Sun snoop, atmsnoop, Shomiti / Finisar Surveyor, Novell LANalyzer, Microsoft Network Monitor, AIX's iptrace); – можливість фільтрації пакетів по безлічі критеріїв; – пошук пакетів по безлічі критеріїв; – підсвічування захоплених пакетів різних протоколів; – великі можливості по створенню різноманітної статистики.
Wireshark надає три сценарії взаємодії	– прямий виклик (безпосередній виклик розбирача); – зворотній виклик (викликається розборщик визначається значенням деякого ключового поля, отриманим при розборі більш низькорівневого протоколу; наприклад, значення поля «Порт» в заголовку TCP пакету); – евристична прив'язка (викликається розборщик визначається шляхом пошуку патернів в уже згадуваному буфері).
Wireshark підтримує два види фільтрів	– перехоплення трафіку (capture filters); – відображення (display filters).
Переваги Wireshark	– підтримка великої кількості мережних протоколів (в тому числі протоколів IP-телефонії); – підтримка різних форматів мережних трас;

Продовження табл.2.1

	– можливість розширення (можливість створення і підключення 6 додаткових модулів розбору); – детальна система фільтрації мережних пакетів; – можливість відновлення потоків TCP. – кросплатформеність (є версії для Linux, Mac, Unix); – утиліта абсолютно безкоштовна; – володіє широким функціоналом; – гнучкість настройки; – можливість фільтрації трафіку; – створення власних фільтрів; – перехоплення пакетів в реальному часі.
Недоліки Wireshark	– відновлений потік не розглядається інструментом як єдиний буфер пам'яті, внаслідок чого його подальша обробка неможлива; – код модулів розбору містить функції, що відповідають за візуалізацію результатів (логіка розбору перемішується з логікою відображення в графічному інтерфейсі); – відсутня можливість виконання деякого дії в разі виявлення сигнатур у трафіку.

Перша підсистема у Wireshark від бібліотеки Pcap, яка надає низькорівневий API, щоб працювати з мережними інтерфейсами. Захоплення трафіка під час передачі, дає зекономити оперативну пам'ять. Фільтр це як вираз із групи примітивів, за необхідністю об'єднані логічними функціями (and, or, not). Має записуватись у поле «Capture Filter» у діалоговому вікні «Capture

options». Найбільш популярні зберігаються у профіль, щоб повторно використати (рис. 2.2) [8].

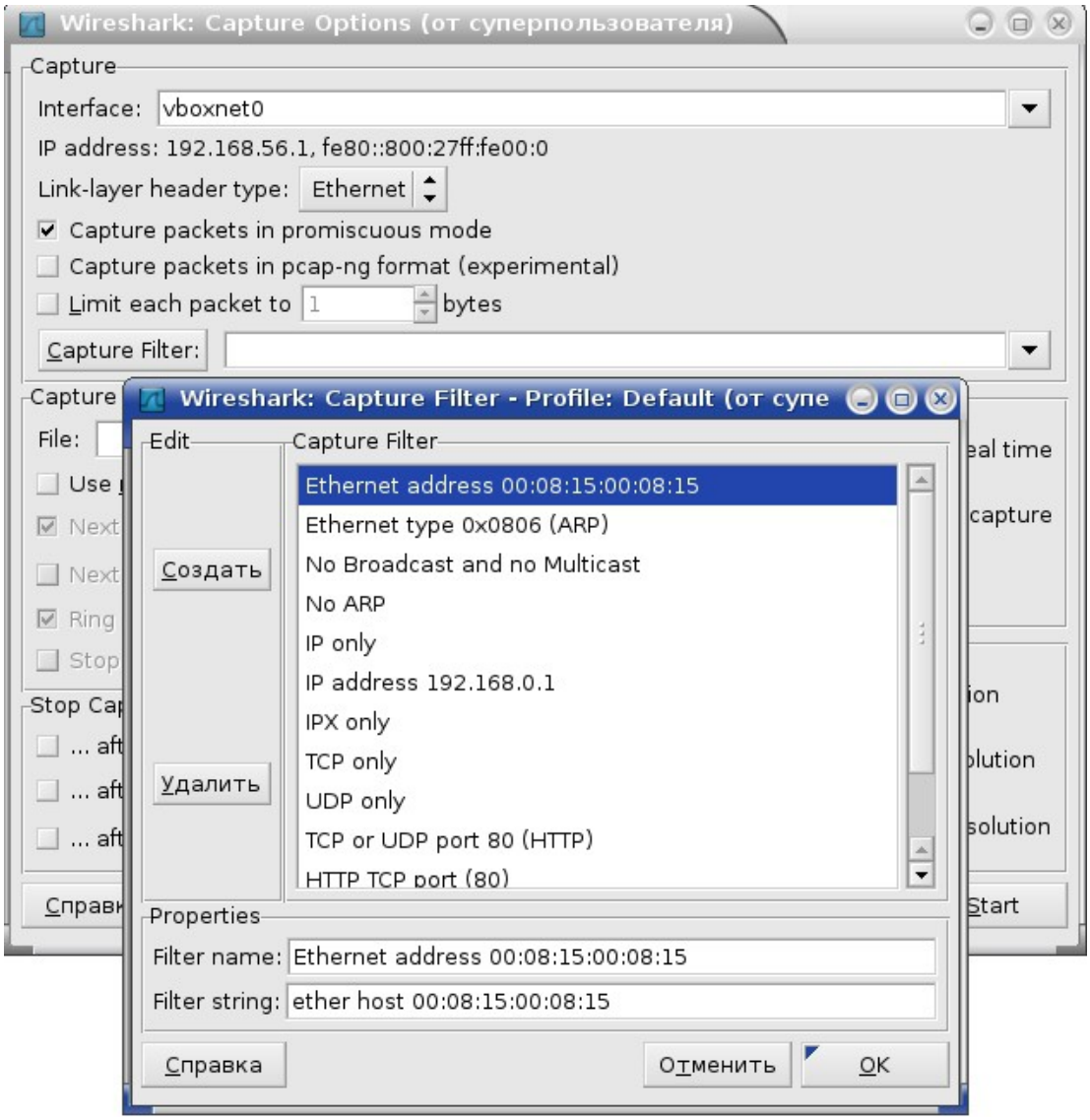


Рисунок 2.2 – Профіль фільтрів перехоплення

Фільтр відображення працює з перехопленим трафіком та є «рідним» для Wireshark. Особливості від Pcap – формат; наявна англійська нотація та підтримка рядів [8].

Записати фільтр з відображенням можливо у спеціальне поле у головному вікні програми, скористувавшись кнопкою «Filter». Якщо натиснути кнопку «Expression ...», то буде видно вікно багатофункціонального конструктора для виразів (рис. 2.3).

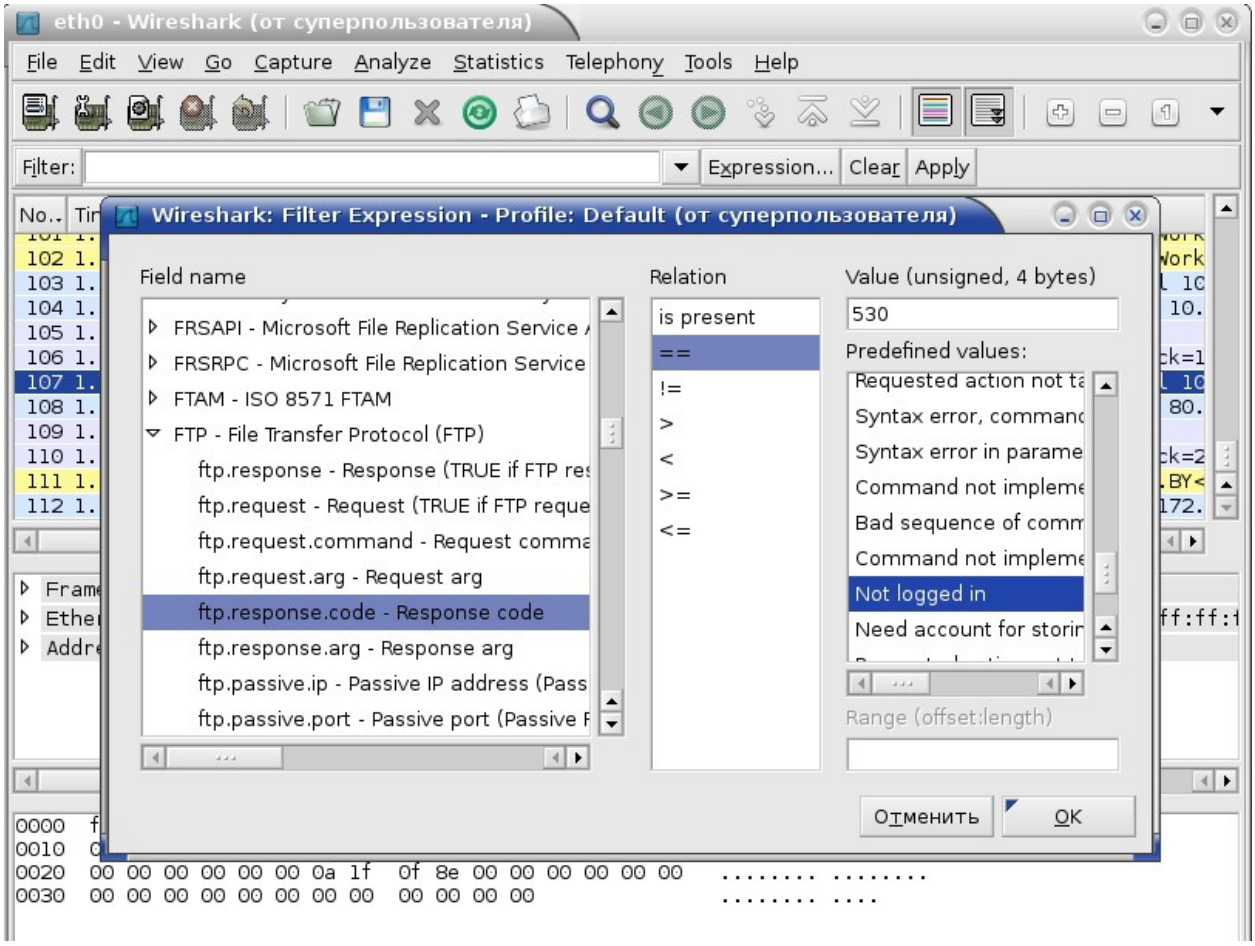


Рисунок 2.3 – Конструктор фільтрів відображення

Зліва (Field Name) зображено упорядковане по алфавіту дерево полів повідомлення протоколу. У дане поле є можливість записати логічний оператор (Relation), значення (Value), діапазон (Range) чи обрати значення із списка (Predefined Value). Це повна мережна енциклопедія у єдиному вікні.

Wireshark базується на аналізі тунельного трафіку, проте представляється компонента по відображенню результатів, що вкрай незручно. Тому, що кожний розбирач, якийз застосовується до мережного пакету записує заново дані у головному вікні. Проте, коли аналізується тунель, то необхідно візуалізувати результати усіх розбирачів. Ці недоліки не рекомендують застосовувати програму Wireshark, щоб аналізувати дані, передані багаторівневим тунелем і ефективної роботи з потоками, що відновлено [8].

На початку аналіза мережного трафіка треба зробити налаштування мережного інтерфейсу і потім зробити запуск програми аналізатора Wireshark. Після запуску Wireshark безперервно проводить відображаення одержуваних пакетів з мережного інтерфейсу (рис 2.4).

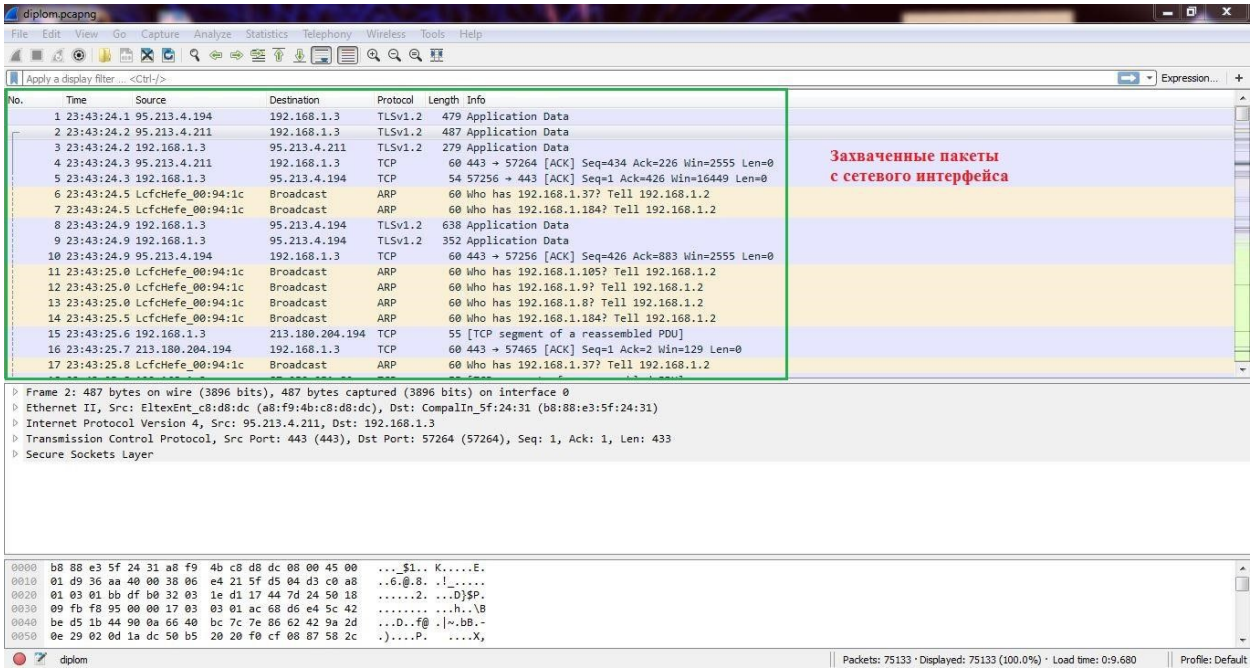


Рисунок 2.4 - Відображення захоплених пакетів

Щоб аналіз був ефективний, треба працювати із трафіком, що захоплено у пасивному режимі.

Всю інформацію, щоб виконати наступні кроки аналіза представлено у головній панелі інтерфейса програми Wireshark, в якій є основна інформація про захоплені пакети.

Для аналіза треба зробити відображення статистичних даних по захопленому мережному трафіку в табл. 2.2, щоб користуватись цими значеннями у подальших етапах аналіза [8].

Таблиця 2.2 - Статистичні дані захопленого трафіку

Характеристика	Значення
First packet/Початок захвату	2020-05-19 23:23:24
Last packet/ Останній захоплений пакет	2020-05-19 23:59:51
Elapsed/ Час захоплення, хв	00:36:27
Packets/Захоплені пакети	75133
Packets size/ Розмір всіх пакетів, Мбайт	68 Mb
Average kbytes/s Середня швидкість пакетів	67 kbytes/s
Average kbits/s / Середня швидкість	538 kbit/s

Використання Wireshark дозволяє отримати інформацію про розподіл трафіка, необхідну для інтерпретації протоколу. Для цього треба зробити впорядкування усього захопленого трафіку за наявністю різних типів протоколів. Це представлено у табл. 2.3.

Таблиця 2.3 - Використані протоколи в захоплених пакетах

Protocol /Протокол	Packets/Пакети, kbit	Packets size byte/Розмір усіх пакетів	Average kbits/s / Середня швидкість	Packets/Пакети, %
Ipv6	796	72940	591	1.1
Ipv4	60635,7	6600731	534	62.4
UDP	678	107824	873	3.4
DNS	504	99700	808	0.7
TCP	16426,3	63665319,17	534	24.5
HTP	820	548548	444	0.9
ARP	5273	315822	456	7
ВСЬОГО	75133 пакетів	71303168 Byte	608 kbits/s	100%

У програмі Wireshark є інструмент IO Graphs, необхідний, щоб можна було візуально представити захоплені пакети. Можна представити графік появи пакетів, що відносяться до основних чотирьох протоколів мережі. На графіку буде показано, що більшість пакетів відносяться до протокола ip. Можна помітити, що захоплення пакетів з даними у конкретному проміжку часу нерівномірне, а стрибкоподібне, тому що швидкість з'єднання з інтернетом не постійне.

Інформація про обраний пакет надається у виді списку у порядку ієрархії. Ця ієрархія загалом відповідає інкапсуляції даних, яка є при застосуванні мережних протоколів для обміна даними.

На рис. 2.5 представлено приклад захопленого пакету, за допомогою чого можна зробити аналіз інформації, щопредставлена у середній панелі.

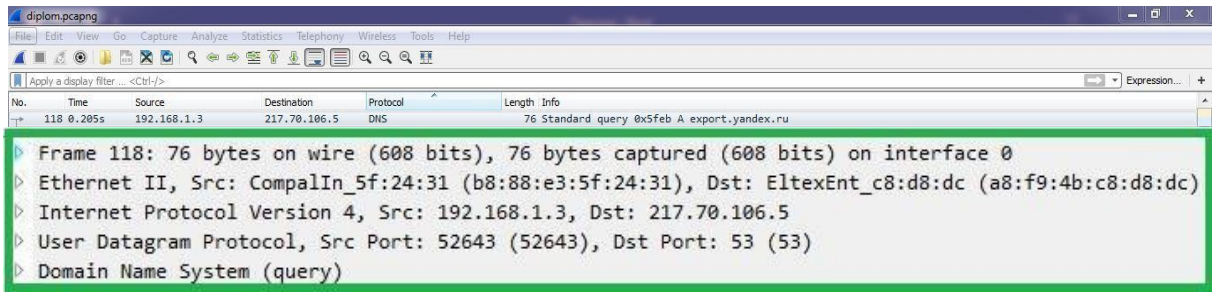


Рисунок 2.5 – Інформація про захоплений пакет

Інформацію представлено, як вкладений список відповідно до послідовності полів, що знаходяться у заголовках протокола, які застосовуєть при інкапсуляції даних (рис. 2.6).

Перший вкладений список – це Frame, у ньому зберігаються основні дані про пакет, це і час захоплення, довжина пакета, тип протокола, номер пакету.

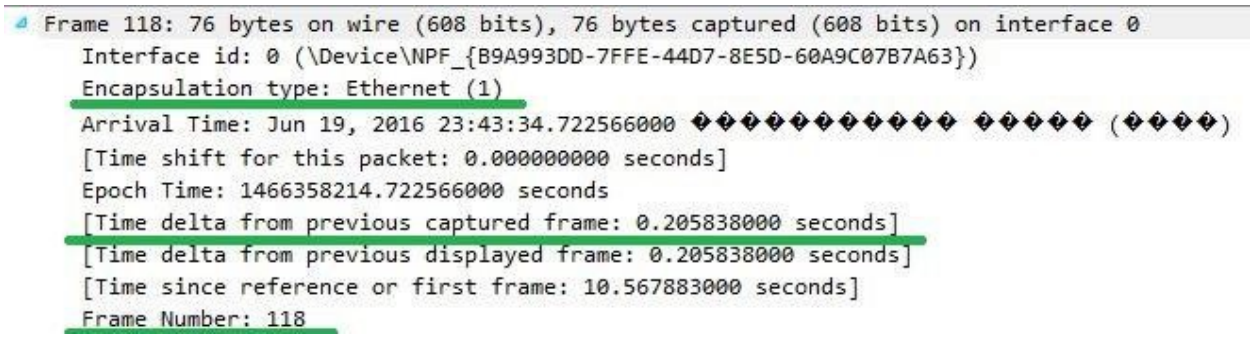


Рисунок 2.6 – Вкладений список Frame

Після аналізу цієї інформації у списку Ethernet II робиться висновок: Ethernet II - кадр протоколу Ethernet

- Src: Compalin_5f: 24: 31 (b8: 88: e3: 24: 31), Dst: Eltex_c8: d8: dc a8: f9: 4b: c8: d8: dc) дані про відправника (фізична адреса, назва виробу в мережі;
- Srs - пристрій який відправив дані;
- Dst - пристрій який отримав пакет;
- Type - мережний рівень застосовує мереженй протокол ipv4.

Наступний вкладений список має інформацію про заголовок мережного рівня.

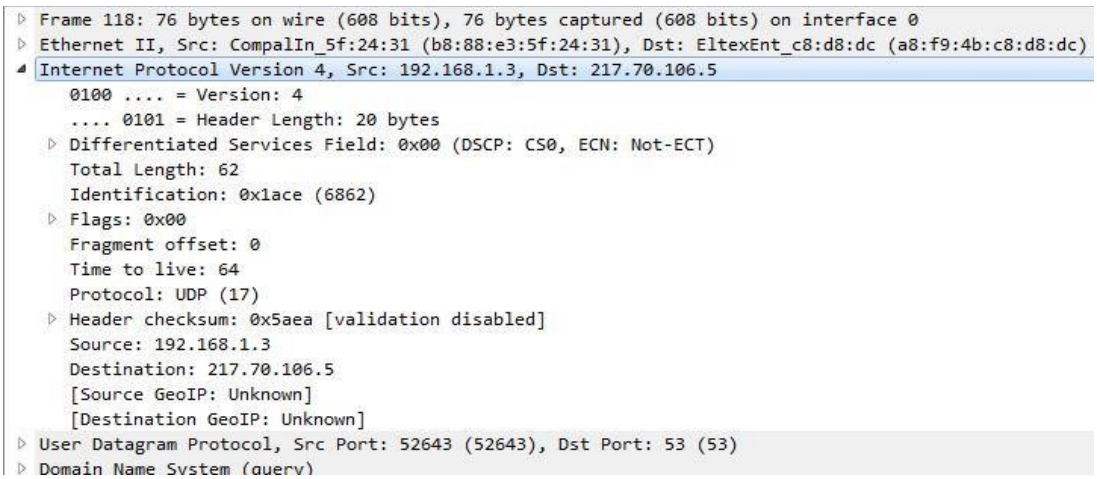


Рисунок 2.7 – Інформація про заголовку мережного рівня

Інформація вкладеного списку містить:

– Internet Protocol - дані протоколу ipv4;
– Src: 192.168.1.3 - адреса відправника;
– Dst: 217.70.106.5 - адреса одержувача;
– Time to Live - 64, максимальне значення кількості мережних засобів;
– Protocol - на транспортному рівні використовують протокол UDP.

З аналізу обраного пакету можна зробити наступний висновок: програма аналізатор надає загальну інформацію та дає дані про протоколи, які відповідають формату кадру протокола [8].

Список User Datagram Protocol видає дані про заголовок протоколу на транспортному рівні.

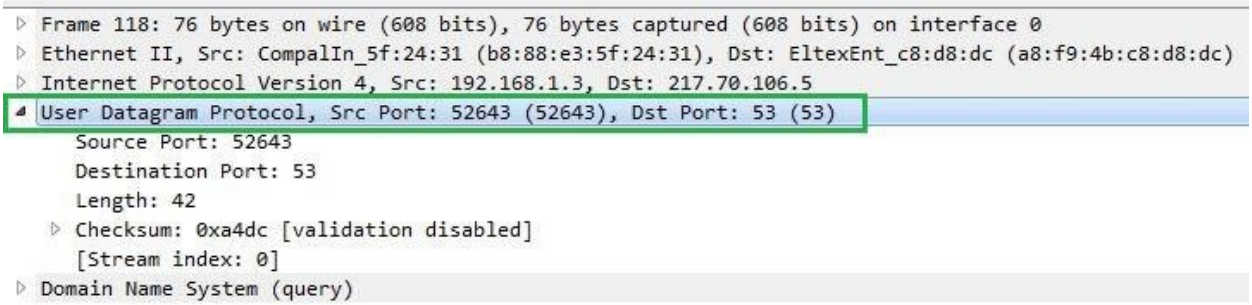


Рисунок 2.8 – Вкладений список User Datagram Protocol

У даному списку наявна така інформація:

– Source Port - 52643, номер порта, що використовує пристрій, щоб відправити пакет;
– Destination Port -, 53, номер порта який використовує пристрій, щоб отримати пакет;
– Length - довжина датаграми, яка дорівнює 42.

В процесі аналіза мережного трафіку завдяки системному інструменту можливо зробити визначення наявністі пакетів з помилками чи попередженнями.

Це можна зробити за допомогою спеціального інструменту у програмі Wireshark, Expert Information. Це журнал у якому є помилки чи примітки, що з’явились з мережними «аномаліями».

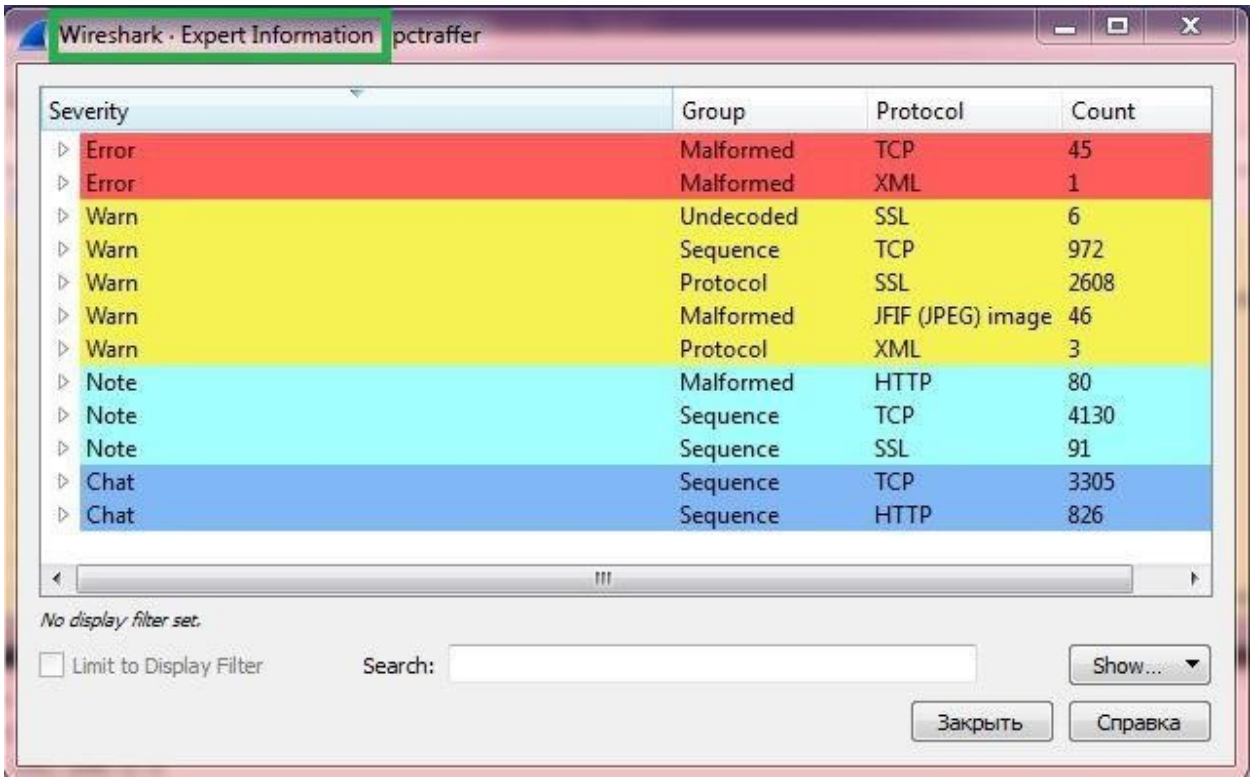


Рисунок 2.9 – Expert information

Expert information має комфортний та легкий інтерфейс, у якому відображена поведінка мережі. Він допомогає скоріше знаходити помилки, ніж проводити аналіз усіх пакетів вручну.

Також у програмі Wireshark є корисний інструмент – GeoIp Database.

Цей інструмент дає можливість додати додаткові дані до захоплений пакетів. Додаткова інформація буде прикріплена до захопленого пакета, це і інформація ip адреси і його місце знаходження. З цього можна дізнатись звідки отримано пакет.

І далі додати до використання цю базу даних ip адрес через інтерфейс Wireshark (рис. 2.10).

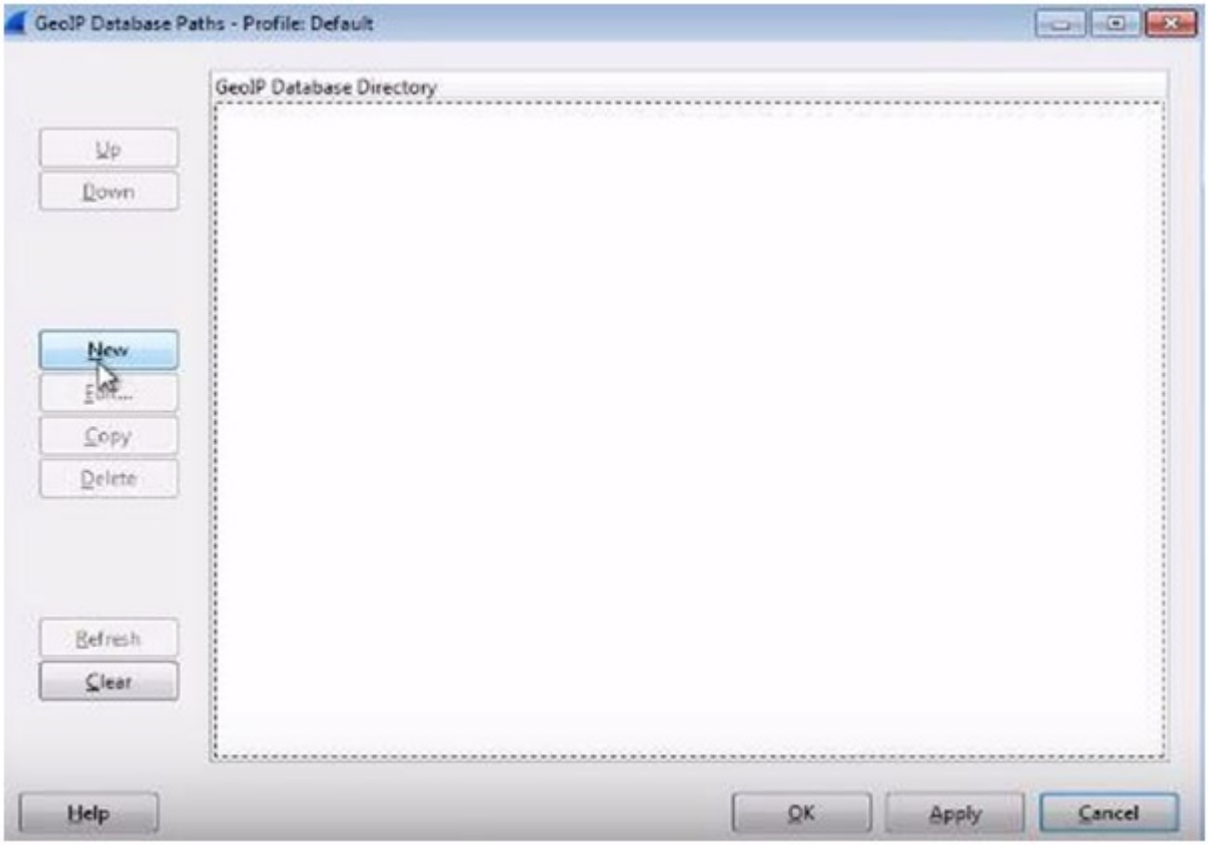


Рисунок 2.10 – Додавання бази даних ip-адрес

Коли успішно додано базу даних, тоді можна звернутись до статистики кінцевих точок та побачити додаткову інформацію про присутні ip адреси (рис. 2.11).

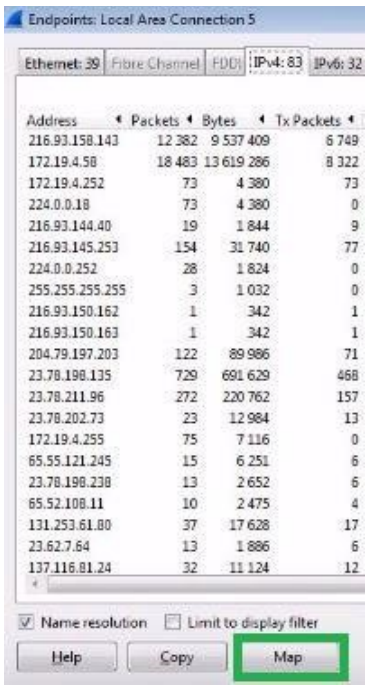


Рисунок 2.11 - Відображення на карті

Зробивши аналіз захопленого трафіку мережі, можна побачити, що саме завантажено до комп'ютера (рис. 2.12). Проведемо фільтрацію всього трафіку по фільтру http.

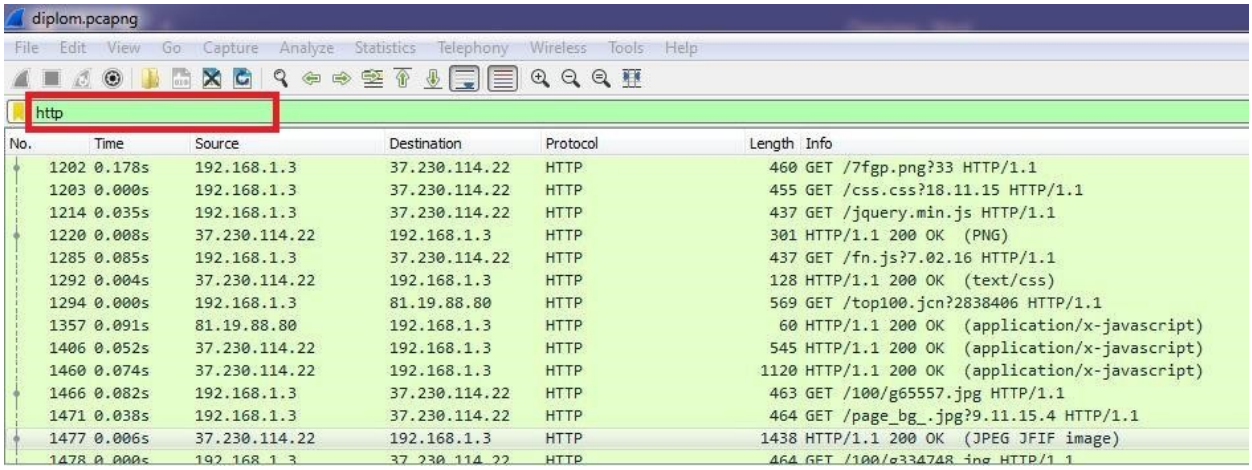


Рисунок 2.12- Фільтрація трафіка

Коли захоплений трафік відфільтровано, бвчимо відображення усіх пакетів, що використовували http протокол. Треба перейти до вкладки export objects та обрати HTTP.

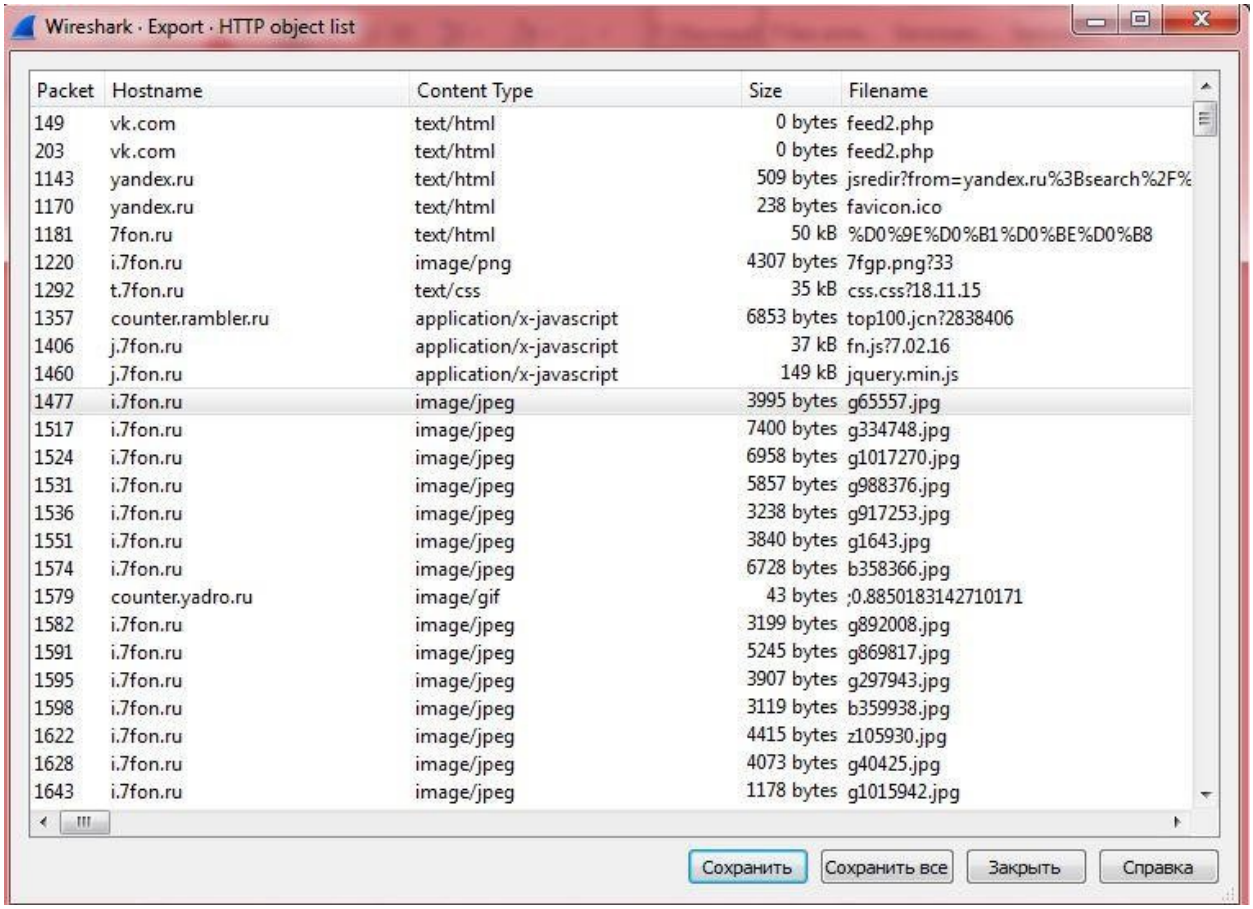


Рисунок 2.13 – Список файлів які можна отримати із захопленого трафіку

2.2 Iris Network Traffic Analyzer

Програма має стандартні функції збору, обробки, фільтрування і пошуку пакетів, а також і має особливі можливості, щоб реконструювати дані. Iris Network Traffic Analyzer дає можливість детально відтворювати сеанс роботи користувача із різноматніми web-ресурсами і також можна імітувати відправку паролів для доступа до захищених web-серверів завдяки cookies. Цю

технологію з реконструювання даних, реалізовано у модулі дешифрування (decode module), що змінює сотні зібраних мережних пакетів у звичайнii електронні листи, web-сторінки, повідомлення ICQ та ін. За допомогою EEye Iris можна переглядати повідомлення web-пошти, що незашифровані і програм миттєвого обміна повідомленням, поширюючи можливість засобу моніторинга і аудиту.

Графічний інтерфейс даної програми зрозумілий та простий і звичайний для пакетних сніферів. Має три вікна, у першому –пакети, що перехоплено з детальною інформацією про кожний пакет, який має MAC- і IP-адресу відправника, тип пакету, розмір пакету, а ще порядковий номер SEQ і ACK. У другому вікні – декодовані дані по кожному окремому пакету і в третьому вікні – вміст кожного пакету (рис 2.14).

Figure 1: IrisNet Architecture

Рисунок 2.14 – Архітектура Iris Network Traffic Analyzer

Програма Iris дає можливість дуже просто налаштувати фільтри для перехоплення даних. За допомогою діалогового вікна Edit filter settings, можна створити фільтри по MAC-адресам та IP-адресам джерела та одержувача, по

портам, протоколам. Також, є можливість налаштувати фільтри на розмір пакету і на фрагмент пакету [9].

Можна сказати, що це один із самих зручних аналізаторів мережного трафіку Windows. Необхідний при вивченні мережних протоколів, функціональності мережних додатків, а також вирішенню різноманітних проблем у мережі.

Основні можливості програми Iris наведено у табл. 2.4.

Таблиця 2.4 – Основні можливості програми Iris

№	Основні можливості програми Iris
1	перехоплення мережного трафіку (Capture);
2	декодування перехопленого трафіку і реконструкція перехоплених сесій (Decode);
3	фіксування спроб підключення до комп'ютера (Guard);
4	ведення журналів перехоплених (Capture) і декодованих (Decode) сесій;
5	можливість створення різних фільтрів для сесій перехоплення (Filter), що дозволяють здійснювати вибіркове перехоплення по безлічі критеріїв (MAC-адресу, тип протоколу, номер порту, напрям обміну, ключові слова тощо);
6	відображення мережної статистики по протоколам, хостам, розмірам пакетам і т.п;
7	можливість використання вбудованого планувальника для перехоплення пакетів в обрані інтервали часу;
8	є редактор пакетів, що дозволяє переглядати їх структуру і дані, змінювати вміст, створювати свої пакети і виконувати їх відправку як поодинці, так і групами, одноразово, циклічно або задану кількість разів;
9	зручне відображення структури пакета (заголовки MAC, IP, ICMP, TCP, UDP, дані відображаються у вигляді дерева з декодувати значеннями);

Продовження табл. 2.4

10	можливість ведення внутрішньої адресної книги, що дозволяє робити більш зручним вид сесій за рахунок заміни фізичних адрес і елементів з'єднань символічними іменами;
11	можливість відображення декодованих сесій у вигляді пакетів, тексту, або HTML, що дозволяє в зручному вигляді переглядати сесії обміну клієнта з сервером;
12	підтримка друку з попереднім переглядом, буфера обміну, можливість збереження пакетів на диск, збереження перехоплених сесій і їх завантаження для подальшого аналізу;
13	зручний інтерфейс.

Можна сказати, що один недолік даної програми у тому, що пакети, які відображаються у першому вікні не кольорові (як у інших програмах), це створює якусь незручність при візуальному сприйнятті даних [9].

Відмінністю даної програми є те, що під час запуску перехоплення пакетів можна відобразити у графічній формі статистичні дані. Тому, є можливість відобразити графік швидкості передачі пакетів, діаграму розподілу розмірів пакетів (рис. 2.15, рис. 2.16).

Окрім можливостей з табл. 2.4, програма дає можливість створити HTML-звіти про сеанс зв'язку, куди додається більш важливі дані, у тому числі і статистика з відвідувань сайтів, обсяг переданих і прийнятих даних. У Iris вбудован генератор трафіка, це зручно, щоб проводити діагностику вузьких місць у мережі.

Також у програмі Iris є вбудований модуль, який дає змогу зафіксувати усі спроби з'єднання із комп'ютером, це і забезпечує відстеження несанкціонованого проникнення у мережу.

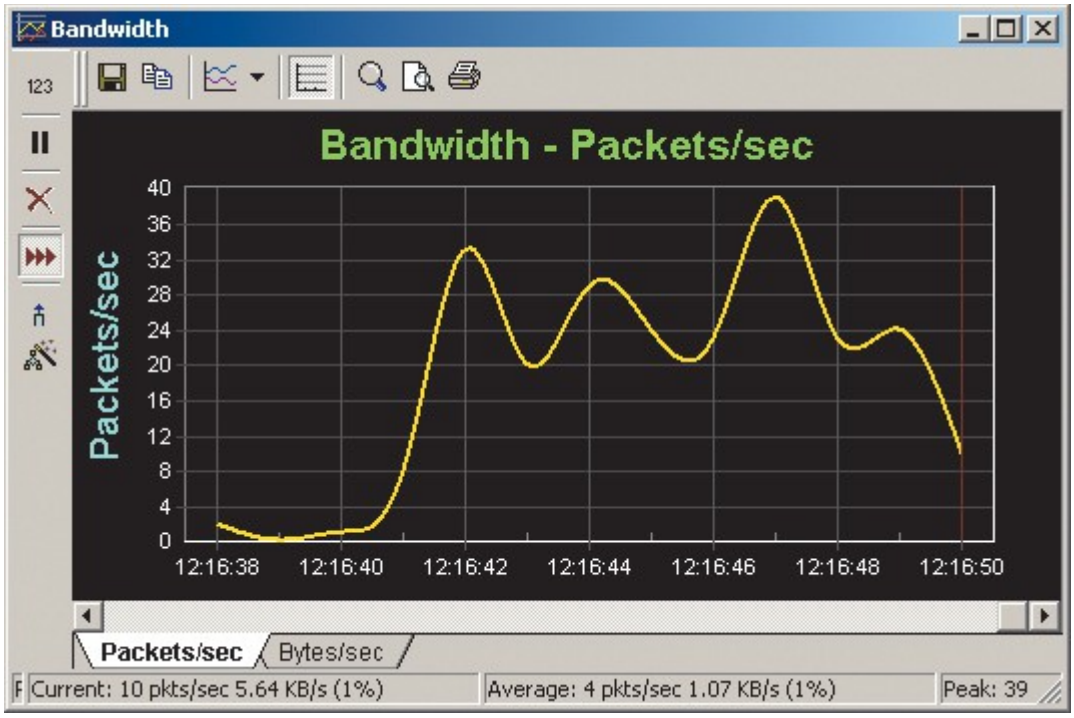


Рисунок 2.15 – Графік швидкості передачі пакетів в аналізаторі Iris

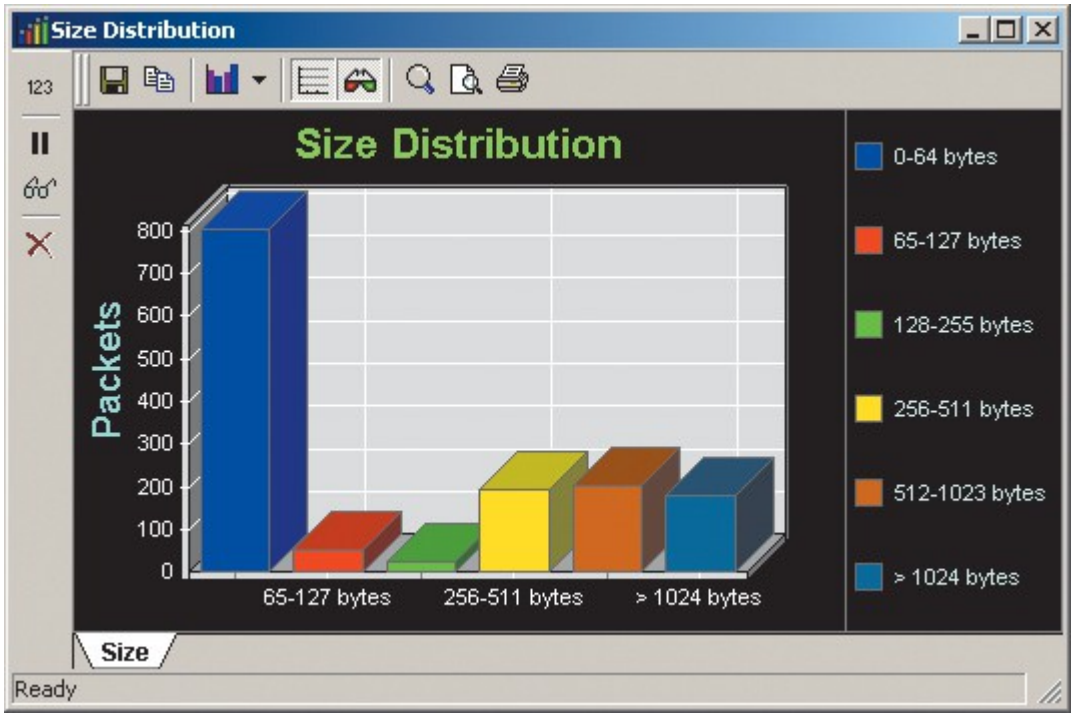


Рисунок 2.16 – Діаграма розподілу розмірів пакетів в аналізаторі Iris

2.3 NetFlow Traffic Analyzer

За допомогою NetFlow можна робити аналіз і відстежити пропускну здатність та визначати обсяг переданого трафіка, який генерується IP-адресами, протоколами чи програмами. NetFlow підтримується в основному роутерами та комутаторами Cisco. Для виконання аналізу трафіку маршрутизатори мають налаштуватись так, щоб пакети протоколів Flow перенаправлялись на комп'ютер із встановленим зондом PRTG. Технологія Flow дає мінімальне навантаження на центральний процесор та має адаптацію до мереж з великими обсягами трафіка даних.

Архітектура програми NetFlow Traffic Analyzer представлена у рис.2.17.

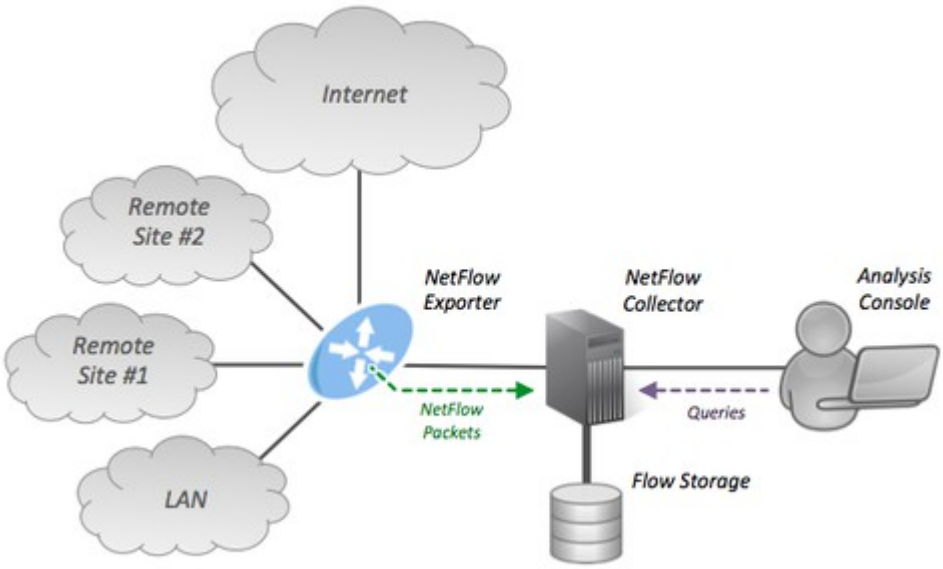


Рисунок 2.17 – Архітектура NetFlow traffic analyzer

Програма дає змогу записати дані із безперервного потіку мережного трафіка, проводити аналіз трафіка та робити графіки і таблиці, завдяки яким є можливість переглянути, ким саме та навіщо була використана корпоративна мережа. Із моніторингом CBQoS можна зробити призначення потрібних пріоритетів трафіку у мережі. За допомогою програми NetFlow Traffic Analyzer

можна зробити повну картину про мережу трафіку, обмежити пропускну здатність деяких співробітників[10].

Можливості NetFlow Traffic Analyzer описані у табл. 2.5.

Таблиця 2.5 – Можливості програми NetFlow Traffic Analyzer

№	Можливості програми NetFlow Traffic Analyzer
1	визначає, які користувачі, додатки та протоколи споживають найбільше мережної пропускної здатності і вказує IP адреси найбільш активних користувачів в мережі;
2	моніторинг мережного трафіку шляхом захоплення потоку даних від мережних пристроїв, в тому числі Cisco ® NetFlow v5 або v9, Juniper ® J-Flow, IPFIX і SFlow;
3	складає карти трафіку надходять від призначених портів, в яких вказує: IP-адреси джерела, призначення IP-адрес, і навіть протоколи, щоб можна було дізнатися імена додатків;
4	забезпечує миттєве повідомлення адміністратора про перевищення порога використання пропускної здатності;
5	за допомогою Class-Based Quality of Service (CBQoS) можна призначати необхідний рівень пріоритету трафіку;
6	генерує звіти мережного трафіку за допомогою всього лише кількох кліків.

Аналіз роботи програми NetFlow Traffic Analyzer показано на рис. 2.18.

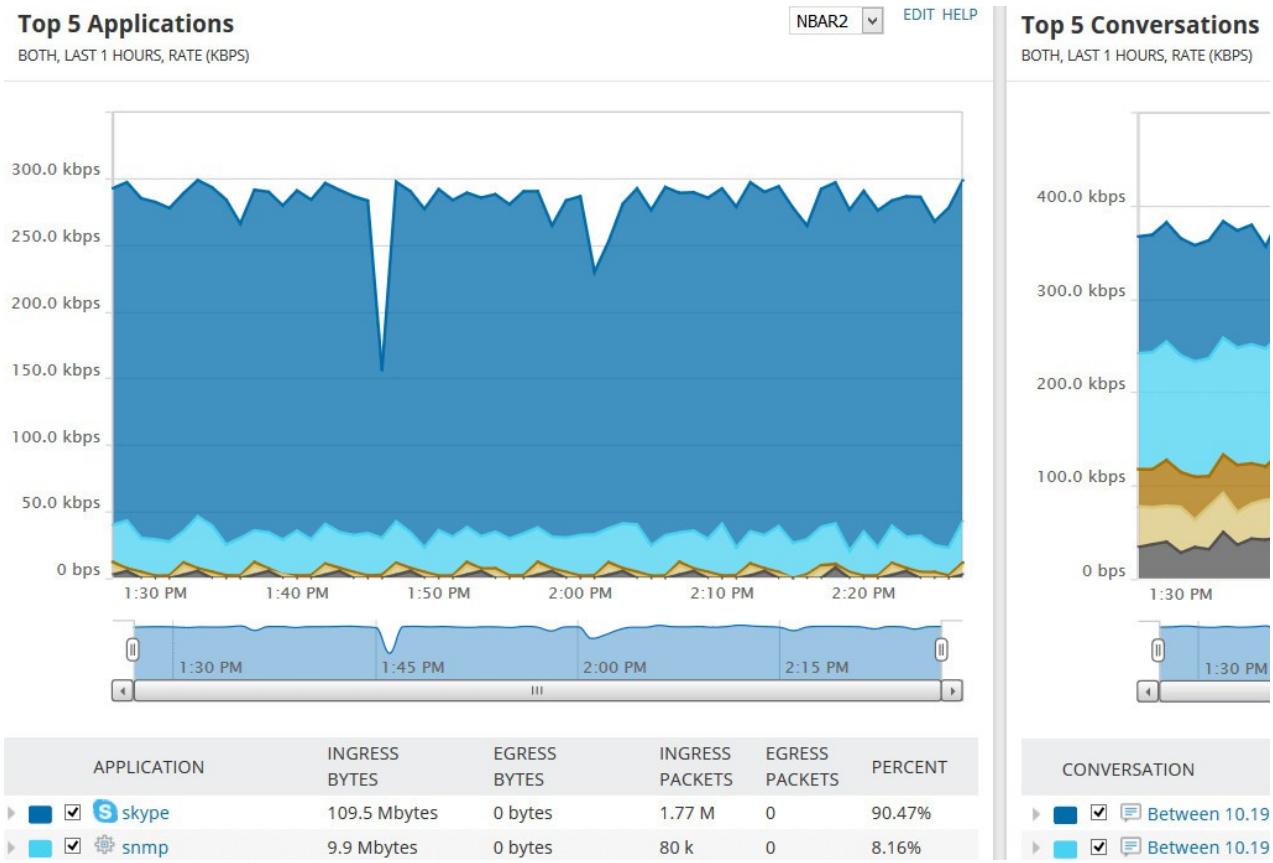


Рисунок 2.18 – Аналіз роботи програми

2.4 Bro Network Security Monitor

За допомогою інструменту Bro Network Security Monitor (далі Bro) можна проводити аналіз трафіку у реальному часі. Програма Bro підтримує операційну систему на основі Unix (Linux, FreeBSD, Mac OS X) та є однопоточним додатком.

Архітектуру програми Bro наведено на рис. 2.19. Є два компоненти: генератор подій (проводить аналіз трафіка, який одержаного за допомогою libpcap, генерує події); та обробники подій (власна мова створення скриптів, що дозволяє показувати попередження і проводити запуск сторонніх додатів).

Програма підтримує проведення аналізу трафіку у режимі реального часу, і аналіз мережних трас (у форматі pcap).

Загалом із системою йде велика кількість скриптів. Мова скриптів має певний набір типів та атрибутів, це і тип event (подія). Кожній події можна надати у відповідність обробник (один або кілька) – у разі цієї події буде викликано певний обробник. Якщо до одної події додано декілька обробників, то треба записати атрибут пріоритетності, який дає порядок виклика цих обробників. Події будуть сгенеровані ядром системи Bro [11].

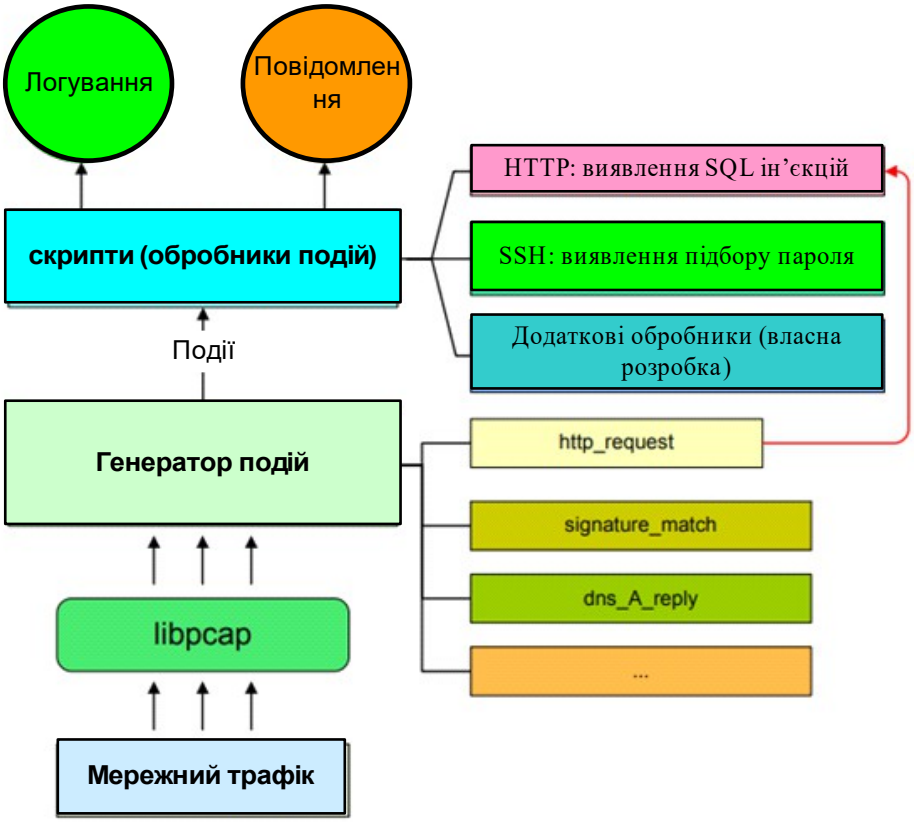


Рисунок 2.19 Архітектура Bro Network Security Monitor

Подія signature_math є одною із найбільш важливих із точки зору аналізу. Вона генерується у разі надання деякої інформації в розглядувальному мережному пакеті.

```
signature
myFirstSignature
{
    ip-proto == tcp
    dst-port == 80
    payload /.*root/
    event "Found root!"
}
```

Рисунок 2.20 – Приклад сігнатури

Завдяки сигнатурі (рис. 2.20) робиться пошук виразу (/.*root/) в усіх пакетах протоколу TCP, що відправлені на порт 80. У кожній сигнатурі є набір атрибутів. Це conditions (умови) та actions (дії). Умови, це критерії збігу, а дії визначають операції, що є у разі цього збігу. Умови застосовують як до заголовків пакетів так і до їх навантаження.

У програмі Bro зв'язок встановлюється завдяки механізму подій. Також у системі Bro реалізовано систему динамічного розпізнавання протоколу за допомогою сигнатурного пошуку. Програма підтримує протоколи ftp, http, bittorrent, ssh, ssl, pop3, smtp, ayiya. На рис. 2.21 зображена сигнатура для протоколу HTTP.

```
signature dpd_http_client
{
    ip-proto == tcp
    payload /^[[:space:]]*(GET|HEAD|POST)[[:space:]]*/
    tcp-state originator
}
```

Рисунок 2.21 – Сигнатура для протоколу HTTP

Керування системою робиться за допомогою консолі, графічного інтерфейсу немає. Програма підтримує аналіз тунелів. Проте, автоматичне

відновлення стека протоколу тунелю відсутнє. Кількість підтримуваних тунельних протоколів вкрай невелика [11].

Аналіз трафіку за допомогою програми Bro наведено на рис. 2.22.

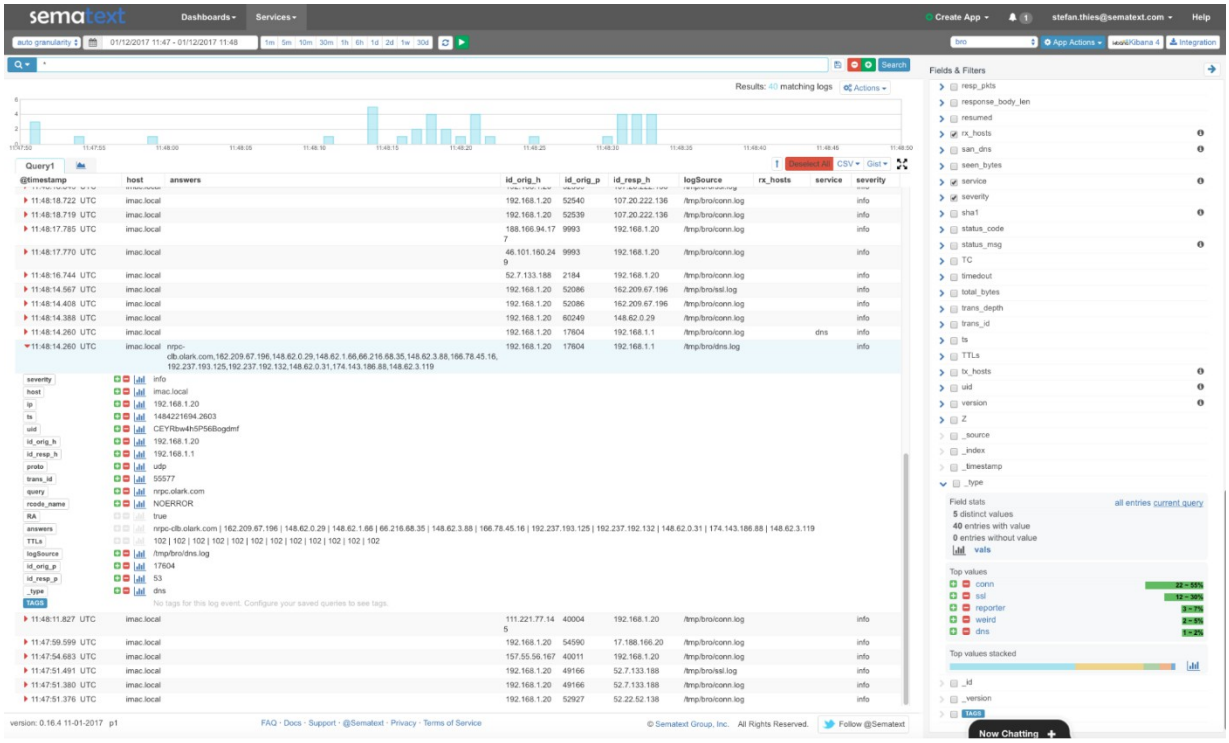


Рисунок 2.22 – Аналіз трафіку за допомогою Bro

2.5 Snort

Snort – це система, за допомогою якої можна виявити атаку та запобігти їй. Програма підтримує методи зіставлення по сигнатурам, засоби для перегляду протоколів та механізми, щоб виявити помилки.

Аналіз трафіку у системі Snort заснован на сигнатурного пошуку. Підтримується операційними системами: Unix (Apple Mac OS X, FreeBSD), Linux (Ubuntu, Fedora, Debian), Microsoft Windows. Snort може працювати у режимі реального часу.

Аналіз проводиться шляхом пошуку зазначених у файлі конфігурацій в мережних пакетах (сигнатурний пошук). Якщо успішно, то виконуються певні дії. Архітектуру програми Snort наведено у рис. 2.23.

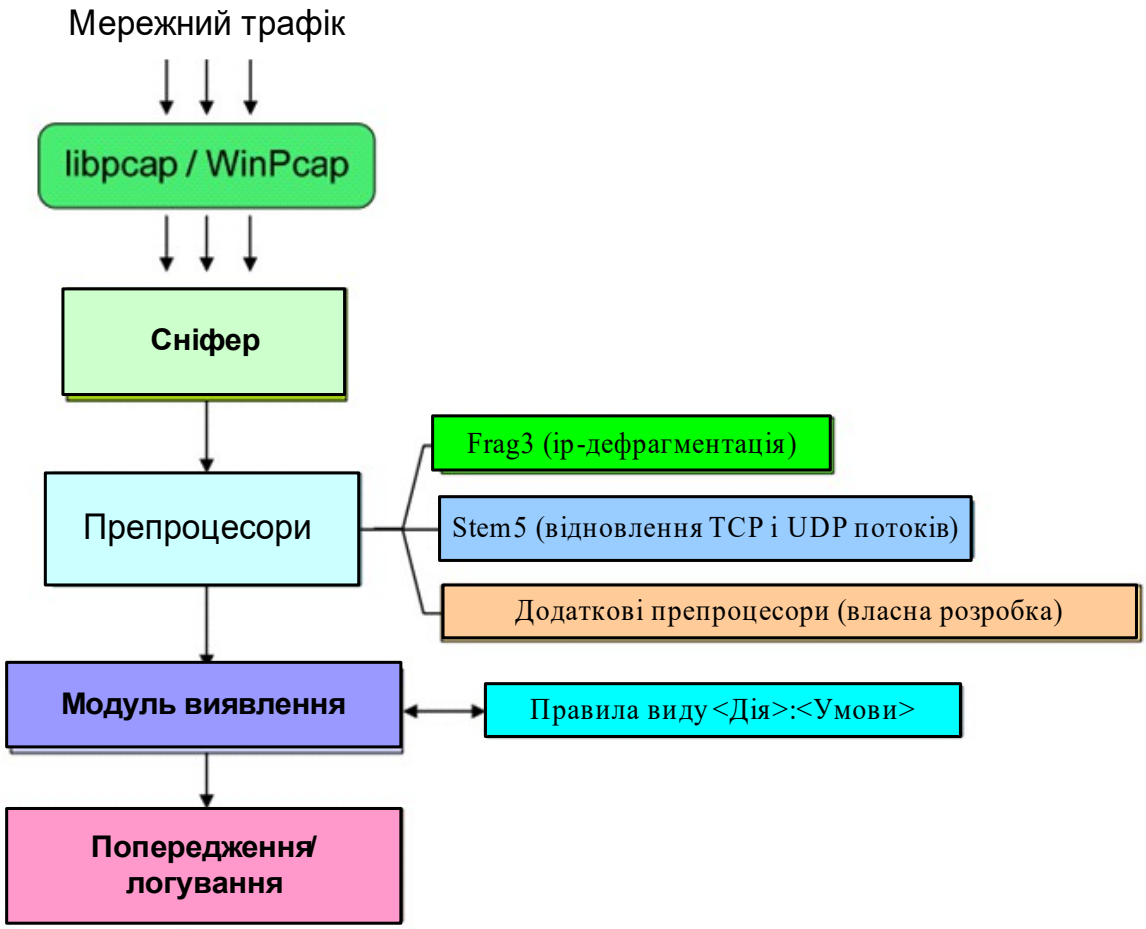


Рисунок 2.23 – Архітектура Snort

З рис. 2.23 можна побачити два найбільш головних компонента – набір препроцесорів та модуль виявлення. Препроцесори необхідні для розбору мережних протоколів (аналіз пакетів, відновлення потоків). Програма Snort дає до двадцяти базових препроцесорів. Користувач може створити додаткові препроцесори. У кожного препроцесора є власний певний набір параметрів. Необхідність модуля виявлення у тому, щоб робити певні дії у разі виявлення заданих користувачем патернів у розібраних пакетах та відновлених потоках.

```
alert tcp any any -> 192.168.1.0/24 111 \
    (content:"|00 01 86 a5|"; msg:"mountd access";)
```

Рисунок 2.24 – Правило для Snort

Правило на рис. 2.24 згенерує подію alert та виведе у консоль повідомлення «mountd access», якщо у пакеті протокола TCP, котрий прийшов на порт 111 і ip-адреса 192.168.1.0/24, буде виявлено сукупність електронних даних «00 01 86 a5» [12].

Як і для ip-адреси (пари ip-адрес) можна записати any і правило застосується до усіх пакетів протоколу. Snort не має підтримки доменних імен.

2.6 ClearSight Analyzer

ClearSight Analyzer це частина програмно-апаратного комплекса Network Time Machine. Архітектура цієї програми наведена на рис. 2.25.

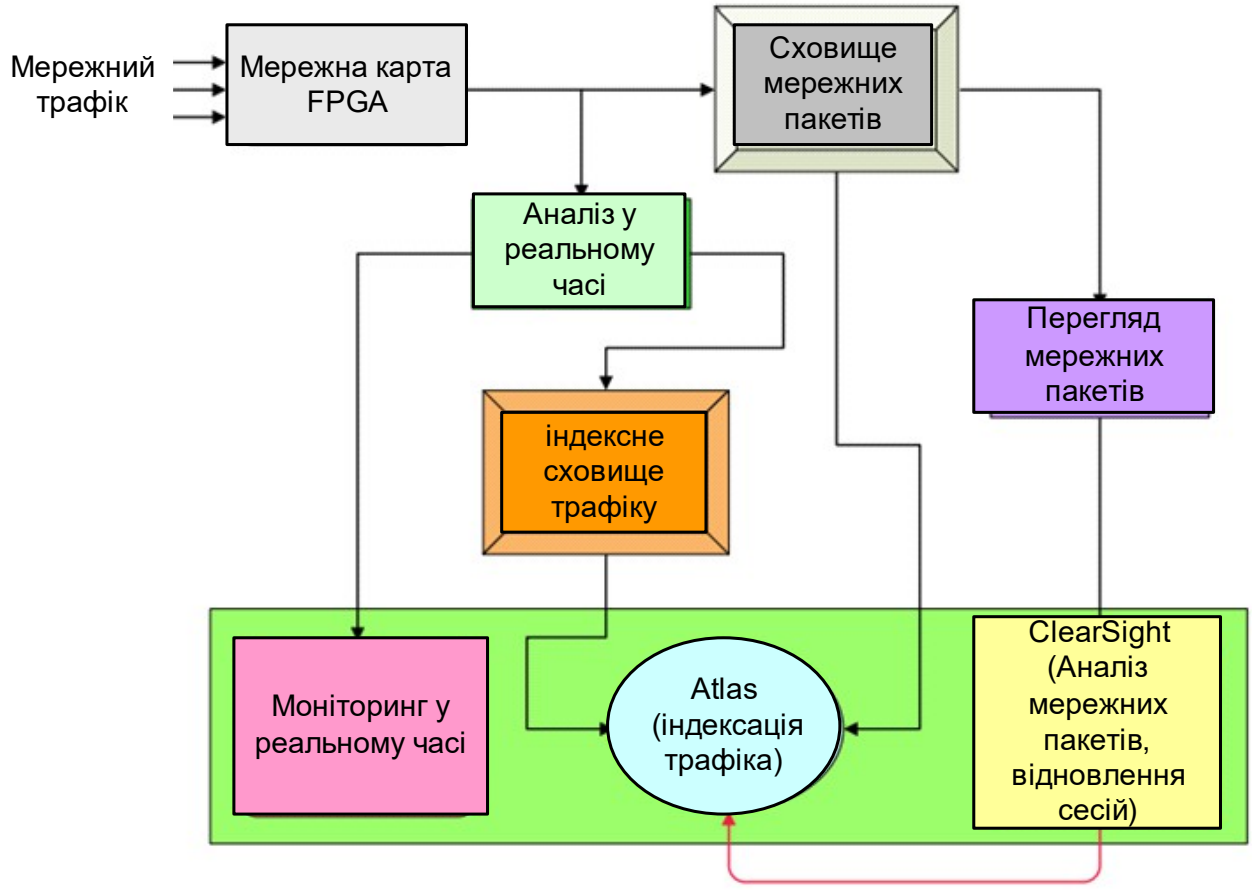


Рисунок 2.25 – Архітектура ClearSight Analyzer

Спеціалізована FPGA мережна карта дає можливість захопити 100% трафіка, який передається без затримок і швидкість якого 10-20 Gbps. Також, вона дає змогу фільтрувати мережні пакети. Трафік, що захоплено мережною картою зразу пишеться на жорсткому диску. Компонент ClearSight робить збірку пакету у сесії та аналізує його. Завдяки апаратній частині (FPGA мережна карта, індексація трафіку) виходять гарний результат з аналізу високошвидкісних каналів зв'язку. Якщо мережний канал, який аналізують має пропускну здатність приблизно100 Mbps, то апаратна підтримка не обов'язкова.

Для протоколів ClearSight Analyzer дає змогу встановити «порогові» значення. Якщо значення буде перевищено, користувач отримає повідомлення. Також, трафік, що «викликав» більше порогове значення, буде збережено окремо та остаточно не буде записано надалі.

На рис. 2.26 зображено усю активність для додатку HTTP, щоб можна було переглянуть дії на кожному з серверів, і потім донизу у сервер-потік, щоб побачити фактичний мультимедійний вміст потоку.

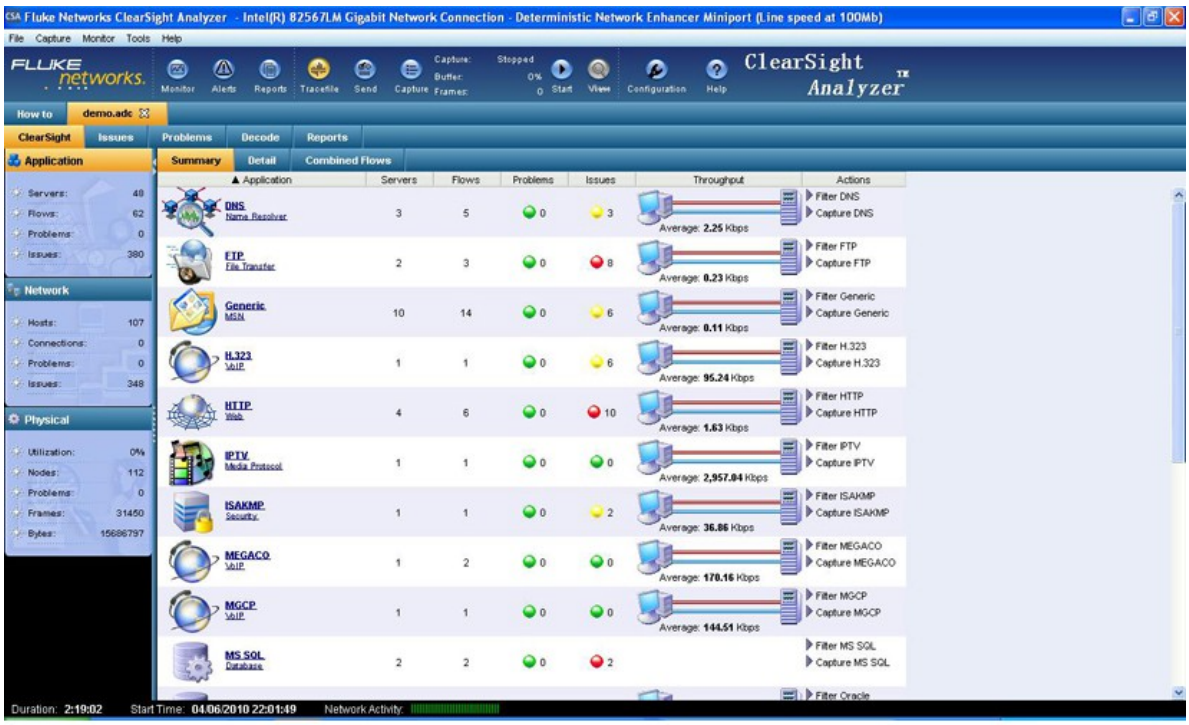


Рисунок 2.26 – Активність у мережі

Цей рівень контролю та відимості зменшує час на вирішення проблем з додатками та мінімізує загальний час у мережі [13].

2.7 CommView

CommView – програма, що робить моніторинг мережної активності за допомогою збору та подальшого аналіза пакетів у будь-який Ethernet-мережі. Завдяки цій програмі є змога побачити списки мережних з'єднань, IP-статистики, і проаналізувати вміст пакетів з даними.

Правильна система фільтрів дає змогу відкинути непотрібні пакети з даними або перехопити які необхідно.

На рис. 2.27 зображено головне вікно програми CommView

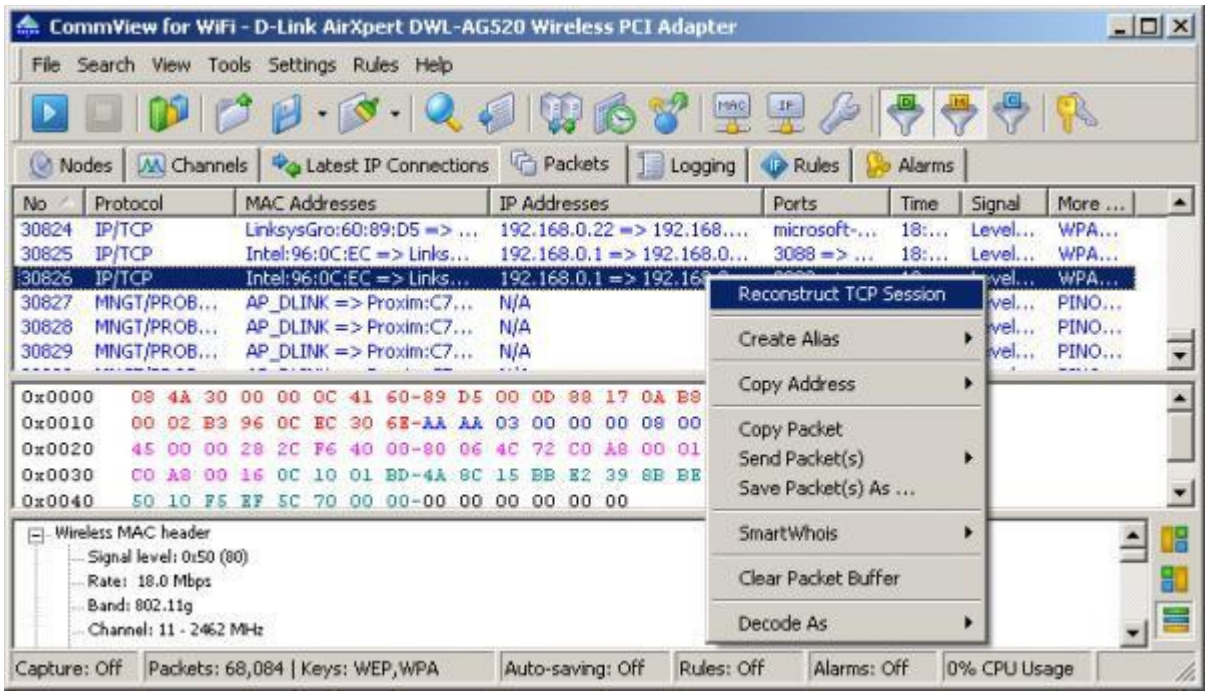


Рисунок 2.27 – Головне вікно програми CommView

У CommView є модуль VoIP, призначення якого зробити поглиблений аналіз, запис і відтворення стандартів SIP та H.323. Це необхідний інструмент

для адміністраторів, користувачів. Тому, що можна побачити повний аналіз трафіку.

Переваги даної програми наведені у табл. 2.6.

Таблиця 2.6 – Переваги програми CommView

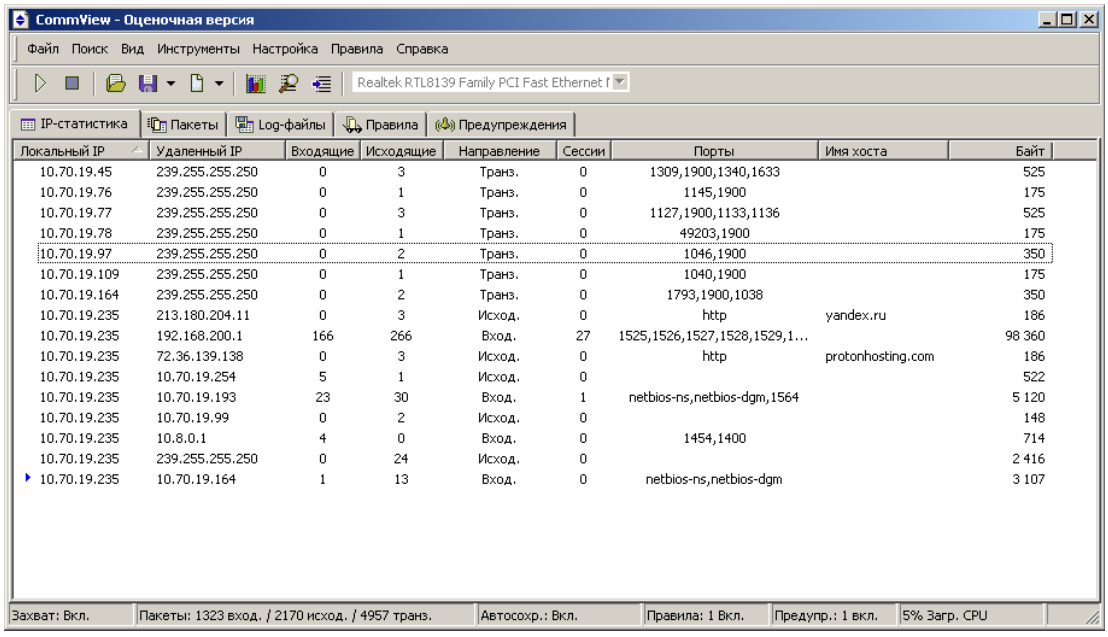
№	Переваги програми CommView
1	здійснює повний аналіз багатьох протоколів;
2	дозволяє користувачам CommView спостерігати мережний трафік комп'ютера з встановленим на ньому CommView Remote Agent, де б такий комп'ютер не був розташований фізично;
3	можна перехоплювати інтернет-трафік і / або трафік локальної мережі, що проходить через вашу мережну карту або контролер віддаленого доступу (dial-up);
4	бачити докладну статистику IP-з'єднань: IP-адреси, порти, сесії;
5	відтворювати TCP-сесії;
6	налаштовувати попередження, які повідомляють вам про важливі події, таких як підозрілі пакети, високе завантаження мережі, невідомі адреси і т. д.;
7	бачити діаграми IP-протоколів і протоколів верхнього рівня;
8	стежити за завантаженням мережі;
9	переглядати перехоплені і декодувати пакети в реальному часі;
10	робити пошук по рядках або hex-даними по вмісту перехоплених пакетів.
11	зберігати окремі пакети або всі пакети в архівах;

Продовження табл. 2.6

12	завантажувати і переглядати перехоплені пакети при вимкненому з'єднанні з мережею;
13	експортувати і імпортувати архіви зі збереженими пакетами в / з форматів NI Observer або NAI Sniffer;
14	передавати будь-який IP-адреса SmartWhois для швидкого і простого отримання інформації про нього.

На початку роботи програми аналізатора треба обрати мережний інтерфейс у меню «Налаштування\Установки» та розпочати захоплення мережних пакетів у меню «Файл \ почати захоплення».

Якщо захоплення пакетів успішне, то у головному вікні програми буде показана мережна статистика (рис 2.28).



Локальный IP	Удаленный IP	Входящие	Исходящие	Направление	Сессии	Порты	Имя хоста	Байт
10.70.19.45	239.255.255.250	0	3	Транз.	0	1309,1900,1340,1633		525
10.70.19.76	239.255.255.250	0	1	Транз.	0	1145,1900		175
10.70.19.77	239.255.255.250	0	3	Транз.	0	1127,1900,1133,1136		525
10.70.19.78	239.255.255.250	0	1	Транз.	0	49203,1900		175
10.70.19.97	239.255.255.250	0	2	Транз.	0	1046,1900		350
10.70.19.109	239.255.255.250	0	1	Транз.	0	1040,1900		175
10.70.19.164	239.255.255.250	0	2	Транз.	0	1793,1900,1038		350
10.70.19.235	213.180.204.11	0	3	Исход.	0	http	yandex.ru	186
10.70.19.235	192.168.200.1	166	266	Вход.	27	1525,1526,1527,1528,1529,1...		98 360
10.70.19.235	72.36.139.138	0	3	Исход.	0	http	protonhosting.com	186
10.70.19.235	10.70.19.254	5	1	Исход.	0			522
10.70.19.235	10.70.19.193	23	30	Вход.	1	netbios-ns,netbios-dgm,1564		5 120
10.70.19.235	10.70.19.99	0	2	Исход.	0			148
10.70.19.235	10.8.0.1	4	0	Вход.	0	1454,1400		714
10.70.19.235	239.255.255.250	0	24	Исход.	0			2 416
10.70.19.235	10.70.19.164	1	13	Вход.	0	netbios-ns,netbios-dgm		3 107

Рисунок 2.28 – Мережна статистика пакетів

Статистика показує одержувачів пакетів з даними, відправника, число пакетів, напрямок, порт за яким відбувається обмін.

У вкладці «Пакети» на головному вікні програми можна побачити дані за змістом мережного пакета, обравши його зі списку. На рис. 2.29 зображено пакет з номером 67 протокола IP/TCP. У центральній частині вікна показані основні параметри пакету (внутрішній номер пакета, протокол, MAC-адреси) Справа подана детальна інформація з декодуванням структури пакета, що наведена у нижній частині вікна [14].

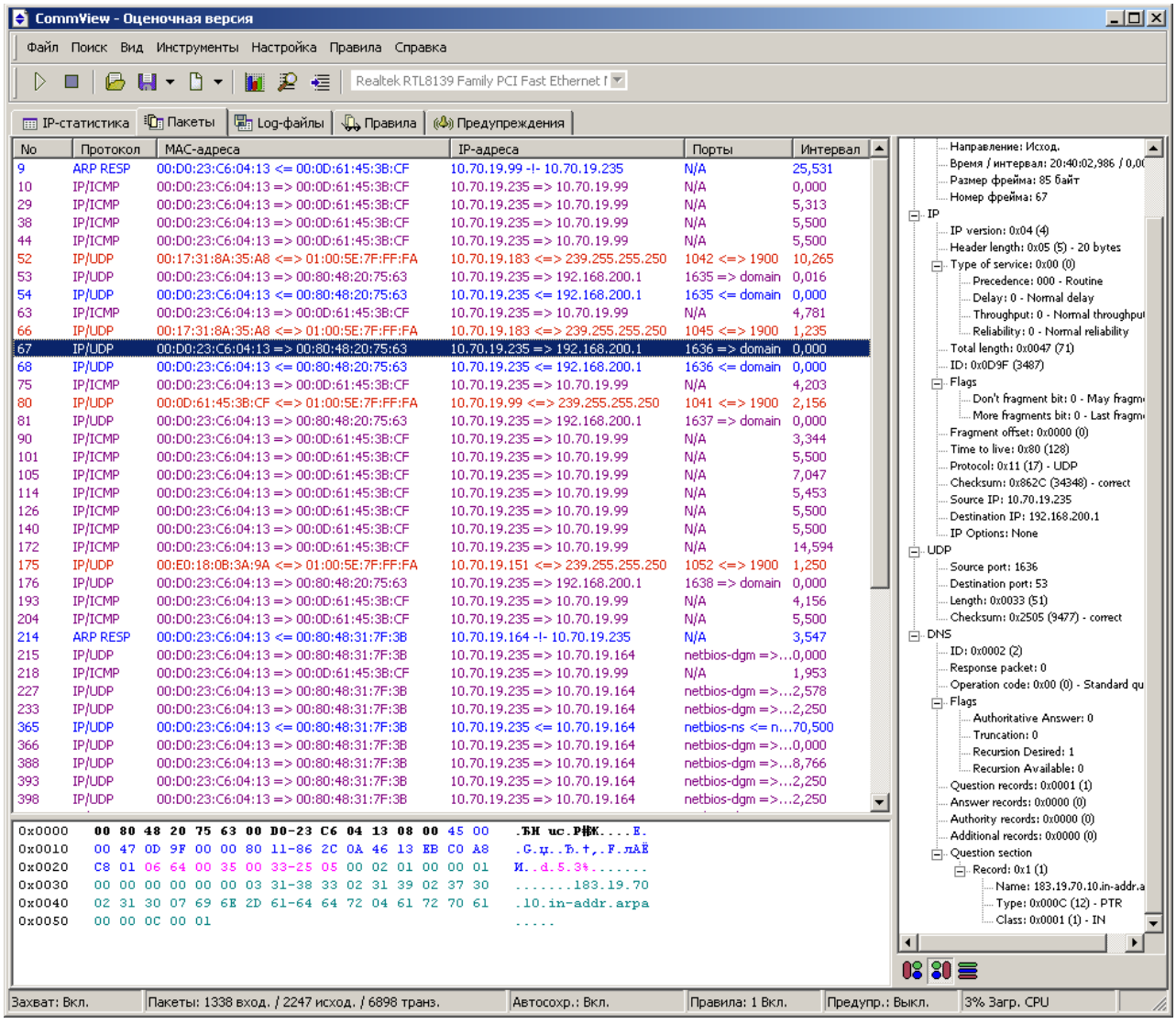


Рисунок 2.29 – Детальне вивчення мережного пакету

Створені правила для ігнорування при зборі мережних пакетів з широкомовною MAC адресою. Для цього треба перейти на вкладку «Правила»,

потім «MAC-адреси» далі «Включити правила для MAC-адрес» і ввести MAC-адреса FF FF FF FF FF FF. Вказати «Додати запіст» в будь-якому напрямку і як «Дії» ігнорувати (рис. 2.30).

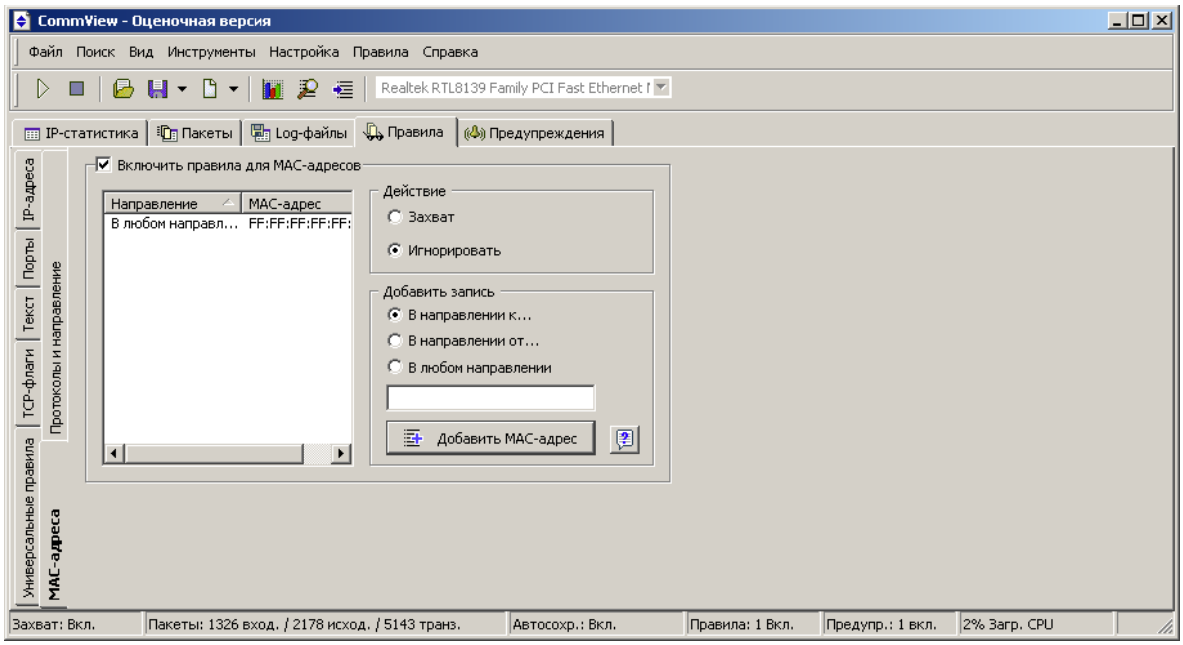


Рисунок 2.30 – Налаштування правил фільтрації мережних пакетів

Програма дає змогу зробити число розкритих пакетів у головному вікні програми, та інша інформація буде зафіксована у файли журнала і розміщена у зведену статистику.

При необхідності перегляду всіх пакетів можна зайти через головне меню «Файл \ Перегляд log- файлів». Параметри log-файлів налаштовуються на вкладці log-файли.

Для відображення загальної картини по мережним пакетам можна скористатися розширеною статистикою через головне меню «Вид\ Статистика».

3 АНАЛІЗ МЕРЕЖНОГО ТРАФІКУ НА БАЗІ ВІДНОВЛЕННЯ TCP-СЕСІЙ ТА РОЗПІЗНАВАННЯ ПРОТОКОЛІВ

Кожна з розглянутих програм була протестована на наборі, до якого входить 8 мережних трас (у кожній трасі є пакет протокола TCP) які наведені в табл. 3.1.

Таблиця 3.1 – Мережні траси

№	Мережні траси	Призначення
1	gen-googlemaps.pcap	відкриття сайту maps.google.com
2	gen-googleopen.pcap	відкриття сайту google.com
3	google-http.pcap	пошук в Google
4	google-https.pcap	пошук в Google з використанням SSL
5	http-google.pcap	завантаження сайту Google
6	http-googlesearch.pcap	робота спливаючих підказок при пошуку в Google

Замість цього необхідно проаналізувати послідовність даних в пакетах за порядком їх надходження, проте це не дуже зручно. У табл. 3.2 представлені TCP-з'єднання.

Таблиця 3.2 – Відмінності при відновленні TCP сесій

№	Кінцеві точки	Розмір відновленої сесії			
		Wireshark	Snort	Bro	ClearSight Analyzer
google-http.pcap					

Продовження табл. 3.2

1	192.168.0.105:25162 – 74.125.19.104:80	22925	22925	-	22925
2	192.168.0.105:25161 – 74.125.19.104:80	1216	1216		1216
3	192.168.0.105:25160 – 68.142.205.139:80	1897	1897		1897
4	192.168.0.105:25168 – 74.125.19.104:80	20125	20125	20125	20125
5	192.168.0.105:25175 – 68.142.205.139:80	6515	6515	6515	6515
6	192.168.0.105:25180 – 68.142.205.139:80	7087	7087	7087	7087
google-https.pcap					
7	192.168.0.105:24044 – 74.125.205.113:80	10480	10527	10480	10527
8	192.168.0.105:24053 – 68.142.205.139:80	6515	6515	6515	6515
9	192.168.0.105:24060 – 68.142.205.139:80	6797	6797	6797	6797
10	192.168.0.105:24089 – 68.142.205.139:80	123832	123832	123832	123832
http-google.pcap					
11	192.168.0.115:37927 – 74.125.19.106:80	31166	3166	-	31166
12	192.168.0.115:37903 – 74.125.19.106:80	15207	15207	-	15207
13	192.168.0.115:37979 – 74.125.36.37:80	0	0	-	0

Продовження табл. 3.2

14	192.168.0.115:37905 – 74.125.19.100:80	773	773	-	773
http-googlesearch.pcap					
15	24.6.173.220:49771 – 74.125.224.105:80	13244	13244	-	13244
16	24.6.173.220:49795 – 74.125.224.83:80	0	0	-	0
17	24.6.173.220:49831 – 63.245.209.93:80	0	0	-	0
18	24.6.173.220:49832 – 96.17.148.90:80	0	0	-	0

Бачимо, що в деяких з'єднаннях програма Bro не відновила дані. Теж, розмір сесії, який відновлено за допомогою Snort і ClearSight Analyzer, більше розміру сесії, яку відновлено Wireshark і Bro. Вміст сесій, які відновлено теж різний[15, 16]. Результат аналізу наведено в табл. 3.3.

Таблиця 3.3 – Результат аналізу

№	Результат тестування
1	– Bro починає відновлювати дані з'єднання з моменту його встановлення, а Wireshark, Snort і ClearSight - з моменту виявлення першого TCP-сегмента між даними парами адрес- порт. З'єднання з номерами 11, 11 - 18 були встановлені до початку запису відповідної траси. Тому Bro не зміг їх відновити;
2	– кожне із з'єднань 4 - 6, 8 - 10 має по 2 сегмента, які потрапили в трасу в неправильному порядку (з точки зору збирання TCP-потоку). При розборі інструменти Bro і Wireshark вірно додали дані цих сегментів в правильному порядку. Snort і ClearSight додали дані в тому порядку, в якому вони прийшли;

Продовження табл. 3.3

3	– з'єднання 7 має сегмент повторної передачі. Дані цих сегментів були відкинуті Wireshark і Bro, але додані Snort і ClearSight;
4	- Тестування показало, що інструменти Wireshark і Bro найбільш точно відновлюють дані TCP-з'єднань. Однак Bro не відновлює (хоча б частково) з'єднання, встановлені до моменту початку перехоплення трафіку. Snort і ClearSight не виробляють необхідного перепорядкування даних, додаючи їх в порядку приходу, а також не відкидають сегменти, передані повторно.

На прикладі 9 мережних трас протестовано кожну програму, зроблено, також, розпізнавання протоколів:

- ppp-general.pcap;
- sec-clientdying.pcap;
- sec-nmap-ipscan.pcap;
- smb-joindomain.pcap;
- tcp-pktloss94040.pcap;
- udp-mcaststream-queued2.pcap;
- udp-pentest.pcap;
- vlan-general.pcap;
- voip-extension.pcap.

Траси, які є у набірі, мають майже весь список протоколів, які підтримуються програмою Wireshark. Програми Bro та ClearSight не дозволяють отримання статистики по протоколам, які виявлено у трасі. З аналізу вихідного коду програми Bro виявлено, що програма орієнтована на протоколи, які належать першим чотирьом рівням моделі OSI. Система ClearSight може розпізнавати протоколи усіх рівнів. Отримані результати з тестування розпізнавання протоколів для програм Wireshark, Snort і Colasoft Capsa наведено у табл. 3.4.

Таблиця 3.4 – Результати тестування розпізнавання протоколів

Траса	Програми		
	Wireshark	Snort	ClearSight
1	eth, ip, gre. ppp, Kp. chap, ccp, ipcp	Eth, IP4, GRE, GRE PPTP	Ethernet II, IP, GRE, PPP, lst Choise
2	eth, ip, udp, dns, tcp, http, dcerpc, data, smb, irc, nbss, pipe, nntp, mgmt, isystemactivator	Eth, lP4, UDP, TCP	Compression, Link Control Protocol, Challenge Handshake, IP Control Protocol
3	eth, ip, igmp, icmpv6, vines_frp, ncs	Eth, IP4, ICMP, UDP, TCP, IP6, IP4/IP4, lP6/IP6, GRE	Ethernet ll, IP, UDP, TFTP, DNS, TCP, HTTP, IRC, NNTP, ClFS, FTP
4	eth, ip, udp, dns,tcp, dcerpc, icmp, arp,smb, cldap, kerberos,nbss, pipe, Isarpc, samr, rpc_netlogon, Idap cldap, kerberos, nbss, pipe, Isarpc, samr	Eth, IPA, ICMP, UDP, TCP, ARP	Ethernet II, IP, VRRP, UDP, TLSP, TCP, SPS, SNP, SMP, SDRP, SCTP, RSVP, RDP, PVP, PUP, PTP, PRM, PIPE, PIM, OSPF, NETBLT

Бачимо, що при розпізнаванні Snort «зупиняється» на протоколах транспортного рівня та не йде «нагору». При тестуванні було використано версію Snort зі стандартним набором правил. Програми Wireshark і ClearSight однаково гарно розпізнають протоколи усіх рівнів моделі OSI [16].

У табл. 3.5 наведено порівняльну характеристику програм-аналізаторів мережного трафіку.

Таблиця 3.5 – Порівняльна таблиця характеристик розглянутих програм-аналізаторів мережного трафіку

	Wireshark	Iris	NetFlow	Bro	ClearSight	Comm View
Розмір файлу, МБ	17,4	5,04	20,6	17,7	18,1	29,9
Мова інтерфейсу	англ.	рос.	англ.	англ.	англ.	англ.
Графік швидкості	+	+	+	-	+	+
Графік трафіку	+	+	+	-	+	-
Експорт, Імпорт	+	+	-	-	-	+
Запуск моніторингу	-	-	-	-	-	-
Min крок між звітами, с	0,001	1	1	1	0,001	1
Зміна min кроку між звітами	+	+	+	-	+	-

ВИСНОВКИ

В роботі було розглянуто і проаналізовано програми з інжинірингу мережного трафіку: Wireshark, Iris Network traffic Analyzer, NetFlow Traffic Analyzer, Bro Network Security Monitor, Snort, ClearSight Analyzer, CommView. Для кожної з програм зроблено опис архітектури і основних переваг та недоліків з функціональності та легкісті у використанні.

Досліджено основні можливості програм з висновками їх переваг і недоліків. Результати досліджень наведено у таблицях.

З найпопулярніших програм є Wireshark. Ця програма дає змогу зробити розбір та провести розпізнавання більш ніж 1000 мережних протоколів. Стосовно інших програм, вони не мають таку кількість підтримуваних протоколів.

Wireshark має більш ефективний засіб перегляду, збору та аналізу статистики трафіку.

ПЕРЕЛІК ПОСИЛАНЬ

1. Таненбаум Е., Уезеролл Д. Т18 Комп'ютерні мережі. 5-е изд. - СПб .: Пітер, 2012. – 32 с.

2. Оліфер В. Г., Оліфер Н.А. Комп'ютерні мережі. Принципи, технології, протоколи, 4-е видання - СПб .: Питер, 2010. – 944 с.

3. Петров В.В. Структура телетрафіка і алгоритм забезпечення якості обслуговування при впливі ефекту самоподібності. Дисертація на здобуття наукового ступеня кандидата технічних наук, Москва, 2004. – 199.

4. Платов В.В., Петров В.В. Дослідження структури телетрафіка бездротової мережі - М .: ОКБ МЕІ. 2004. №3. С. 58-62.

5. Мамаєв М. Телекомунікаційні технології (Мережі TCP / IP). Навчальний посібник. Владивосток. 2001. – 147 с.

6. Семенов Ю.А. Протоколи Internet. Енциклопедія. - М .: Гаряча лінія – Телеком, 2001. – 1100 с.

7. А.Н.Андрончік, В.В. Богданов, Н.А. Домуховскій, А.С., Захист інформації в комп'ютерних мережах. 2008. – 248 с.

8. Моніторинг мережі. Сніффер Wireshark [Електронний ресурс] – Режим доступ : www/ URL: http://www.4stud.info/networking/work2.html – 15.02.2018 р. – Загл. з екрану.

9. Iris Network Traffic Analyzer [Електронний ресурс] – Режим доступ : www/ URL: https://iris-network-traffic-analyzer.en – 15.03.2018 р. – Загл. з екрану.

10. Networktrafficanalyzerandmonitoringsoftware [Електронний ресурс] – Режим доступ : www/ URL: https://www.solarwinds.com/netflow-traffic-analyzer – 10.03.2018 р. – Загл. з екрану.

11. Bro Network Security Monitor [Електронний ресурс] – Режим доступ : www/ URL: https://www.bro.org/sphinx/intro/index.html – 20.03.2018 р. – Загл. з екрану.

12. Snort [Електронний ресурс] – Режим доступ : www/ URL: https://www.snort.org – 15.04.2018 р. – Загл. з екрану.

13. ClearSight Analyzer [Електронний ресурс] – Режим доступ : www/ URL: https://www.networkworld.com/article/2283763/lan-wan/clearsight-analyzer-serves-up-clear-view-of-voip-activity.html – 15.04.2018 р. – Загл. з екрану.

14. CommView [Електронний ресурс] – Режим доступ : www/ URL: https://www.tamos.ru/products/commview – 15.04.2018 р. – Загл. з екрану.

15. Аналіз мережного трафіку в режимі реального часу [Електронний ресурс] – Режим доступ : www/ URL: http://www.ispras.ru/preprints/docs – 21.05.2018 р. – Загл. з екрану.

16. Скорик Ю.В., Кузьмінов Ю.О. Порівняльний аналіз програмного забезпечення інжинірингу трафіку / Одинадцята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління» 8-9 квітня 2021 року. Баку – Харків – Київ – Жиліна – 2021. – С. 87.