Міністерство освіти і науки України
Тернопільський національний педагогічний університет ім. В. Гнатюка
Фізико-математичний факультет

Кафедра інформатики
та методики її викладання

ІНДЗ

на тему:

Моніторинг інтерфейсів Ethernet за допомогою програми Wireshark

Виконала:
студентки групи І-24
Віятик Христина
Науковий керівник:
Олексюк В. П.

Тернопіль 2013

Зміст

Вступ

Моніторинг — комплекс наукових, технічних, технологічних, організаційних та інших засобів, які забезпечують систематичний контроль (стеження) за станом та тенденціями розвитку природних, техногенних та суспільних процесів.

Методологічно моніторинг — це проведення низки однотипних замірів досліджуваного об'єкта і подальший аналіз, оцінка, порівняння отриманих результатів для виявлення певних закономірностей, тенденцій, змінних і їх динаміки.

Всі засоби моніторингу та аналізу мереж, можна розділити на кілька великих класів:

- *Системи управління мережею* (Network Management Systems) – централізовані програмні системи, які збирають дані про стан вузлів і комунікаційних пристроїв мережі, а також дані про трафік в мережі. Ці системи не тільки здійснюють моніторинг і аналіз, а й виконують в автоматичному чи напівавтоматиному режимі управління мережею - включення і відключення портів пристроїв, зміна параметрів мостів адресних таблиць мостів, комутаторів і маршрутизаторів і т.п. Прикладами систем управління можуть служити популярні системи HPOpenView, SunNetManager, IBMNetView.
- *Засоби управління системою* (System Management). Засоби управління системою часто виконують функції, аналогічні функціям систем управління, але стосовно інших об'єктів. У першому випадку об'єктом управління є програмне і апаратне забезпечення комп'ютерів мережі, а у другому - комунікаційне устаткування. Разом з тим, деякі функції цих двох видів систем управління можуть дублюватися, наприклад, засоби управління системою можуть виконувати най простіший аналіз мережевого трафіку. До найбільш відомих систем управління системами відносяться LANDesk, IBM Tivoli, Microsoft Systems Management Server, HP OpenView, Novell ZENworks і CA Unicenter.

- *Вбудовані системи діагностики і управління* (Embedded Systems). Ці системи виконуються у вигляді програмно-апаратних модулів, які встановлюються в комунікаційне обладнання, а також у вигляді програмних модулів, вбудованих в операційні системи. Вони виконують функції діагностики і управління тільки одним пристроєм, і в цьому їх основна відмінність від централізованих систем управління. Прикладом засобів цього класу може служити модуль управління концентратором Distrebuted 5000.

- *Аналізатори протоколів* (Protocolanalyzers). Представляють собою програмні або апаратно-програмні системи, які обмежуються на відміну від систем управління лише функціями моніторингу і аналізу трафіку в мережах. Хороший аналізатор протоколів може захоплювати і декодувати пакети великої кількості протоколів, що застосовуються в мережах - зазвичай кілька десятків.

- *Обладнання для діагностики і сертифікації кабельних систем.* Умовно це устаткування можна поділити на чотири основні групи: мережні монітори, прилади для сертифікації кабельних систем, кабельні сканери і тестери (мультиметри). Мережеві монітори (називають також мережевими аналізаторами) призначені для тестування кабелів різних категорій.

- *Експертні системи.* Цей вид систем акумулює людські знання про виявлення причин аномальної роботи мереж і можливі способи приведення мережі у працездатний стан. Прикладом такої системи є експертна система, вбудована в систему управління Spectrum компанії Cabletron.

- *Багатофункціональні пристрої аналізу та діагностики*. У зв'язку з розповсюдженням локальних мереж виникла необхідність розробки недорогих портативних приладів, які суміщають функції декількох пристроїв: аналізаторів протоколів, кабельних сканерів і, навіть, деяких можливостей ПЗ мережного управління. Як приклад такого роду пристроїв можна привести Compas компанії MicrotestInc. або 675 LANMeterкомпанії FlukeCorp.

Аналізатори протоколів

Програма Wireshark відноситься до аналізаторів протоколів.

Аналізатор протоколів є самостійним спеціалізованим пристроєм, або персональним комп'ютером, зазвичай переносним, класу Notebook, оснащений спеціальною мережевою картою і відповідним програмним забезпеченням. Аналізатор підключається до мережі точно так, як і звичайний вузол. Відмінність полягає в тому, що аналізатор може приймати всі пакети даних, що передаються по мережі, в той час як звичайна станція - лише адресовані їй.

Незважаючи на відносне різноманіття аналізаторів протоколів, представлених на ринку, можна назвати деякі риси, в тій чи іншій мірі притаманні всім їм:

- *Інтерфейс користувача*. Більшість аналізаторів мають розвинений дружній інтерфейс, який базується, як правило, на Windows чи Motif. Цей інтерфейс дозволяє користувачеві: виводити результати аналізу інтенсивності трафіку; отримувати миттєву і середню статистичну оцінку продуктивності мережі; задавати певні події і критичні ситуації для відстежування їх виникнення; робити декодування протоколів різного рівня і представляти в зрозумілій формі вміст пакетів.
- *Буфер захоплення*. Буфери різних аналізаторів відрізняються за обсягом. Буфер може розташовуватися на мережевій карті, або для нього може бути відведено місце в оперативній пам'яті одного з комп'ютерів мережі. Якщо буфер розташований на мережевій карті, то управління ним здійснюється апаратно, і за рахунок цього швидкість введення підвищується.
- Можливість *вимірювання середньостатистичних показників трафіку в сегменті локальної мереж*і, в якому встановлений мережевий адаптер аналізатора.
- Вимірюється *коефіцієнт використання сегменту*, матриці перехресного трафіку вузлів, кількість хороших і поганих кадрів, що пройшли через сегмент.

- Можливість роботи *з декількома агентами*, котрі поставляють захоплені пакети з різних сегментів локальної мережі.
- *Фільтри*. Фільтри дозволяють керувати процесом захоплення даних, і, тим самим, дозволяють економити простір буфера. Залежно від значення певних полів пакета, заданих у вигляді умови фільтрації, пакет або ігнорується, або записується в буфер захоплення. Використання фільтрів значно прискорює і спрощує аналіз, оскільки виключає перегляд непотрібних в даний момент пакетів.
- *Перемикачі* - це деякі умови початку і припинення процесу захоплення даних з мережі, що задаються користувачем. Перемикачі можуть використовуватися спільно з фільтрами, дозволяючи більш детально й тонко проводити аналіз, а також продуктивніше використовувати обмежений обсяг буфера захоплення.
- *Пошук*. Деякі аналізатори протоколів дозволяють автоматизувати перегляд інформації, що знаходиться в буфері, і знаходити в ній дані по заданим критеріям.
- *Багатоканальність*. Деякі аналізатори протоколів дозволяють проводити одночасний запис пакетів від декількох мережевих адаптерів, що зручно для зіставлення процесів, що відбуваються в різних сегментах мережі.

Методологія проведення аналізу може бути представлена у вигляді наступних шести етапів:

- Захоплення даних.
- Перегляд захоплених даних.
- Аналіз даних.
- Пошук помилок
- Дослідження продуктивності.
- Докладне дослідження окремих ділянок мережі.

Зазвичай процес аналізу протоколів займає відносно небагато часу - 1-2 робочих дні.

Розділ 1. Теоретична частина

Аналізатор трафіку (сніфер).

Іноді буває необхідно або корисно виконати моніторинг мережевого трафіку на комп'ютері, адже ми можемо стежити за усіма даними, що входять в комп'ютер, та виходять з нього. Тобто ми може перехоплювати трафік та прослідковувати виконані операції, для чого існують спеціальні програми аналізатори трафіку (сніфери).

Аналізатор трафіку або сніфер — програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу, або тільки аналізу мережного трафіку, призначеного для інших вузлів.

Перехоплення трафіку може здійснюватися:

- звичайним «прослуховуванням» мережевого інтерфейсу (метод ефективний при використанні в сегменті концентраторів (хабів) замість комутаторів (світчей), інакше метод малоефективний, оскільки на сніфер потрапляють лише окремі фрейми);
- підключенням сніфера в розрив каналу;
- відгалуженням (програмним або апаратним) трафіку і спрямуванням його копії на сніфер;
- через аналіз побічних електромагнітних випромінювань і відновлення трафіку, що таким чином прослуховується;
- через атаку на канальному (2) (MAC-spoofing) або мережевому (3) рівні (IP-spoofing), що приводить до пере направлення трафіку жертви або всього трафіку сегменту на сніфер з подальшим поверненням трафіку в належну адресу.

На початку 1990-х широко застосовувався хакерами для захоплення призначених для користувача логінів і паролів, які у ряді мережевих протоколів передаються в незашифрованому або слабо-зашифрованому вигляді. Широке розповсю-

дження хабів дозволяло захоплювати трафік без великих зусиль у великих сегментах локальної мережі практично без ризику бути виявленим.

Сніфери застосовуються як в благих, так і в деструктивних цілях. Аналіз трафіку, що пройшов через сніфер, дозволяє:

- виявити паразитний, вірусний і закільцьований трафік, наявність якого збільшує завантаження мережного устаткування і каналів зв'язку (сніфери тут малоефективні; як правило, для цих цілей використовують збір різноманітної статистики серверами і активним мережним устаткуванням і її подальший аналіз).
- виявити в мережі шкідливе і несанкціоноване ПЗ, наприклад, мережеві сканери, флудери, троянські програми, клієнти пірінгових мереж та інші (це зазвичай роблять за допомогою спеціалізованих сніферів — моніторів мережної активності).
- Перехопити будь-який незашифрований (а деколи і зашифрований) призначений для користувача трафік з метою отримання паролів і іншої інформації.
- Локалізувати несправність мережі або помилку конфігурації мережних агентів (для цієї мети сніфери часто застосовуються системними адміністраторами)

Оскільки в «класичному» сніфері аналіз трафіку відбувається вручну, із застосуванням лише простих засобів автоматизації (аналіз протоколів, відновлення TCP-потоку), то він підходить для аналізу лише невеликих його обсягів.

Як не дивно, в природі існує безліч сніферів, тому їх поділяють на категорії :

- HTTP сніфери (HTTP Analyzer, IEWatch Professional, EffeTech HTTP Sniffer), перехоплюють HTTP заголовки;
- принт-сніфери (O & K PrintWatch , PrintMonitor , PrintInspector) , дозволяють контролювати і керувати процесом друку в мережі;

- аналізатори протоколів (Wireshark, TracePlus32 WebDetective, Comm-View);
- сніфери IM систем (MSN Shiffer, ICQ Sniffer, AIM Sniff, IM- Sniffer), надають перехоплену переписку у зручно читається вигляді ;
- парольні сніфери (Cain&Abel, AcePasswordSniffer), перехоплюють і контролюють різноманітні паролі;
- сніфери бездротових мереж (Kismet, airodump - ng, CommViewforWiFi), перехоплюють трафік бездротових мереж навіть без підключення до цих мереж;
- пакетні сніфери (NetworkProbe, EtherscanAnalyzer).

Зупинимось на програмі Wireshark.

Wireshark

Wireshark (раніше Ethereal) — програма для аналізу мережевих пакетів Ethernet і інших мереж (сніфер). Має графічний інтерфейс користувача. У червні 2006 року проект був перейменований на Wireshark через проблеми з торговою маркою.

Функціональність, яку надає Wireshark, дуже схожа з можливостями програми tcpdump (сніфер, утиліта UNIX, що дозволяє захоплювати і аналізувати мережний трафік, що проходить через комп'ютер, на якому запущена ця програма), проте Wireshark має графічний інтерфейс користувача і значно більше можливостей із сортування і фільтрації інформації. Програма дозволяє користувачеві переглядати весь трафік, що проходить по мережі, в режимі реального часу, переводячи мережну карту в широкомовний режим.

Wireshark — це програма, яка розпізнає структуру найбільш різних мережевих протоколів, і тому дозволяє розібрати мережевий пакет, відображаючи значення кожного поля протоколу будь-якого рівня. Оскільки для захоплення пакетів використовується pcap, існує можливість захоплення даних тільки з тих мереж, які підтримуються цією бібліотекою. Проте, Wireshark вміє працювати з безліччю форматів початкових даних, відповідно, можна відкривати файли даних, захоплених іншими програмами, що розширює можливості захоплення.

Основи програми Wireshark

Wireshark - це аналізатор мережевого трафіку. Його завдання полягає в тому , щоб перехоплювати мережевий трафік і відображати його в детальному вигляді. Аналізатор мережевого трафіку можна порівняти з вимірювальним пристроєм, який використовується для перегляду того , що відбувається всередині мережевого кабелю , як наприклад вольтметр використовується електриками для того щоб дізнатися що відбувається всередині електропроводки (але , звичайно , на більш високому рівні) .

У минулому такі інструменти були дуже дорогими і складними. Однак , з моменту появи такого інструменту як Wireshark ситуація змінилася. Wireshark - це один з кращих аналізаторів мережевого трафіку , доступних на сьогоднішній момент. Wireshark працює на основі бібліотеки pcap . Бібліотека Pcap (PacketCapture) дозволяє створювати програми аналізу мережевих даних, що надходять на мережеву карту комп'ютера . Різноманітні програми моніторингу та тестування мережі , сніфери використовують цю бібліотеку. Для Unix- подібних систем використовують libpcap бібліотеку , а для Microsoft Windows NT використовують WinPcap бібліотеку. Програмне забезпечення мережевого моніторингу може використовувати libpcap або WinPcap , щоб захопити пакети , які подорожують по мережі і в більш нових версіях для передачі пакетів в мережі. Libpcap і WinPcapтакож підтримують збереження захоплених пакетів у файл і читання файлів містять збережені пакети. Програми написані на основі libpcap або WinPcap можуть захопити мережевий трафік , аналізувати його . Файл захопленого трафіку зберігається у форматі , зрозумілому для додатків, що використовують Pcap .

Для чого використовується Wireshark?

Системні адміністратори використовують його для вирішення проблем в мережі, аудитори безпеки використовують його для виявлення проблем в мережі, розробники використовують його для налагодження мережевих додатків, звичайні користувачі використовують його для вивчення внутрішнього устрою мережевих протоколів.

Можливості Wireshark.

- ✓ Працює на більшості сучасних ОС (Microsoft Windows , Mac OS X , UNIX) . Wireshark - продукт з відкритим вихідним кодом, який поширюється на підставі ліцензії GPL. Його можна використовувати на будь-якій кількості комп'ютерів , не побоюючись за введення ліцензійних ключів , продовження ліцензії та інші неприємні заходи. Тому спільноті дуже легко додавати в нього підтримку нових протоколів у вигляді плагінів або безпосередньо вшити її у вихідний код .

✓ Перехоплення трафіку мережевого інтерфейсу в режимі реального часу. Wireshark може перехоплювати трафік різних мережевих пристроїв, відображаючи його ім'я (включаючи бездротові пристрої) . Підтримування того або іншого пристрою залежить від багатьох факторів , наприклад від операційної системи.

✓ Безліч протокольних декодувальників (TELNET , FTP , POP , RLOGIN , ICQ , SMB , MySQL , HTTP , NNTP , X11 , NAPSTER , IRC , RIP , BGP , SOCKS 5 , IMAP 4 , VNC , LDAP , NFS , SNMP , MSN , YMSG і інші).

✓ Збереження і відкриття раніше збереженого мережевого трафіку.

✓ Імпорт та експорт файлів з інших пакетних аналізаторів . Wireshark може зберігати перехоплені пакети в велику кількість форматів інших пакетних аналізаторів, наприклад: libpcap, tcpdump, Sunsnoop, atmsnoop, Shomiti/FinisarSurveyor, NovellLANalyzer, Microsoft NetworkMonitor, AIX'siptrace.

✓ Дозволяє фільтрувати пакети по безлічі критерій .

✓ Дозволяє шукати пакети по безлічі критерій .

✓ Дозволяє підсвічувати захоплені пакети різних протоколів.

✓ Дозволяє створювати різноманітну статистику.

Програма Wireshark не може:

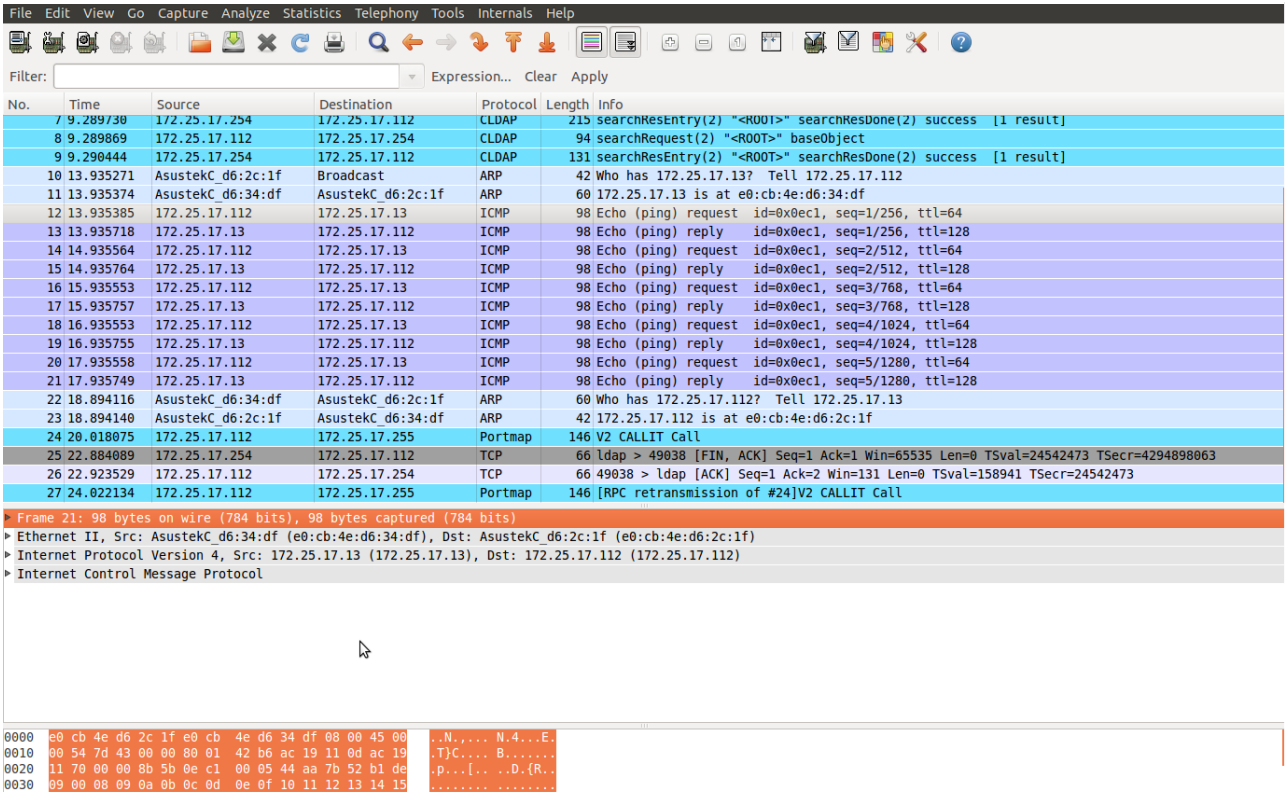
– Wireshark - це не система виявлення вторгнень. Він не попередить про те, якщо хтось робить дивні речі в мережі. Однак якщо це відбувається, Wireshark допоможе зрозуміти що ж насправді сталося.

– Wireshark не вміє генерувати мережевий трафік, він може лише аналізувати наявний. У цілому, Wireshark ніяк не проявляє себе в мережі, окрім як при резолвінгу доменних імен , але і цю функцію можна відключити.

Інтерфейс Wireshark.

Інтерфейс програми Wireshark представлений на малюнку:

Рисунок1



Розглянемо інтерфейс більш докладно. Зверху знаходиться стандартні для Linux додатків меню, на них детально зупинятися сенсу не має. Далі слідує фільтр, в ньому можна задавати критерії фільтрації пакетів, докладний опис роботи з ним розглянемо пізніше. Слідом йде вікно зі списком усіх перехоплених пакетів. У ньому доступна така інформація як: номер пакету, відносний час отримання пакету (відлік проводиться від першого пакету ; параметри відображення часу можна змінити в настройках), IP адреса відправника, IP адреса одержувача , протокол, за яким пересилається пакет, а також додаткову інформацію про ньому. Як можна помітити, різні протоколи підсвічені різними кольорами, що додає наочності і спрощує аналіз.

Далі видно вікно, в якому представлена детальна інформація про пакет згідно мережевої моделі OSI (абстрактна мережева модель для комунікацій і розробки

мережевих протоколів. Представляє рівневий підхід до мережі. Кожен рівень обслуговує свою частину процесу взаємодії. Завдяки такій структурі спільна робота мережного обладнання й програмного забезпечення стає набагато простішою, прозорішою й зрозумілішою.).

Ну, і найнижче вікно показує нам пакет в сирому HEX вигляді, тобто побайтово. Конфігурація інтерфейсу може бути легко змінена в меню View. Наприклад , можна прибрати вікно побайтового подання пакета (воно ж PacketBytes в меню View), так як в більшості випадків (крім аналізу даних у пакеті) воно не потрібно і тільки дублює інформацію з вікна детального опису.

Розділ 2. Практична частина

Перехоплення трафіку є однією з ключових можливостей Wireshark. Програма Wireshark з перехоплення надає такі можливості:

- ✓ перехоплення трафіку різних видів мережевого обладнання (Ethernet, TokenRing, ATM та інші);
- ✓ припинення перехоплення на основі різних подій: розміру перехоплених да-них , тривалість перехоплення за часом , кількість перехоплених пакетів;
- ✓ показ декодованих пакетів під час перехоплення;
- ✓ фільтрація пакетів з метою зменшити розмір перехопленої інформації;
- ✓ запис дампів в кілька файлів , якщо перехоплення триває довго.

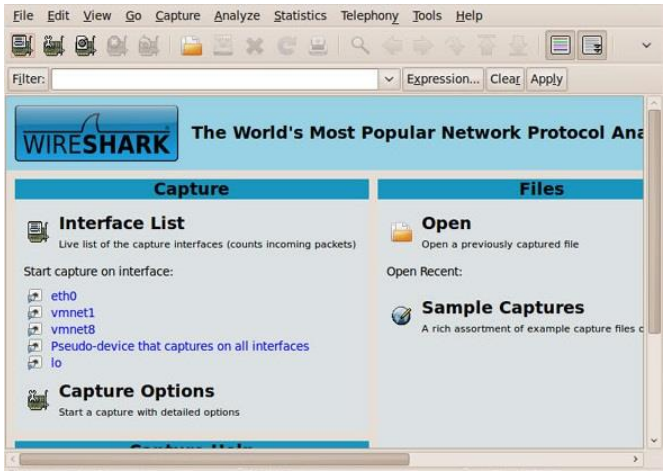
Програма не може виконувати наступні функції:

- перехоплення трафіку з декількох мережевих інтерфейсів одночасно (однак, існує можливість запустити кілька копій Wireshark - кожна для свого інтерфейсу);
- припинення перехоплення залежно від перехопленої інформації.

Щоб почати перехоплення трафіку потрібно мати права Адміністратора на даній системі і вибрати правильний мережевий інтерфейс. Тому, щоб запустити програму Wireshark в ОС Linux потрібно в терміналі ввести ряд команд:
«sudo –s→Password: →Wireshark», що запустить програму з правами адміністратора.

При першому запуску програма Wireshark буде виглядати наступним чином:

Рисунок 2



Клацнувши по кнопці List the available capture interfaces... (Список наявних відслідковуваних інтерфейсів ...):

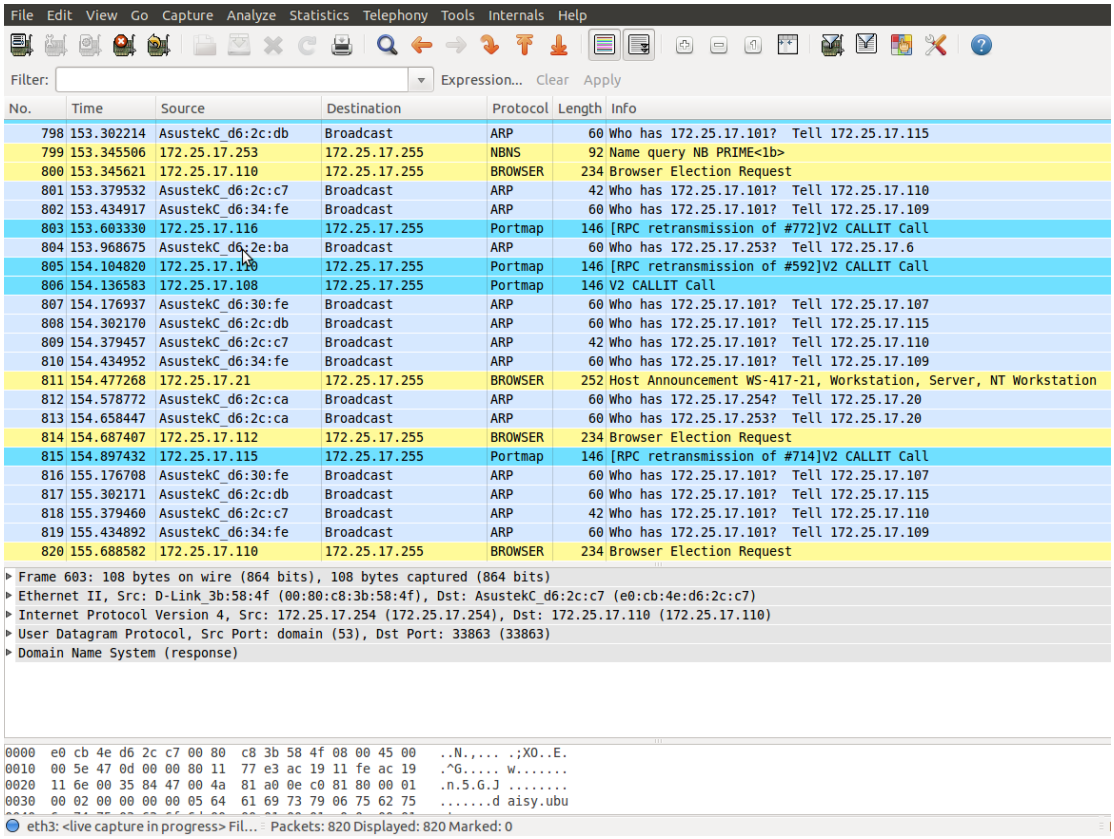
Рисунок 3

, відкриється нове вікно зі списком мережевих інтерфейсів, наявних у вашій системі.

Рисунок 4

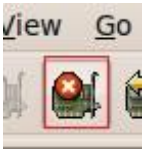
Тепер в головному вікні ми можемо слідкувати за пакетами, відстежувати для різних протоколів:

Рисунок 5



Збір даних триватиме до тих пір, поки не натиснути кнопку Stop:

Рисунок 6



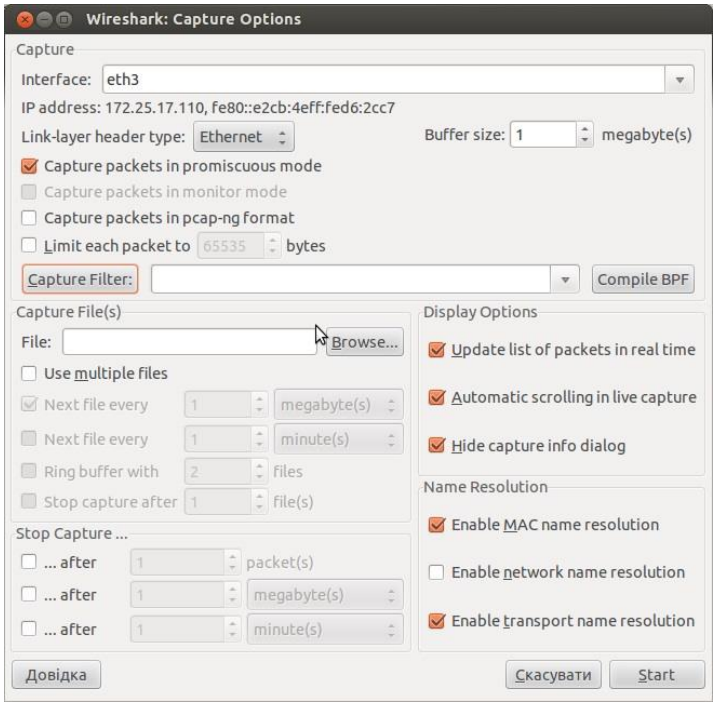
Після цього ми можемо переглянути результати, застосувати фільтри, зайнятися пошуком проблем і т.п.

Для того, щоб виконати більш тонке налаштування, клацніть по кнопці Show the capture options (Показати параметри збору даних):

Рисунок 7

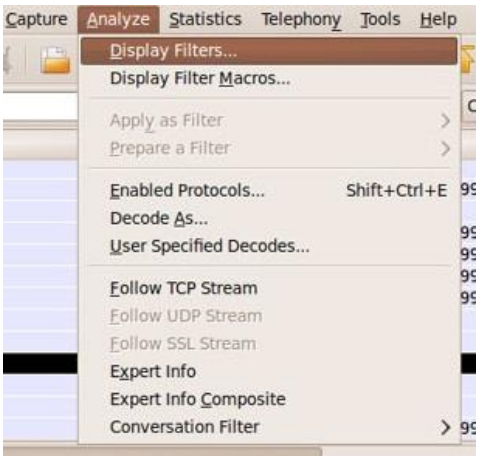
Відкриється нове вікно, в якому ми можемо встановити параметри, які будуть використані при наступному зборі даних. Після цього клацнемо по кнопці Start з тим, щоб почати збір даних:

Рисунок 8



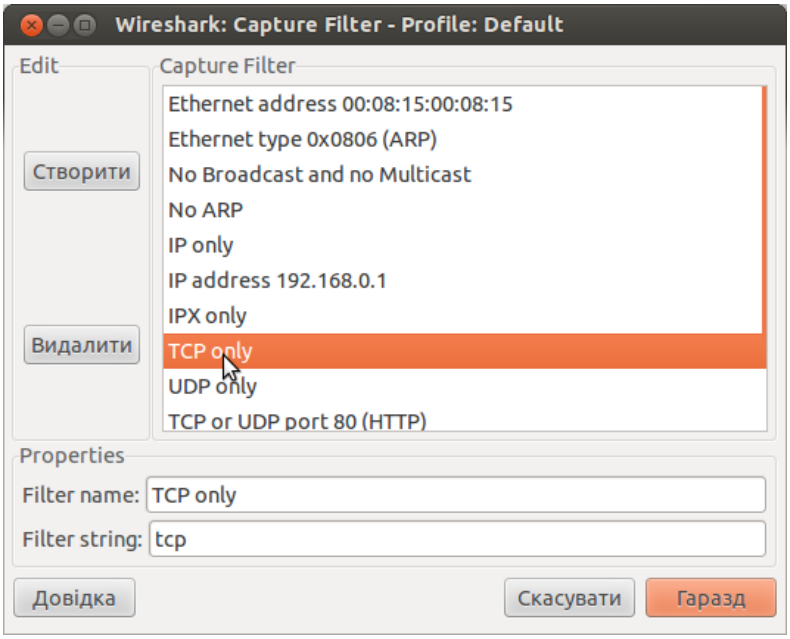
За замовчуванням в результатах будуть приведені дані по всіх знайдених протоколам. Якщо ми захочемо сконцентруватися на якомусь певному протоколі, ми можемо до отриманого результату застосувати фільтр. Перейдемо до пункту Analyze>Display Filters ...:

Рисунок 9



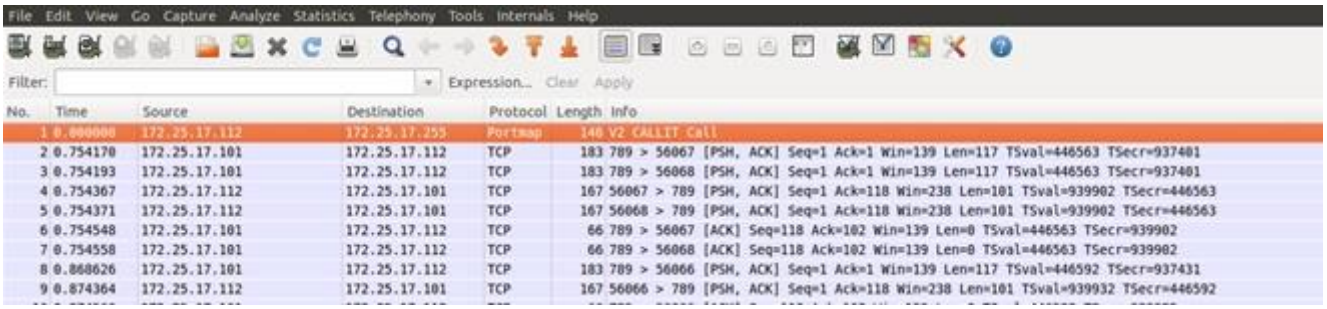
Відкриється нове вікно, в якому можна вибрати потрібний протокол (наприлад, TCP). Після цього клацнути по кнопці OK:

Рисунок 10



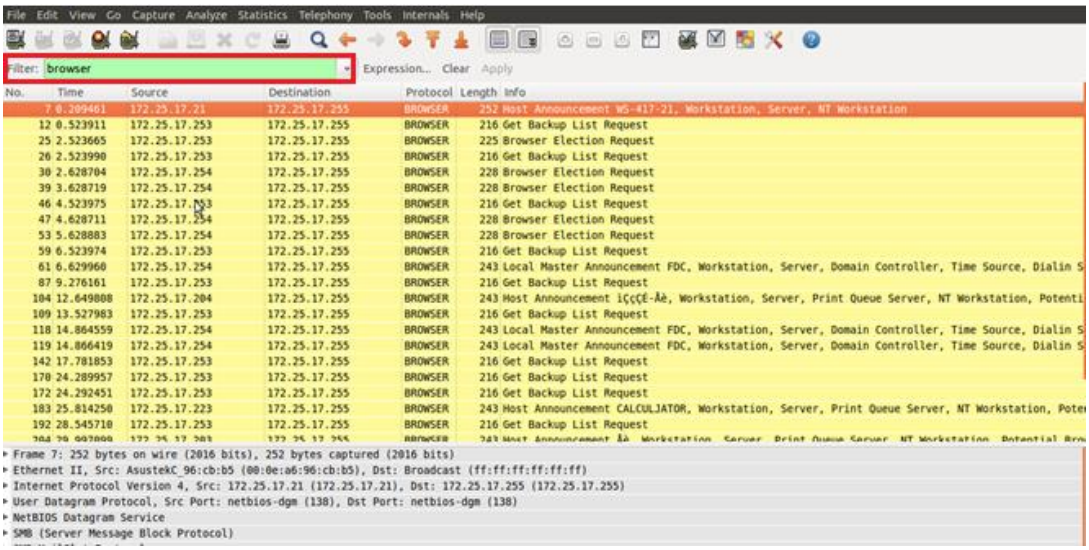
Тепер у вікні з результуючими даними, бачимо тільки трафік для протоколу TCP - усі інші протоколи будуть відфільтровані:

Рисунок 11



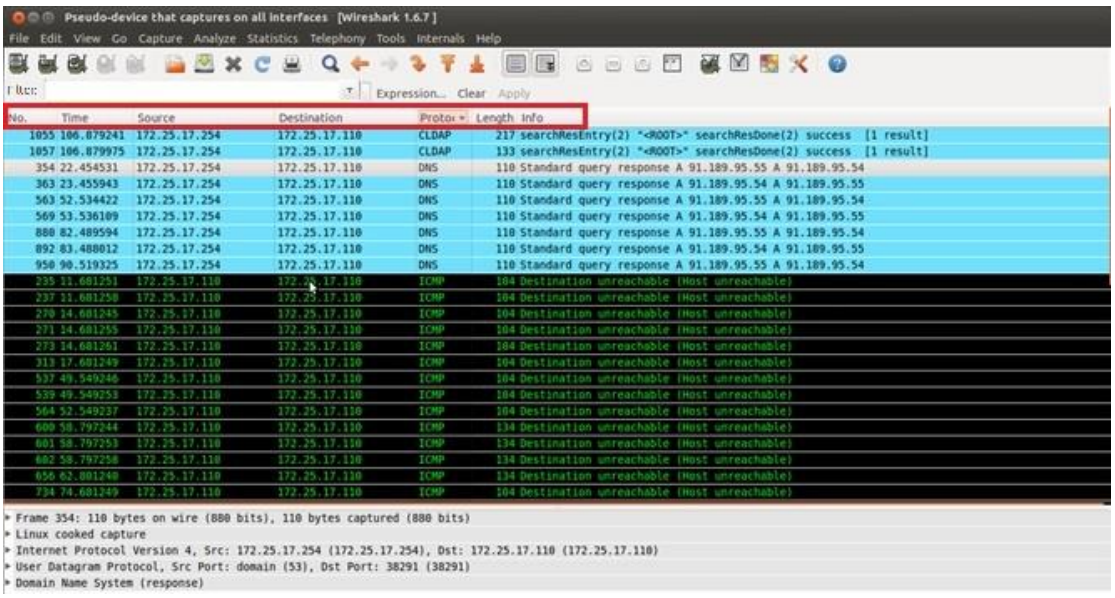
Фільтрацію за протоколом можна здійснювати, не тільки через Capture Filter, але і через Filter основного вікна:

Рисунок12



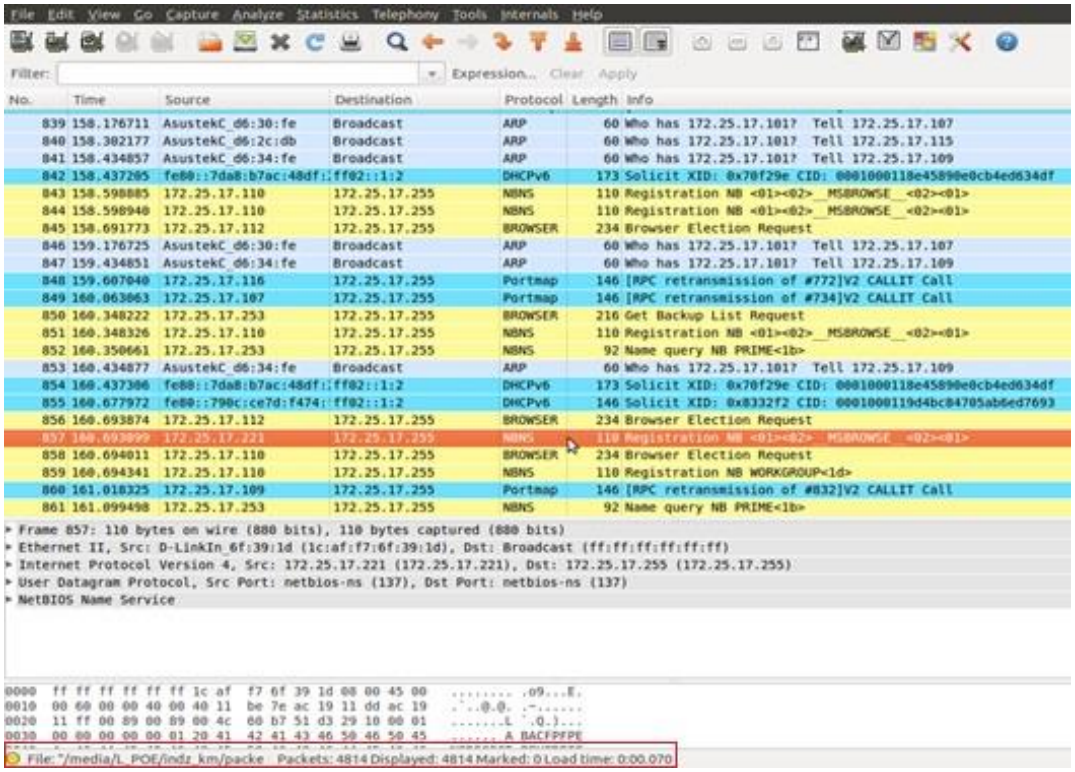
Дані в Wiresharkможна впорядковувати:

Рисунок 13



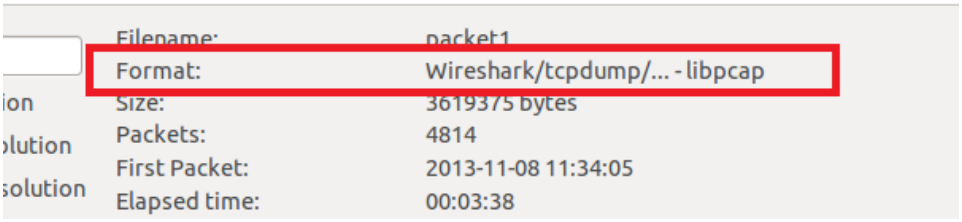
Для збереження захоплених даних у файл потрібно зайти в меню File→Save As... Після чого пакет даних можна буде відкрити знову для подальшого аналізу.

Рисунок 14



Формат збереженого файлу:

Рисунок 15

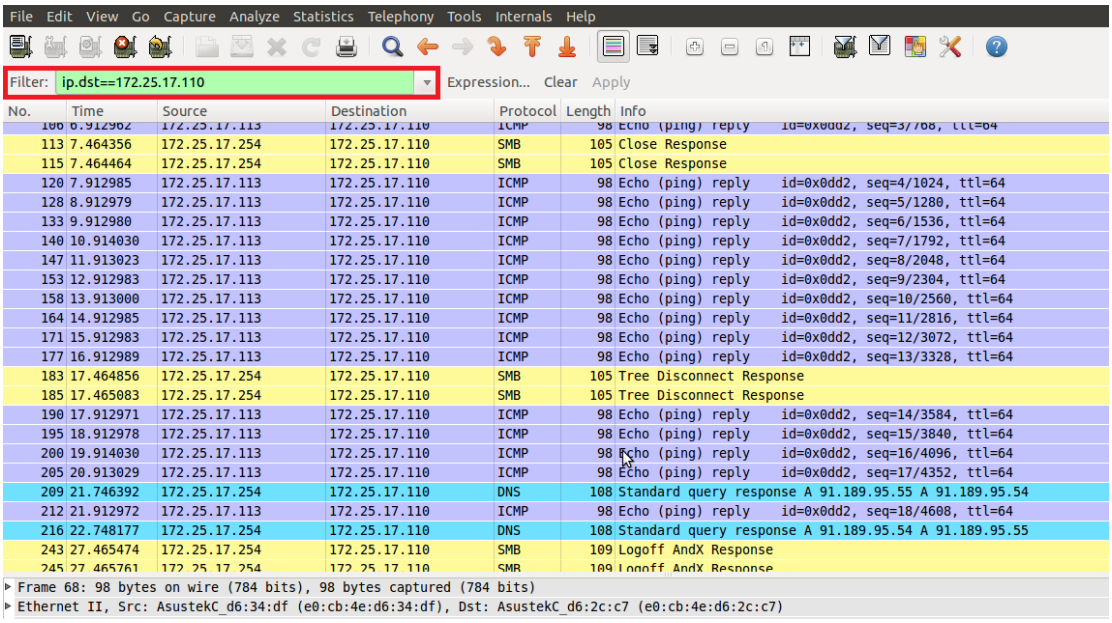


Для зручності пошуку/перегляду інформації про потрібні пакети у програмі Wireshark можна відфільтрувати захоплені пакети за IP-адресою або номером порту.

Наведемо приклади:

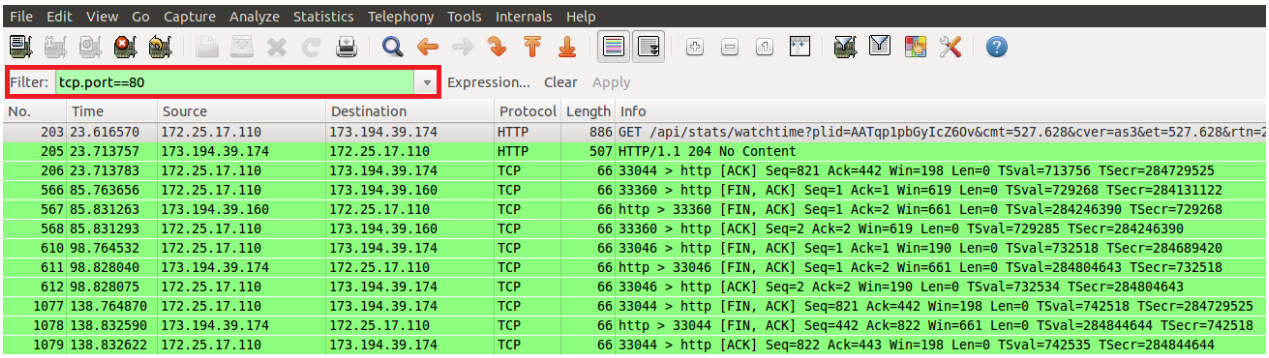
Щоб зробити фільтрацію захоплених пакетів по IP-адресою призначення 172.25.17.110, в полі Filter вкажемо правило фільтр aip.dst==172.25.17.110:

Рисунок 16



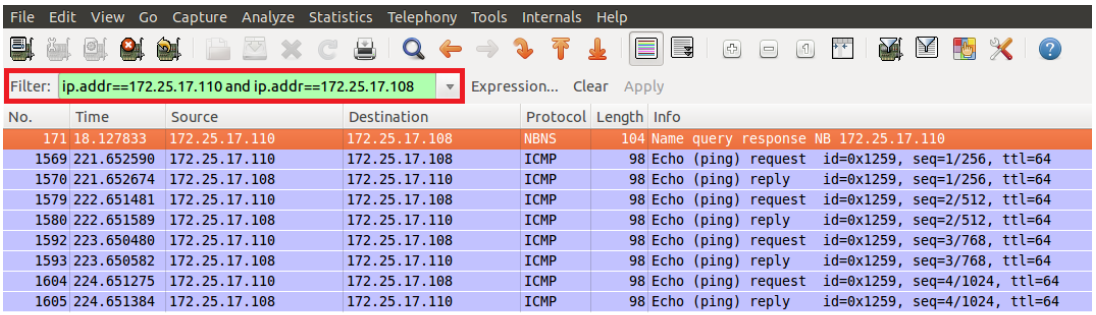
Щоб зробити фільтрацію захоплених пакетів за певним порту TCP (наприклад, за80 порту), в полі Filter вкажемо правило фільтра tcp.port==80

Рисунок 17



Щоб зробити фільтрацію захоплених пакетів зо двома певними IP-адресами (наприклад, за IP-адресами 172.25.17.110 та 172.25.17.108), в полі Filter вкажіть правило фільтра ip.addr==172.25.17.110 and ip.addr==172.25.17.108.

Рисунок 18



Додаткова фільтрація здійснюється такими командами:

ip.addr==IP_АДРЕС (весь трафік С і НА дана адреса)

ip.scr==IP_АДРЕС (весь трафік З даної адреси)

ip.dst==IP_АДРЕС (весь трафік НА дана адреса)

Програма Wiresharkвідслідковуючи мережевий трафік, може показати: коли, за яким протоколом, з якою IP-адресою, з яким сайтом відбувалося з'єднання. Наприклад, якщо в терміналі ввести команду:ping www.wikipedia.org, то Wireshark покаже це: в меню Edit→FindPacket…, в рядку Filterвведемо слово wikipedia та натиснемо Знайти.

Рисунок 19

```
root@lw-417-10:~# ping www.wikipedia.org
PING text-lb.esams.wikimedia.org (91.198.174.192) 56(84) bytes of data.
64 bytes from text-lb.esams.wikimedia.org (91.198.174.192): icmp_req=1 ttl=59 ti
me=43.6 ms
64 bytes from text-lb.esams.wikimedia.org (91.198.174.192): icmp_req=2 ttl=59 ti
me=42.7 ms
64 bytes from text-lb.esams.wikimedia.org (91.198.174.192): icmp_req=3 ttl=59 ti
me=42.5 ms
^Z
[18]+  Зупинено          ping www.wikipedia.org
root@lw-417-10:~#
```

Рисунок 20

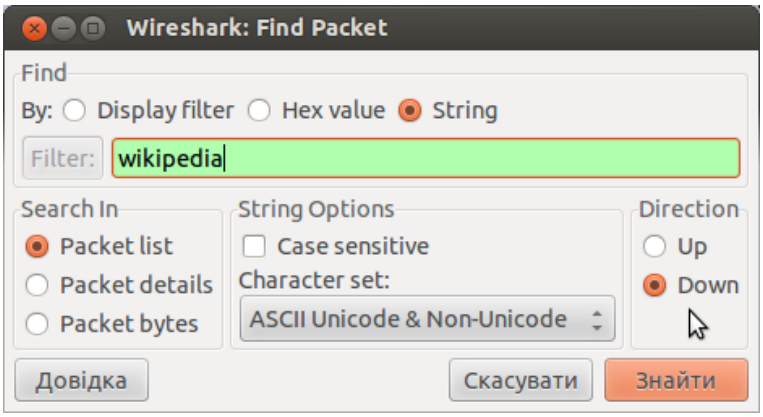
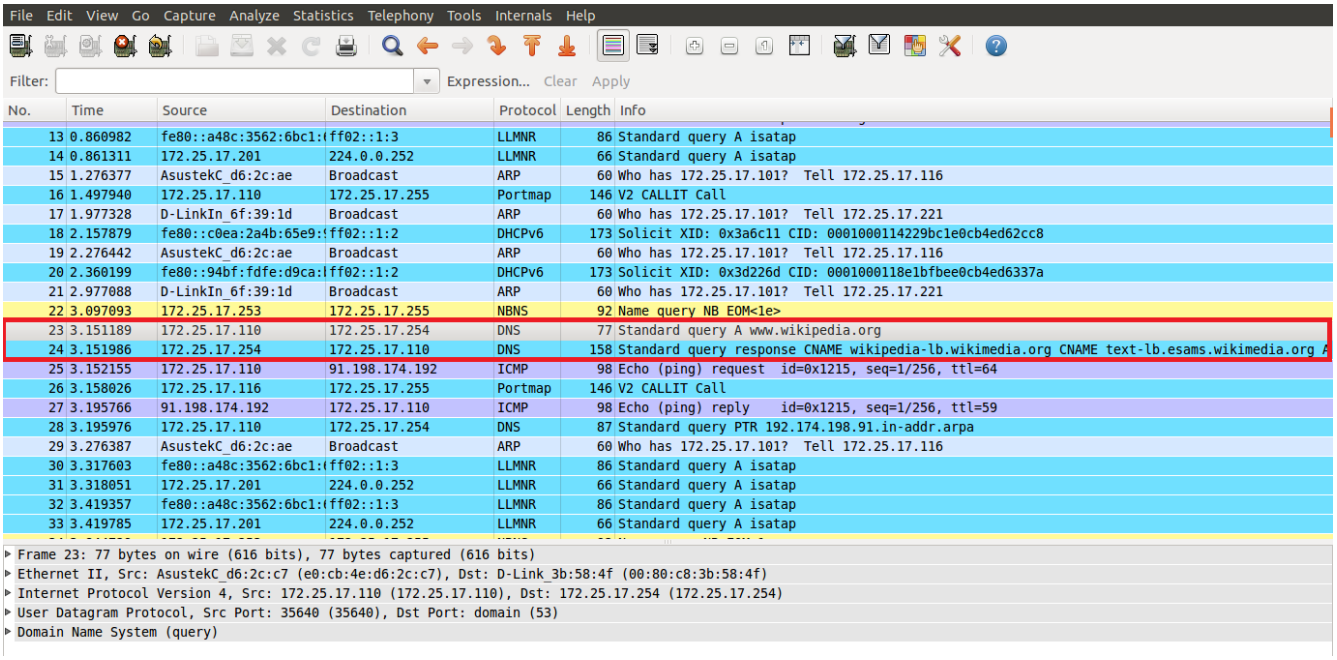


Рисунок 21



Висновок

Програма Wireshark має найбільшу кількість функціональних можливостей для моніторингу інтерфейсів Ethernet.

Ця програма Wireshark стала стандартом при дослідженні мереж та аналізі протоколів серед додатків з відкритим вихідним кодом. Вона надає можли-вість проводити низькорівневу фільтрацію пакетів і їх аналіз. Файли із захоп-леними даними з мережі (trace files) можуть бути відкриті в Wireshark і розглянуті аж до кожного пакета.

Wireshark має широке використання, оскільки є зручною у роботі:

- Адміністратори мереж використовують її для виявлення причин неполадок в мережах.
- Фахівці з безпеки мереж використовують її для пошуку проблем з безпекою.
- Розробники використовують її для налагодження реалізацій протоколів.
- Користувачі використовують її для вивчення принципів роботи мережевих протоколів.

Список літератури

1. [Електронний ресурс]. – Режим доступу до документа:http://soft.mydiv.net/win/download-Ethereal.html
2. [Електронний ресурс]. – Режим доступу до документа http://zyxel.ru/kb/1793
3. [Електронний ресурс]. – Режим доступу до документа http://pi.314159.ru/volotka/volotka1.htm