Аналізатор пакетів Wireshark

Основним інструментом для спостереження повідомлень, якими обмінюються хости є сніфер пакетів. Як випливає з назви, сніфер пакетів захоплює ("нюхає") повідомлення, передані з комп'ютера або отримані ним. Крім цього програма-сніфер, як правило зберігає та відображає вміст різних полів протоколів у цих захоплених повідомленнях. Сніфер пакетів – це пасивна програма. Вона досліджує повідомлення, що відправляються і одержуються програмами і протоколами, які працюють на комп'ютері, але ніколи не відправляє пакети сама. Отримані пакети ніколи не адресуються сніферу. Сніфер пакетів отримує копію пакетів, переданих / отриманих додатками або протоколами, які виконуються на комп'ютері.

На рис. 1 показана структура сніферу пакетів. У правій частині малюнка знаходяться протоколи (у даному випадку, інтернет-протоколи) і додатки (такі як веб-браузер або FTP-клієнт), який зазвичай запускається на комп'ютері. Сніфер пакетів, показаний у пунктирному прямокутнику на рис. 1 є доповненням до звичайної програми на вашому комп'ютері, і складається з двох частин. Бібліотека захоплення пакетів отримує копію кожного фрейму канального рівня, що передається або одержується комп'ютером. Нагадаємо, що повідомлення, якими обмінюються протоколи верхнього рівня, такі як HTTP, FTP, TCP, UDP, DNS або IP, у кінцевому підсумку, інкапсульовані в кадрах канального рівня, які будуть передані через фізичні носії (наприклад, кабель Ethernet). Захоплення кадрів канального рівня таким чином, дає всі повідомлення, послані / отримані усіма протоколами та програмами, що виконуються на комп'ютері.

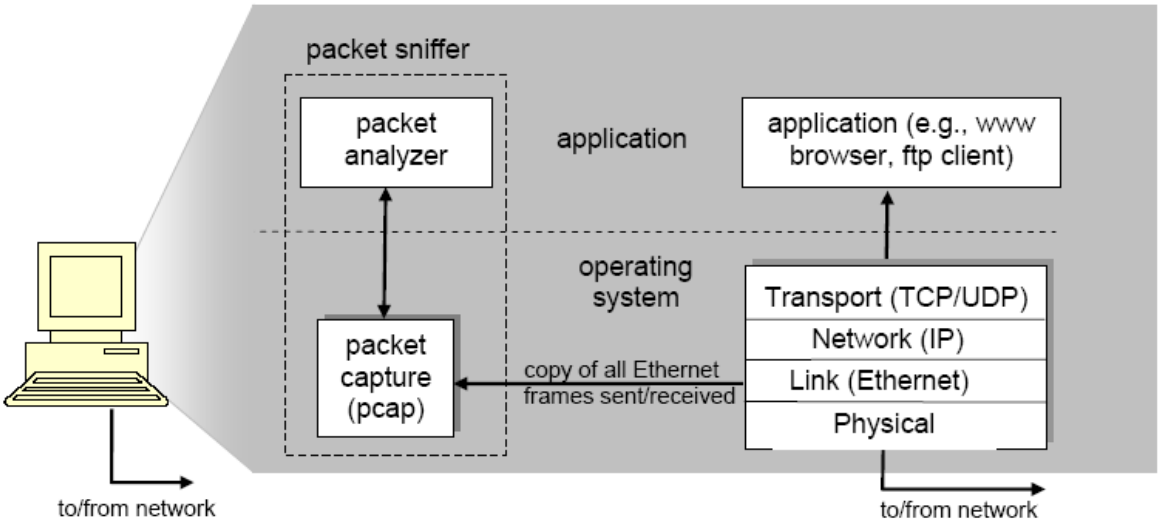

Рис. 1. Структура «нюхача» пакетів

Другим компонентом сніферу пакетів є аналізатор пакетів, який відображає зміст усіх полів у повідомленнях протоколу. Для того, щоб зробити це, аналізатор пакетів повинен "розуміти" структуру всіх повідомлень, якими обмінюються протоколи. Наприклад, припустимо, ми зацікавлені у відображенні різних полів у повідомленнях, якими обмінюється протокол HTTP на рис. 1. Аналізатор пакетів розуміє формат кадрів Ethernet, і тому може розпізнати IP дейтаграму в Ethernet-кадрі. Він також розуміє формат IP дейтаграм, так що він може отримати сегмент TCP в IP-дейтаграмі. І нарешті, він розуміє структуру TCP сегменту, тому він може отримати повідомлення HTTP, що містяться в сегменті TCP.

Ми будемо використовувати сніфер пакетів Wireshark [http://www.wireshark.org/] для аналізу змісту повідомлень, відправлених / отриманих різними рівнями стеку протоколів. З технічної точки зору, Wireshark є аналізатором пакетів, який використовує бібліотеку захоплення пакетів комп'ютера PCap (Packet Capture). Wireshark є вільним аналізатором

мережевих протоколів, який працює на Windows, Linux / Unix, і Mac-комп'ютерах. Це ідеальний аналізатор пакетів для лабораторних досліджень – він стабільний, має багато прихильників і добре документований (http://www.wireshark.org/docs/wsug_html_chunked/), http://www.wireshark.org/docs/man-pages/), а також докладний FAQ http://www.wireshark.org/faq.html).

Він має багату функціональність, яка включає в себе можливість аналізувати сотні протоколів, і добре розроблений для користувача інтерфейс. Він працює в комп'ютерах з Ethernet, Token-Ring, FDDI, бездротовими локальними мережами 802.11.

Інтерфейс програми Wireshark

Графічний інтерфейс користувача Wireshark показано на рис. 2.

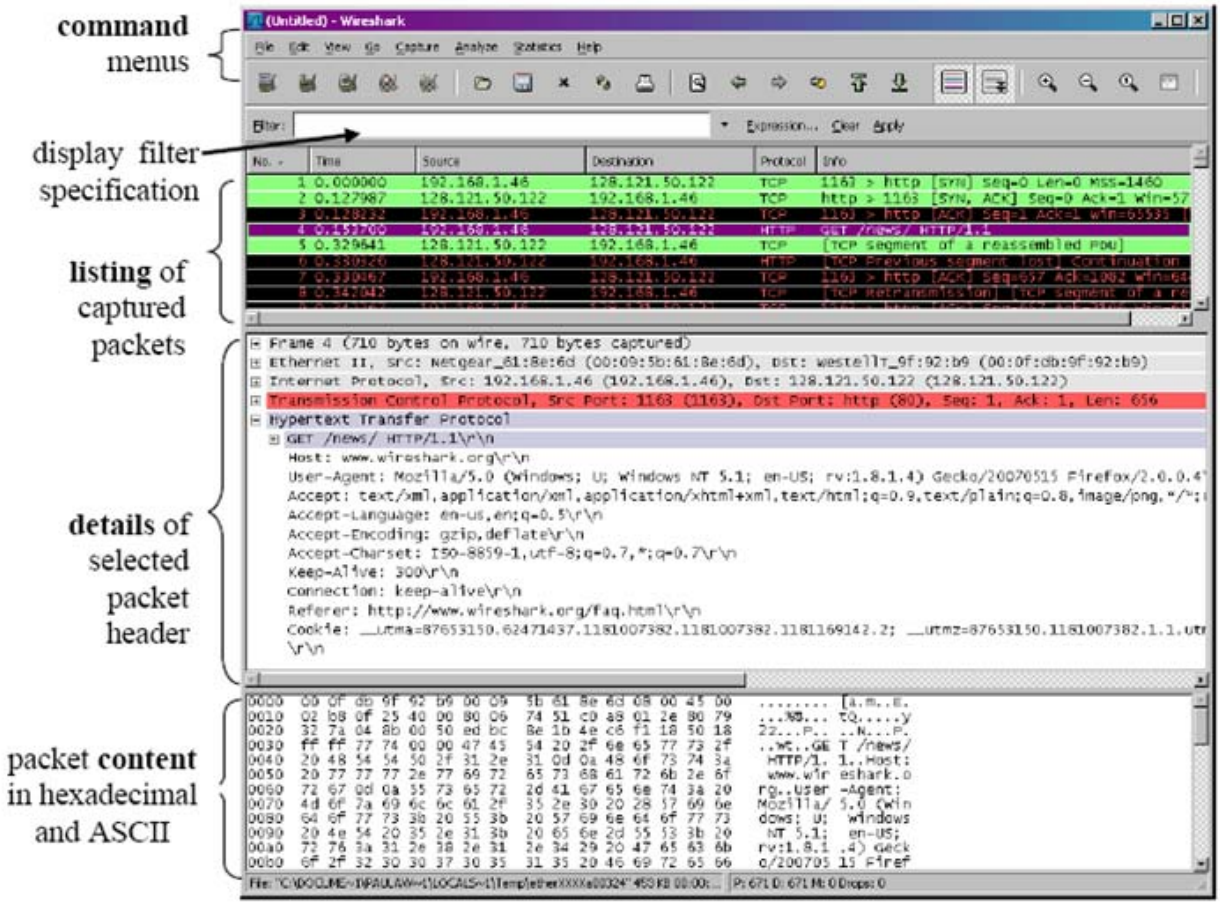

Рис. 2. Графічний інтерфейс програми Wireshark.

Інтерфейс Wireshark має п'ять основних компонентів:

- **меню команд** – це стандартне меню у верхній частині вікна. Насамперед нас цікавлять пункти File (файл) і Capture (захоплення). Меню «Файл» дозволяє зберігати захоплені пакети даних у файл або відкрити файл, що містить раніше захоплені пакети даних. Меню «Захоплення» дозволяє розпочати / закінчити захоплення пакетів із вибраного інтерфейсу.
- **поле фільтру** відображення пакетів, в яке може бути введене ім'я протоколу або інша інформація, з метою фільтрації даних, що відображаються у вікні списку пакетів (а, отже, і вікнах заголовків пакету і вмісту пакета).
- **вікно із списком** захоплених пакетів відображає однорядкове резюме для кожного захопленого пакету, у тому числі номер пакету (присвоєний Wireshark, а не номер пакету, який міститься в заголовку будь-якого протоколу), час, коли пакет був захоплений, адреси джерела і призначення пакету, тип протоколу і специфічну для протоколу інформацію, що міститься в пакеті. Список пакетів можна сортувати по

будь-якій із цих категорій, клацнувши заголовок стовпчика. Поле тип протоколу відображає найвищий рівень протоколу, який відправив або отримав цей пакет, тобто протокол, який є джерелом або кінцевим пунктом для цього пакета.

- **вікно подробиць заголовку** пакета містить відомості про пакет вибраний (виділений) у вікні із списком пакетів. Ці подробиці включають інформацію про кадр Ethernet (передбачається, що пакет був відправлений / прийнятий на інтерфейс Ethernet) і IP-дейтаграму, яку містить цей пакет. Кількість подробиць про рівні Ethernet і IP може бути розширена або мінімізована, якщо натиснути на квадратик плюс-мінус зліва від рядка кадру Ethernet або IP-дейтаграми у вікні деталей пакету. Якщо пакет був перенесений TCP або UDP, то деталі TCP або UDP також будуть відображатися у цьому вікні. І нарешті, інформація про найвищий рівень протоколу, який відправив або отримав цей пакет також надається.
- **вікно вмісту** пакетів відображає весь вміст захопленого кадру, як у шістнадцятковому так і в ASCII-форматі.

Запуск Wireshark

Кращий спосіб дізнатися про нове програмне забезпечення, це спробувати його! Будемо вважати, що ваш комп'ютер підключений до Інтернету через Ethernet інтерфейс. Виконайте наступні дії:

1. Запустіть ваш улюблений веб-браузер, який буде відображати вибрану сторінку.
2. Запустіть програму Wireshark. Ви спочатку побачите вікно, показане на малюнку 3.

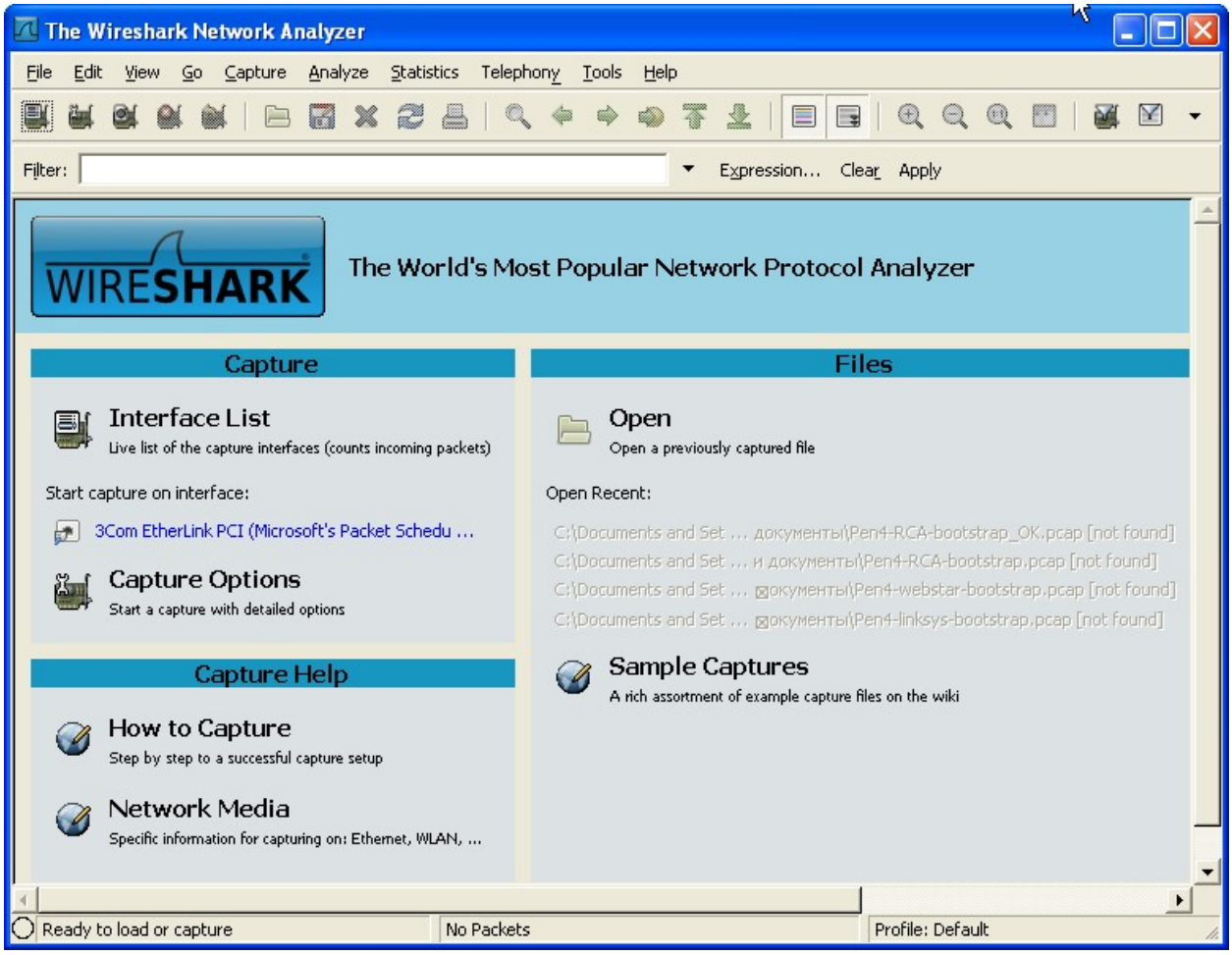

Рис. 3. Стартове вікно Wireshark.

3. Щоб розпочати захоплення пакетів, виберіть пункт Capture Options. Відкриється вікно "Wireshark: Опції захоплення" (Wireshark: Capture Options), яке буде відображатися, як показано на малюнку.

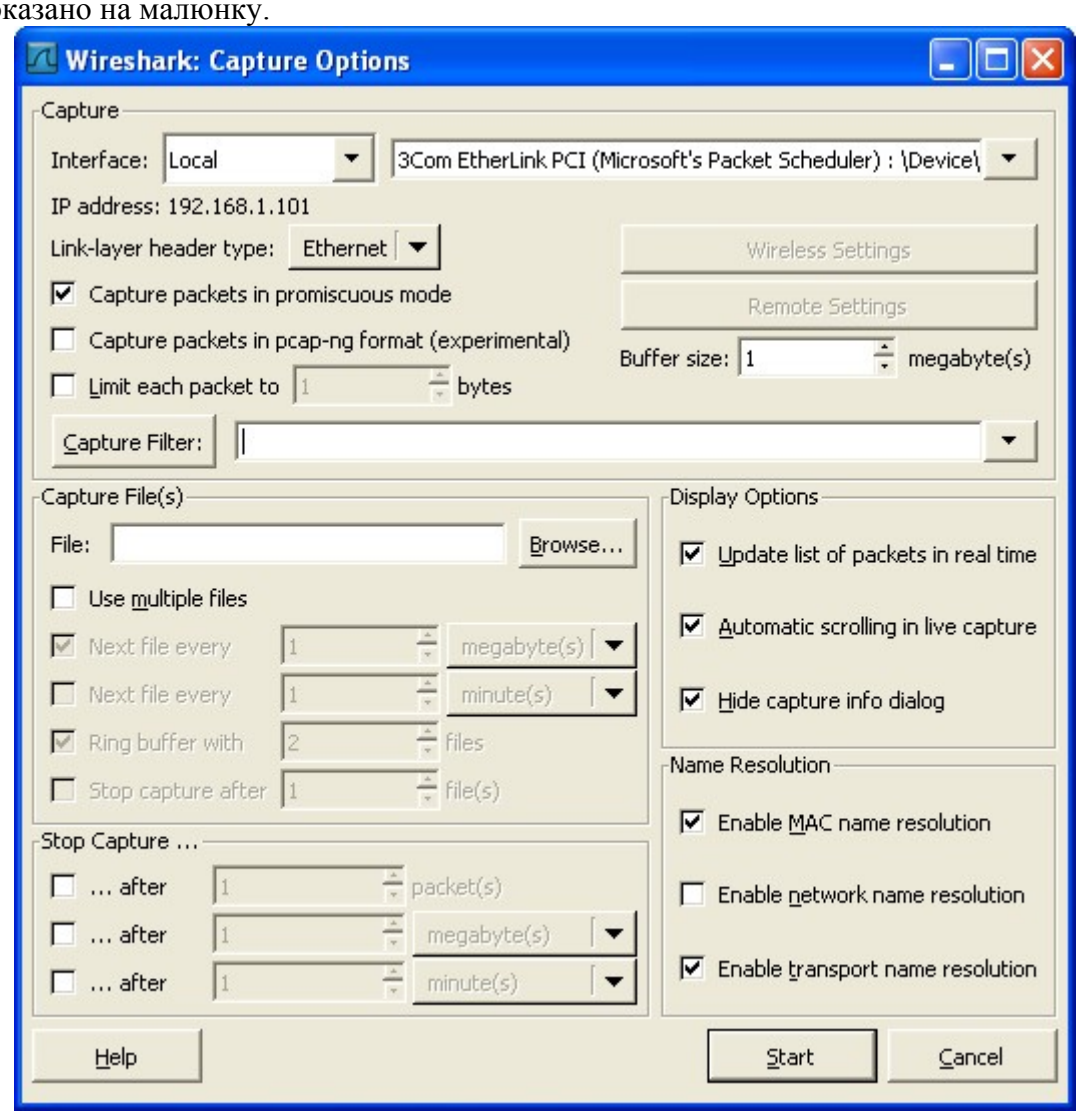

Рис. 4. Параметри захоплення програми Wireshark.

4. Ви можете використовувати більшість значень за умовчанням в цьому вікні, але зніміть прапорець "Приховати діалог з інформацією про захоплення" (Hide capture info dialog) у групі «Опції відображення» (Display Options). Мережеві інтерфейси вашого комп'ютера будуть показані у випадаючому списку «Інтерфейс» (Interface) у верхній частині вікна. У разі, якщо ваш комп'ютер має більше одного активного мережtdro інтерфейсу, вам потрібно вибрати інтерфейс, який використовується для відправки та отримання пакетів (найчастіше Ethernet). Після вибору мережевого інтерфейсу натисніть кнопку Пуск. Починається захоплення пакетів - усі пакети, які передаються / приймаються комп'ютером захоплюються Wireshark!
5. Як тільки почалося захоплення пакетів, з'явиться вікно підсумків захоплення пакетів, як показано на малюнку 4. У цьому вікні наводяться дані про кількість захоплених пакетів різних типів, і воно (важливо!) містить кнопку Стоп, що дозволить зупинити захоплення пакетів. Зараз не зупиняйте захоплення.

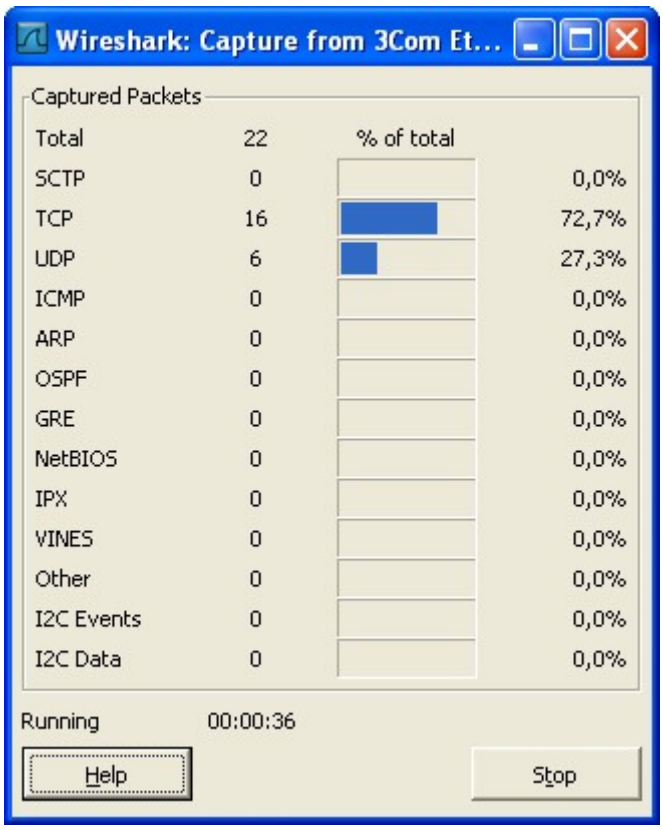

Рис. 5. Статистика захоплення пакетів.

6. Поки Wireshark працює, введіть URL-адресу:
   http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
   і дочекайтеся відображення сторінки браузером. Для того щоб відобразити цю сторінку, браузер зв'яжеться з сервером HTTP на gaia.cs.umass.edu і обміняється повідомленнями з HTTP сервером, щоб завантажити сторінку. Ethernet кадри, що містять ці HTTP повідомлення будуть захоплені Wireshark.
7. Після відображення сторінки браузером, зупиніть захоплення пакетів, натиснувши кнопку Стоп у вікні «Wireshark: Capture from…».
8. Введіть **http** (без лапок, у нижньому регістрі) у поле вибору фільтру (Filter) у верхній частині головного вікна Wireshark. Потім натисніть Застосувати (Apply). Фільтр дозволяє відображати лише повідомлення одного протоколу, наприклад HTTP.
9. Виберіть перше повідомлення HTTP показано у вікні пакета зі списку. Це має бути HTTP GET повідомлення, яке було надіслано з вашого комп'ютера на сервер gaia.cs.umass.edu HTTP. При виборі HTTP GET повідомлення, заголовки Ethernet кадру, IP датаграми, TCP сегменту, і HTTP-повідомлення будуть відображатися у вікні подробиць заголовку пакетів. Натискаючи квадратики плюс-мінус зліва від заголовків мінімізуйте інформацію про Frames, Ethernet, Internet Protocoli Transmission Control Protocol. Розкрийте інформацію про протокол HTTP. Ваш Wireshark дисплей повинен виглядати приблизно як показано на малюнку 5. (Зверніть увагу на мінімальну інформацію про всі протоколи, окрім HTTP).

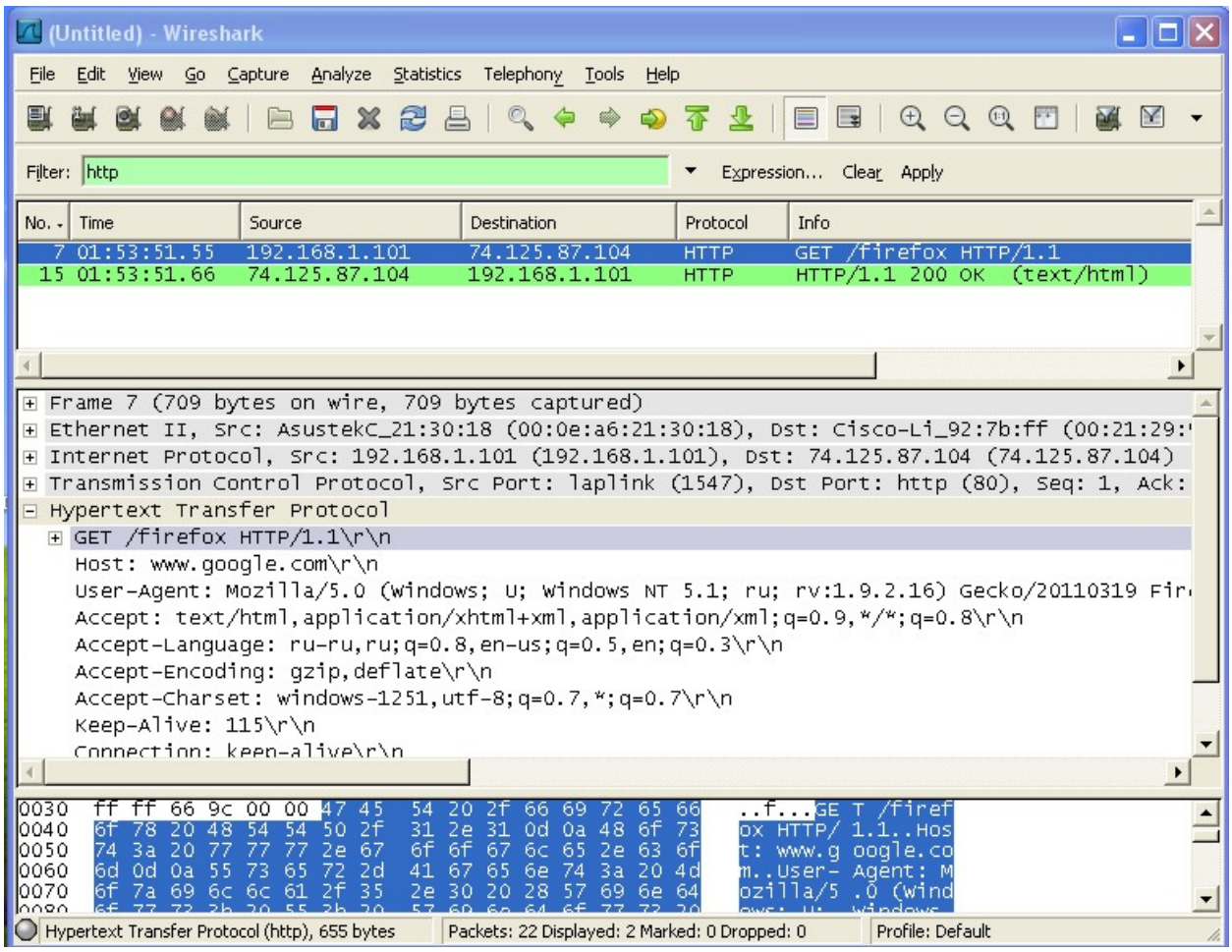

Рис. 6. Аналіз протоколу HTTP.