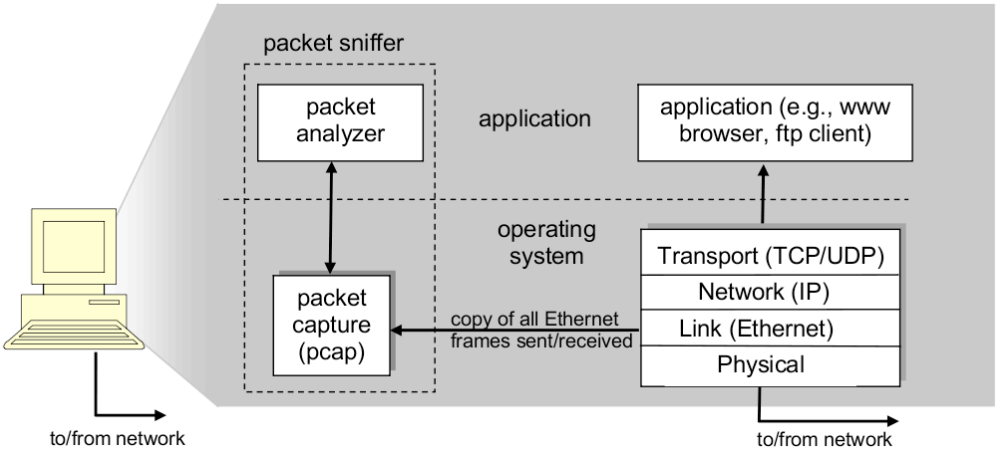
1. Основи захоплення та аналізу пакетів

Мета роботи: оволодіти методами роботи в середовищі захоплення та аналізу пакетів Wireshark, необхідними для дослідження мережевих протоколів.

1.1. Теоретичні відомості

Основним інструментом для спостереження за обміном повідомленнями між робочими станціями, що підтримують деякий протокол комунікації є снифер пакетів. Як випливає з назви, сніфер захоплює ("нюхає") повідомлення, відправлені/отримані з/в робочої станції. Також сніфер, як правило, зберігає та/або відображає вміст значень заголовків протоколів у цих захоплених повідомленнях.

Сніфер пакетів являє собою пасивну компоненту. Це означає, що відбувається спостереження повідомлень, відправлених та отриманих прикладними процесами декількох робочих станцій, але сніфер ніколи не відправляє нові чи модифікує виявлені пакети. Аналогічним чином, неможливо адресувати пакети напряму процесу перехоплювача пакетів. Замість цього, пакет сніфер отримує копії пакетів, які відправляються/отримуються додатками та протоколами його робочої станції.



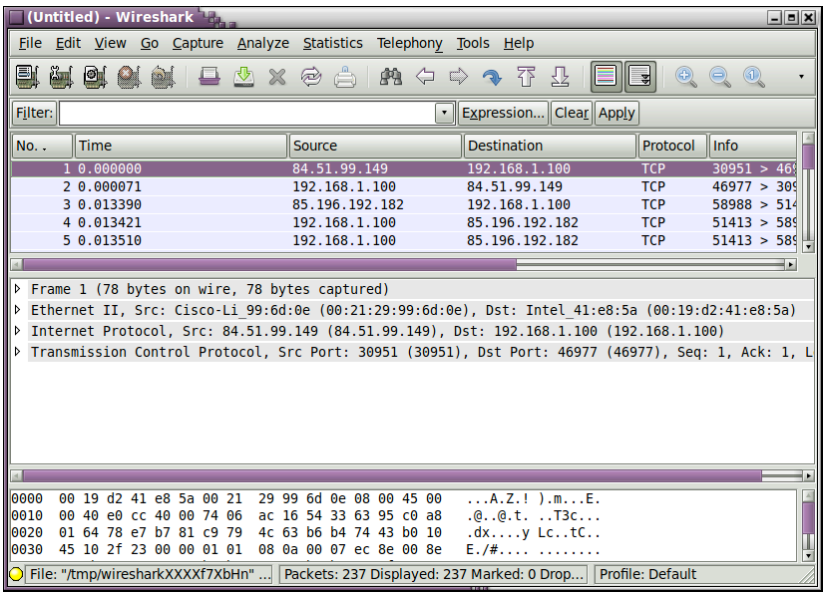
Малюнок 1. Архітектура сніферу пакетів.

Малюнок 1 показує структуру сніферу пакетів. Справа показані протоколи (в даному випадку, інтернет-протоколи) і додатки наприклад, веб-браузер або FTP-клієнт), які зазвичай запускаються на комп'ютері. Перехоплювач пакетів, як показано в пунктирному прямокутнику на малюнку 1 є доповненням до звичайних програмних додатків на комп'ютері, і складається з двох частин. Бібліотеки Packet Capture отримують копію кожного фрейма канального рівня, який передається/отримується комп'ютером. Захоплення всіх кадрів канального рівня, забезпечує можливість аналізу усіх повідомлень, що надіслані/отримані від/для всіх протоколів і програм, виконуваних робочою станцією. Другим компонентом сніферу є аналізатор пакетів, що відображає зміст усіх заголовків пакету для кожного з протоколів. Для того щоб зробити це, то пакет Аналізатор повинен "розуміти" структуру заголовків для більшості протоколів.

Для виконання лабораторних робіт рекомендується використовувати сніфер Wireshark, за допомогою якого ми зможемо відобразити вміст повідомлень та заголовків для різних рівнів стеку мережевих протоколів. В аудиторіях використовується віртуальна машина з заздалегідь встановленим Wireshark.

1.1.1. Інтерфейс Wireshark

Після запуску Wireshark відображається вікно, схоже з показаним на малюнку 2. В початковому стані програма не відображає даних.



Малюнок 2. Інтерфейс користувача програми Wireshark.

Вікно програми складається з п’яти основних компонент:

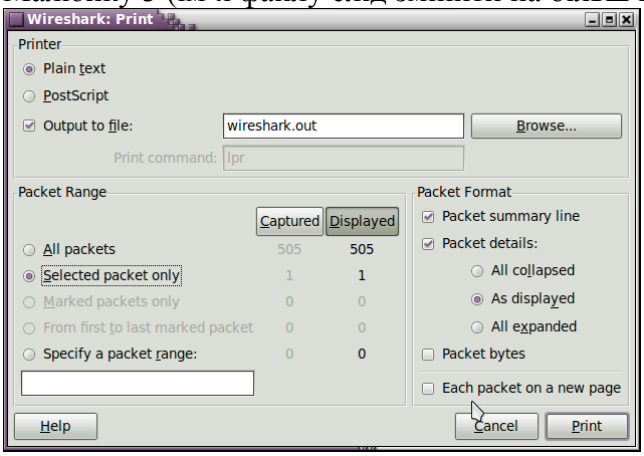
1. **Командні меню**, серед яких для нас найважливіші категорії File (дозволяє зберегти та відновити захоплені пакети, а також вийти з програми) та Capture (дозволяє розпочати захоплення пакетів).
2. **Вікно лістингу пакетів**, яке відображає сумарну інформацію про кожний захоплений пакет: послідовний номер пакета (не пов'язаний з полями протоколів), час захоплення, початкову та цільову адреси, тип протоколу та коротку інформацію, специфічну для протоколу. Лістинг можна відсортувати по будь-якому з цих значень. Поле типу протоколу зазначає протокол найвищого рівня, пов'язаний з цим пакетом – тобто початковий/кінцевий протокол, який створив/отримав повідомлення цього протоколу.
3. **Вікно деталей заголовків пакету** дозволяє переглянути деталі пакету, виділеного в вікні лістингу пакетів. Ці деталі включають інформацію про поля фрейму Ethernet, IP-датаграми. За умови використання пакетом протоколів TCP/UDP інформація про заголовки цих протоколів також буде відображатися в вікні деталей. Також будуть відображатися деталі протоколів прикладного рівня, якщо вони включені в пакет.
4. **Вікно деталей пакету** відображає байтовий дамп пакету в текстовому та шістнадцятковому форматі.
5. Над вікном лістингу пакетів знаходиться **поле фільтрації лістингу**, яке дозволяє сховати не релевантні пакети в вікні лістингу.

1.2. Хід роботи

Необхідно виконати наступні дії:

1. Запустіть веб-браузер.
2. Запустіть Wireshark.
3. В Wireshark активуйте діалог вибору мережевого інтерфейсу для захоплення: Capture >> Interfaces (або ж Ctrl + I)
4. Далі виберіть той інтерфейс, для якого відображається найбільша кількість захоплених пакетів та натисніть кнопку Start навпроти нього
    a. в випадку коли інтерфейс ще не ввімкнено можна вибрати any;
    b. в випадку, коли ви плануєте тестувати локальну комунікацію процесів, можна вибрати lo, loopback або any;

5. Поки Wireshark захоплює пакети, відкрийте в браузері сторінку за наступною адресою:
   http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
   Пакети зі вмістом зазначеної веб-сторінки повинні бути захоплені Wireshark.
6. Зупиніть захоплення пакетів за допомогою команди
   Capture >> Stop (або Ctrl + E)
7. Введіть текст «http» в поле фільтрації та натисніть Apply, в вікні лістингу пакетів мають залишитися тільки пакети, які були створені протоколом HTTP.
8. Виберіть перший пакет HTTP, який відображається в вікні лістингу, це має бути повідомлення GET протоколу HTTP. Також цей пакет має вміщувати інформації інших протоколів нижчих рівнів: TCP, IP, Ethernet.
9. У вікні деталей заголовків розкрийте деталі, пов'язані з протоколом HTTP та скрийте детальну інформацію про інші протоколи.
10. Роздрукуйте перші пакети запиту та відповіді. Для цього слід виділити пакет, який бажано роздрукувати, та активувати команду File > Print, та налаштувати його так як показано на Малюнку 3 (ім'я файлу слід змінити на більш інформативне).



Малюнок 3. Типові налаштування діалогу роздруківки.

11. Перевірте, що у роздрукованих файлах присутні необхідні для захисту пакети та відображені необхідні для захисту протоколу.
12. Закрийте Wireshark.

1.3. Контрольні запитання

Форма звітності: роздруківки збережених в ході ЛР пакетів з фаміліями, ініціалами та групами виконавців (бажано на кожній сторінці).

Контрольні запитання:

1. Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?
2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?
3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?
4. Якими були вихідна та цільова адреси пакетів із запитом та із відповіддю?
5. Яким був перший рядок запиту на рівні протоколу HTTP?
6. Яким був перший рядок відповіді на рівні протоколу HTTP?