# Introducció a l'analitzador de protocols *WireShark*

Els analitzadors de protocols o de xarxa, també coneguts vulgarment com "*sniffers*" són eines de gran ajuda per als administradors de les xarxes de computadors, ja que permeten l'anàlisi detallada de molts factors del comportament de les xarxes. Aquestes aplicacions permeten capturar una còpia dels paquets que circulen per la xarxa per a la seua anàlisi posterior. Els més avançats inclouen una interfície gràfica capaç de mostrar els camps dels protocols de comunicació dels diferents nivells, obtenir estadístiques d'utilització i facilitar considerablement la posterior anàlisi de les dades capturades. D'aquesta manera es facilita la detecció de problemes, així com la depuració del programari de xarxa durant la seua fase d'elaboració. Per exemple, un administrador de xarxa que detecte que les prestacions de la xarxa són baixes pot utilitzar un d'aquests analitzadors per a detectar quins segments de la xarxa, protocols i màquines estan generant més trànsit, i d'aqueixa forma dur a terme les accions necessàries, o bé verificar el correcte funcionament dels diferents dispositius de xarxa (*hosts*, servidors, *routers*, tallafocs, NAT, etc).

Des del punt de vista docent, els analitzadors de protocols permeten veure de forma pràctica els protocols de comunicació ja presentats en les classes de teoria, així com les relacions entre els protocols de diferent nivell. Per tot açò, intentarem familiaritzar a l'alumne amb l'ús d'una d'aquestes eines.

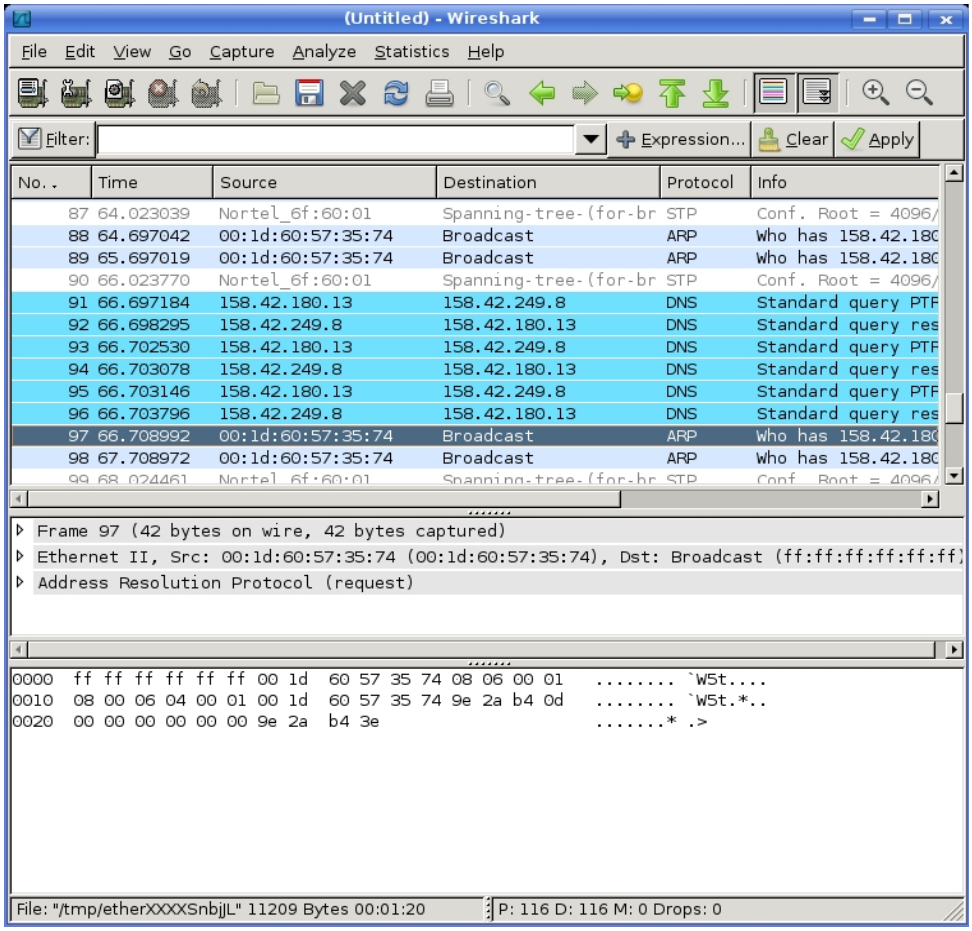
En aquesta introducció es pretenen adquirir les capacitats necessàries per a capturar paquets usant l'eina *WireShark*. Atès que per la xarxa viatgen multitud de paquets, serà necessari seleccionar aquells que ens resulten d'interès. Per açò anem a aprendre a capturar paquets utilitzant els filtres que ens proporciona *WireShark*, de manera que acceptarem uns paquets i rebutjarem uns altres. També, es pretén introduir a l'alumne en la interpretació del contingut dels paquets capturats per a afermar els conceptes relatius als protocols estudiats en classe. Tot açò permetrà posar en pràctica els coneixements adquirits al llarg de diversos temes tractats en les classes de teoria, adquirint una major comprensió dels processos que ocorren en la xarxa quan es duen a terme diverses accions a nivell d'usuari.

## 1. L'analitzador de protocols: *WireShark*

A l'hora de triar un analitzador de protocols ens trobem amb una abundant oferta, tant de productes comercials com de programari de lliure distribució. Un dels més populars, i el triat per a les pràctiques de l'assignatura, és *WireShark.* Es tracta d'un producte gratuït i molt versàtil, que pot descarregar-se des de http://www.wireshark.org . Està disponible tant per a sistemes Windows com Unix, i permet no solament capturar trànsit d'una xarxa, sinó també filtrar-lo i analitzar-lo. A més, permet llegir fitxers de dades arreplegades amb altres analitzadors de protocols com *tcpdump* o *NetXRay*, amb el que poden aprofitar-se altres captures prèviament realitzades.

Per seguretat, els analitzadors de protocols requereixen permisos d'administrador del sistema per a poder realitzar captures del trànsit de la xarxa.

*Figura 1. Descripció de WireShark*




Començarem comentant l'aspecte habitual del programa, que es mostra en la figura 1. *WireShark* comprèn tres finestres o àrees principals.

1) La finestra superior és la llista dels paquets. Mostra una breu descripció de cada paquet capturat. Prement en algun dels paquets d'aquesta llista podem controlar el que es visualitza en les dues finestres restants.

2) La finestra intermèdia mostra amb major detall el paquet seleccionat en la primera finestra. Indica els protocols emprats en els diferents nivells de l'arquitectura, així com els valors de cadascun dels camps de cada protocol.

3) Finalment, la finestra inferior mostra el valor de les dades, en hexadecimal i en ASCII, del paquet seleccionat en la finestra superior, i marca en negre les dades seleccionades en la finestra intermèdia.

A més d'aquestes tres finestres, la finestra principal de *WireShark* ofereix (en la part inferior) el filtrat en pantalla dels paquets capturats en funció del tipus de paquets i/o contingut dels seus camps. Aquest filtrat *a posteriori* és complementari al filtrat de paquets en el moment de la captura, tal com s'explicarà més endavant.

## 2. Com capturar paquets

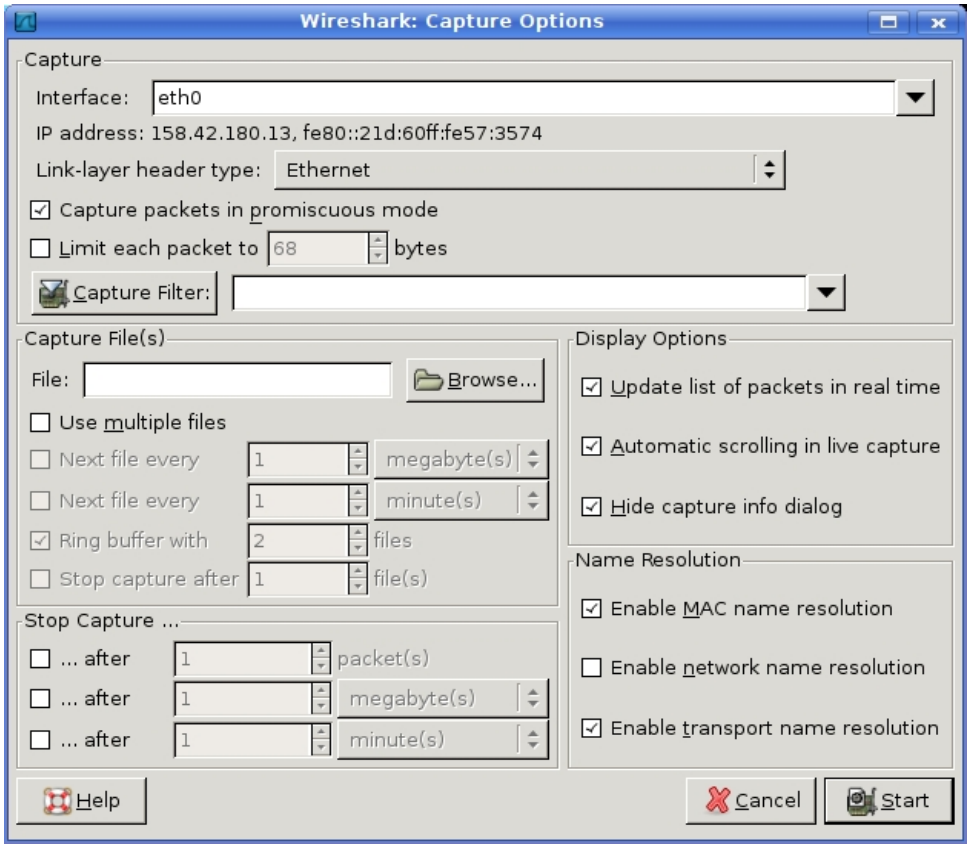



*Figura 2. Finestra de captura de paquets*

Realitzar una captura de paquets és senzill. Primer accedirem al menú *Capture* i allí seleccionarem l'opció *Options*. Açò ens porta a una nova finestra similar a la mostrada en la figura 2, anomenada *Capture Options*. En aquesta finestra podrem especificar els diversos paràmetres relacionats amb la captura.

El primer paràmetre que podem especificar és l'interfície, és a dir, la targeta de xarxa sobre la qual volem realitzar la captura. Aquesta opció només té sentit si disposem de diverses targetes de xarxa (possiblement connectades a diferents xarxes), com és el cas dels computadors del laboratori. En aquest cas, l'interfície a seleccionar és *eth0*.

Amb la finalitat d'evitar un consum excessiu de memòria també podem indicar la quantitat de bytes que anem a guardar de cada paquet capturat. No obstant açò, per a captures xicotetes com les quue anem a realitzar, aquesta opció no és necessària.

Una altra opció que podem detallar és si desitgem realitzar una captura en mode promiscu. En aquest mode el programa capturarà qualsevol paquet que siga visible a la targeta de xarxa, independentment de si està adreçat a ella o no. Per contra, podem seleccionar la captura d'únicament aquells paquets que van adreçats a, o que provenen de, la nostra targeta de xarxa.

En aquesta finestra també podem introduir un **filtre de captura**, amb la finalitat de processar després més fàcilment la informació obtinguda. L'ús d'aquest tipus de filtres el descriurem més endavant.

Una altra possibilitat que ens ofereix aquesta finestra és la de guardar els paquets capturats a un fitxer. Açò pot resultar interessant per a tenir un registre del trànsit capturat. No obstant açò, atès que també podem emmagatzemar les captures després de realitzar-les, des del menú *File/Save*, no anem a fer ús d'aquesta possibilitat de moment.

Altres opcions que aquesta finestra ens permet detallar estan relacionades amb la visualització en pantalla de la captura. Podem optar per veure en temps real els paquets que es van capturant i també podem triar que es realitze un desplaçament vertical automàtic de la pantalla (*scrolling*).

Finalment, podem indicar que la captura s'acabe automàticament quan s'hagen capturat un cert nombre de paquets, o s'haja capturat una quantitat determinada de KBytes, o bé quan haja transcorregut certa quantitat de temps. En cas de no seleccionar cap de les opcions, haurem de finalitzar la captura de forma manual. Per a iniciar la captura pressionarem el botó *Start*.

## 3. Filtres de captura i de pantalla

En intentar analitzar el trànsit de qualsevol xarxa, en particular el de la xarxa de la UPV, resulta habitual trobar-se gran quantitat de paquets que empren protocols en els quals no estem interessats. Tal quantitat de trànsit dificulta l'anàlisi dels paquets capturats i augmenta innecessàriament la grandària dels fitxers de captura, per la qual cosa es fa indispensable filtrar tota aqueixa informació.

Per a filtrar els paquets i facilitar l'anàlisi del trànsit capturat podem usar dues alternatives, no excloents entre elles. La primera és definir un filtre de captura, de manera que el propi *WireShark*, quan arriba un nou paquet, decideix si aqueix paquet s'ajusta o no als criteris establits pel filtre. En cas que s'ajuste, el paquet és acceptat i mostrat en pantalla, mentre que en cas contrari el paquet es descarta.

L'altra alternativa per a filtrar la informació dels paquets és establir un filtre de pantalla. En aquest cas l'habitual és capturar tots els paquets que circulen per la xarxa,

sense restricció alguna, i especificar un filtre per a poder extraure entre tot aqueix trànsit capturat aquells paquets que ens interessen. En qualsevol cas, és possible usar un filtre de captura i posteriorment, sobre els paquets capturats, usar un filtre de pantalla per a veure millor els detalls que estiguem cercant a cada moment.

Els filtres de captura es poden especificar des de la finestra de captura (*Capture Options*). Podem especificar un filtre escrivint l'expressió corresponent en la caixa de text situada al costat del botó *Filter*. La sintaxi d'aquestes expressions és la mateixa que la usada en l'ordre **tcpdump**, disponible habitualment en els sistemes Unix i Linux. En l'apartat següent es mostrarà un resum d'aquesta sintaxi.

D'altra banda, els filtres de pantalla es poden especificar des de la part inferior de la finestra principal de *WireShark*. La sintaxi per a aquest tipus de filtres és lleugerament diferent. És possible disposar d'un assistent per a especificar aquests filtres.

És convenient anar amb compte amb aquests filtres de visualització, ja que poden, en ocasions, portar a error. Per exemple, aquests filtres s'empraran més davant en TCP de forma automàtica per a seguir un flux TCP. Per tant, per a tornar a visualitzar tots els paquets capturats és necessari netejar aquest filtre de visualització, bé amb l'opció corresponent (*clear filter*), o bé emprant un filtre buit (línia en blanc).

## 3.1 Expressions de filtres de captura

Per a seleccionar quins paquets seran capturats s'empra una expressió de filtre, de manera que el paquet serà emmagatzemat si compleix amb els criteris del filtre (l'expressió s'avalua a ***true***). Les expressions de filtre s'empren sempre en minúscules, i consisteixen en una o diverses primitives connectades mitjançant operadors lògics (and, or, not). Cadascuna d'aquestes primitives consten d'un identificador precedit, almenys, d'algun dels següents tres tipus de qualificadors:

- De tipus: Indiquen a què fa referència l'identificador
    1. **Computadors concrets (*host*)**. Per exemple, el filtre:

        ```
        host 158.42.180.62
        ```

        captura totes les trames dirigides o procedents d'aqueixa adreça IP.
    2. Xarxes concretes (*net*). Per exemple, el filtre:

        ```
        net 158.42
        ```

        captura totes les trames dirigides o procedents d'aquesta xarxa IP.
    3. **Ports determinats (*port*)**. Així, el filtre:

```
port 7
```

captura totes les trames dirigides o procedents del port 7 de qualsevol computador, tant TCP com UDP.

Si no s'especifica el tipus s'assumeix el tipus *host*. També es troba especificat l'identificador *broadcast*, que permet fer referència a les adreces de difusió.

- D'adreça: Especifiquen si l'identificador ha d'entendre's sobre l'origen, la destinació o tots dos. Els qualificadors d'adreça possibles són `src`, `dst`, `src or dst`, i `src and dst`. S'aplicaran sobre algun dels qualificadors de tipus. Exemples:

```
src 158.42.181.18
src port 25
src or dst net 158.42
```

- De protocol: Indiquen un tipus de protocol. En el nostre cas resulten d'interès els protocols `arp`, `ip`, `icmp`, `tcp`, o `udp`. Com a norma general, no existeixen qualificadors de nivell d'aplicació, havent d'emprar-se el nombre de port i protocol de transport per a capturar el trànsit corresponent a un protocol d'aplicació concret.

Es poden combinar diverses primitives mitjançant els connectors `and` i `or`. També és possible usar l'operador `not`.

Exemple: `udp and dst 158.42.148.3`

Açò mateix és aplicable també als identificadors.

Exemple: `dst 158.42.181.4 or 158.42.181.15`

També es pot fer ús de parèntesi per a indicar les precedències desitjades.

Exemple: `dst 158.42.181.4 and (udp or icmp)`

De moment, per a la pràctica 1 només es requereix l'ús dels filtres `port` i `host`. Posteriorment, al llarg del curs anirem aprofundint en l'ús de filtres més complexos. Per a accedir a la documentació detallada sobre els filtres i les seues possibilitats es pot acudir al manual en línia de l'ordre **tcpdump**, teclejant en una consola de text l'ordre `man tcpdump`.

Després de completar aquesta lectura i fer algunes proves has d'enviar la captura sol·licitada com a exercici al professor.

**Exercici**:

- Aplica el filtre de captura “port 53”. Amb aquest filtre haurien de capturar-se els accessos que realitzes al DNS per a realitzar la traducció dels noms de domini dels servidors a les seues adreces IP.
- Activa l'inici d'una captura.
- Per a generar trànsit accedeix a una pàgina web (que no tingues en la cau del navegador). Tingues en compte que podries tenir el nom ja resolt en el teu cau local DNS i llavors no apareixeria res en la captura, degut a que no es consultaria al servidor de noms. Si ocorre açò prova a accedir a una altra pàgina web en un altre servidor diferent.
- Una vegada hages aconseguit els resultats, para de capturar i analitza l'encapsulament d'un paquet. Comprova l'adreçament a diferents nivells (hardware, IP, nombres de port).
- **Has d'enviar com a resultat de l'exercici la captura realitzada, indicant les adreces IP font i destinació i els nombres de port font i destinació.**