Introducció al Wireshark

Xavier Tartera

Què és Wireshark?

- Wireshark és un analitzador de paquets i/o protocols de xarxa.
- Un analitzador de paquets de xarxa tractarà de capturar paquets de xarxa i tracta de mostrar-los de la forma més detallada possible.
- Wireshark és potser un dels millors analitzadors de paquets de còdi obert disponibles avui dia per UNIX i Windows.

Analitzador de protocol de xarxa. (Network Protocol Analyzer)

- Intercepta i registra el trànsit que passa per la xarxa, provinents de màquinari o programari (Hardware o software).
- Captura paquets, descodifica i analitza el contingut.
- Un analitzador de xarxa que s'utilitza per:
  - Resolució de problemes a la xarxa.
  - Analitzar el rendiment d'una xarxa per descobrir colls d'ampolla.
  - Xarxa de detecció d'intrusions.
  - Analitzar les operacions d'aplicacions.

Usuaris corrents de Wireshark

- **Administradors de xarxes:**
- Solucionar problemes de xarxa
- Examinar problemes de seguretat

- **Desenvolupadors:**
- Debuging de implementacions de los protocols
- Aprendre com funcionen els protocols internament

"Wireshark no és un sistema de detecció d'intrusos"
"Wireshark no manipula dispositius dins la xarxa, només "mesura" les coses de la xarxa"

Més coses de Wireshark

- Es tracta d'una aplicació informàtica, analitzador de paquets de trànsit de xarxa.
- La funcionalitat és molt similar a tcpdump.
- Té una informació GUI front-end i moltes més opcions de filtre (Interfície gràfica).
- "EWeek Labs" l'ha anomenat com una de les aplicacions de Open Source de tots els temps a partir del 2007.

Origens

- Iniciat per Gerald Combs sota el nom de Ethereal.
- La primera versió va ser llançada el 1998.
- El nom de Wireshark es va adoptar el juny de 2006

Característiques

- "Entén" l'estructura dels diferents protocols de xarxa.
- Mostra camps d'encapsulació i interpreta el seu significat.
- Només es pot capturar en les xarxes recolzades per PCAP.
- És multi-plataforma que s'executa en diferents sistemes operatius (Linux, Mac OS X, Microsoft Windows).

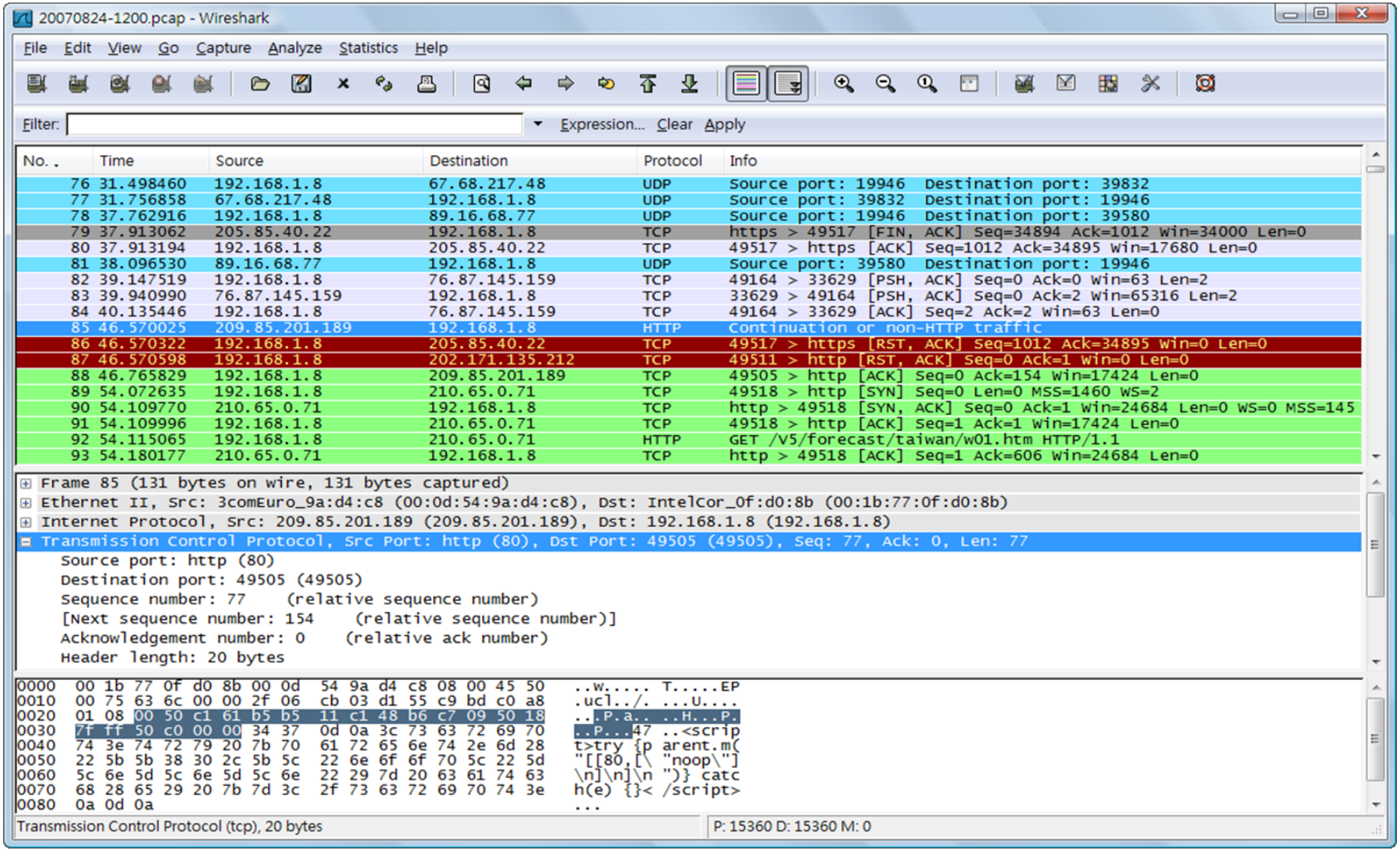
EINES DE MONITORATGE DE XARXES:

WIRESHARK

WinPcap

- Eina estàndard per a l'accés a la xarxa de capa d'enllaç a l'entorn de finestres; l'aplicació et permet capturar i transmetre paquets de xarxa que passa per la pila de protocols.
- Consisteix en un sistema operatiu conductor dirigit a facilitar l'accés de xarxa de baix nivell.
- Consta de biblioteques per facilitar l'accés a les capes baixes del nivell de xarxa.
- També conté una versió per a Windows de libpcap Unix API

EINES DE MONITORATGE DE XARXES:



Wireshark (i WinPcap)

Wireshark

WinPcap – Lib Open Source per la captura de paquets

Sistema Operatiu – Windows & Unix/Linux

Driver de la placa de Xarxa– Ethernet/WiFi Card

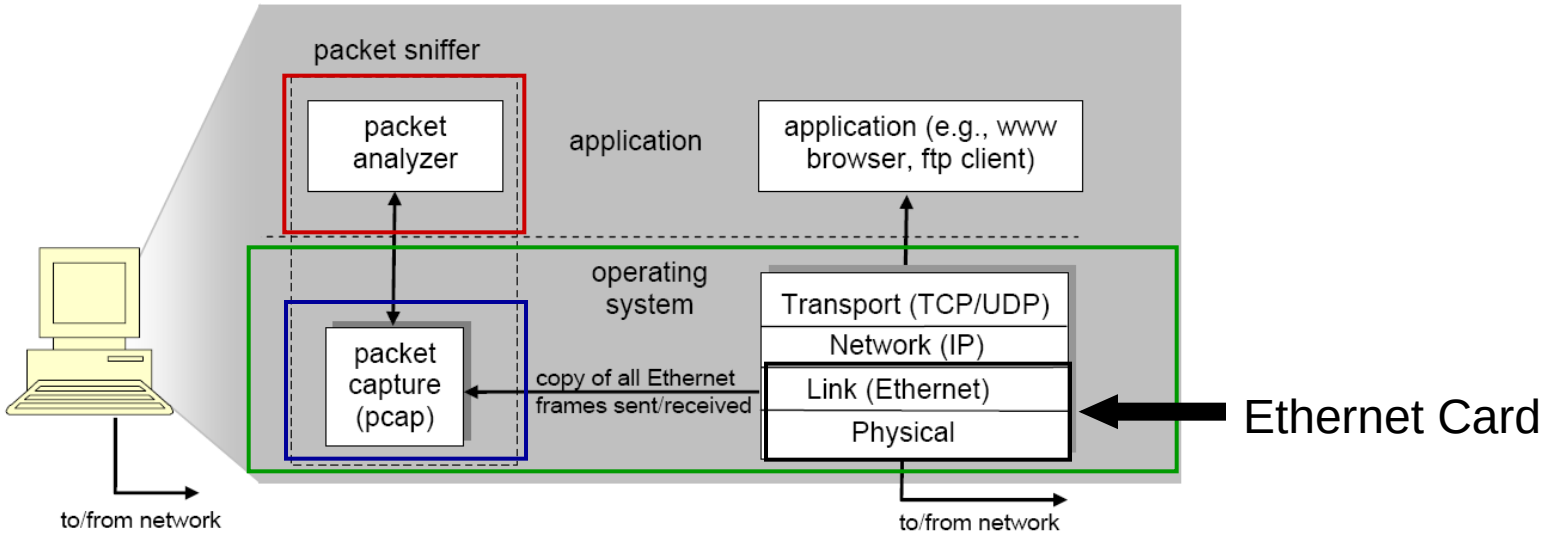
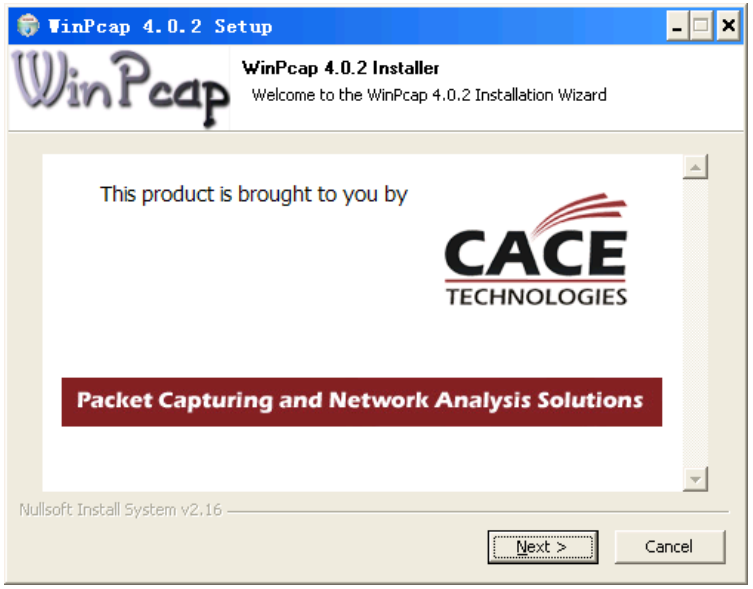


Figure 1: Packet sniffer structure

Instal·lació

- Descarregar des de
  - www.wireshark.org/download.html
- Requerirà instal·lar diferents drivers de captura
  - Windows: winpcap (www.winpcap.org)
  - Linux: libpcap



Esquema de la pantalla de Wireshark

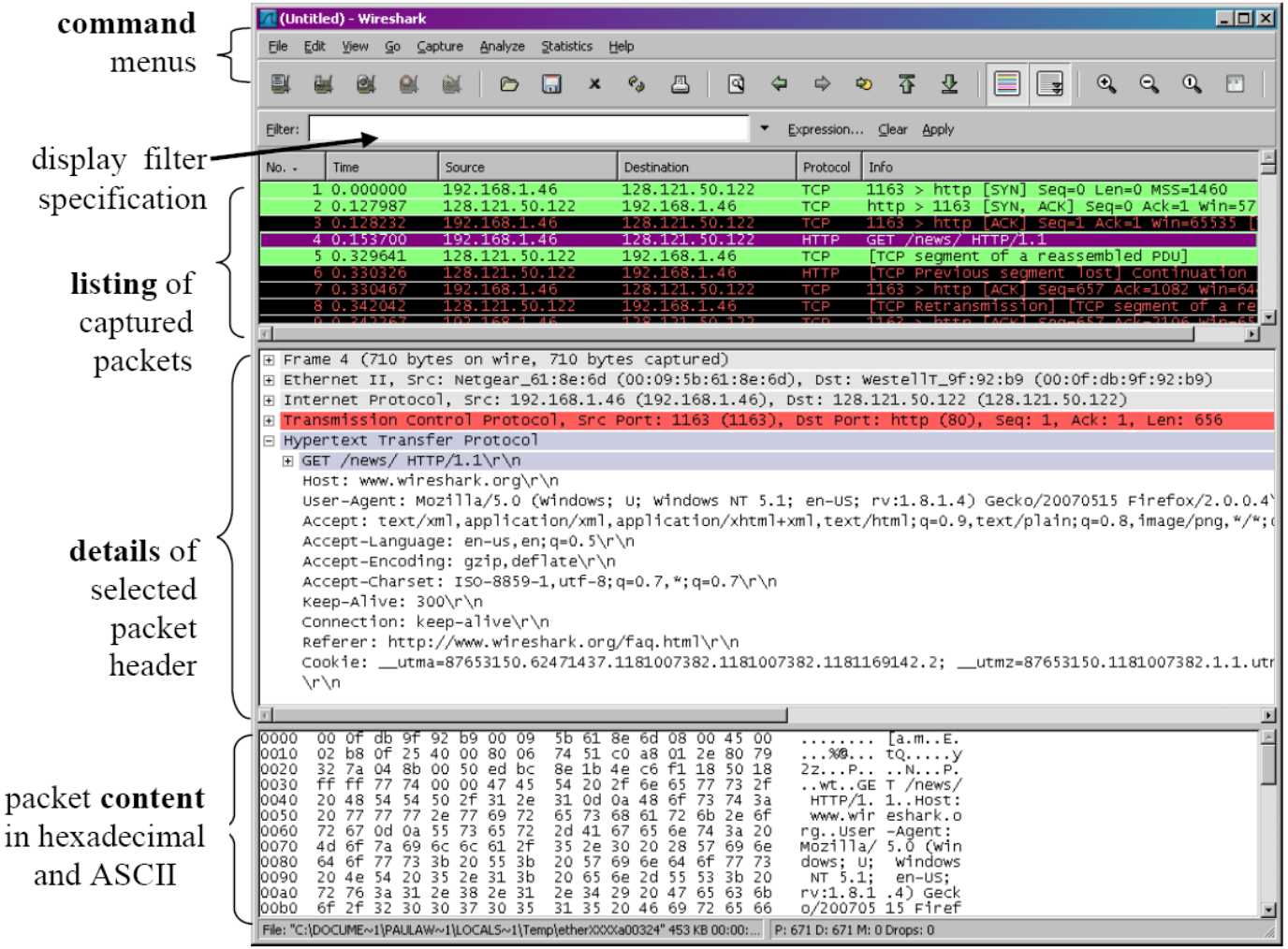
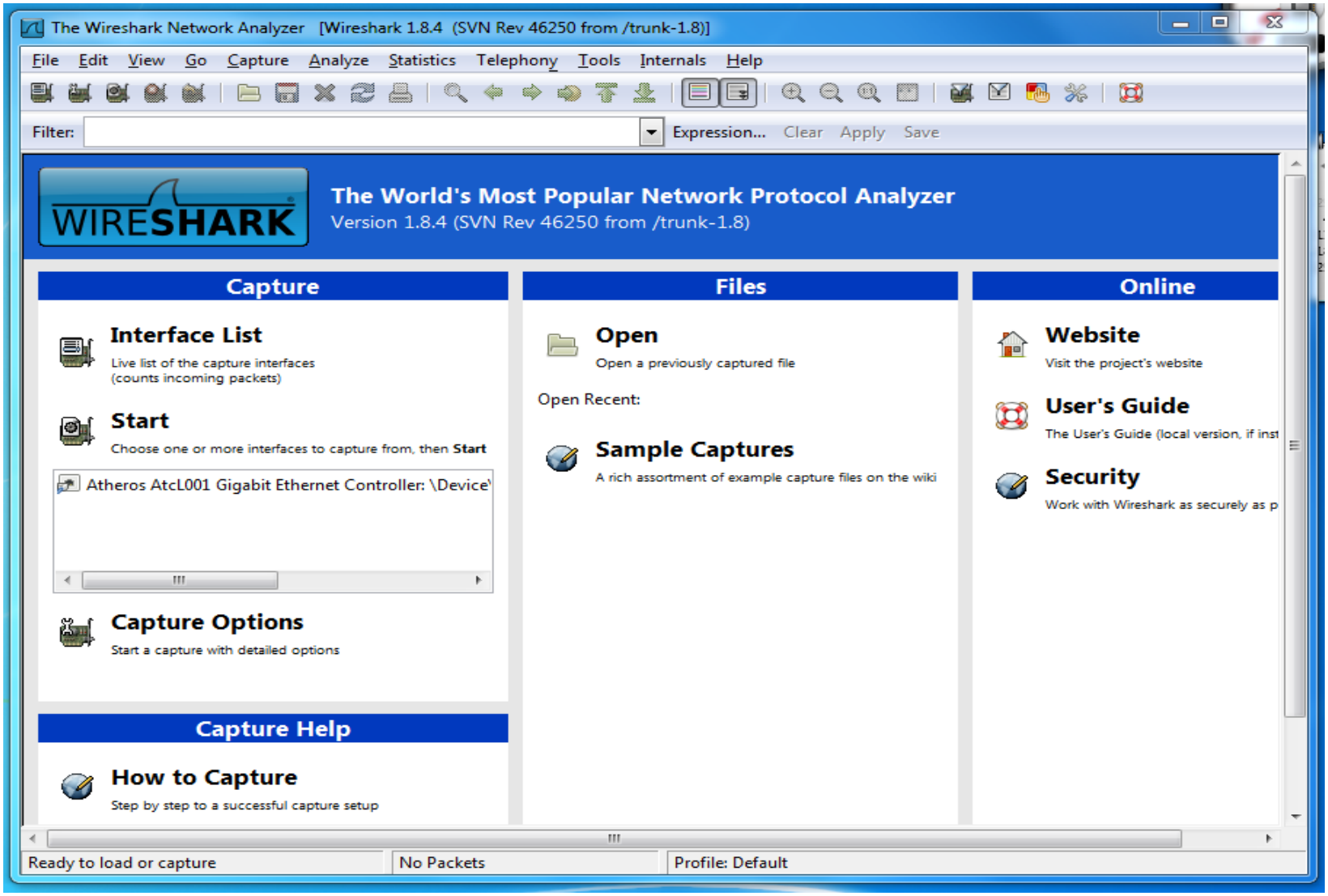


Figure 2: Wireshark Graphical User Interface

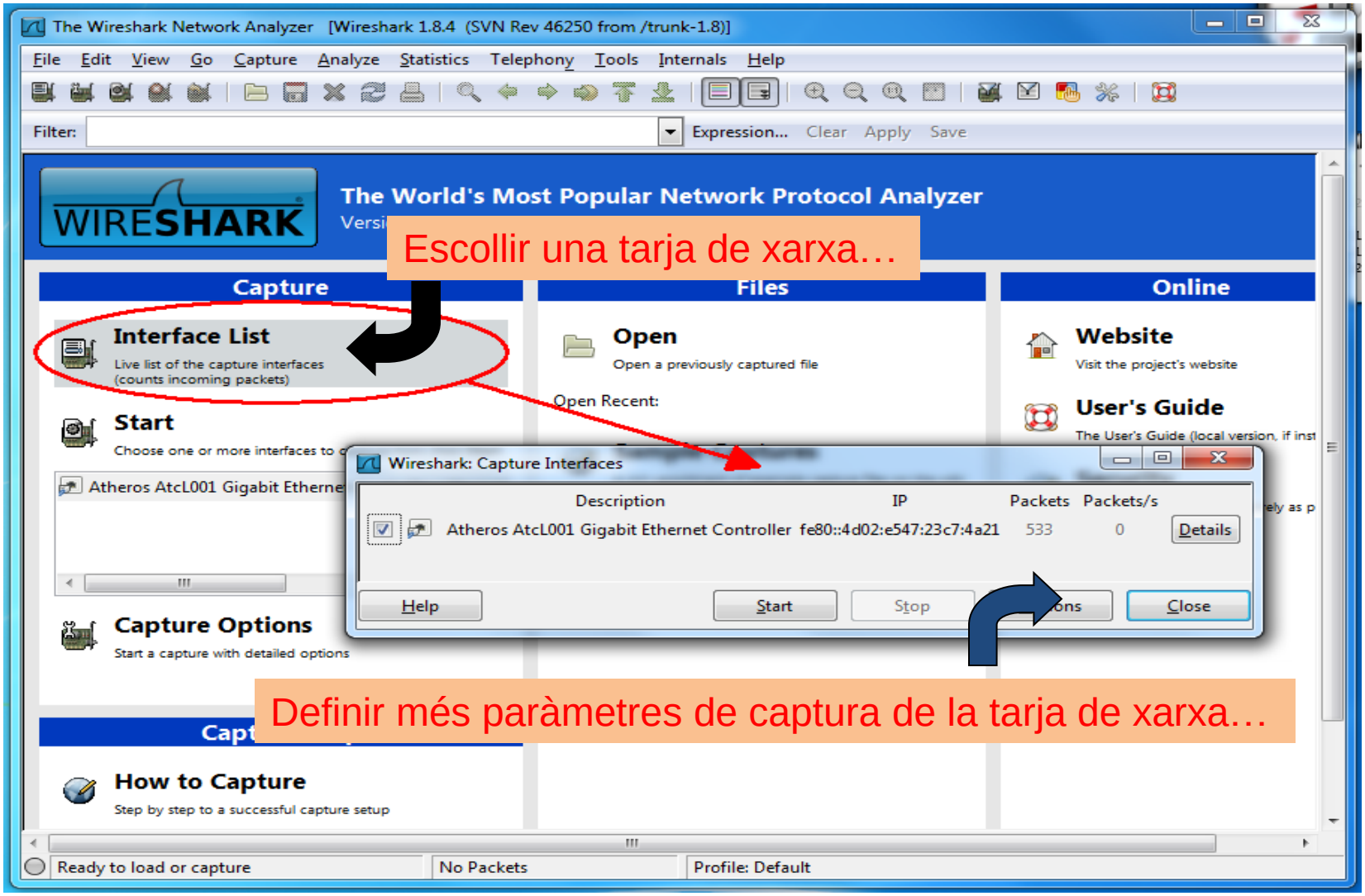
EINES DE MONITORATGE DE XARXES:

Executant Wireshark...

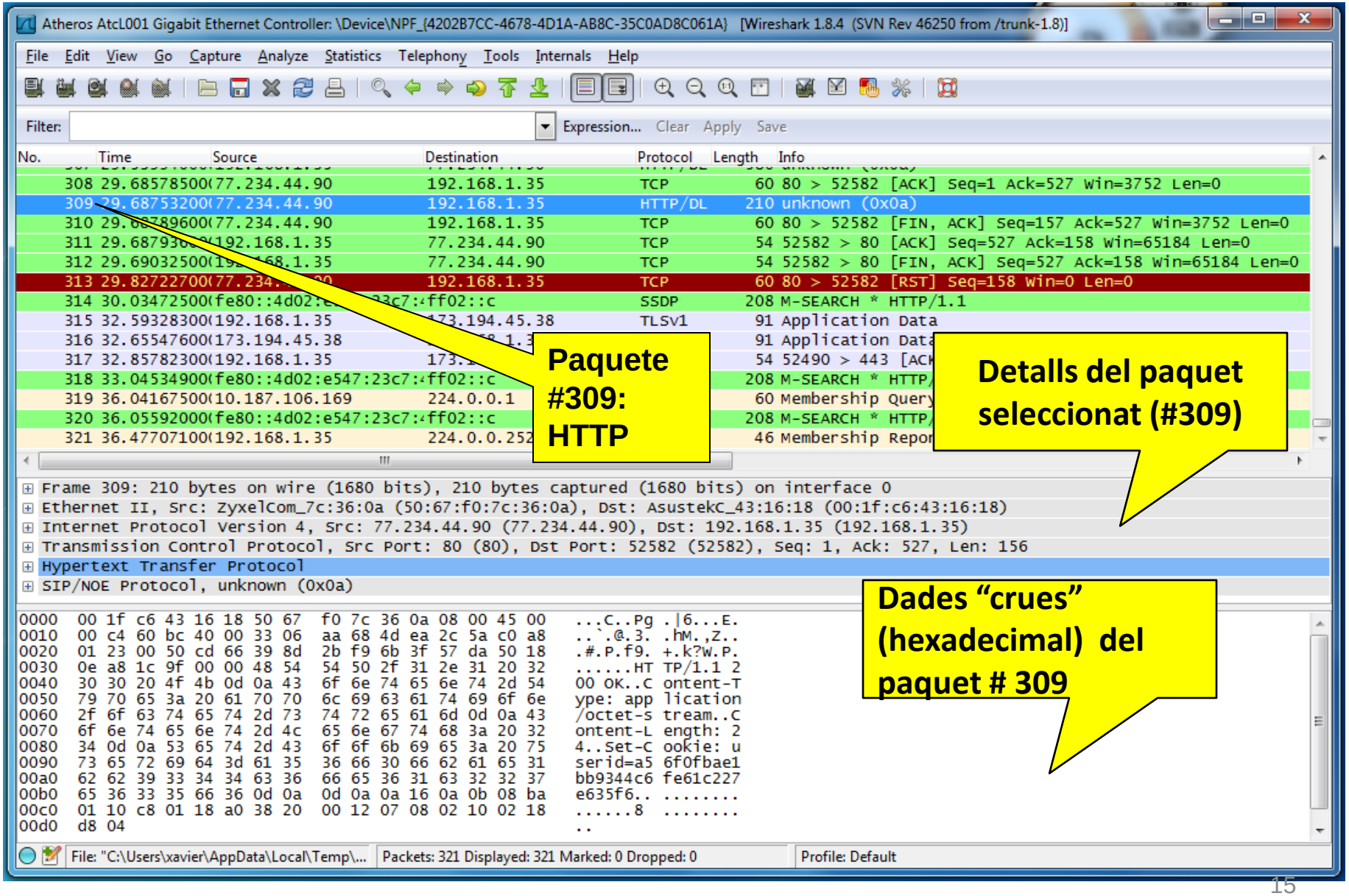


EINES DE MONITORATGE DE XARXES:

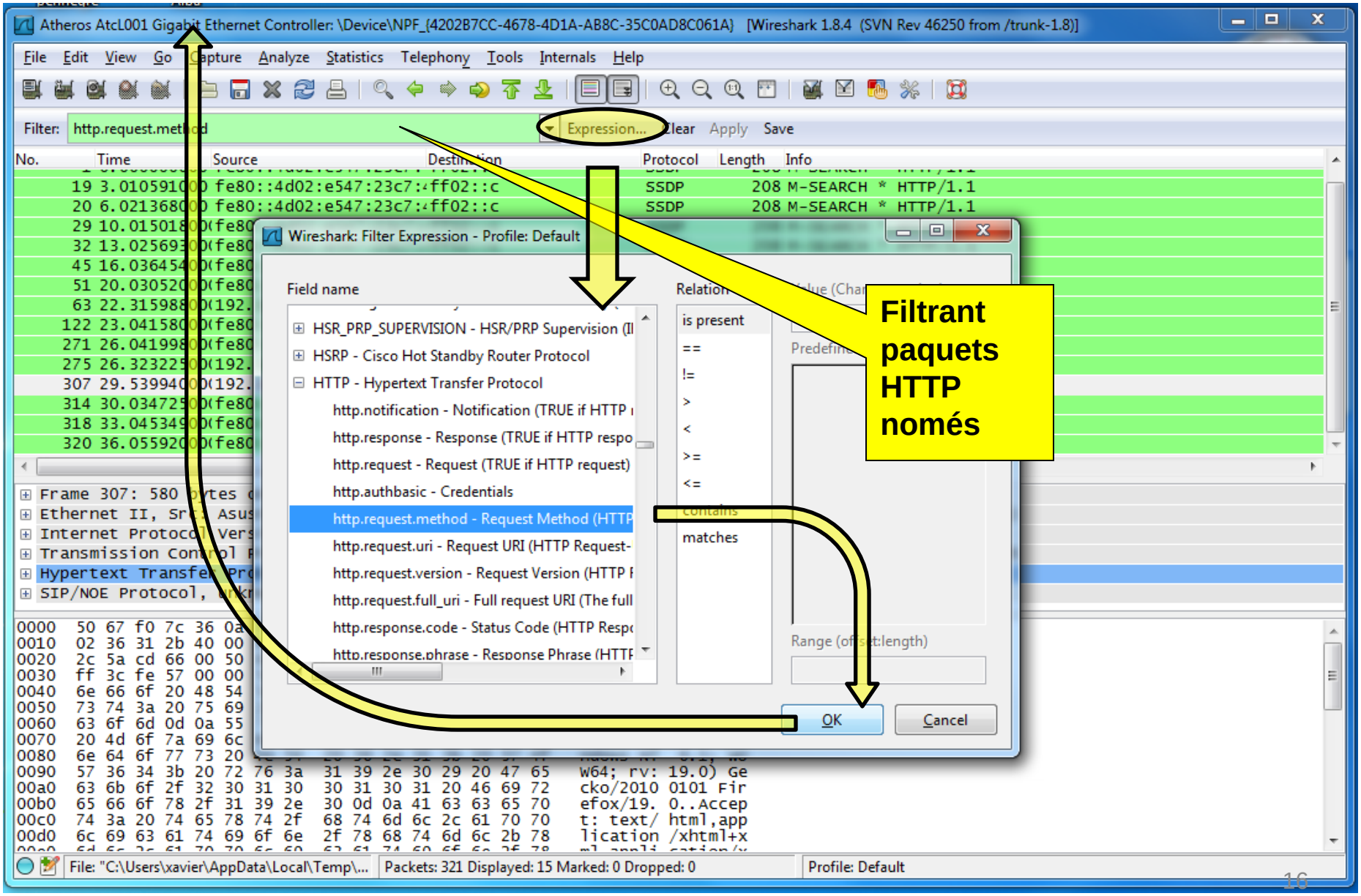
Executant Wireshark…



EINES DE MONITORATGE DE XARXES:



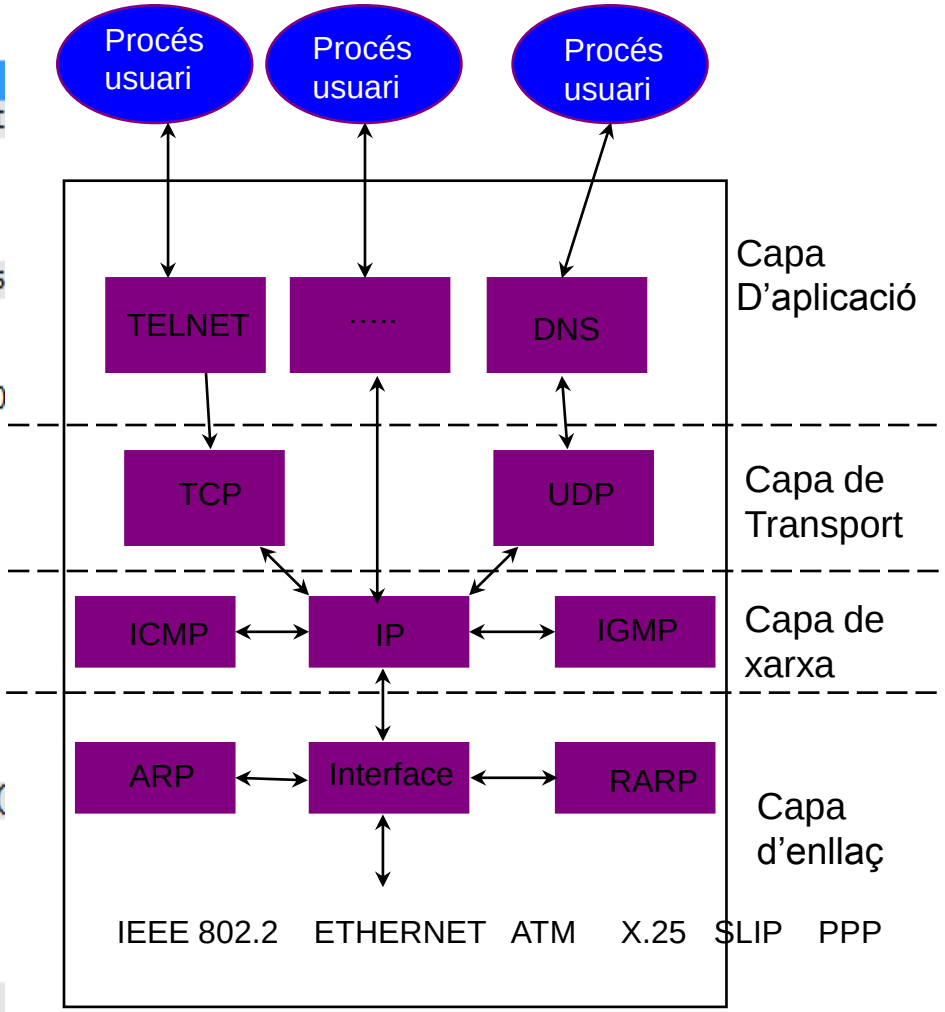
EINES DE MONITORATGE DE XARXES:



EINES DE MONITORATGE DE XARXES:

Capes TCP/IP observables amb Wireshark

```
⊞ Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊟ Ethernet II, Src: AsustekC_b1:0c:ad (00:e0:18:b1:0c:ad), Dst: Quant
  ⊞ Destination: QuantaCo_32:41:8c (00:c0:9f:32:41:8c)
  ⊞ Source: AsustekC_b1:0c:ad (00:e0:18:b1:0c:ad)
    Type: IP (0x0800)
⊟ Internet Protocol Version 4, Src: 192.168.170.8 (192.168.170.8), Ds
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x0
    Total Length: 60
    Identification: 0x6f4c (28492)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
  ⊞ Header checksum: 0xf5f6 [correct]
    Source: 192.168.170.8 (192.168.170.8)
    Destination: 192.168.170.20 (192.168.170.20)
⊟ User Datagram Protocol, Src Port: 32795 (32795), Dst Port: domain (
    Source port: 32795 (32795)
    Destination port: domain (53)
    Length: 40
  ⊞ Checksum: 0x3432 [validation disabled]
⊞ Domain Name System (query)
```



TCP/IP

El que no pot fer…

- No es pot utilitzar per traçar el mapa d'una xarxa.
- No és una eina que generi dades de la xarxa en mode passiu.
- Només mostra informació detallada sobre els protocols que pot entendre.
- Només pot capturar dades, com el tipus de sistema operatiu \ Interfícies \ i informació dels controladors (drivers).
- Un exemple d'això és la captura de dades a través de xarxes sense fils.

Conclusió

- Les funcions d'anàlisi sense fils (wireless) de Wireshark s'han convertit en una eina molt poderosa per a la solució de problemes i anàlisi de xarxes sense fils.
- Amb els filtres de pantalla de Wireshark i potents funcions, es poden "disseccionar" els protocols, es pot realitzar a través de grans quantitats de trànsit de paquets.
- Sense cap dubte, Wireshark és una eina d'avaluació de gran abast i una eina d'anàlisi de xarxes sense fil que ha de ser una part de cada auditor, enginyer, consultor i kit d'eines.