Un po’ di pratica

Gaia Maselli

Strumenti di rete

- Netstat
- host
- nslookup
- Wireshark

`netstat`

- Utile per conoscere lo stato corrente della rete (network status)
- Sessioni TCP attive
  - `netstat -t`
- Listener TCP attivi
  - `netstat -ltn`
- Tabella di routing
  - `netstat -r`
  - netstat -rn
- Interfacce
  - `netstat -i`

host

- DNS lookup utility
- Converte nomi in indirizzi IP
  - `host <name>`
- Converte indirizzi IP in nomi
  - `host <IP address>`
- Trova DNS server responsabili per un dominio
  - `host –t NS <dominio>`
- Trova mailserver per un dominio
  - `host –t MX <dominio>`

nslookup <host>

nslookup is a program to query Internet domain name servers

Il comando senza opzioni permette di richiedere record di tipo A al server DNS locale

```
> nslookup www.google.com
```

Risposta

```
    Server:      151.100.17.15
    Address: 151.100.17.15#53

    Non-authoritative answer:
    Name: www.google.com
    Address: 173.194.35.144
    Name: www.google.com
    Address: 173.194.35.145
    Name: www.google.com
    Address: 173.194.35.146
    Name: www.google.com
    Address: 173.194.35.147
    Name: www.google.com
    Address: 173.194.35.148
```

nslookup –type=NS <dominio>

Permette di richiedere un record di tipo NS al server DNS locale

```
> nslookup -type=NS google.com

    Server:         151.100.17.15
    Address:  151.100.17.15#53

    Non-authoritative answer:
    google.com    nameserver = ns4.google.com.
    google.com    nameserver = ns1.google.com.
    google.com    nameserver = ns2.google.com.
    google.com    nameserver = ns3.google.com.

    Authoritative answers can be found from:
    ns1.google.com   internet address = 216.239.32.10
    ns2.google.com   internet address = 216.239.34.10
    ns3.google.com   internet address = 216.239.36.10
    ns4.google.com   internet address = 216.239.38.10
```

Risposta proveniente dalla cache

Packet sniffing
Wireshark

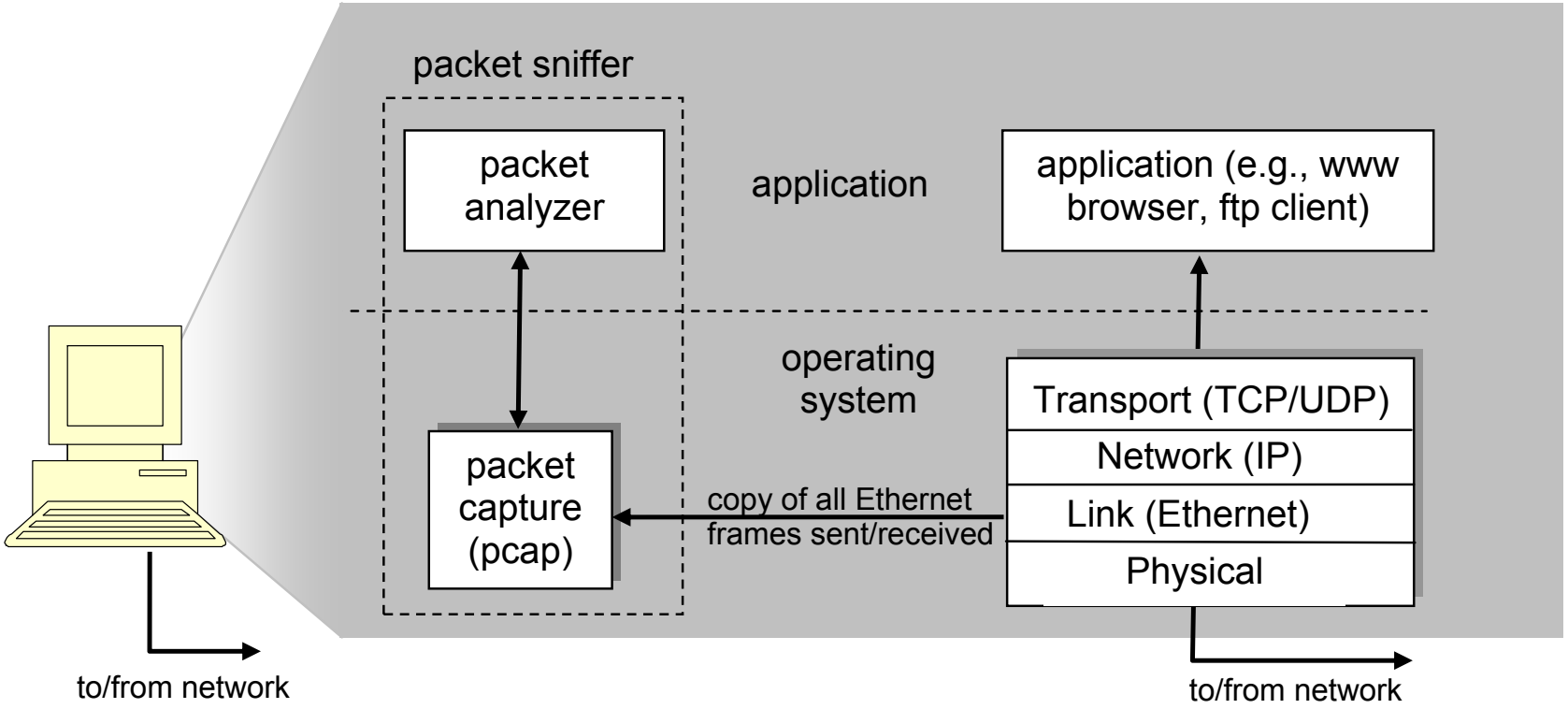
Packet sniffer: Wireshark

- Programma che cattura e analizza tutti i frame entranti e uscenti da una macchina
- Analizzatore passivo di pacchetti
  - Cattura una copia dei **frame** senza modificarli
  - Non immette traffico in rete
- Permette di analizzare i pacchetti a qualsiasi livello dello stack protocollare
  - Estraendo gli header dei vari livelli
- Permette di capire cosa succede all'interno di una rete
  - Utile per didattica
  - Utile agli amministratori di rete
  - Non è un sistema di sicurezza (ma alcuni sistemi di sicurezza si basano su sniffer di pacchetti)
- Deve essere attivo contemporaneamente all'applicazione che vogliamo monitorare
- Comuni packet sniffer: ethereal, tcpdump

Wireshark

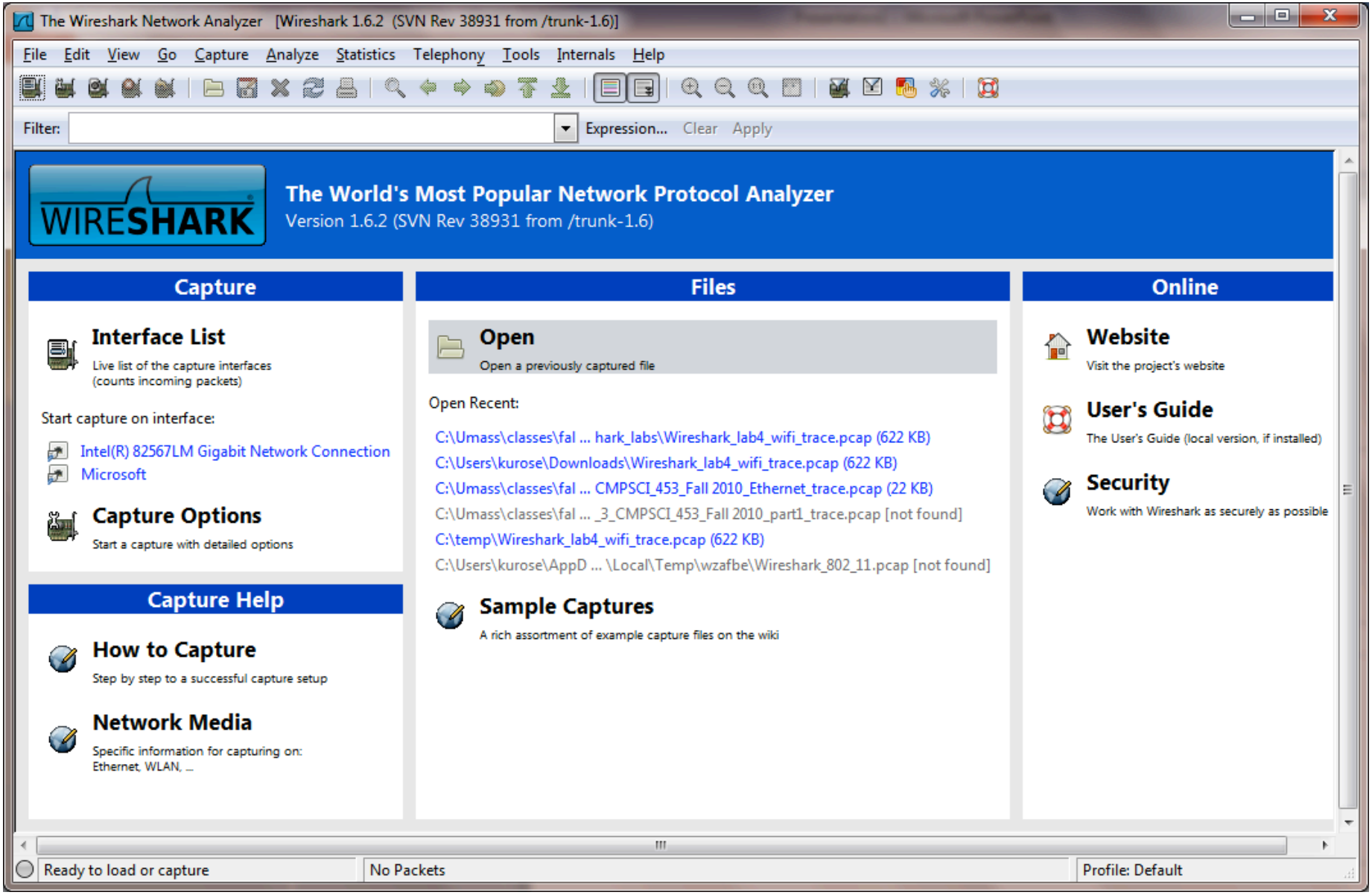
- Tutta la documentazione è disponibile sul sito www.wireshark.org
- Download
  - http://www.wireshark.org/download.html
- Per problemi si può consultare
  - http://wiki.wireshark.org/CaptureSetup
- Funziona su varie tecnologie di trasmissione: Ethernet, seriale (PPP e SLIP), 802.11 wireless LANs, e altre (se il sistema operativo supporta Wireshark).

Wireshark: architecture

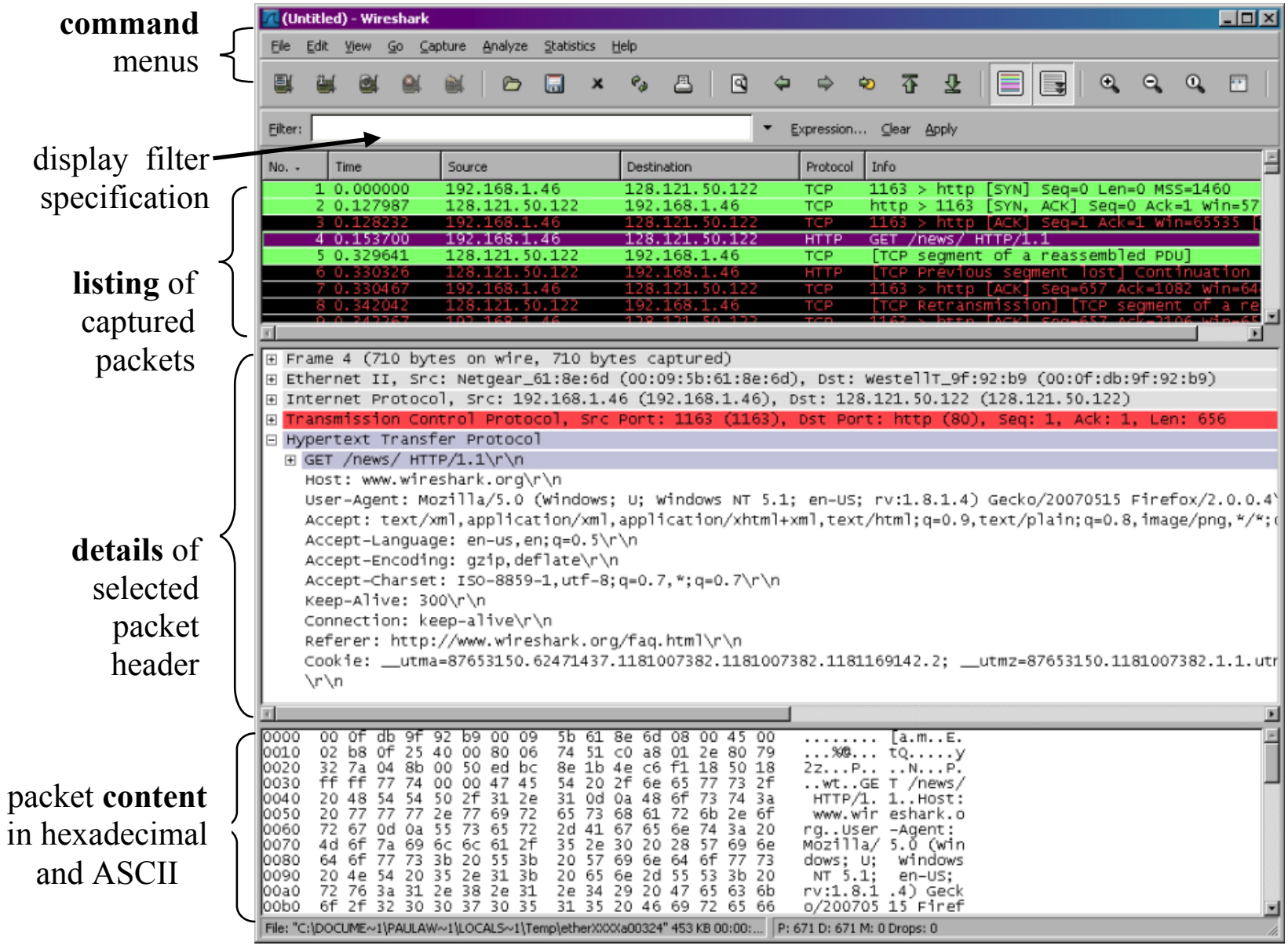


pcap: Packet capture library

Finestra iniziale di Wireshark



Interfaccia grafica



Menu

- The **command menus** are standard pulldown menus located at the top of the window. Of interest to us now are the File and Capture menus. The File menu allows you to save captured packet data or open a file containing previously captured packet data, and exit the Wireshark application. The Capture menu allows you to begin packet capture.

Packet listing

The **packet-listing window** displays one-line summary for each packet captured, including the packet number (assigned by Wireshark; this is *not* a packet number contained in any protocol's header), the time at which the packet was captured, the packet's source and destination addresses, the protocol type, and protocol-specific information contained in the packet. The packet listing can be sorted according to any of these categories by clicking on a column name. The protocol type field lists the highest-level protocol that sent or received this packet, i.e., the protocol that is the source or ultimate sink for this packet.

packet-header details window

The **packet-header details window** provides details about the packet selected (highlighted) in the packet-listing window. (To select a packet in the packet- listing window, place the cursor over the packet's one-line summary in the packet-listing window and click with the left mouse button.). These details include information about the Ethernet frame (assuming the packet was sent/received over an Ethernet interface) and IP datagram that contains this packet. The amount of Ethernet and IP-layer detail displayed can be expanded or minimized by clicking on the plus minus boxes to the left of the Ethernet frame or IP datagram line in the packet details window. If the packet has been carried over TCP or UDP, TCP or UDP details will also be displayed, which can similarly be expanded or minimized. Finally, details about the highest-level protocol that sent or received this packet are also provided.

packet-contents window

The **packet-contents window** displays the entire contents of the captured frame, in both ASCII and hexadecimal format.

Esercizio 1

- Avviare il browser e pulire la cache
- Avviare Wireshark
- Avviare la cattura dei pacchetti
- Tornare sul browser e inserire la URL:

http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

- Dopo aver visualizzato la pagina, interrompere la cattura dei pacchetti di Wireshark
- Osservare la lista di pacchetti scambiati e quali protocolli sono stati utilizzati

Esercizio 1: analisi del traffico

- Filtrare i pacchetti, digitando **http** nel campo f*ilter*, e cliccando su **Apply**
  - Trovare ed esaminare il messaggio GET
  - Trovare ed esaminare il messaggio di risposta
- Rimuovere il filtro http e filtrare i pacchetti DNS
  - Esaminare DNS query e response
  - Numero di porta sorgente e destinazione?
- Analizzare pacchetti TCP
- Confrontare le richieste e risposte HTTP e DNS con il formato dei messaggi visti a lezione

Esercizio 1 alternativo

- Eseguire esercizio 1 collegandosi al seguente link:

http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file3.html

- Osservare variazioni nel traffico

Esercizio 2

- Avviare il browser
- Avviare Wireshark
- Avviare la cattura dei pacchetti
- Tornare sul browser e inserire la URL:

http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file4.html

- Dopo aver visualizzato la pagina, interrompere la cattura dei pacchetti di Wireshark

Esercizio 2: analisi del traffico

- Osservare la lista di pacchetti scambiati e quali protocolli sono stati utilizzati
  - DNS
  - HTTP
  - TCP
- Le due immagini vengono scaricate in seriale e parallelo?
- Si usano connessioni persistenti o non persistenti?
- Visitare una qualsiasi altra pagina contenenti immagini e verificare il risultati

Esercizi

- Utilizzare Wireshark per analizzare il traffico durante:
  - il download di una pagina web contenente immagini e testo
  - Una richiesta/risposta DNS effettuata con nslookup
  - L'invio di una email