

University of Modena and Reggio Emilia

Laboratorio di Comunicazioni Multimediali

WIRESHARK

Daniela Saladino
(daniela.saladino@unimore.it)

Analizzatore di protocollo

- Cattura i pacchetti, decodifica e analizza i contenuti
- Un analizzatore di protocolli di rete viene usato per
  - rilevare problemi di rete
  - analizzare le prestazioni di rete per individuare eventuali bottleneck
  - rilevare possibile intrusioni nella rete
  - analizzare alcune applicazioni



Wireshark

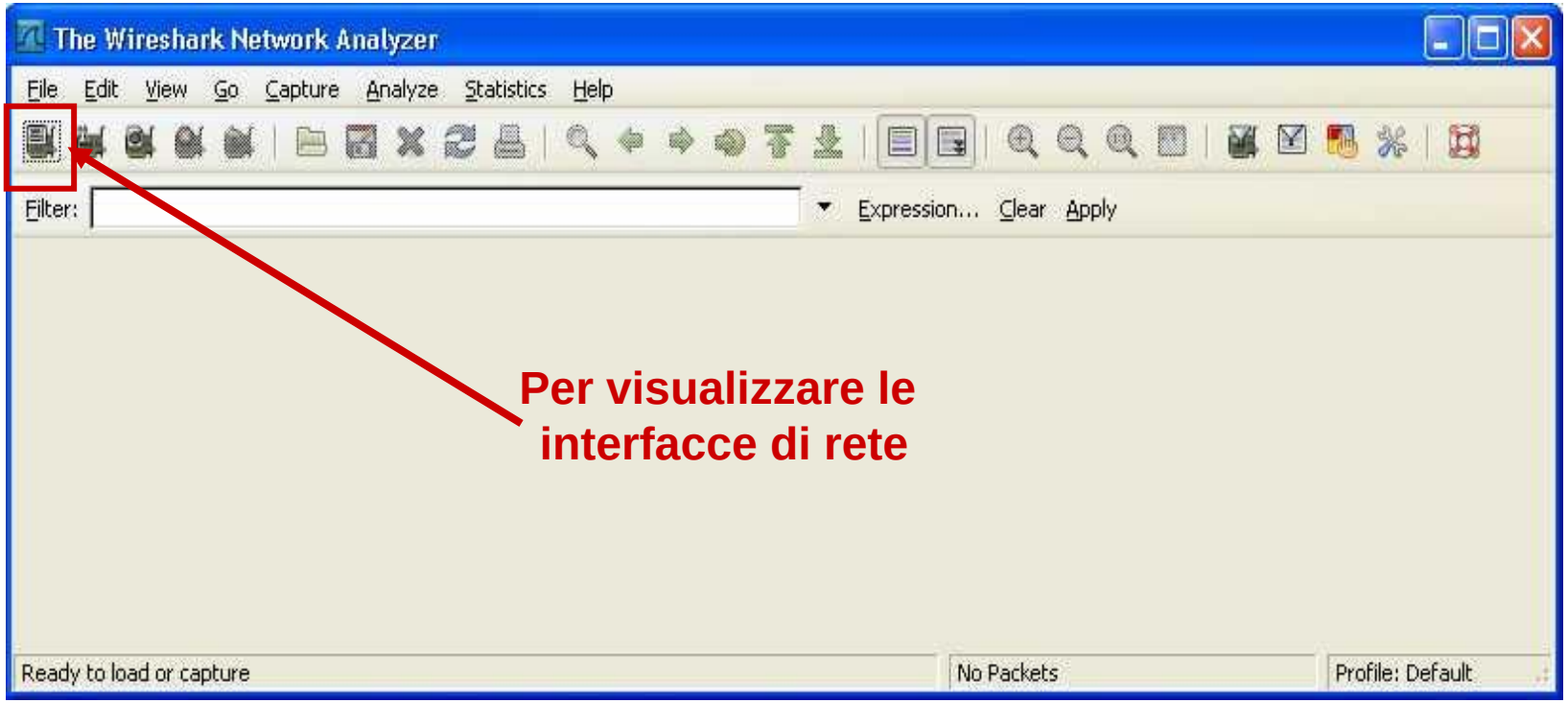
- Software per l'analisi di protocollo (o packet sniffer)
  - cattura tutti i pacchetti in transito su una interfaccia di rete
- Fino al 2006 si chiamava *Ethereal*
- Principale sviluppatore: Gerald Combs
- Funzionalità molto simili a quelle di *tcpdump*
  - interfaccia grafica
  - maggiori funzionalità di ordinamento e filtraggio
- Licenza Open Source



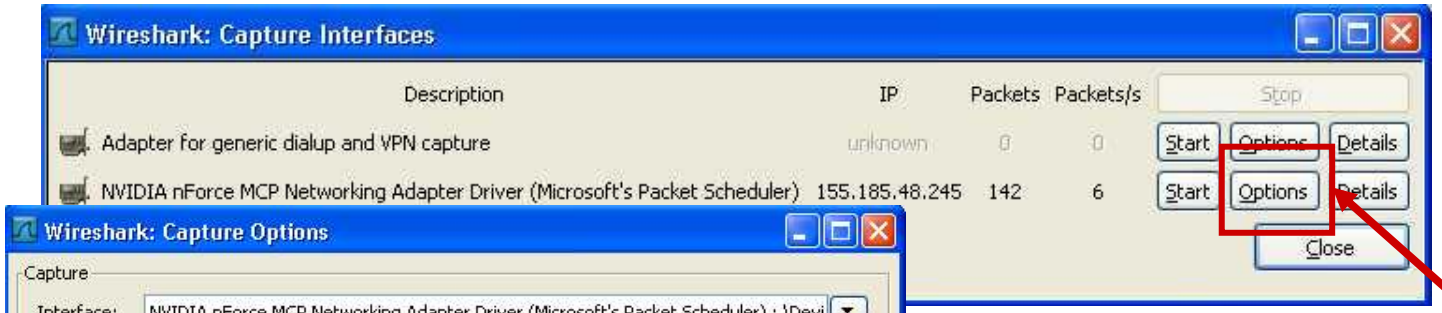
Caratteristiche

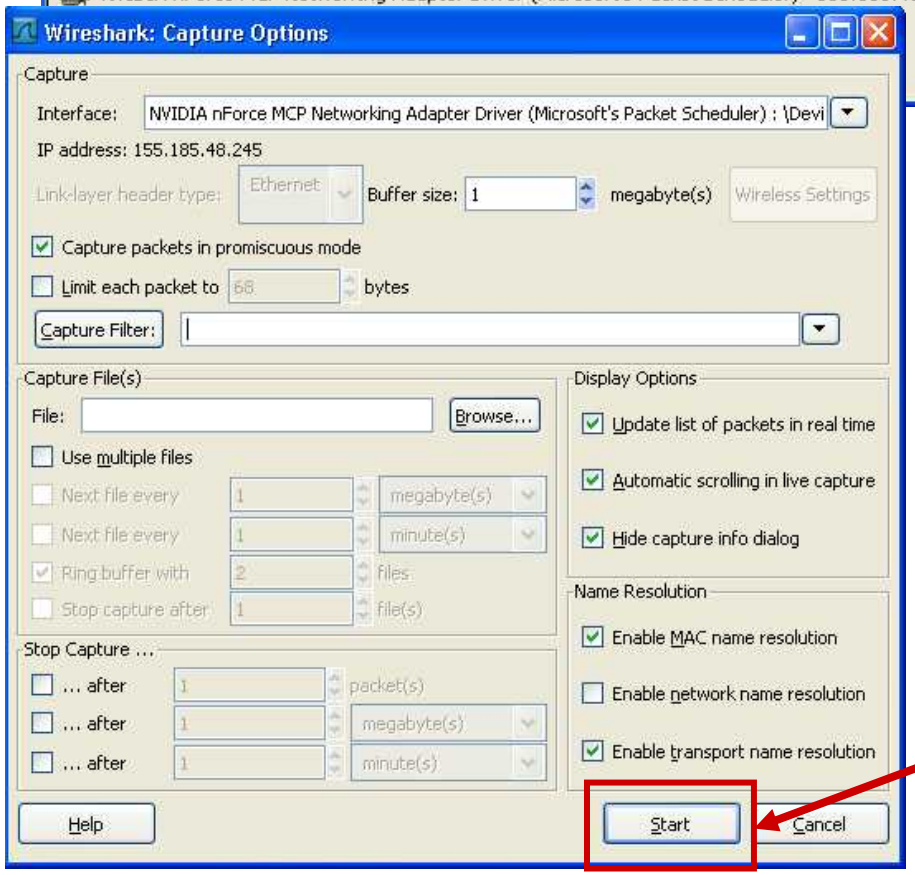
- Permette di:
  - analizzare dati acquisiti in tempo reale o dati salvati su file di cattura (anche da tcpdump)
  - acquisire dati da diversi tipi di interfacce di rete
  - filtrare i dati catturati
  - scomporre e analizzare molti protocolli di comunicazione
  - salvare l'output in diversi formati

Interfaccia



Interfaccia





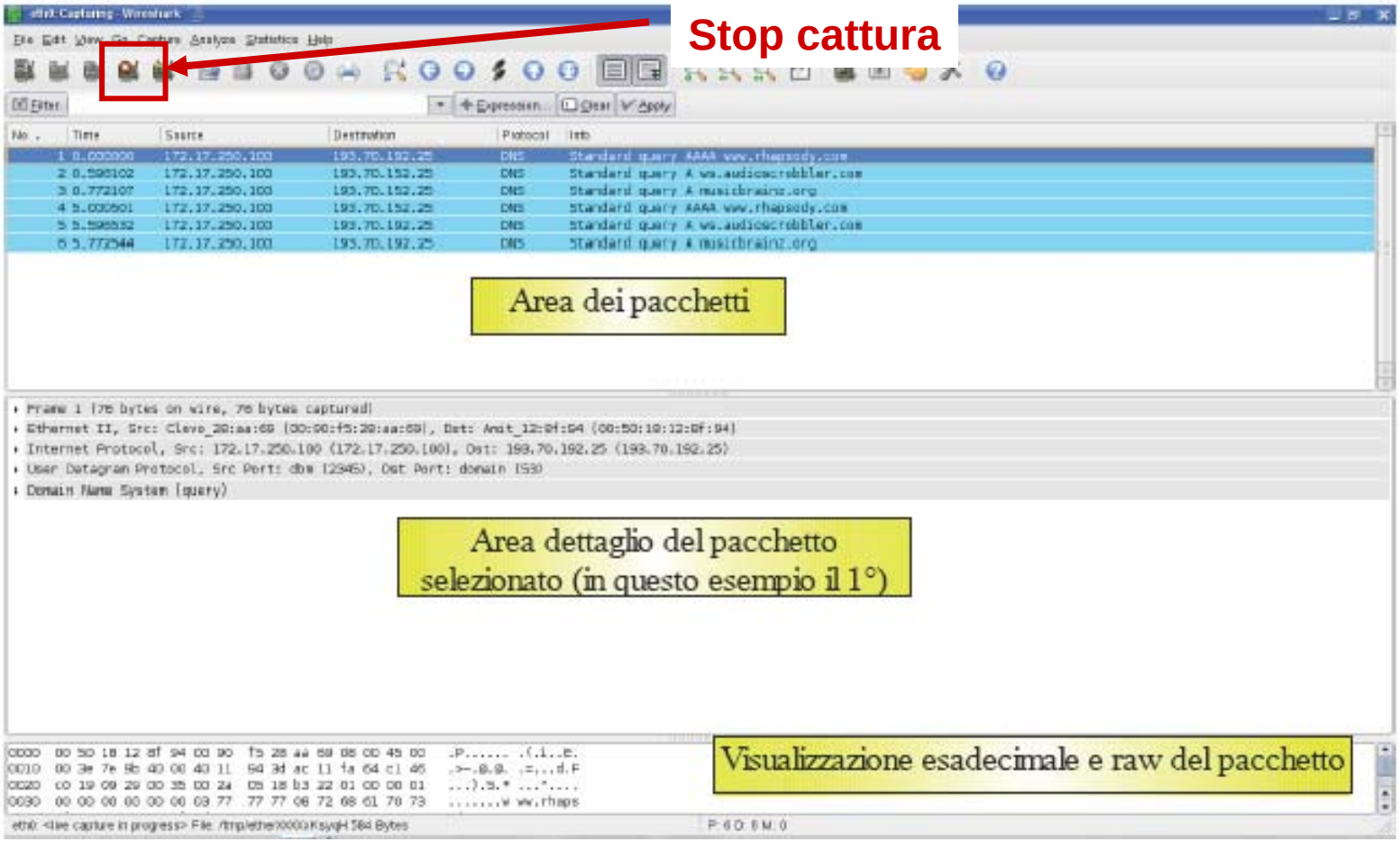
Per impostare le opzioni di cattura

Per avviare la cattura

Opzioni di cattura

- Cattura in modo *promiscuo*
- Specificare un *capture filter* (http://wiki.wireshark.org/CaptureFilters)
  - host 192.168.120.40: cattura solo il traffico diretto da e verso questo indirizzo IP
  - port 80: cattura solo il traffico diretto da e verso la porta 80
  - arp: solo il traffico di tipo ARP (possiamo specificare un altro nome di protocollo, come ad esempio smtp, dns, etc)
  - ip: solo il traffico IP, e quindi non, ad esempio, il traffico ARP, che non possiede una intestazione IP
- *Capture File(s)*: memorizzare il risultato in uno o più file
- *Stop Capture*: temporizzare la fine della cattura

Interfaccia durante la cattura



Filtri

- Sintassi dei filtri:
  - **<protocollo>.<proprietà> <operatore_di_confronto> <valore>**
- Esempi:
  - ip.addr==192.168.1.4 oppure !(ip.addr==192.168.1.4)
    - filtra la cattura visualizzando i pacchetti con protocollo=ip, parametro=addr, quindi tutto quello che ha indirizzo uguale a 162.198.1.4 o tutto tranne pacchetti con quell'indirizzo
  - ip.src==192.168.1.11 && ip.dst==192.168.1.15
    - filtra la cattura visualizzando i pacchetti con hanno indirizzo sorgente pari a 162.198.1.11 e indirizzo destinazione 162.198.1.15
  - tcp.port==25 or icmp
    - mostra solo traffico SMTP (porta 25) o ICMP
  - frame.len > 1024
    - mostra solo i pacchetti che hanno dimensione maggiore di 1024 bytes

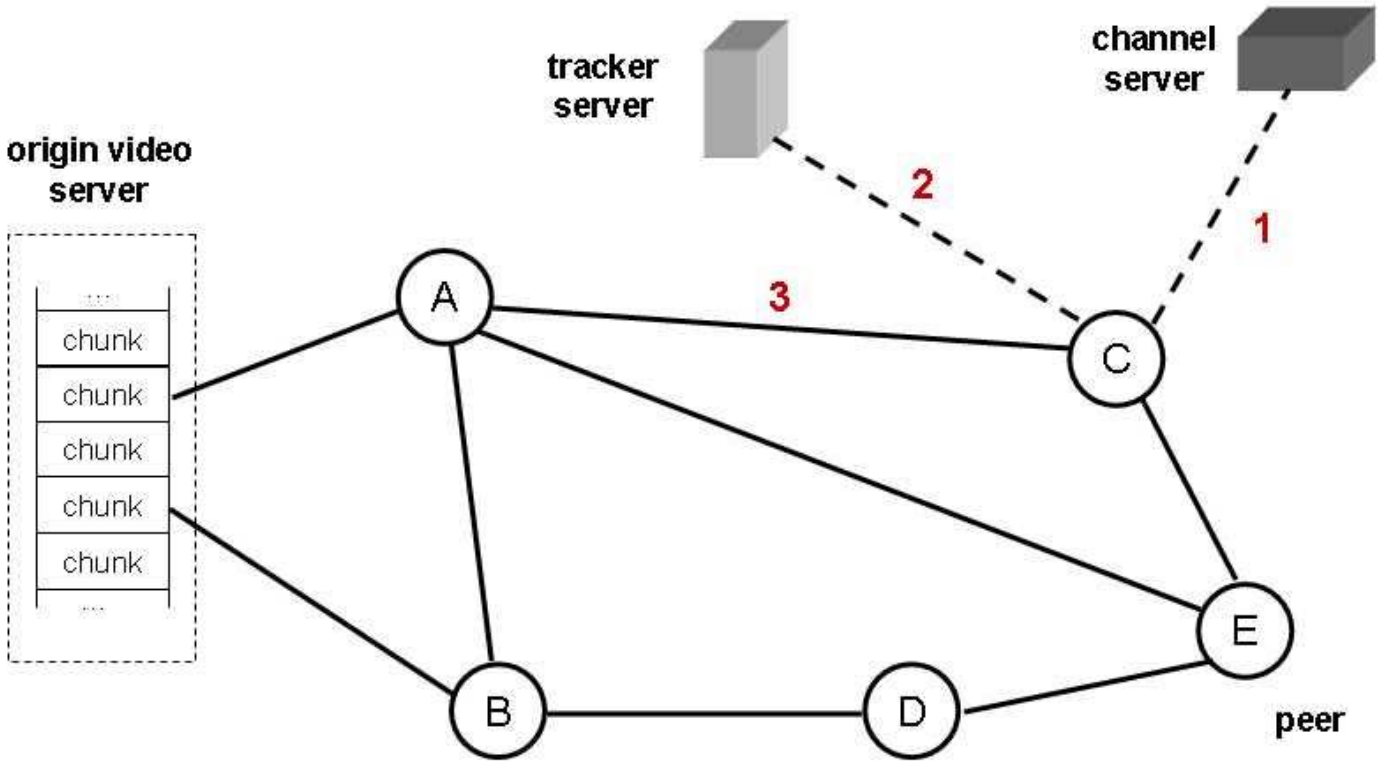
Menù Statistics (1/2)

- *Summary*: sommario dei dati catturati
- *Protocol Hierarchy: gerarchia dei protocolli dei pacchetti catturati e relative statistiche*
- *Conversations*: statistiche delle conversazioni catturate (facendo “Copy” copia la lista dei valori visualizzati in format CSV nella clipboard)
- *Endpoints*: statistiche sugli endpoint catturati
- *I/O Graph*: traffico catturato
  - possibilità di visualizzare diversi tipi di traffico

Menù Statistics (2/2)

- *Packet Length*: ripartizione del traffico su diverse lunghezze di pacchetto
- *Flow Graph*: diagramma temporale dei pacchetti
- *IP Addresses*: mostra tutti indirizzi IP
- *IP Destinations*: mostra ogni destinazione, i protocolli di trasporto e porte sorgenti
- *IP Protocol Types*: numero di pacchetti per ogni tipo di protocollo catturato

P2P live streaming architecture



Comandi (1/2)

- Aprire una shell/terminale e digitare i seguenti comandi per lanciare SopCast e Wireshark:
  - ***cp /opt/src/sp-auth.tgz .*** e poi ***ls*** (per verificare l'avvenuta copia dei file)
  - ***tar xvzf sp-auth.tgz***
  - ***cd sp-auth***
  - ***cat Readme***
- Fare partire Wireshark con:
  - ***sudo wireshark***
- Avviare Wireshark

Comandi (2/2)

- Aprire una nuova shell/tab e digitare:
  - ***./sp-sc-auth sop://broker.sopcast.com:3912/6001 3908 8908 > /dev/null &*** => copiandolo dal Readme visualizzato nell'altra shell
  - ***vlc***
- Una volta avviato VLC, andare in **File => Apri flusso di rete** digitare nel campo HTTP l'url che trovate nel Readme visualizzato nell'altra shell
  - ***http://localhost:8908/tv.asf***
- Ora dovreste visualizzare un canale di SopCast e dovreste vedere i pacchetti che transitano in ingresso e in uscita sulla vostra interfaccia di rete che Wireshark sta catturando.

Esercitazione

- Con quanti peer comunicate (in download e in upload): statistiche
- Quali sono i maggiori fornitori (download) e i maggiori fruitori (upload)
- Tipi di protocolli di trasporto utilizzati: flusso TCP e flusso UDP
- Throughput (Kbyte/sec): in upload e in download
  - complessivo
  - distinguendo tra pacchetti di controllo e pacchetti video (in base alla loro dimensione)
- Traffico in download (Kbyte/sec):
  - complessivo
  - dai 3 migliori peer
  - dal miglior peer
- Numero di pacchetti scambiati distinguendoli per dimensione (range di dimensioni)
- Numero di pacchetti controllo e video scambiati (downlink e uplink)

- Per maggiori informazioni:
  - http://www.wireshark.org/docs/wsug_html_chunked/
  - http://wiki.wireshark.org/

Per chiarimenti:

Daniela Saladino: daniela.saladino@unimore.it