Introduzione a Wireshark

Andrea Atzeni < shocked@polito.it >

Marco Vallini < marco.vallini@polito.it >

Politecnico di Torino

Dip. Automatica e Informatica

Introduzione

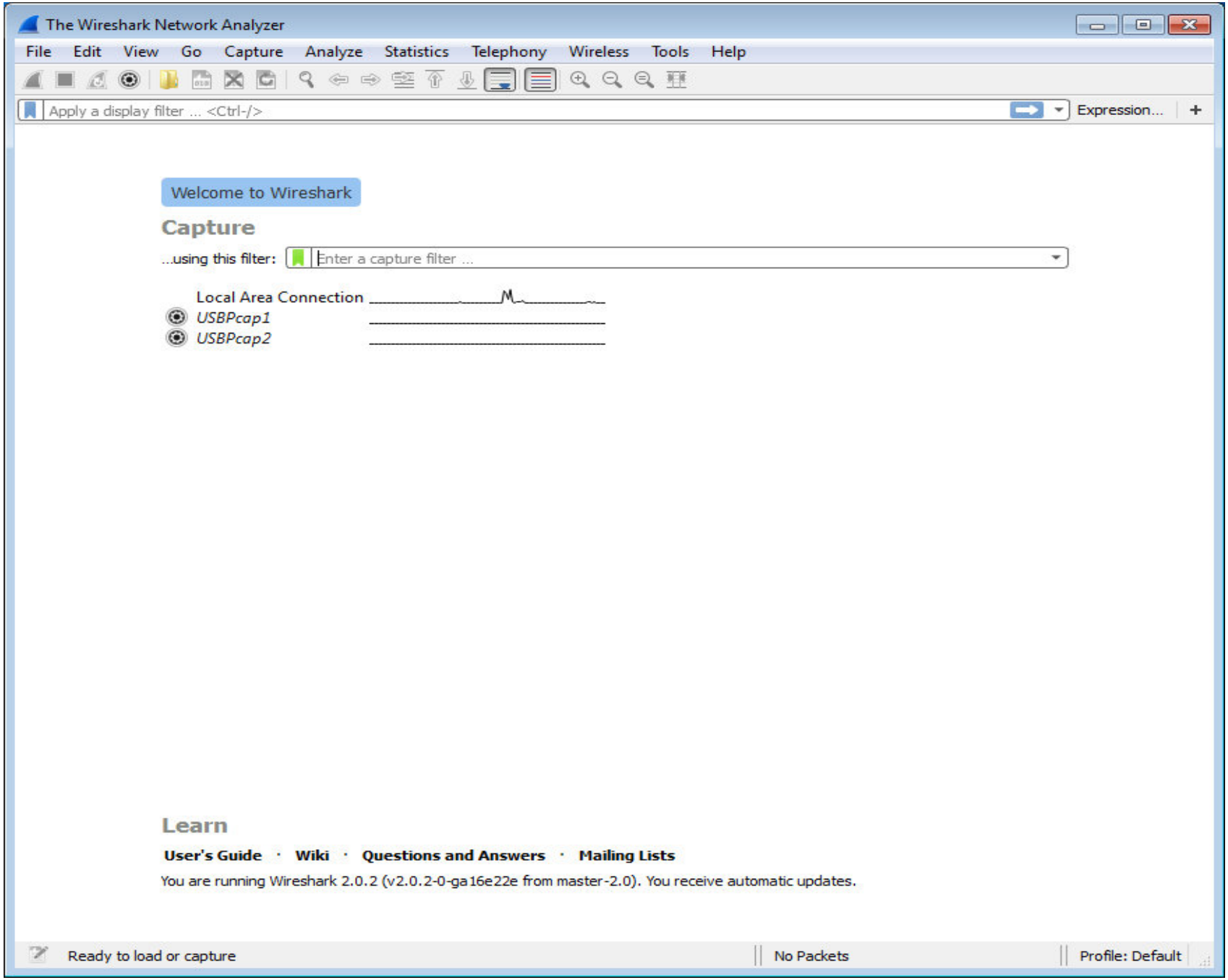
- **intercettare traffico diretto alla scheda di rete**
  - identificare gli host di una comunicazione
  - ed i protocolli impiegati
- **salvataggio del traffico intercettato su file**
  - utile per analisi posticipate (anche diverse) nel tempo
  - usato in caso di reti con molto traffico
- **impiego di filtri**
  - identificare solo il traffico di interesse
  - applicabili prima e dopo l'intercettazione
- **strumento: Wireshark**
  - disponibile per Windows, Linux, macOS, ...
  - ultima versione stabile 3.2.x

Modalità di intercettazione (per IEEE 802)

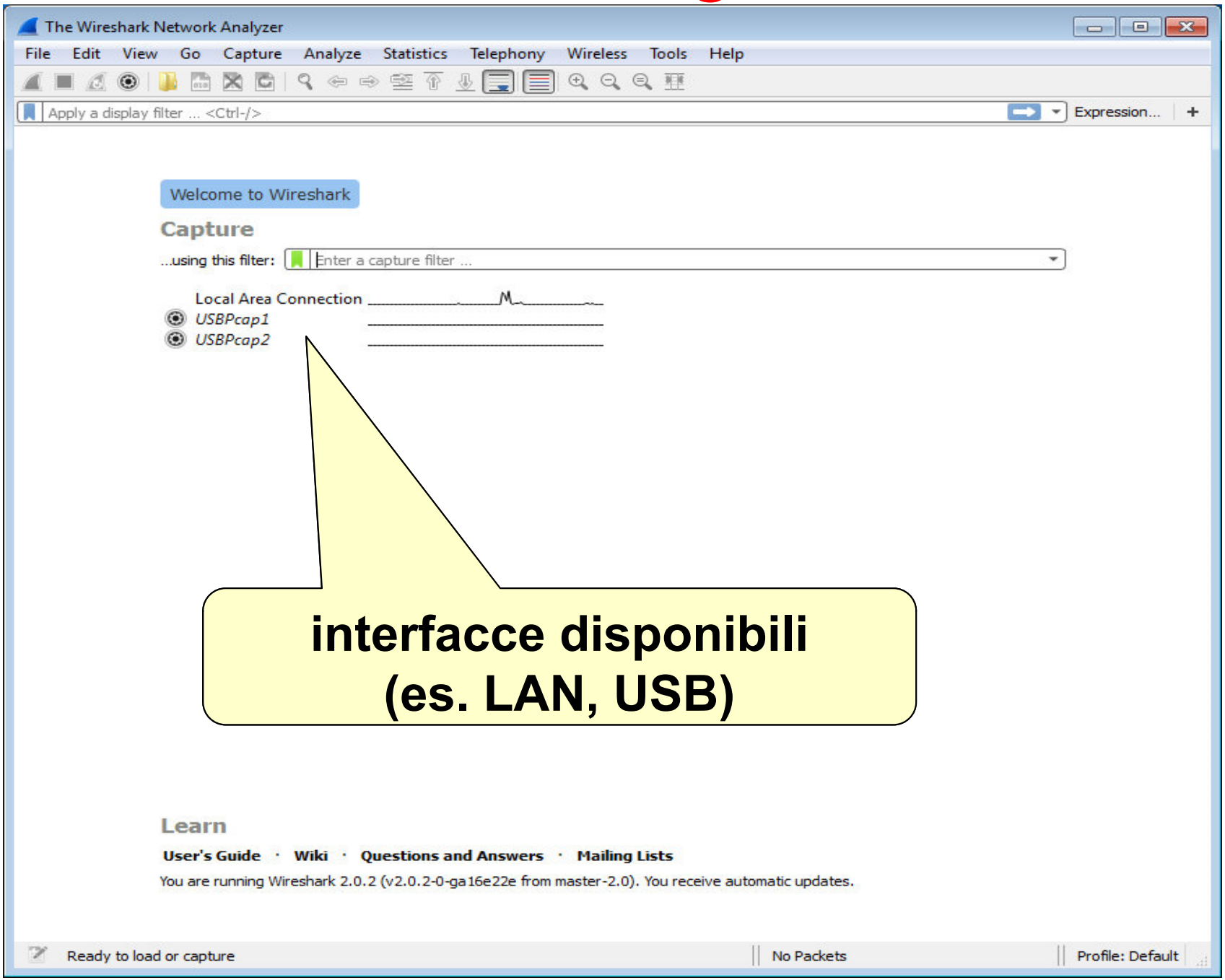
… una scheda di rete può essere impostata in modalità normale o "promiscua" …

- **modalità normale**
  - solo traffico destinato alla scheda di rete (identificata attraverso l'indirizzo MAC)
- **modalità "promiscua" (*Monitor Mode*)**
  - traffico destinato ad altri nodi (anche altri MAC)
    - es. rete wireless/hub = traffico di tutti i nodi collegati
  - utile per controllo del traffico
    - es. protocolli usati nella rete, dati scambiati dalle stazioni
  - può intercettare traffico di utenti diversi!
    - intercettazione fraudolenta = reato penale!

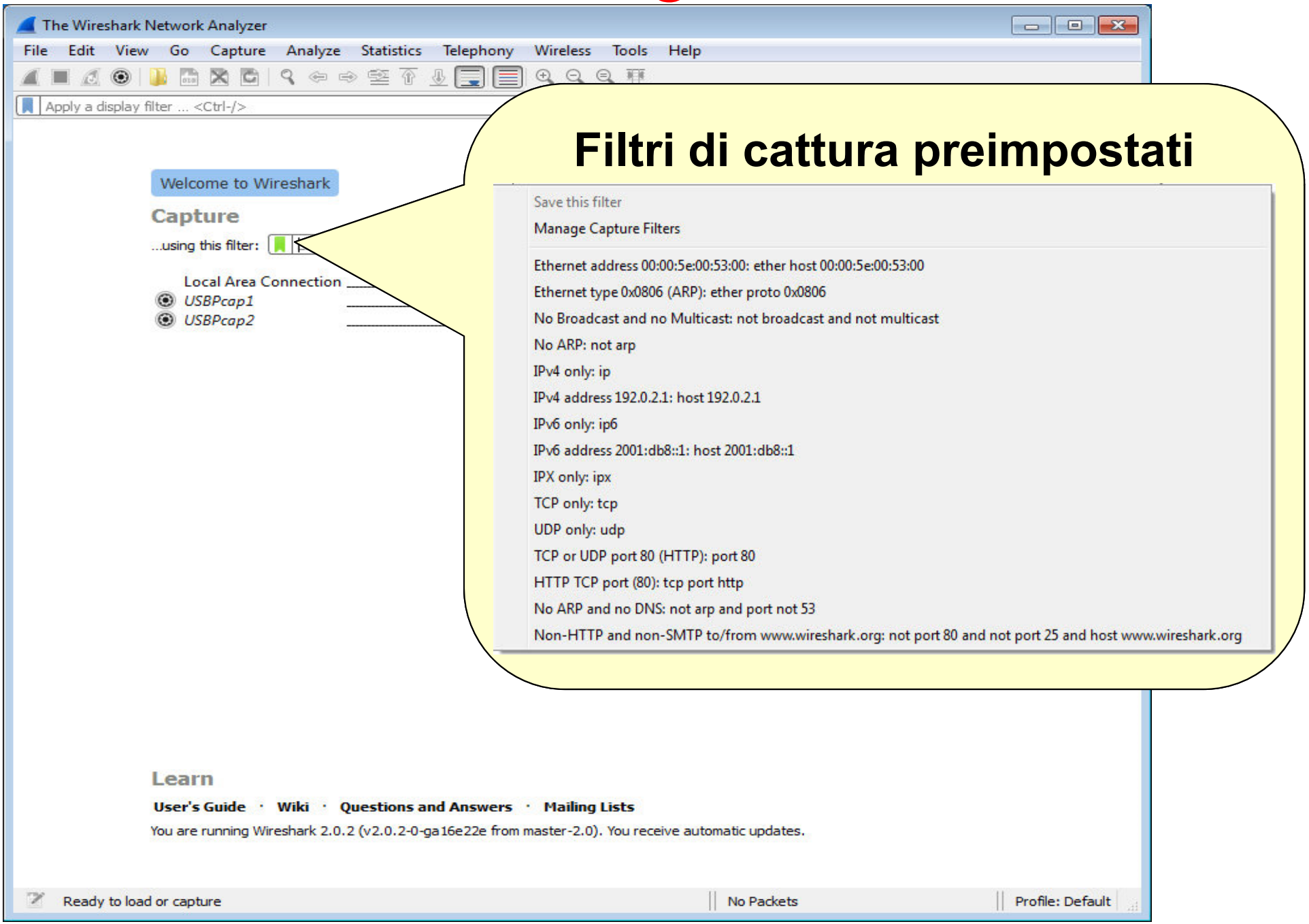
Interfaccia iniziale



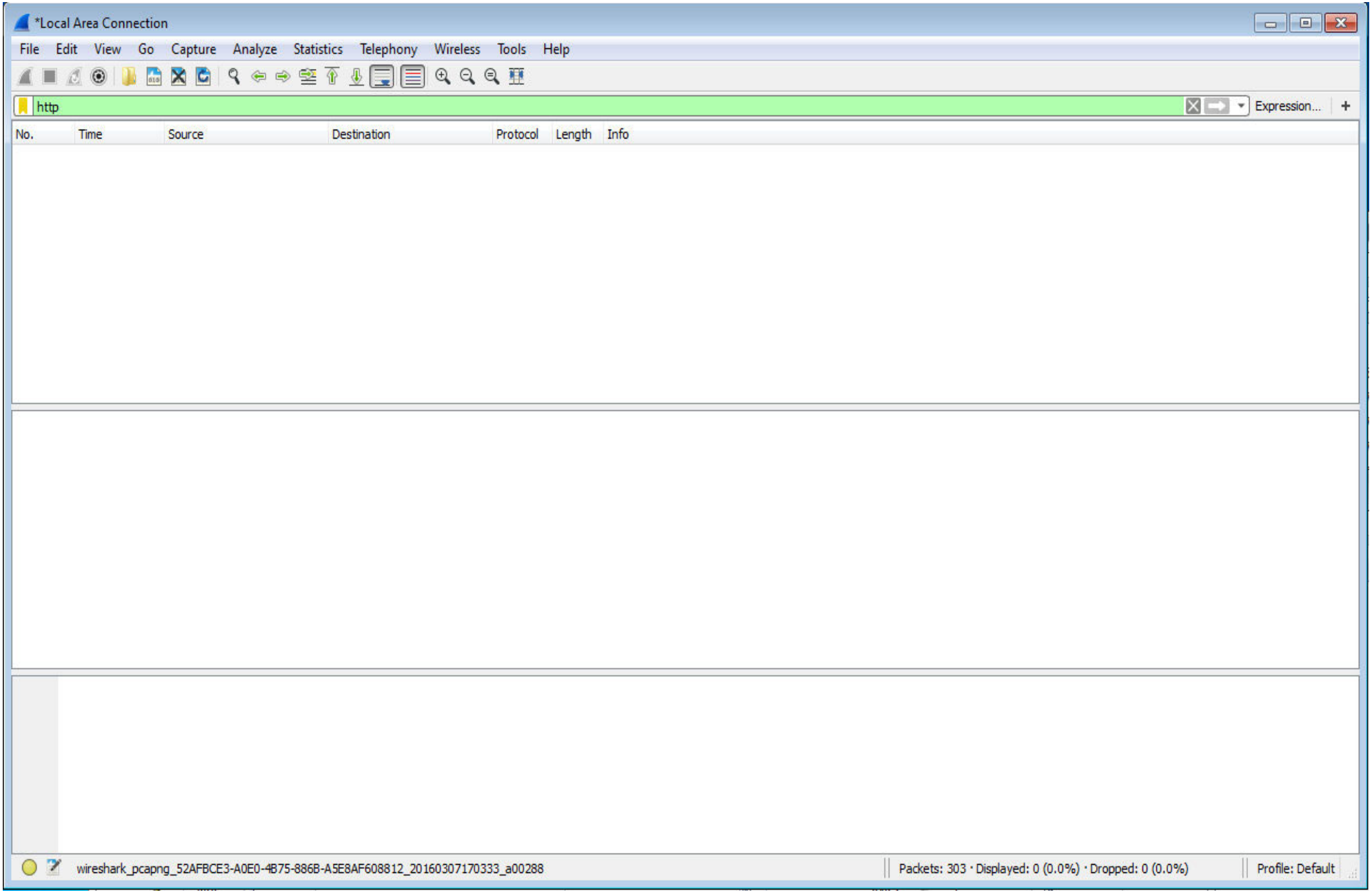
Interfaccia grafica



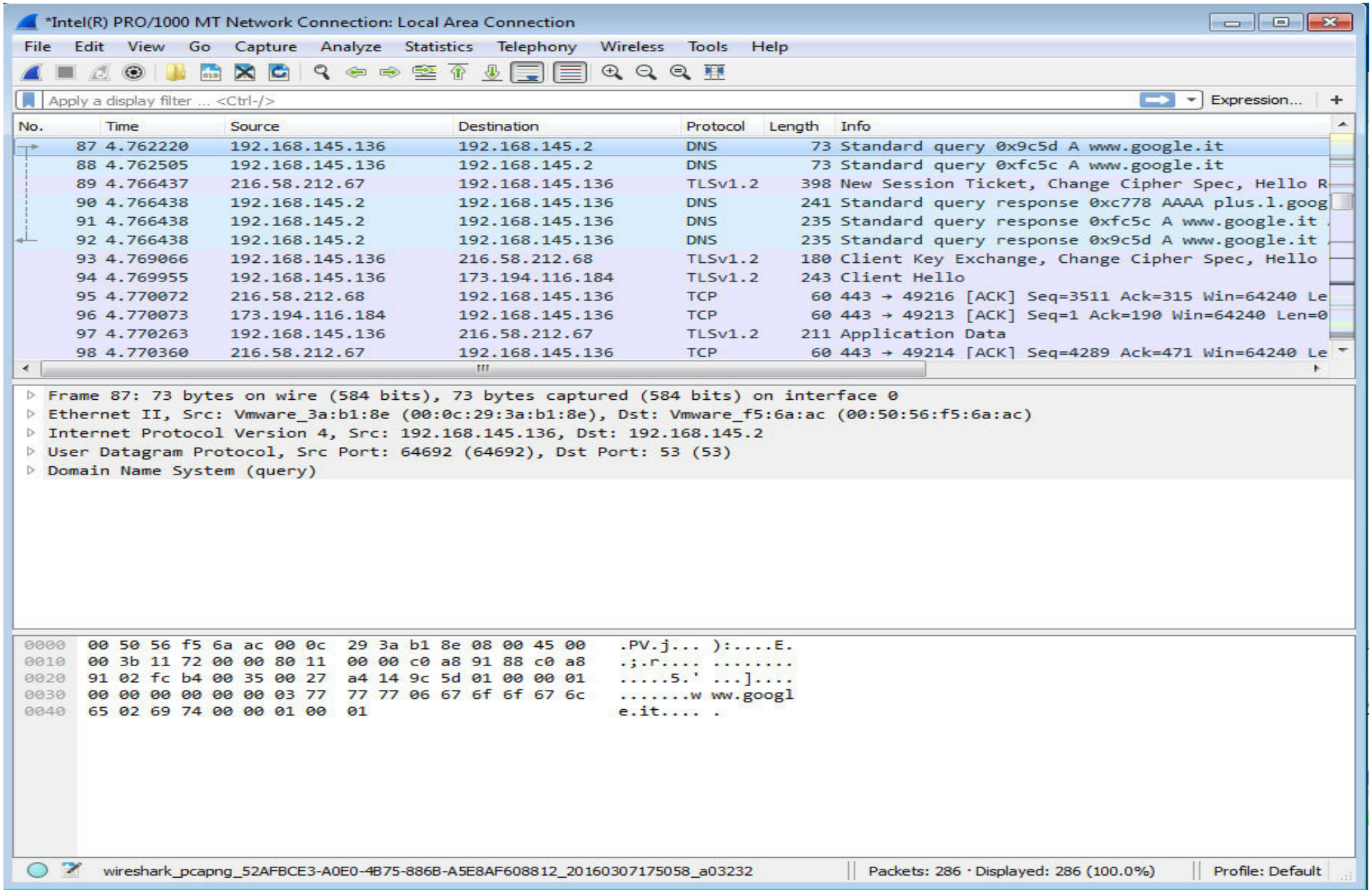
Interfaccia grafica



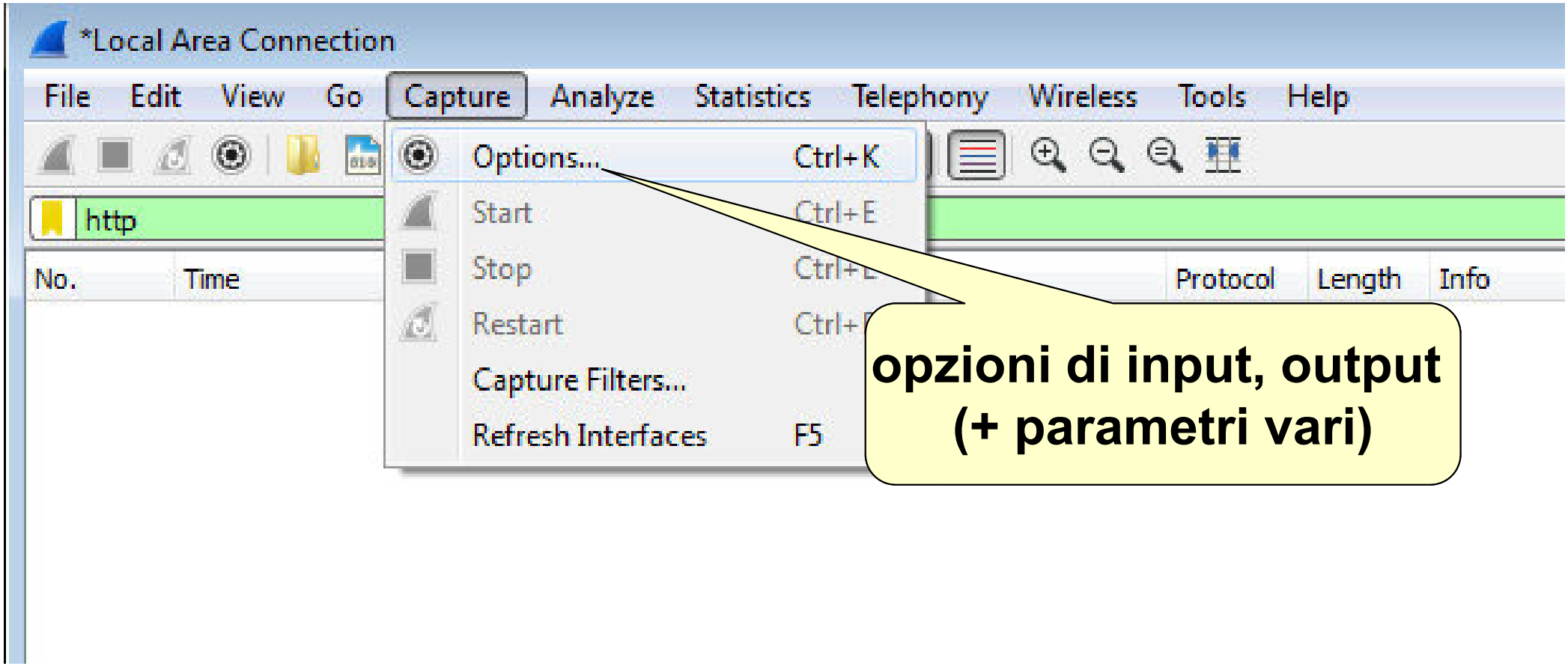
Interfaccia principale



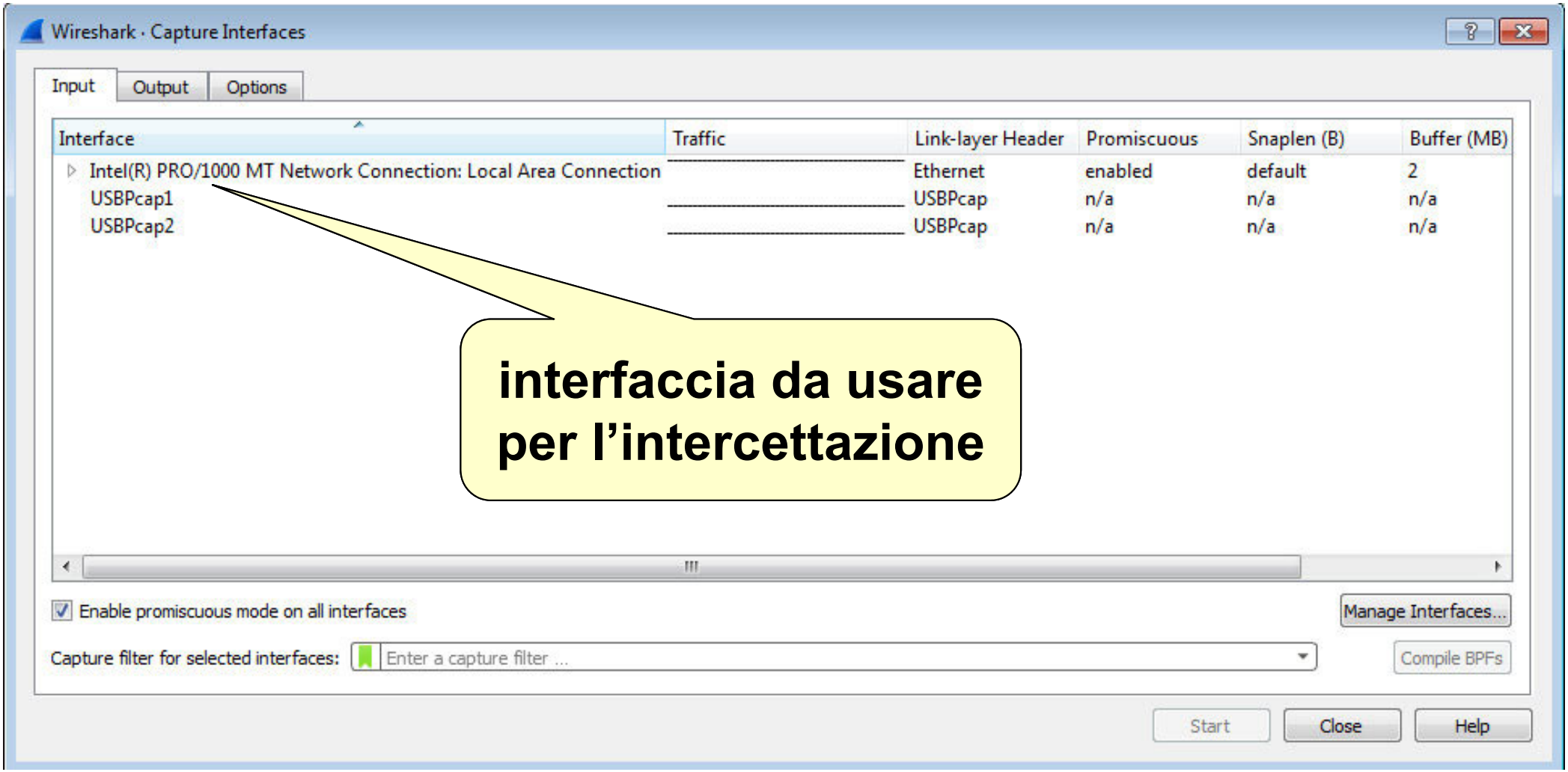
Interfaccia principale



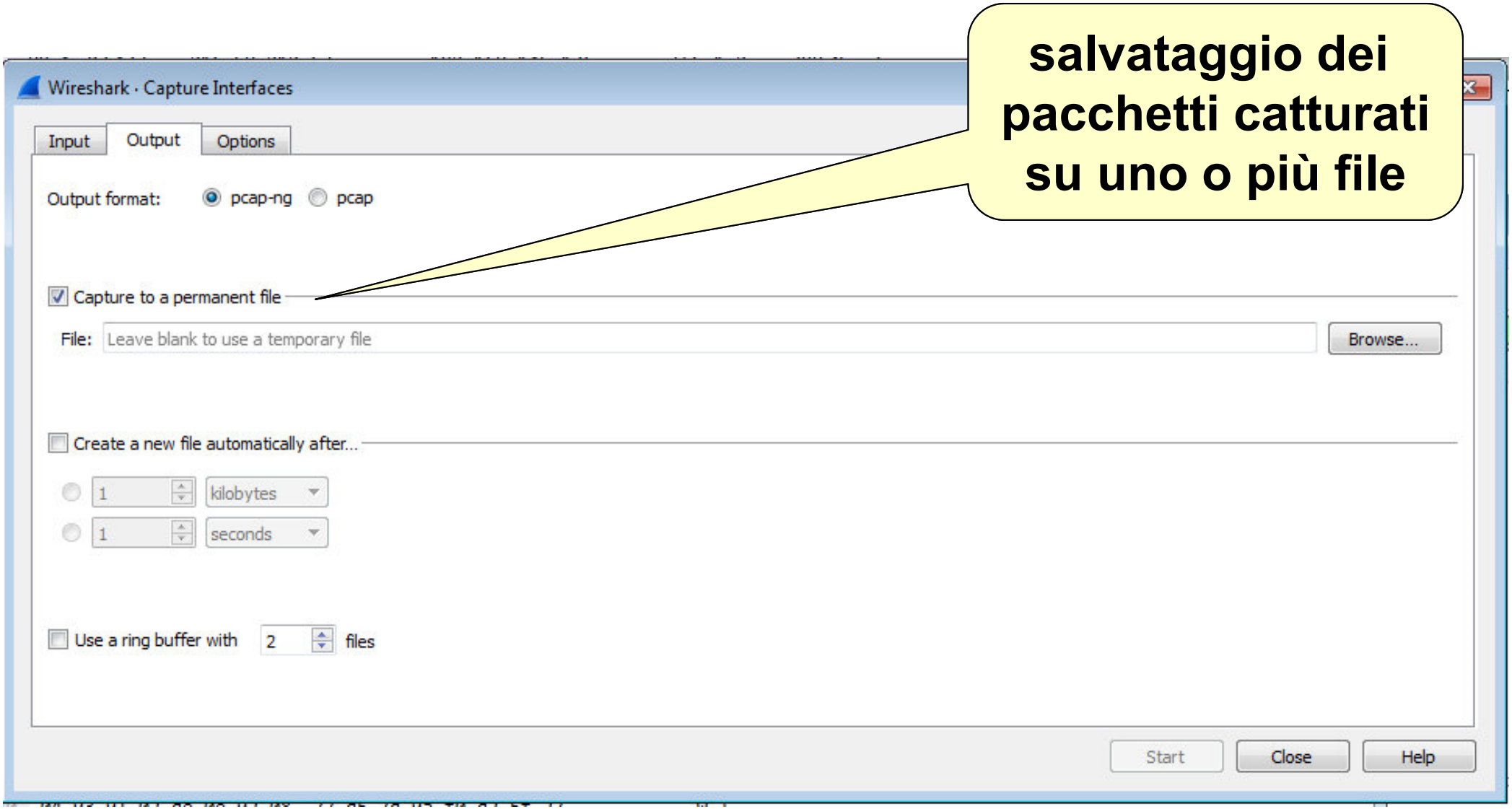
Opzioni per intercettazione



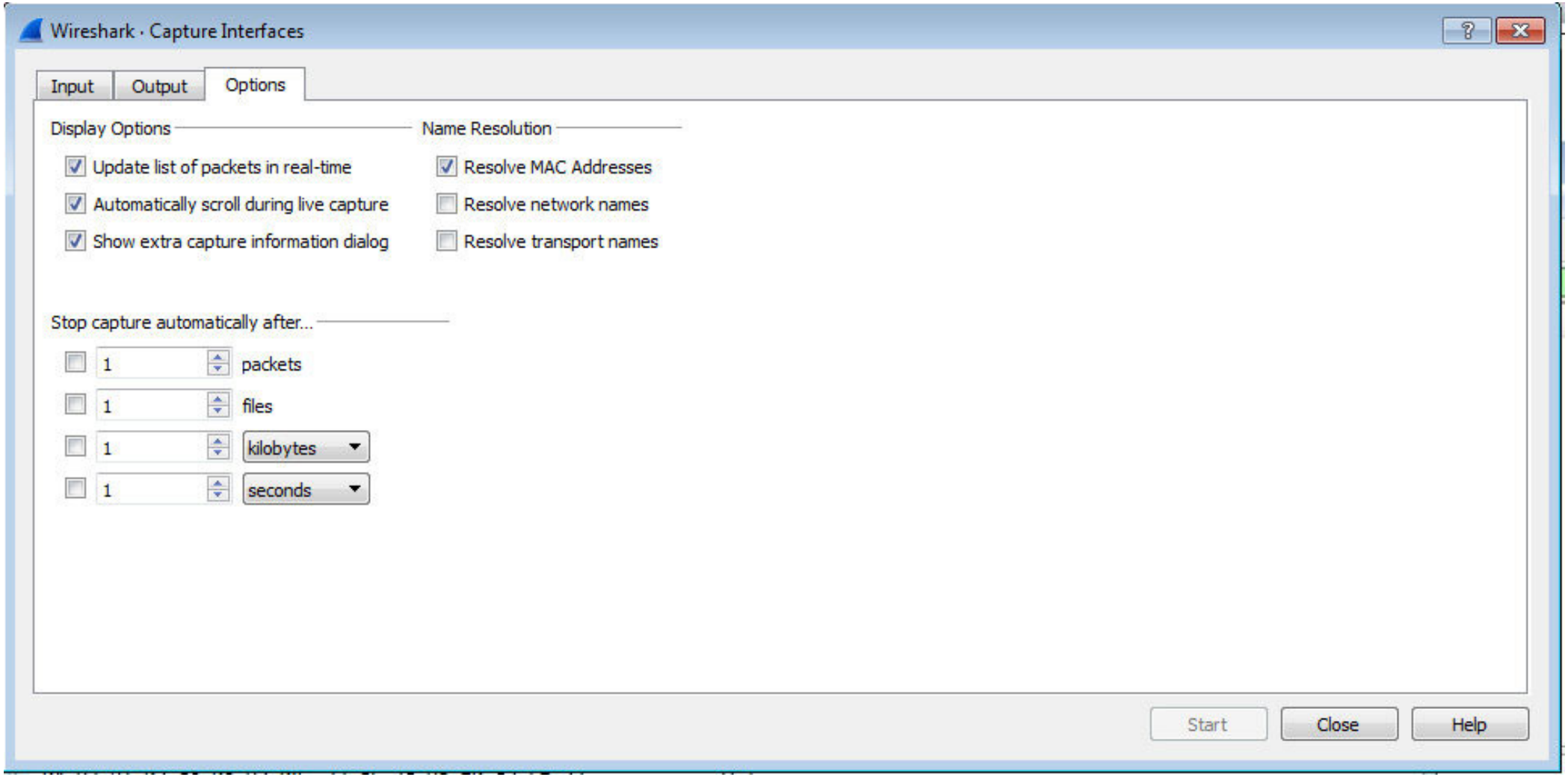
Opzioni per intercettazione



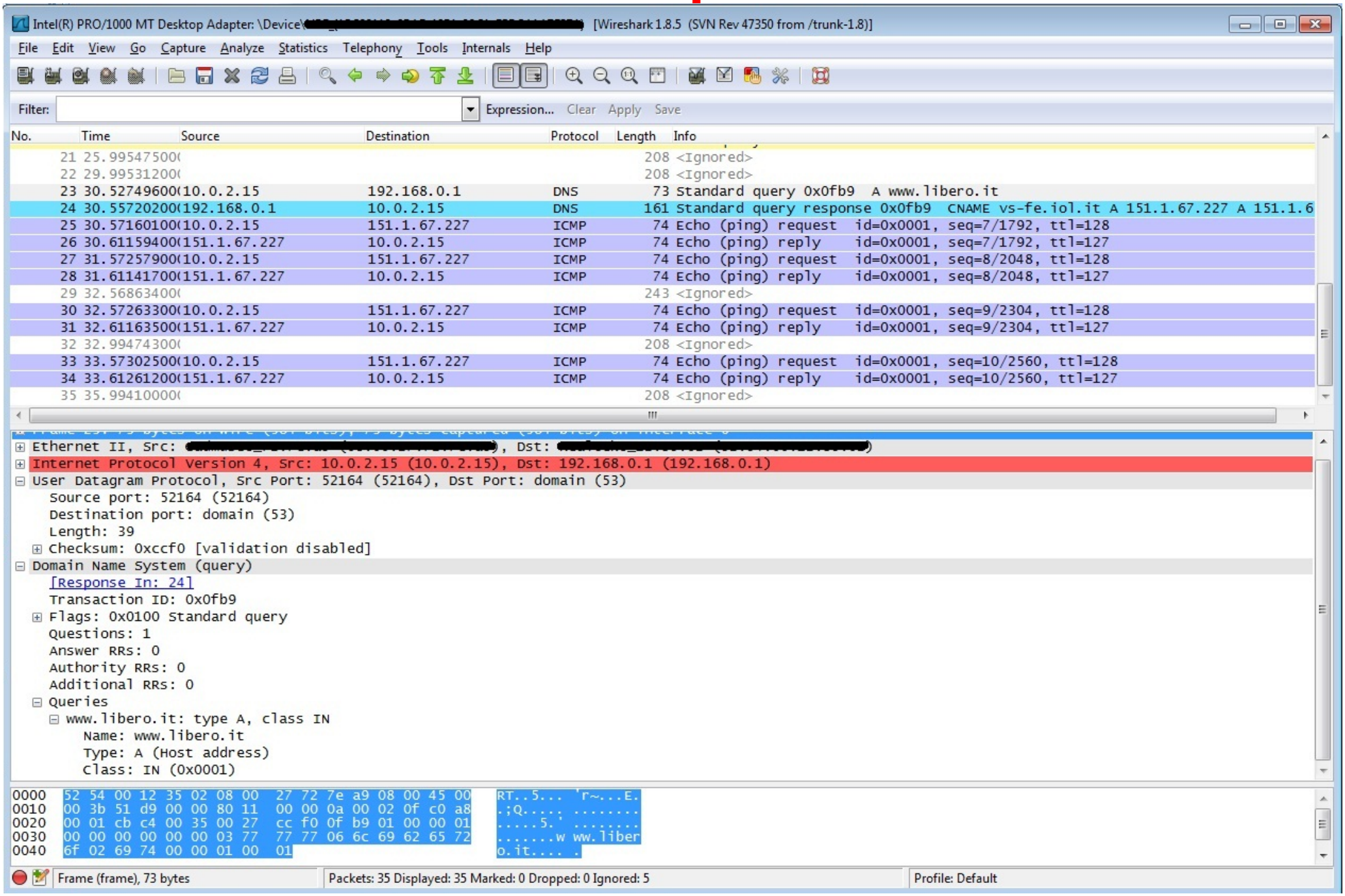
Opzioni per intercettazione



Opzioni per intercettazione



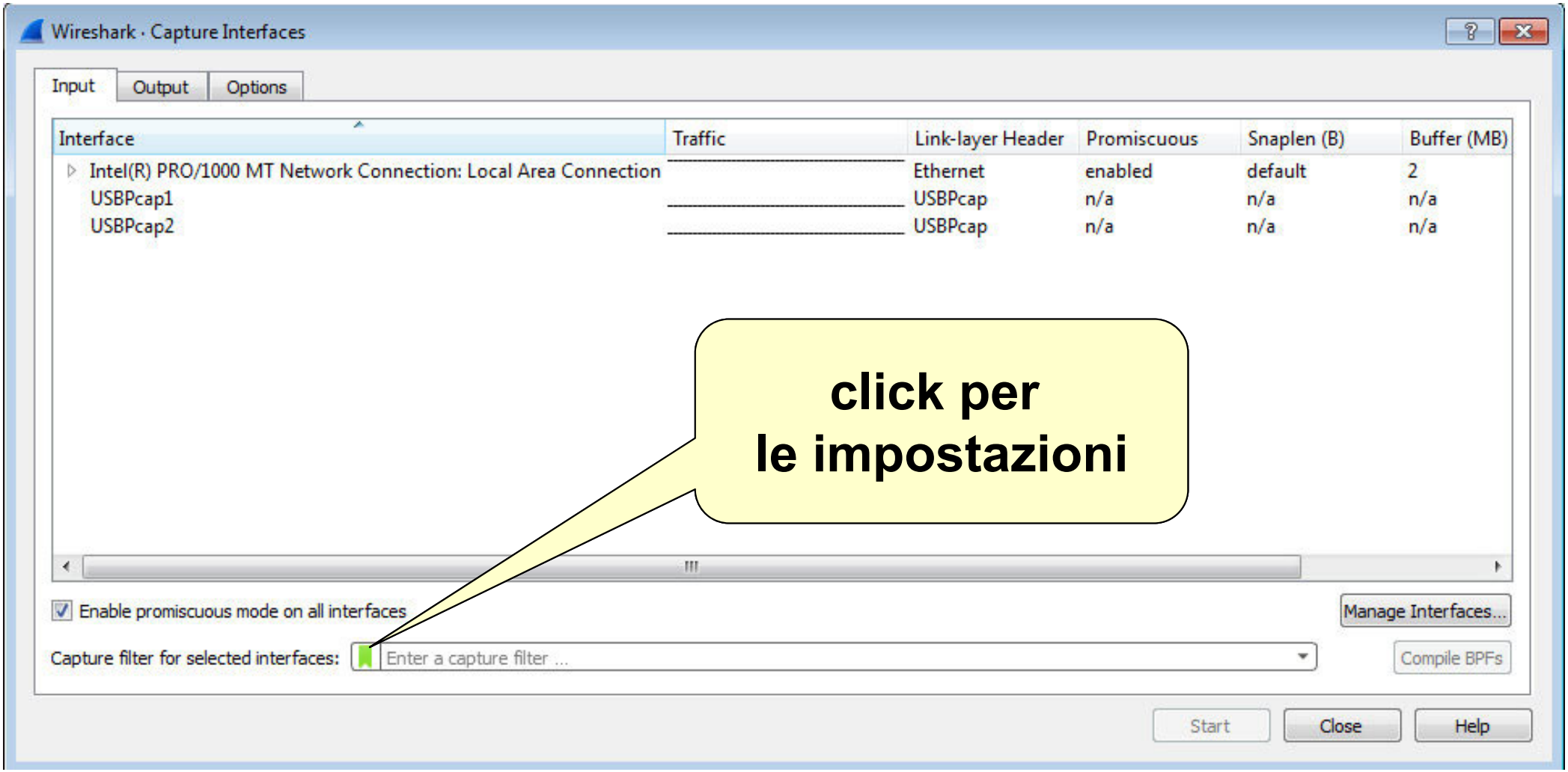
Visualizzazione dei pacchetti catturati



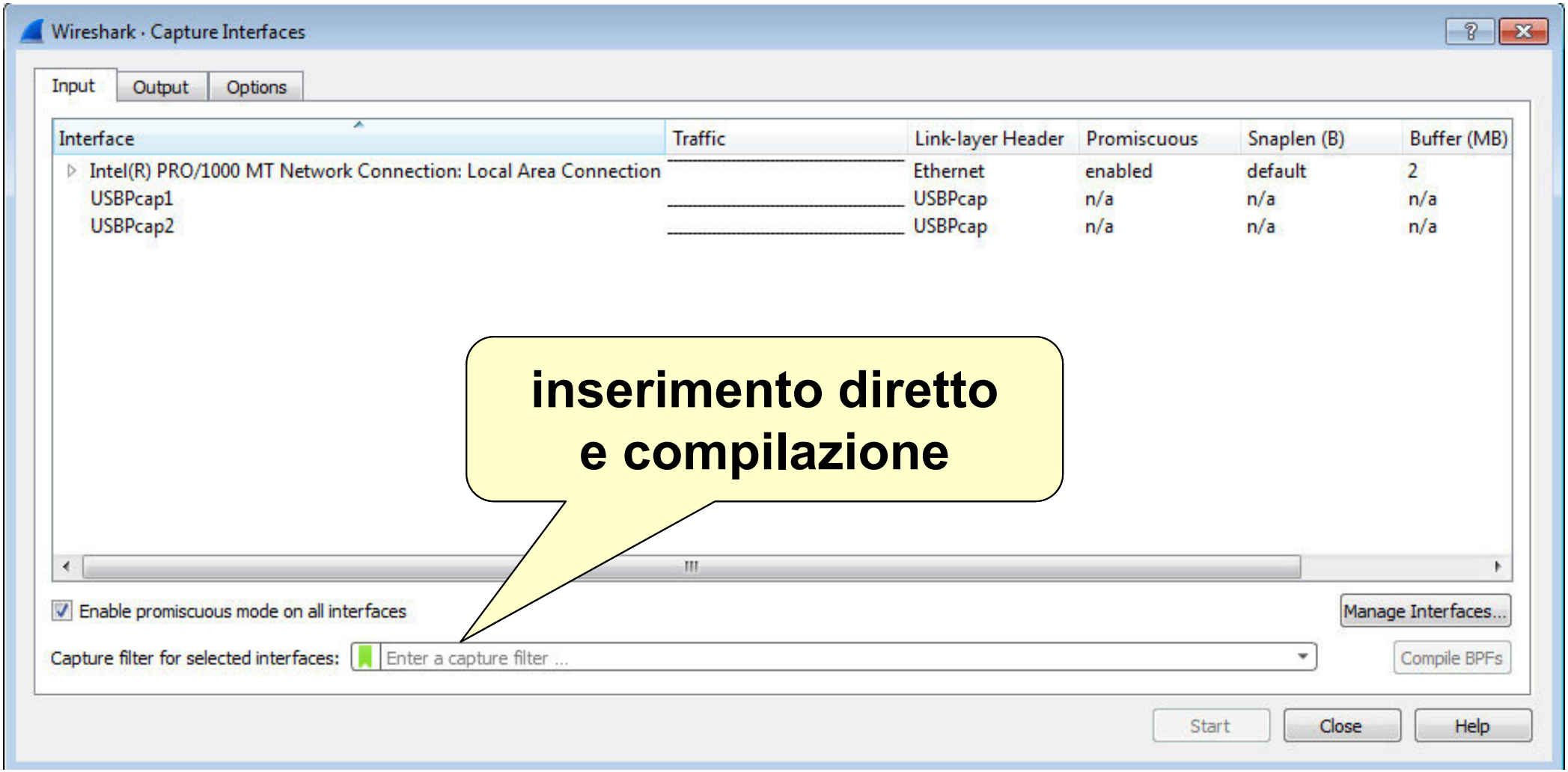
Filtri per intercettazione

- **applicabili prima dell'intercettazione**
- **usati per catturare solo il traffico di interesse**
  - necessario in reti con molto traffico
- **utili per specificare**
  - protocolli
    - udp tcp icmp
  - informazioni specifiche di un pacchetto
    - es. dst host 10.10.10.1, src host 192.168.1.1
  - ...
  - composizione con operatori logici
    - es. host 10.10.10.1 and not (port 80 or port 25)
- **documentazione**
  - http://wiki.wireshark.org/CaptureFilters

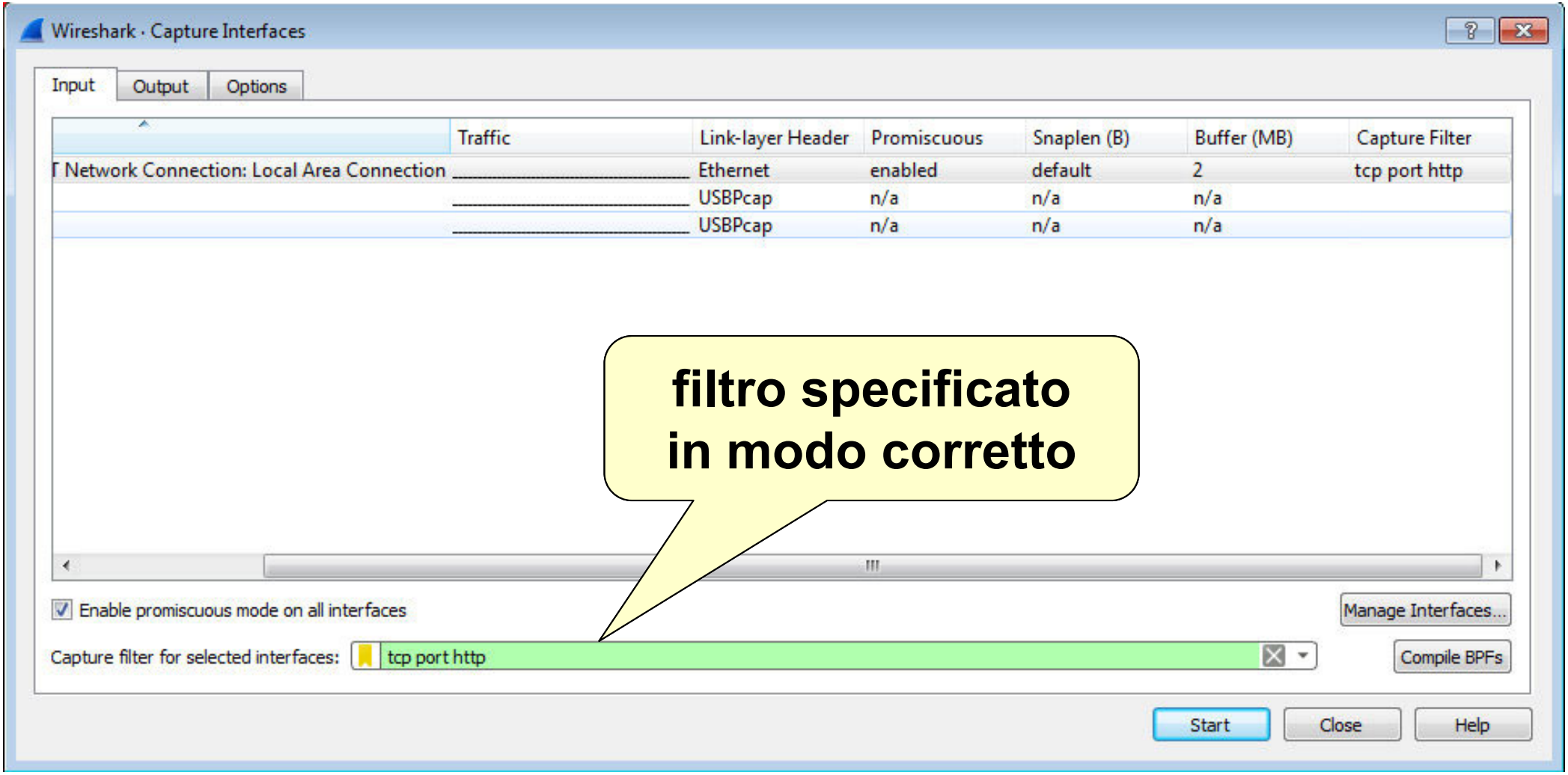
Filtri di intercettazione - esempio



Filtri di intercettazione - esempio



Filtri per intercettazione - esempio

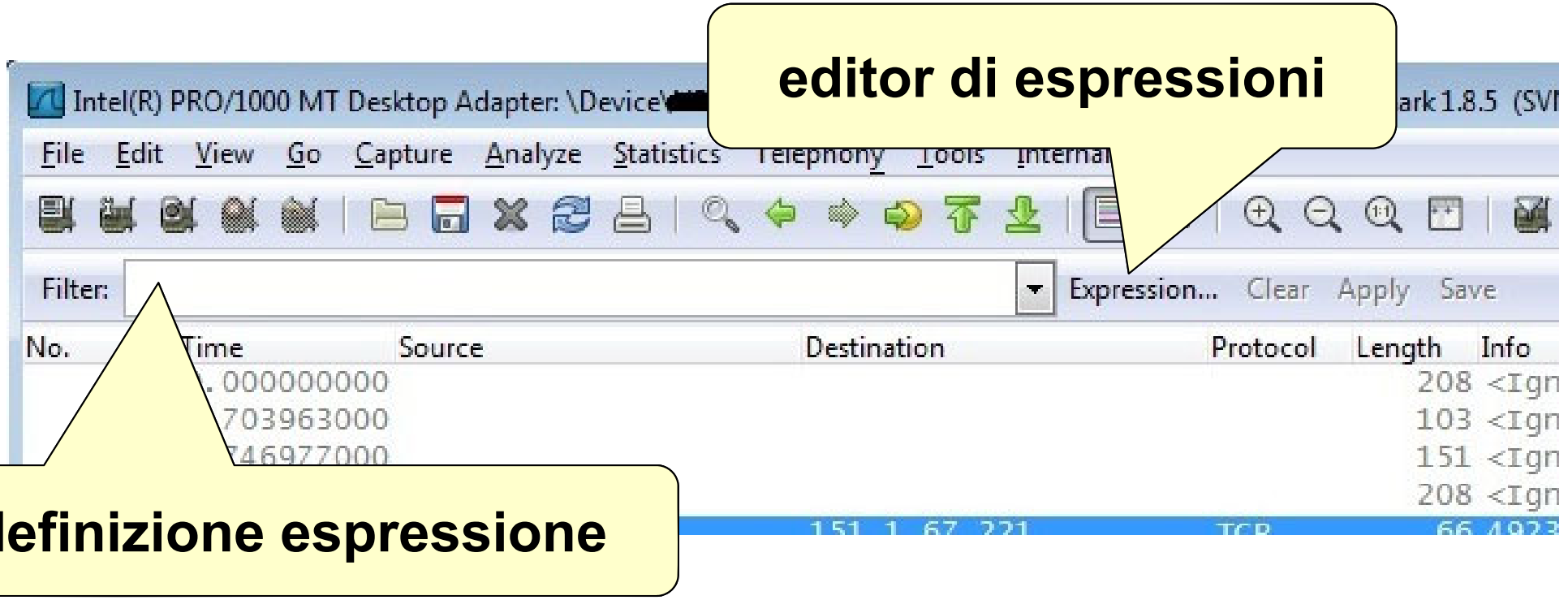


solo pacchetti TCP inviati/ricevuti sulla porta 80/tcp (http)

Filtri per visualizzazione

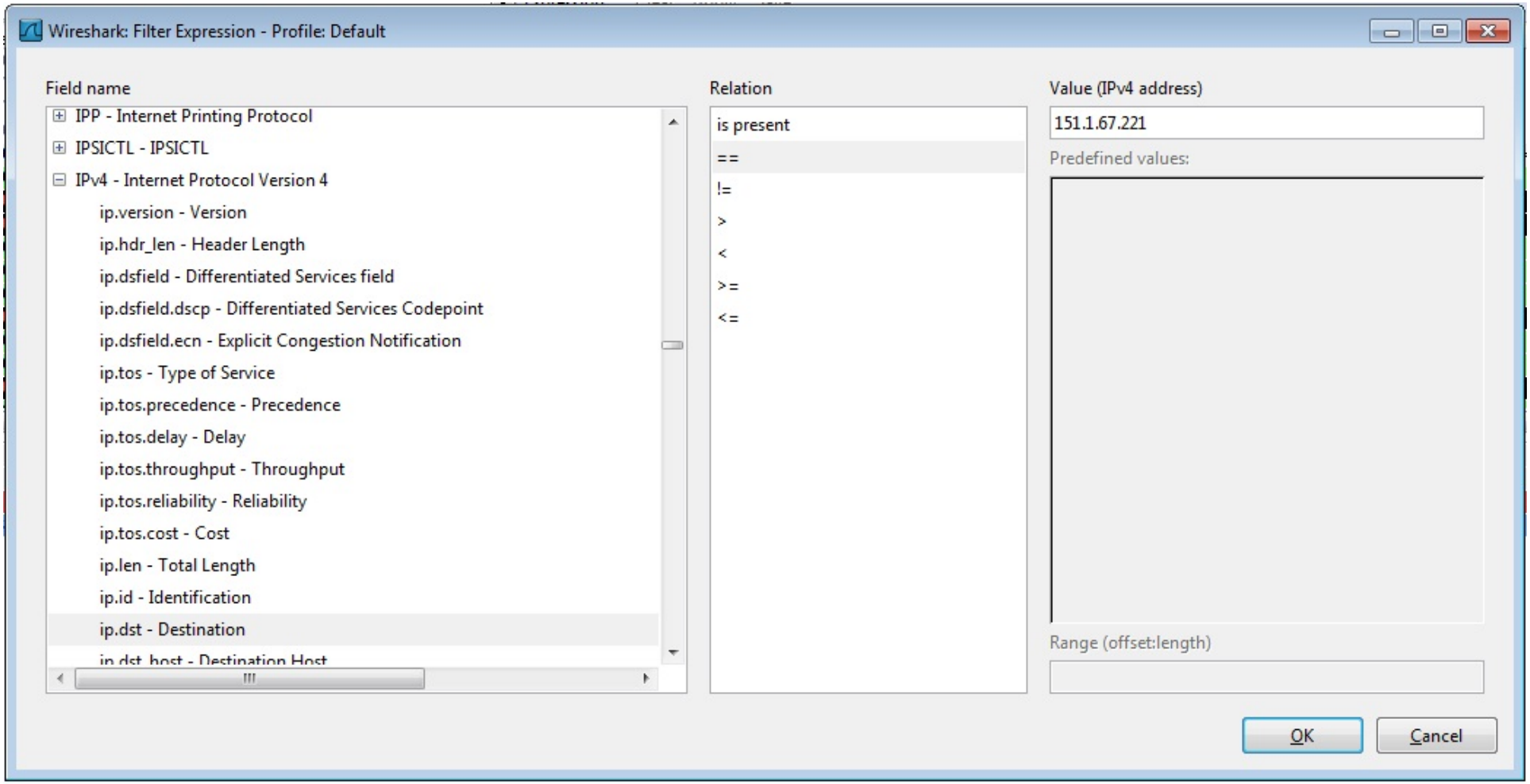
- **applicabili sui pacchetti intercettati**
  - per identificare il traffico di interesse tra quello catturato
  - ATTENZIONE! sintassi diversa dai filtri di cattura
- **utili per specificare**
  - protocolli
    - es. tcp udp icmp
  - informazioni specifiche di un pacchetto
    - es. ip.dst == 10.10.10.1
  - composizione con operatori logici
    - es. ip == 151.1.67.221 && ! (tcp.port eq 80 or tcp.port eq 25)
- **documentazione**
  - http://wiki.wireshark.org/DisplayFilters

Filtri per visualizzazione - esempio



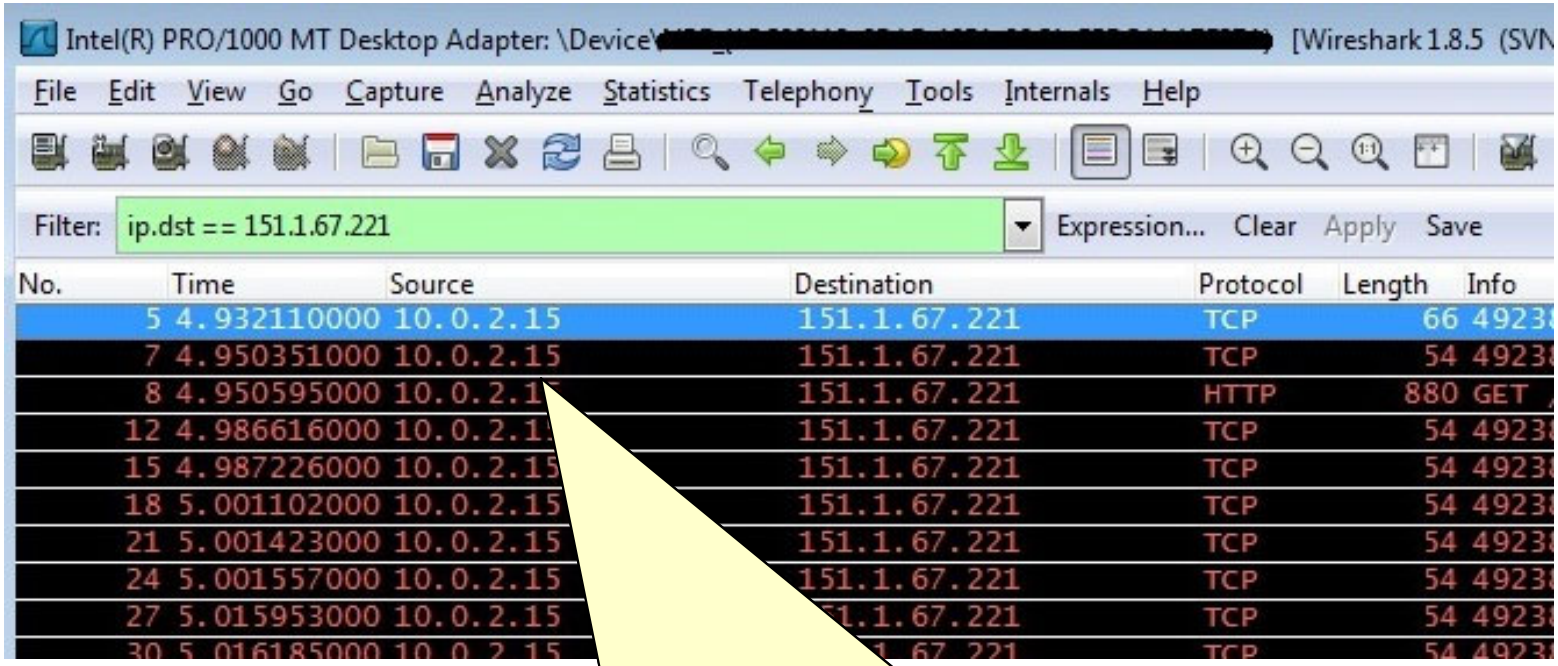
Filtri per visualizzazione - esempio

... usando l'editor definiamo l'espressione …



Filtri per visualizzazione - esempio

... ed applicando l'espressione …

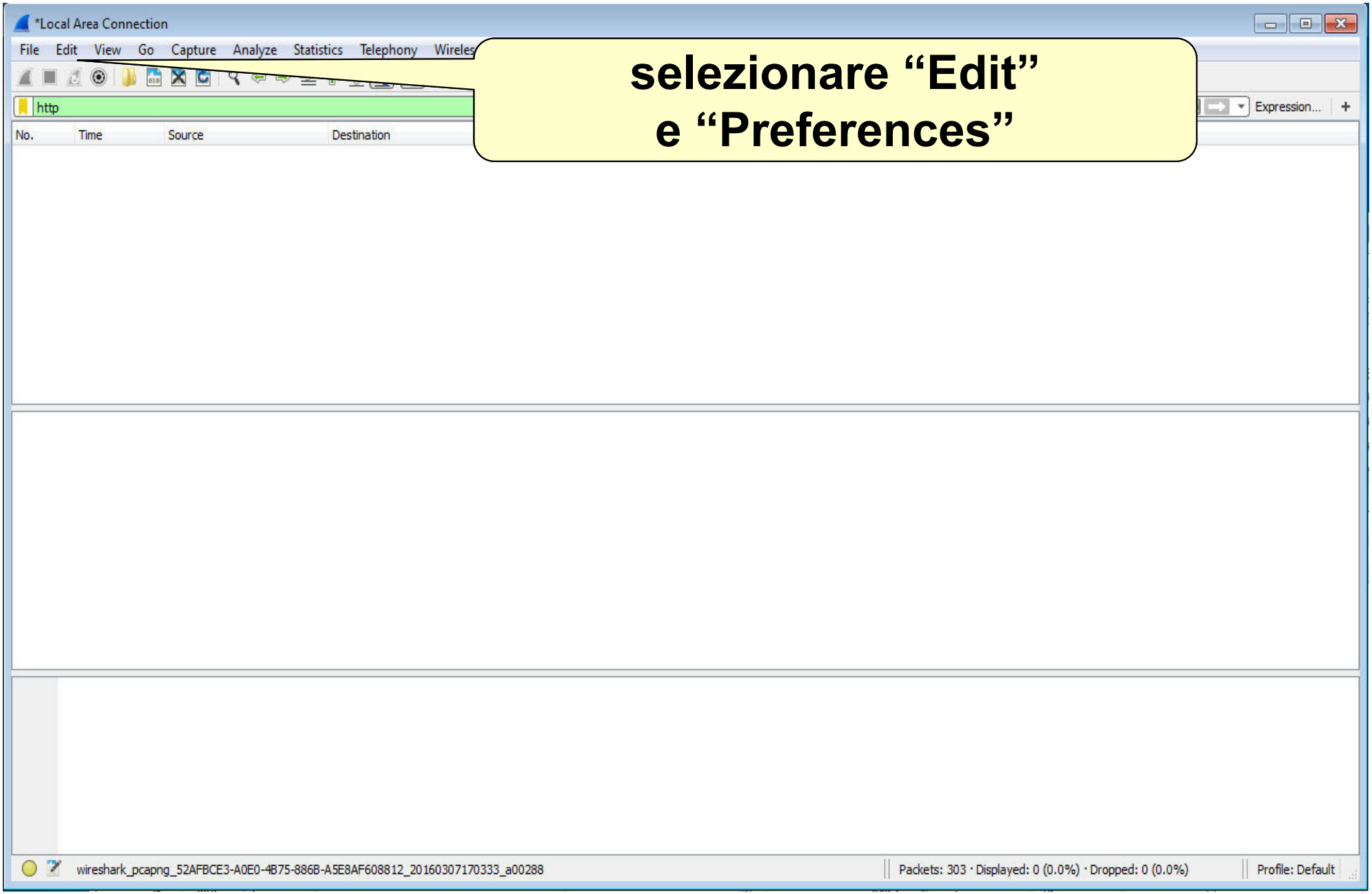


pacchetti che soddisfano l'espressione

Visualizzare elementi aggiuntivi

- **come impostazione di default wireshark visualizza:**
  - ID numerico
  - tempo
  - indirizzo IP sorgente e destinazione
  - protocollo
  - lunghezza del pacchetto (in byte)
  - informazioni sul pacchetto
    - es: “TCP segment of a reassembled PDU”
- **è possibile aggiungere ulteriori colonne**
  - per visualizzare ulteriori campi del pacchetto
    - eventualmente anche non previsti (opzione “custom”)

Aggiunta colonne di visualizzazione



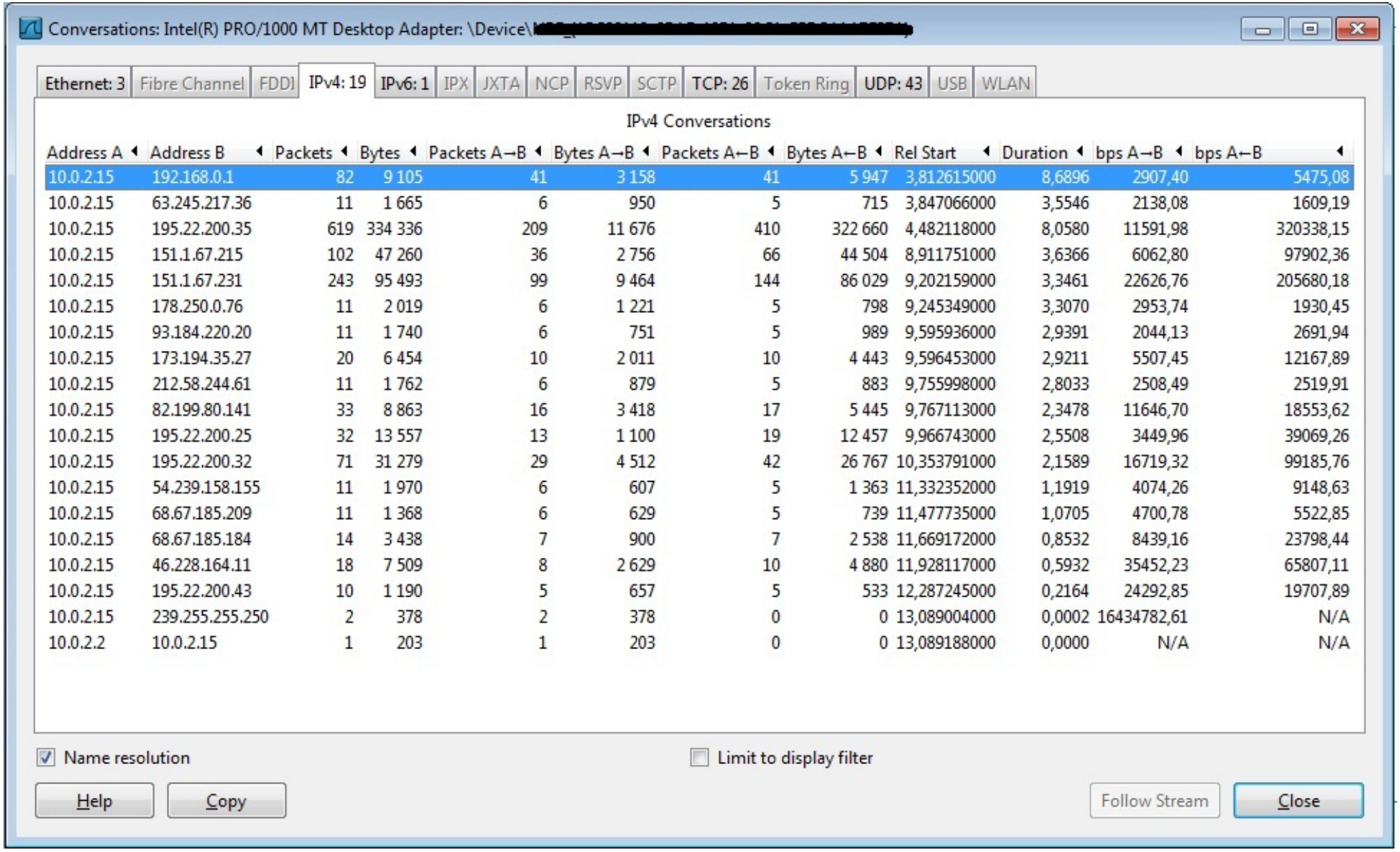
Aggiunta colonne di visualizzazione

Isolare una "network conversation"

- **"network conversation" = comunicazione di rete**
  - traffico scambiato da due specifici endpoint
    - es. indirizzi IP, indirizzi IP + protocollo, …
- **utile per restringere le analisi tra due endpoint**
  - traffico scambiato tra due indirizzi IP
  - traffico scambiato per una quintupla
  - …
- **soluzioni:**
  - definizione manuale di filtri (per l'intercettazione o per la visualizzazione)
  - definizione assistita di filtri attraverso l'interfaccia *Conversations*

Interfaccia Conversations

- **Statistics → Conversations**



Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	Duration	bps A→B	bps A←B
10.0.2.15	192.168.0.1	82	9 105	41	3 158	41	5 947	3,812615000	8,6896	2907,40	5475,08
10.0.2.15	63.245.217.36	11	1 665	6	950	5	715	3,847066000	3,5546	2138,08	1609,19
10.0.2.15	195.22.200.35	619	334 336	209	11 676	410	322 660	4,482118000	8,0580	11591,98	320338,15
10.0.2.15	151.1.67.215	102	47 260	36	2 756	66	44 504	8,911751000	3,6366	6062,80	97902,36
10.0.2.15	151.1.67.231	243	95 493	99	9 464	144	86 029	9,202159000	3,3461	22626,76	205680,18
10.0.2.15	178.250.0.76	11	2 019	6	1 221	5	798	9,245349000	3,3070	2953,74	1930,45
10.0.2.15	93.184.220.20	11	1 740	6	751	5	989	9,595936000	2,9391	2044,13	2691,94
10.0.2.15	173.194.35.27	20	6 454	10	2 011	10	4 443	9,596453000	2,9211	5507,45	12167,89
10.0.2.15	212.58.244.61	11	1 762	6	879	5	883	9,755998000	2,8033	2508,49	2519,91
10.0.2.15	82.199.80.141	33	8 863	16	3 418	17	5 445	9,767113000	2,3478	11646,70	18553,62
10.0.2.15	195.22.200.25	32	13 557	13	1 100	19	12 457	9,966743000	2,5508	3449,96	39069,26
10.0.2.15	195.22.200.32	71	31 279	29	4 512	42	26 767	10,353791000	2,1589	16719,32	99185,76
10.0.2.15	54.239.158.155	11	1 970	6	607	5	1 363	11,332352000	1,1919	4074,26	9148,63
10.0.2.15	68.67.185.209	11	1 368	6	629	5	739	11,477735000	1,0705	4700,78	5522,85
10.0.2.15	68.67.185.184	14	3 438	7	900	7	2 538	11,669172000	0,8532	8439,16	23798,44
10.0.2.15	46.228.164.11	18	7 509	8	2 629	10	4 880	11,928117000	0,5932	35452,23	65807,11
10.0.2.15	195.22.200.43	10	1 190	5	657	5	533	12,287245000	0,2164	24292,85	19707,89
10.0.2.15	239.255.255.250	2	378	2	378	0	0	13,089004000	0,0002	16434782,61	N/A
10.0.2.2	10.0.2.15	1	203	1	203	0	0	13,089188000	0,0000	N/A	N/A

Interfaccia Conversations

- **Statistics → Conversations**