

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” ...

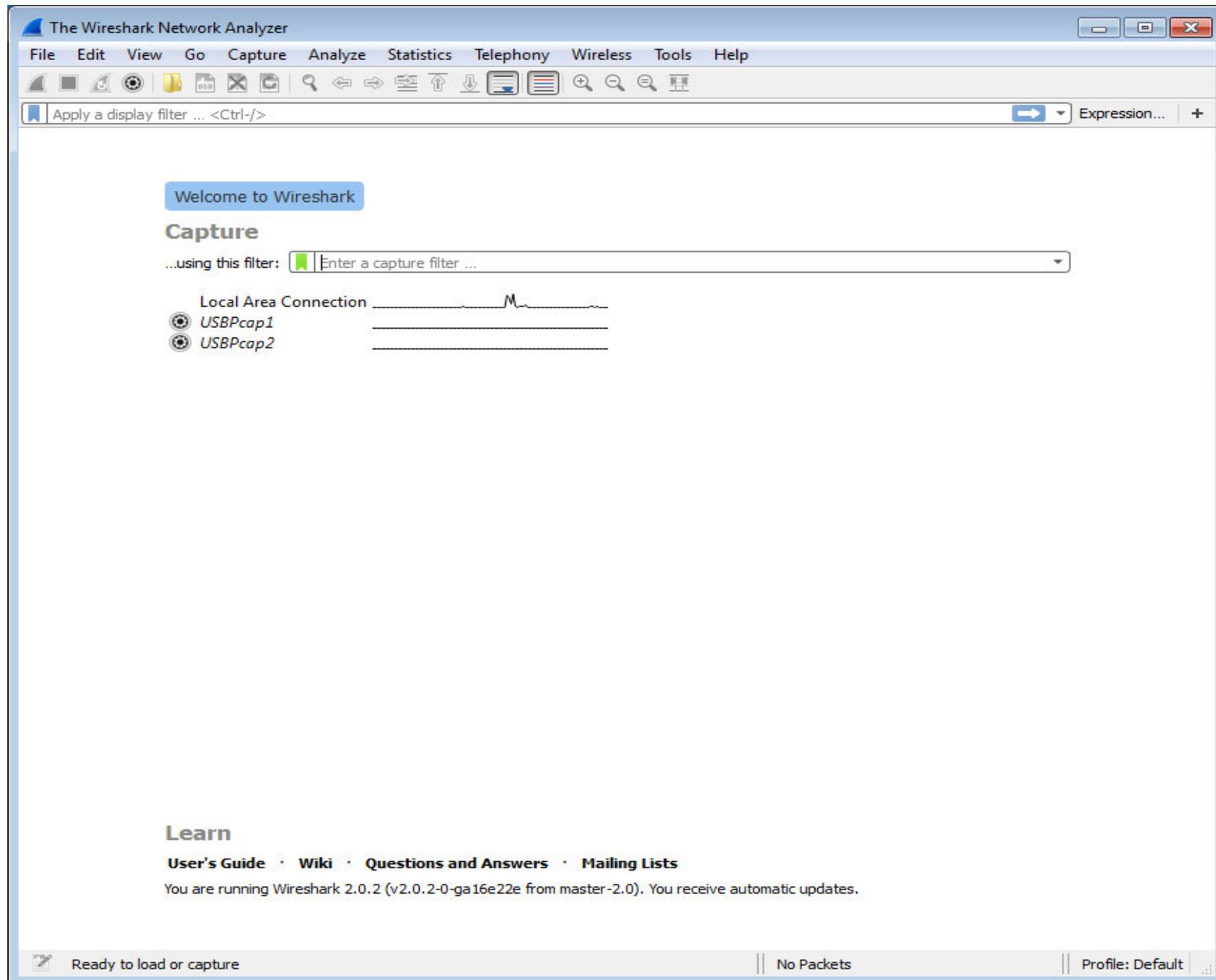
■ modalità normale

- solo traffico destinato alla scheda di rete (identificata attraverso l'indirizzo MAC)

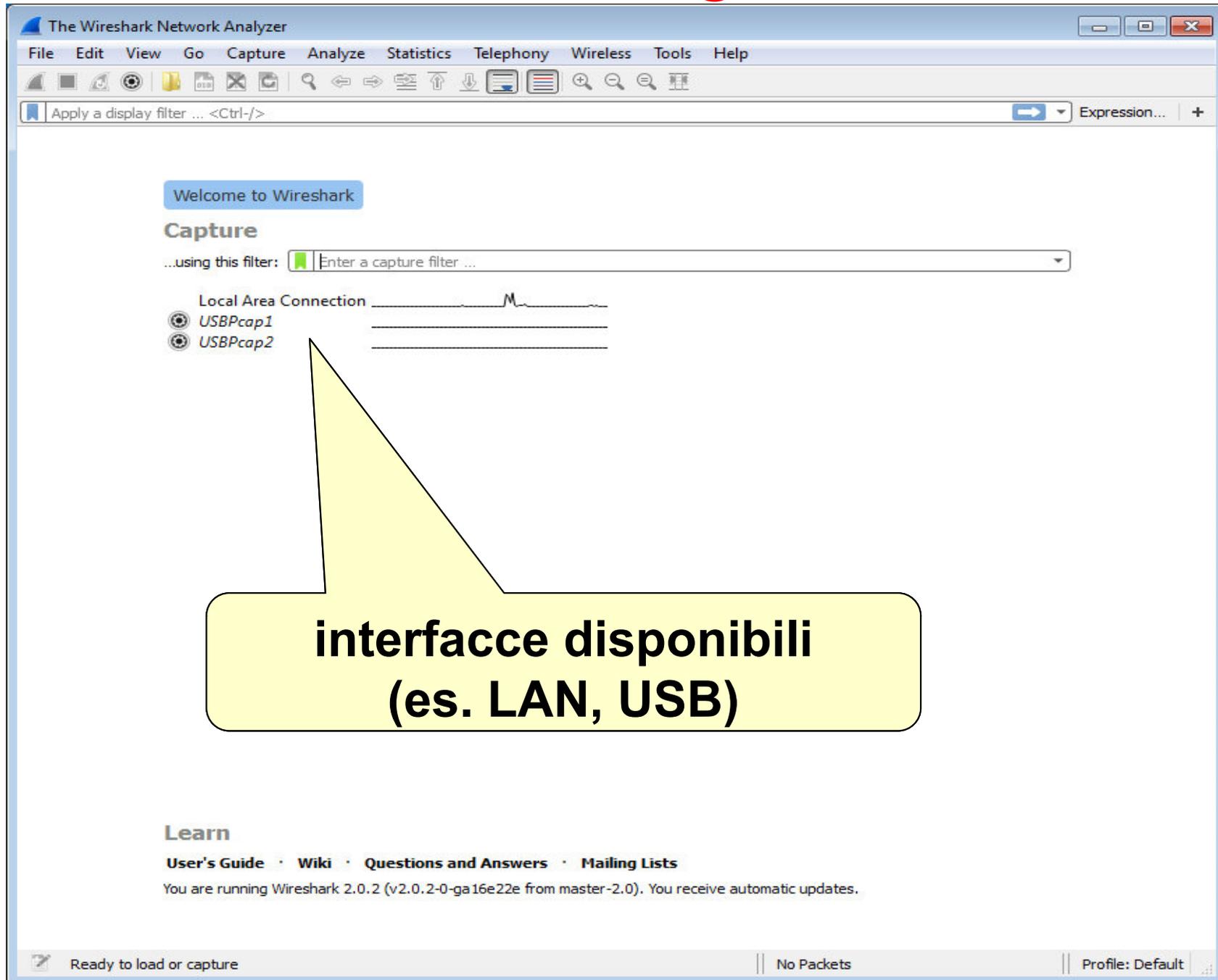
■ modalità “promiscua” (*Monitor Mode*)

- 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!

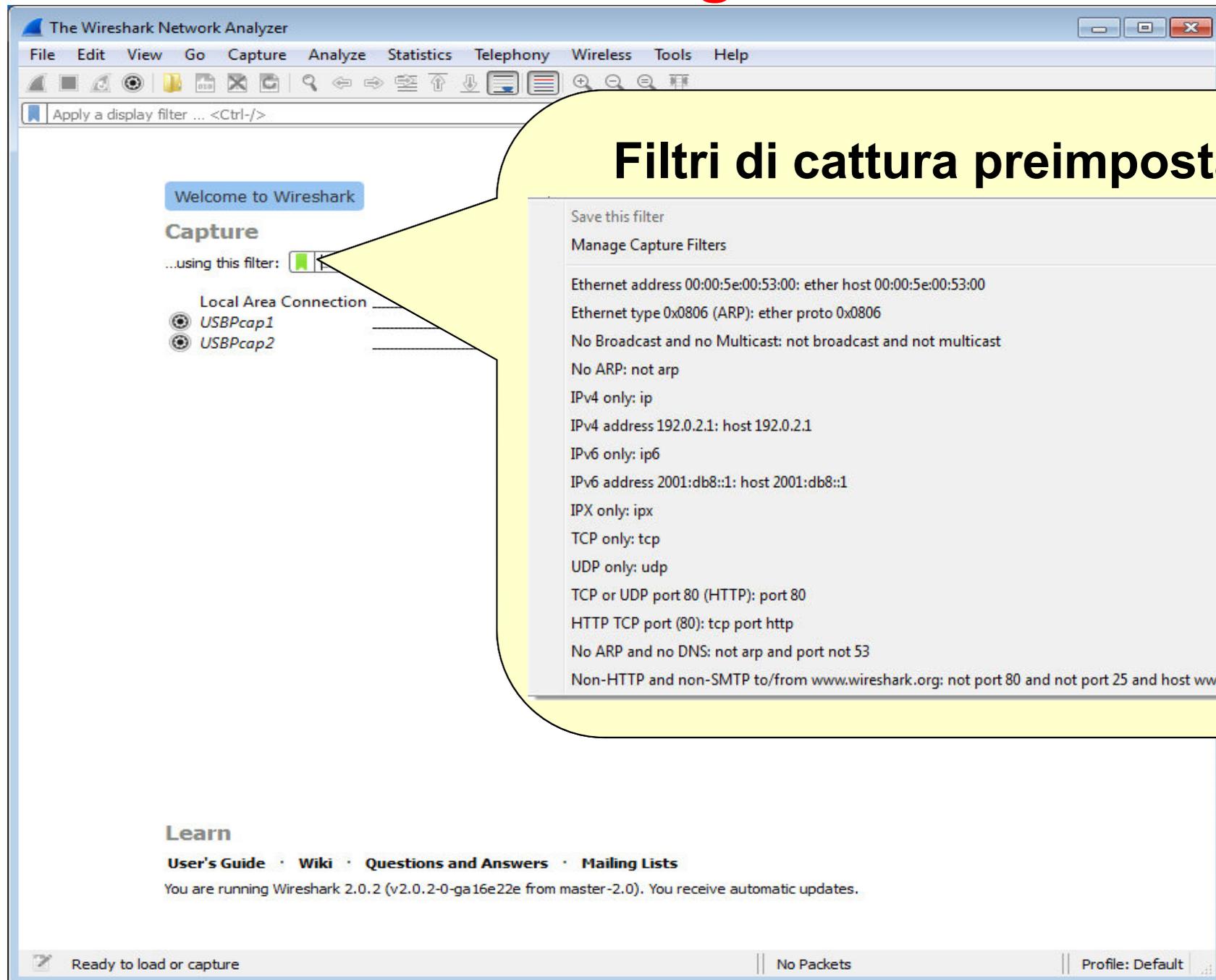
Interfaccia iniziale



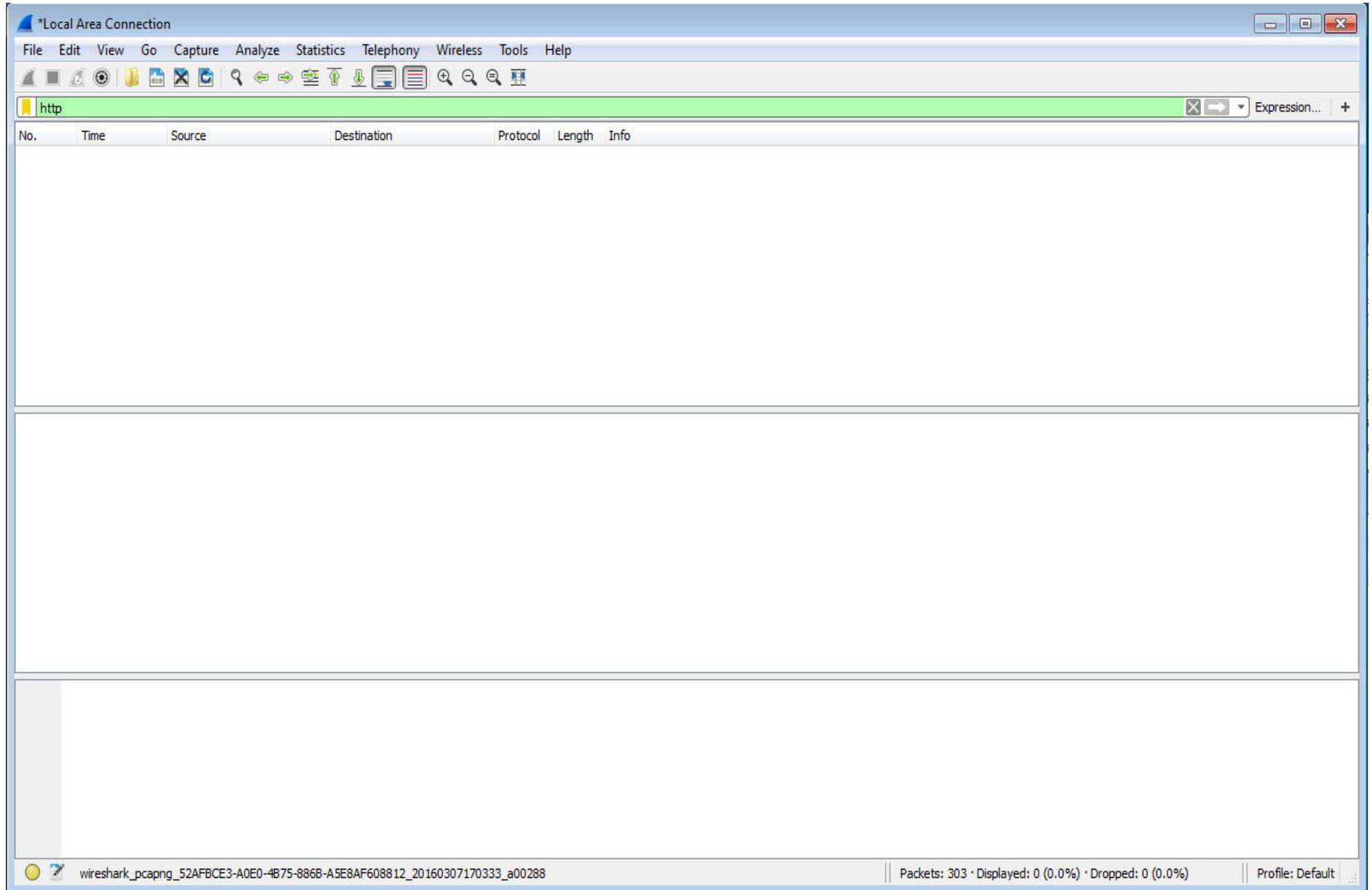
Interfaccia grafica



Interfaccia grafica



Interfaccia principale



Interfaccia principale

The screenshot displays the main interface of Wireshark, titled '*Intel(R) PRO/1000 MT Network Connection: Local Area Connection'. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons for file operations, capture control, and analysis. A display filter is set to 'Apply a display filter ... <Ctrl-/>'. The main pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 87 is selected, and its details pane shows the following structure:

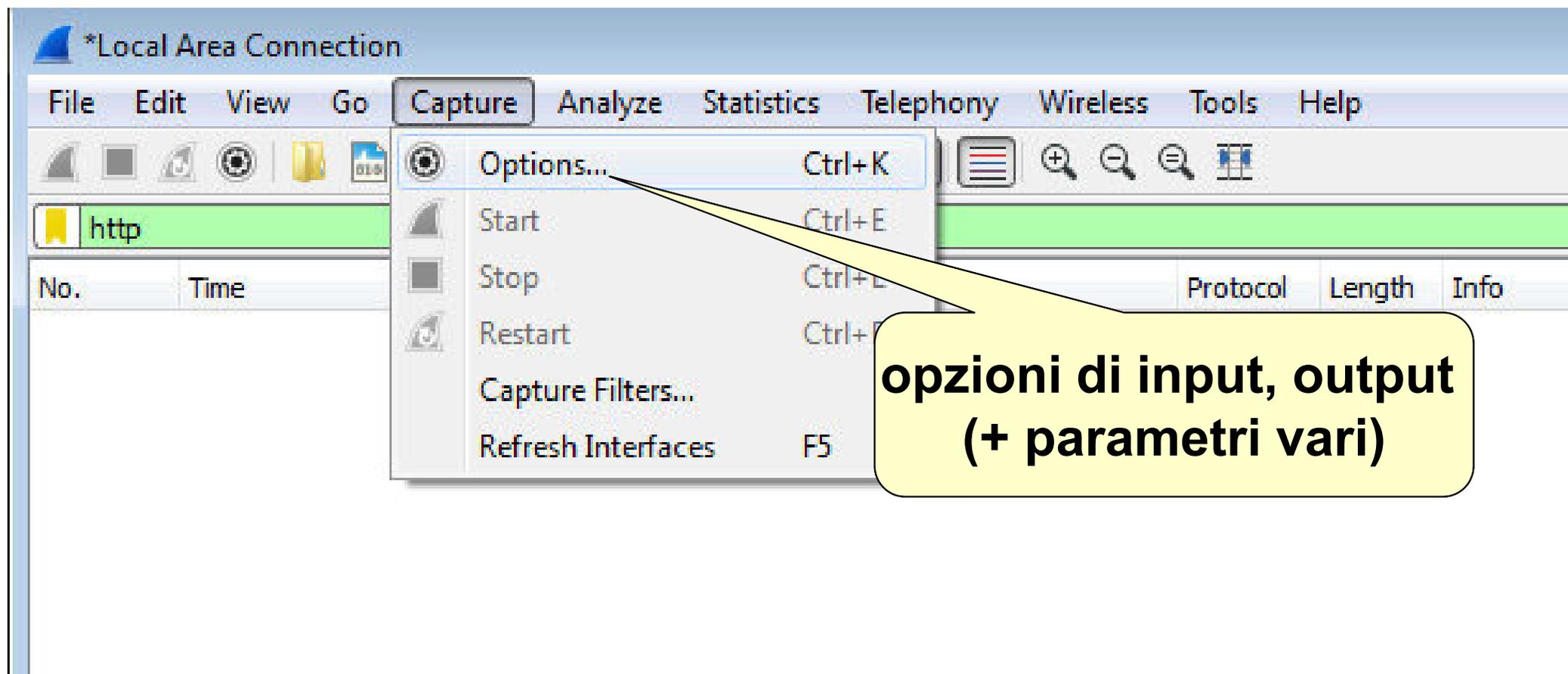
- Frame 87: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
- Ethernet II, Src: Vmware_3a:b1:8e (00:0c:29:3a:b1:8e), Dst: Vmware_f5:6a:ac (00:50:56:f5:6a:ac)
- Internet Protocol Version 4, Src: 192.168.145.136, Dst: 192.168.145.2
- User Datagram Protocol, Src Port: 64692 (64692), Dst Port: 53 (53)
- Domain Name System (query)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

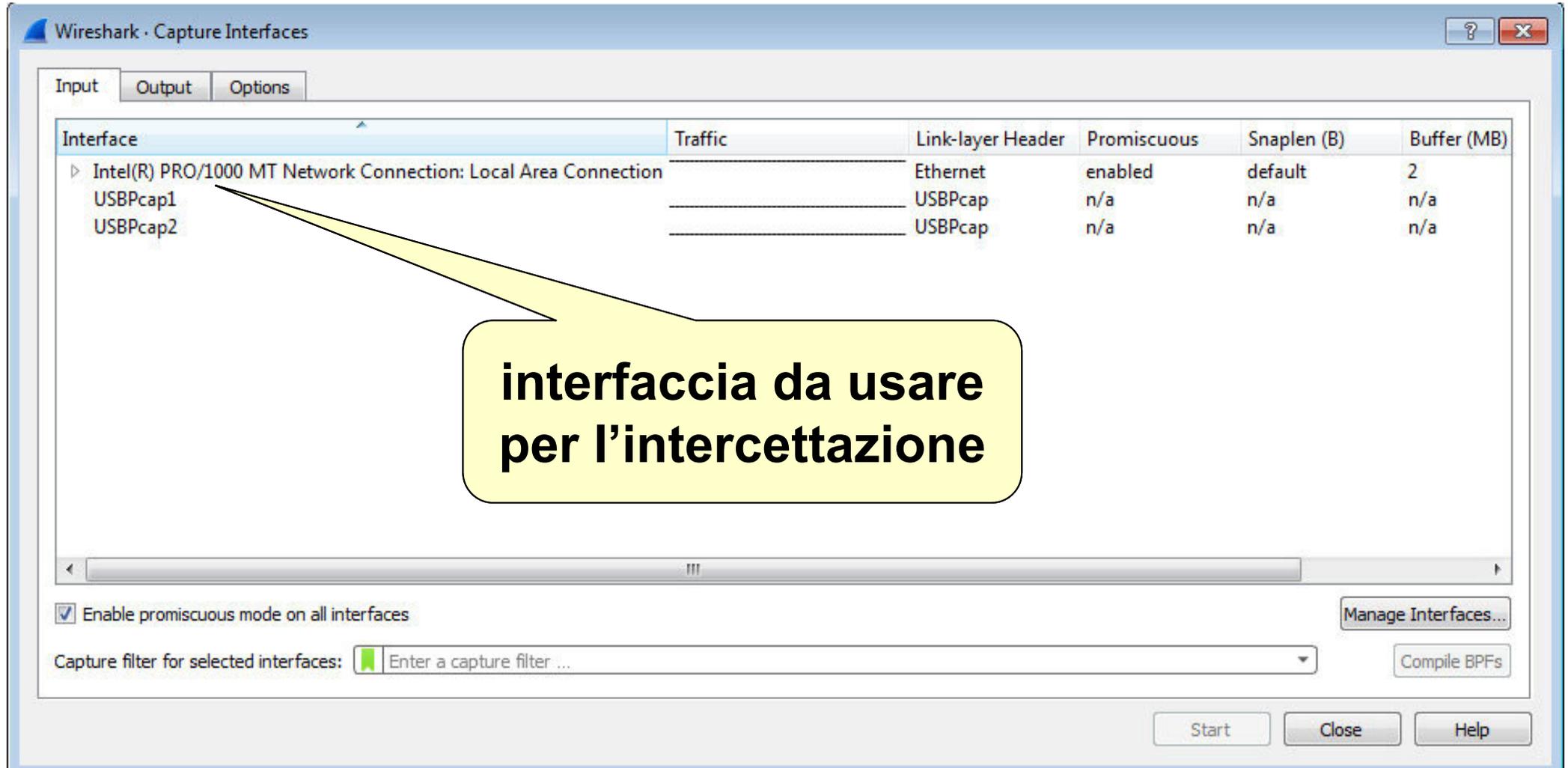
```
0000  00 50 56 f5 6a ac 00 0c 29 3a b1 8e 08 00 45 00  .PV.j... ):....E.
0010  00 3b 11 72 00 00 80 11 00 00 c0 a8 91 88 c0 a8  .;.r....
0020  91 02 fc b4 00 35 00 27 a4 14 9c 5d 01 00 00 01  .....5.' ...]....
0030  00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c  .....w ww.googl
0040  65 02 69 74 00 00 01 00 01  e.it....
```

The status bar at the bottom indicates 'wireshark_pcapng_52AFBCE3-A0E0-4B75-886B-A5E8AF608812_20160307175058_a03232', 'Packets: 286 · Displayed: 286 (100.0%)', and 'Profile: Default'.

Opzioni per intercettazione

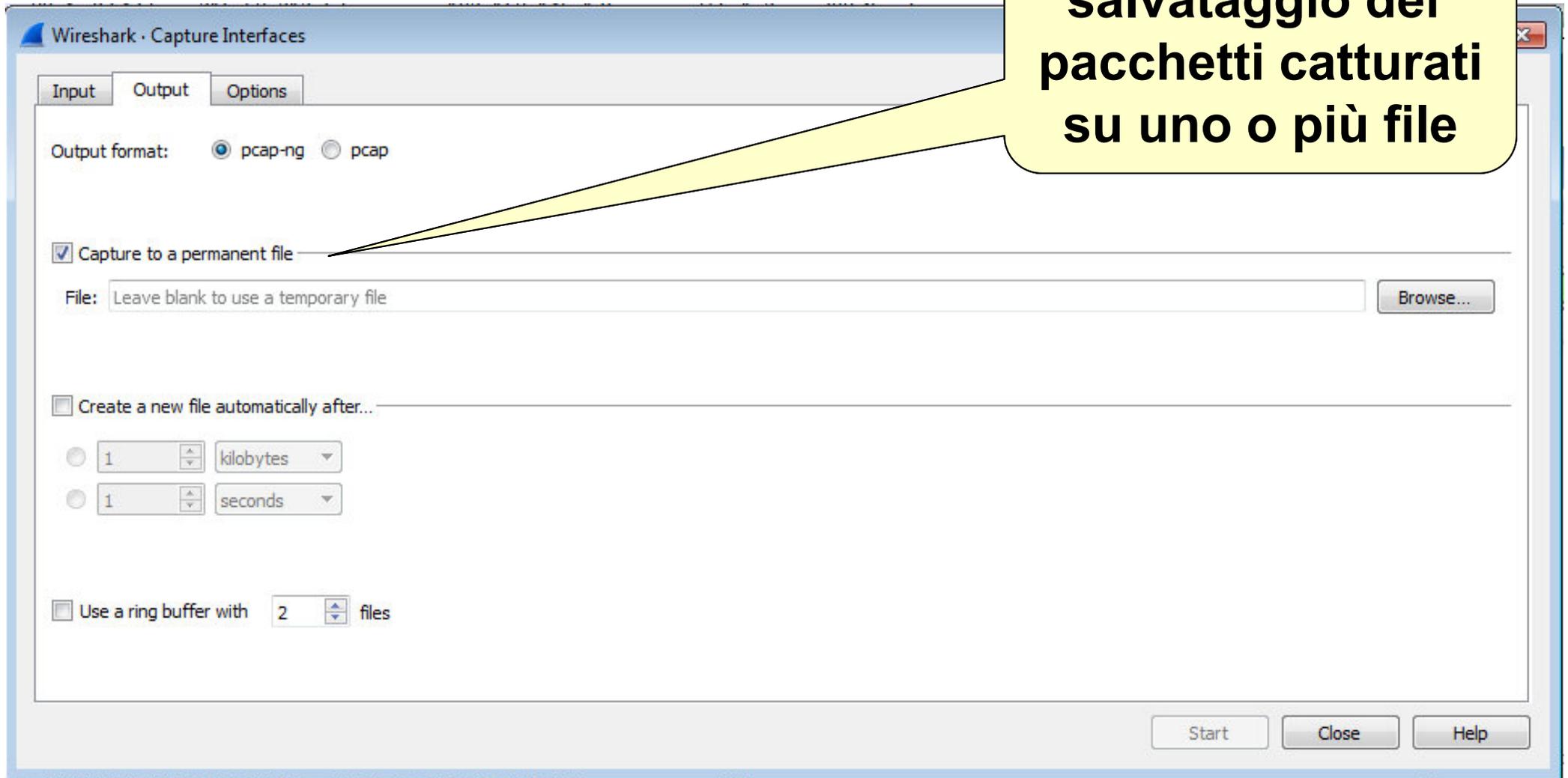


Opzioni per intercettazione

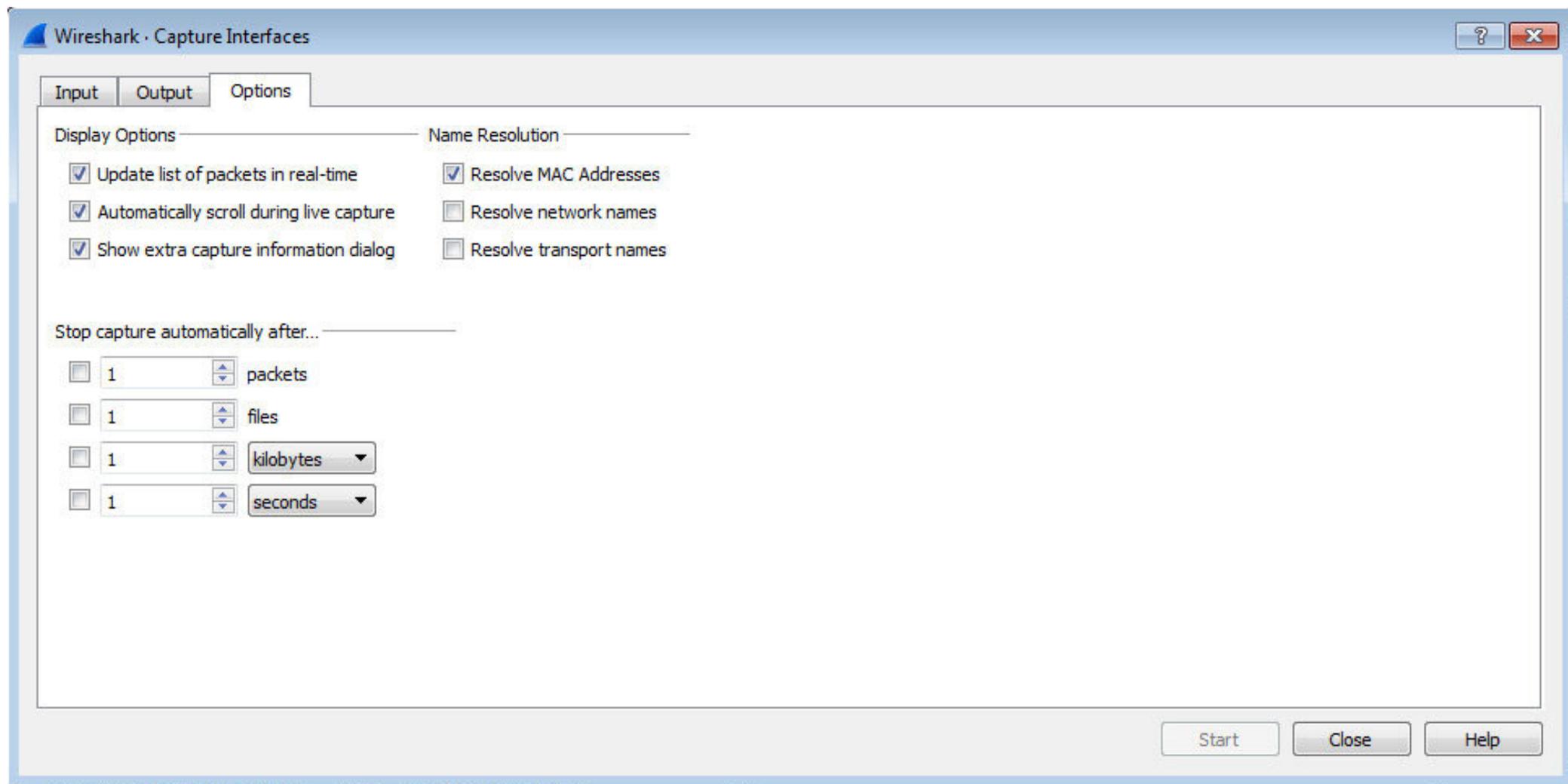


Opzioni per intercettazione

**salvataggio dei
pacchetti catturati
su uno o più file**



Opzioni per intercettazione



Visualizzazione dei pacchetti catturati

Intel(R) PRO/1000 MT Desktop Adapter: \Device\NPF{...} [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
21	25.99547500				208	<Ignored>
22	29.99531200				208	<Ignored>
23	30.52749600	10.0.2.15	192.168.0.1	DNS	73	Standard query 0x0fb9 A www.libero.it
24	30.55720200	192.168.0.1	10.0.2.15	DNS	161	Standard query response 0x0fb9 CNAME vs-fe.io1.it A 151.1.67.227 A 151.1.67.227
25	30.57160100	10.0.2.15	151.1.67.227	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128
26	30.61159400	151.1.67.227	10.0.2.15	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=127
27	31.57257900	10.0.2.15	151.1.67.227	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128
28	31.61141700	151.1.67.227	10.0.2.15	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=127
29	32.56863400				243	<Ignored>
30	32.57263300	10.0.2.15	151.1.67.227	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128
31	32.61163500	151.1.67.227	10.0.2.15	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=127
32	32.99474300				208	<Ignored>
33	33.57302500	10.0.2.15	151.1.67.227	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128
34	33.61261200	151.1.67.227	10.0.2.15	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, ttl=127
35	35.99410000				208	<Ignored>

Frame 24: 161 bytes on wire (130 bytes captured) on interface 0

- Ethernet II, Src: Intel(R) PRO/1000 MT Desktop Adapter (08:00:27:7E:A9:08), Dst: 10.0.2.15 (08:00:0A:00:02:0F)
- Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.168.0.1 (192.168.0.1)
- User Datagram Protocol, Src Port: 52164 (52164), Dst Port: domain (53)
 - Source port: 52164 (52164)
 - Destination port: domain (53)
 - Length: 39
 - Checksum: 0xccf0 [validation disabled]
- Domain Name System (query)
 - [Response in: 24]
 - Transaction ID: 0x0fb9
 - Flags: 0x0100 standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - www.libero.it: type A, class IN
 - Name: www.libero.it
 - Type: A (Host address)
 - Class: IN (0x0001)

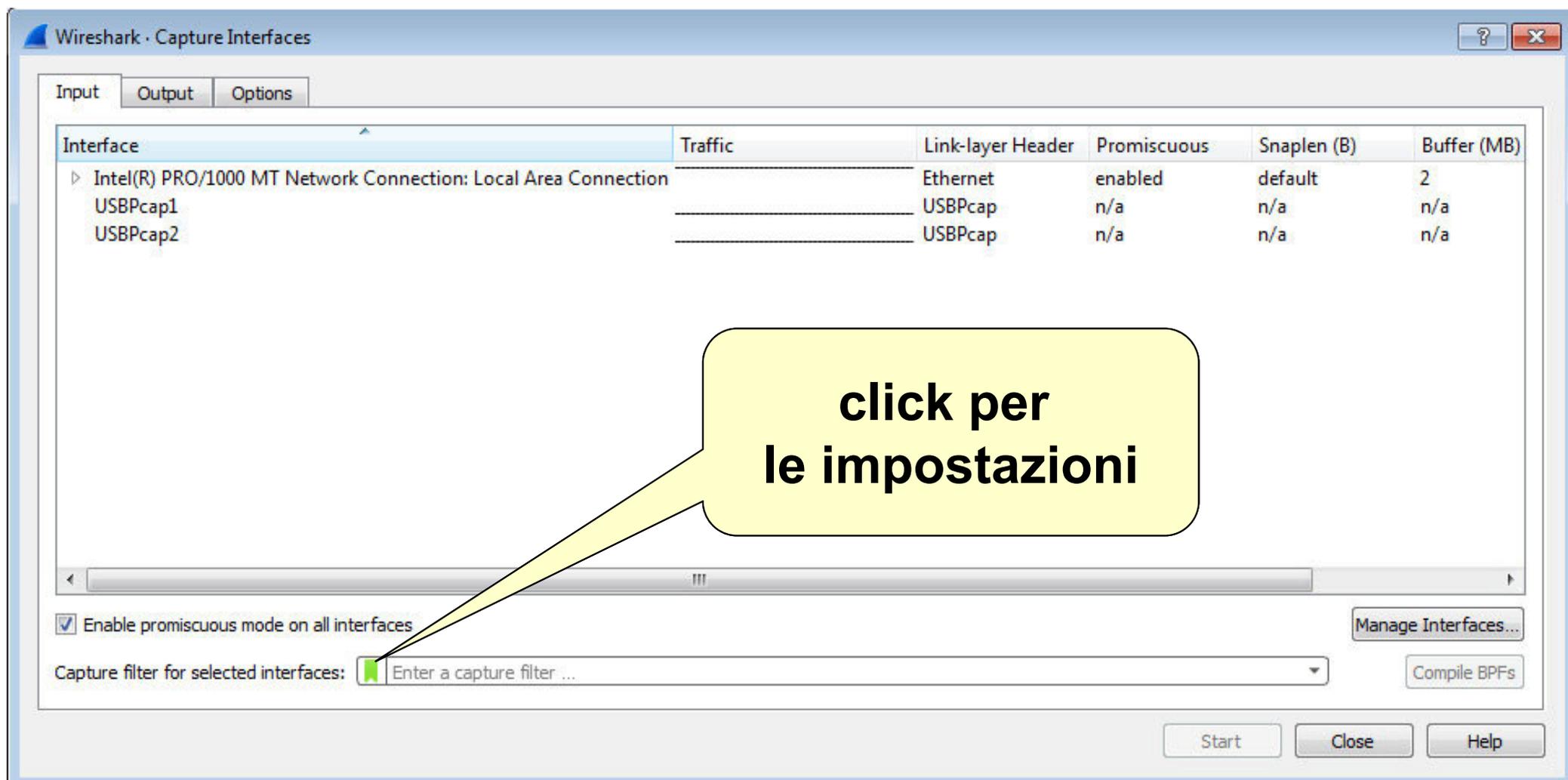
```
0000 52 54 00 12 35 02 08 00 27 72 7e a9 08 00 45 00  RT..5...T~...E.
0010 00 3b 51 d9 00 00 80 11 00 00 0a 00 02 0f c0 a8  .;Q.....
0020 00 01 cb c4 00 35 00 27 cc f0 0f b9 01 00 00 01  .....5.....
0030 00 00 00 00 00 00 03 77 77 77 06 6c 69 62 65 72  .....w ww.libero
0040 6f 02 69 74 00 00 01 00 01 01 01 01 01 01 01 01  o.it....
```

Frame (frame), 73 bytes Packets: 35 Displayed: 35 Marked: 0 Dropped: 0 Ignored: 5 Profile: Default

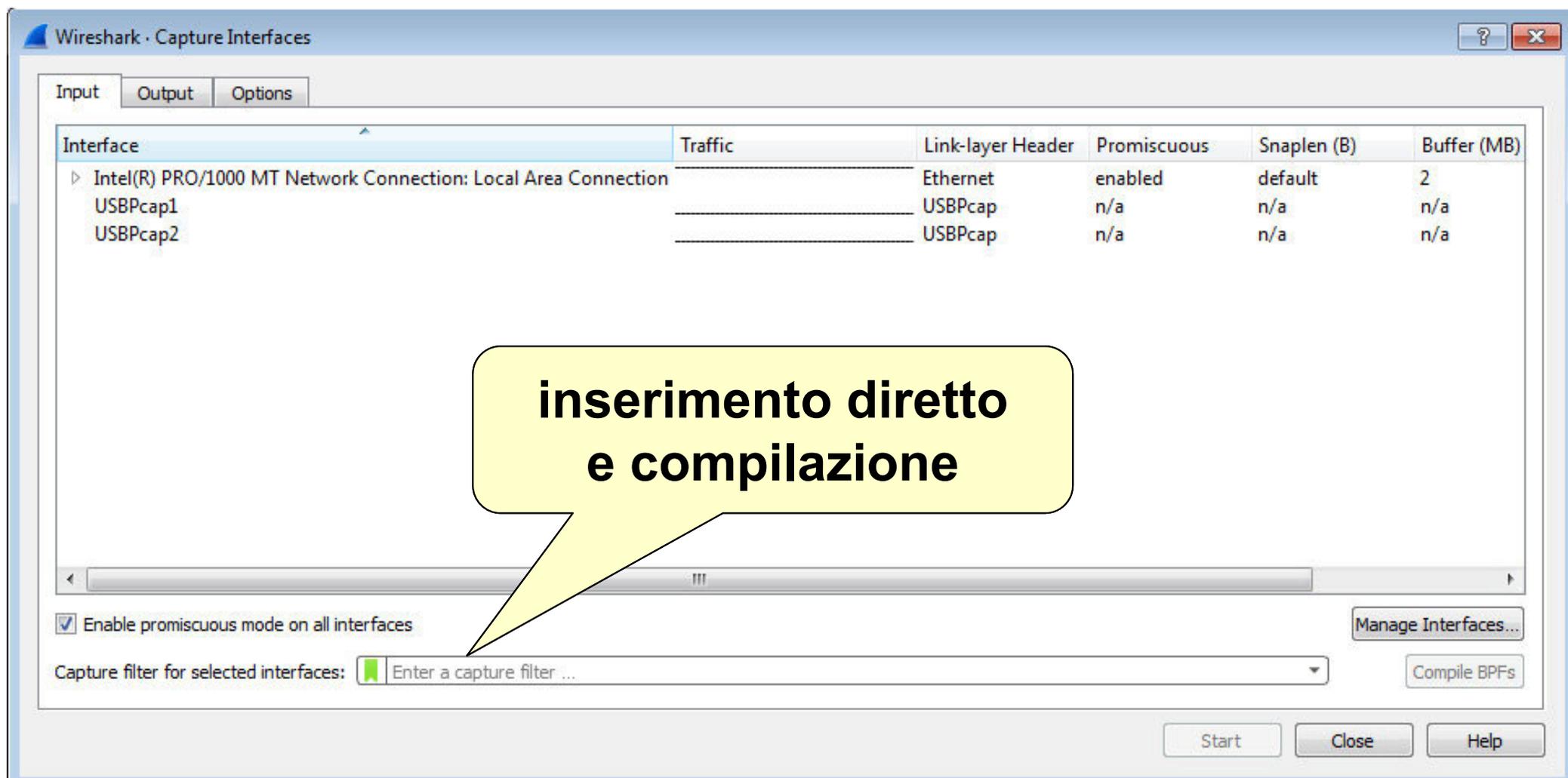
Filtri per intercettazione

- 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



**filtro specificato
in modo corretto**

**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

editor di espressioni

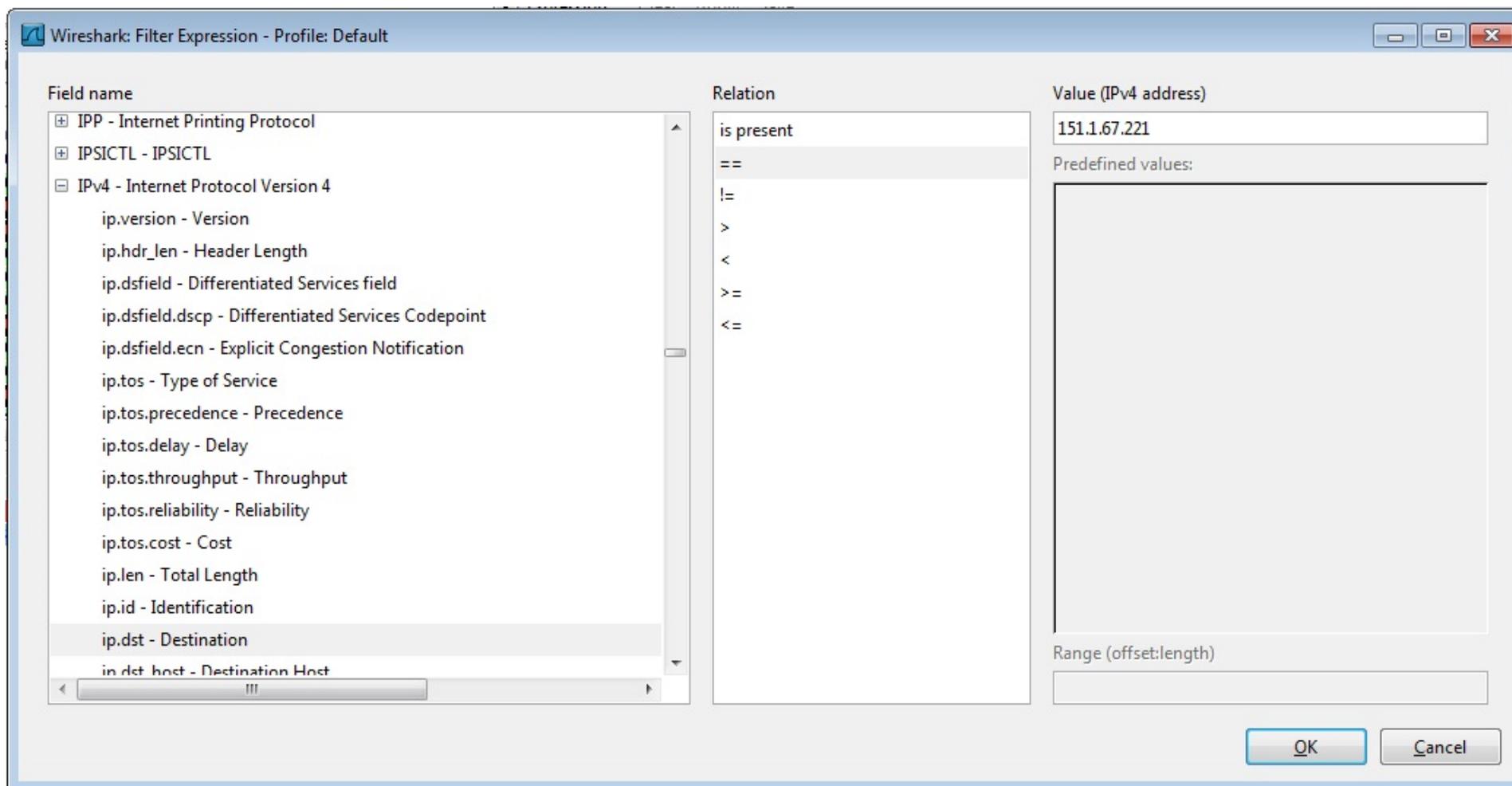
definizione espressione

The screenshot shows the Wireshark interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, and Internal. Below the menu is a toolbar with various icons. A yellow callout box labeled "editor di espressioni" points to the "Expression..." button in the toolbar. Below the toolbar is a "Filter:" input field with a dropdown arrow. A yellow callout box labeled "definizione espressione" points to this field. Below the filter field is a table of captured packets. The table has columns: No., Time, Source, Destination, Protocol, Length, and Info. The first four rows are filtered out and dimmed. The fifth row is highlighted in blue and contains the following data:

No.	Time	Source	Destination	Protocol	Length	Info
	0.000000000				208	<Ign
	0.703963000				103	<Ign
	0.746977000				151	<Ign
					208	<Ign
151	1.67221			TCP	66	4923

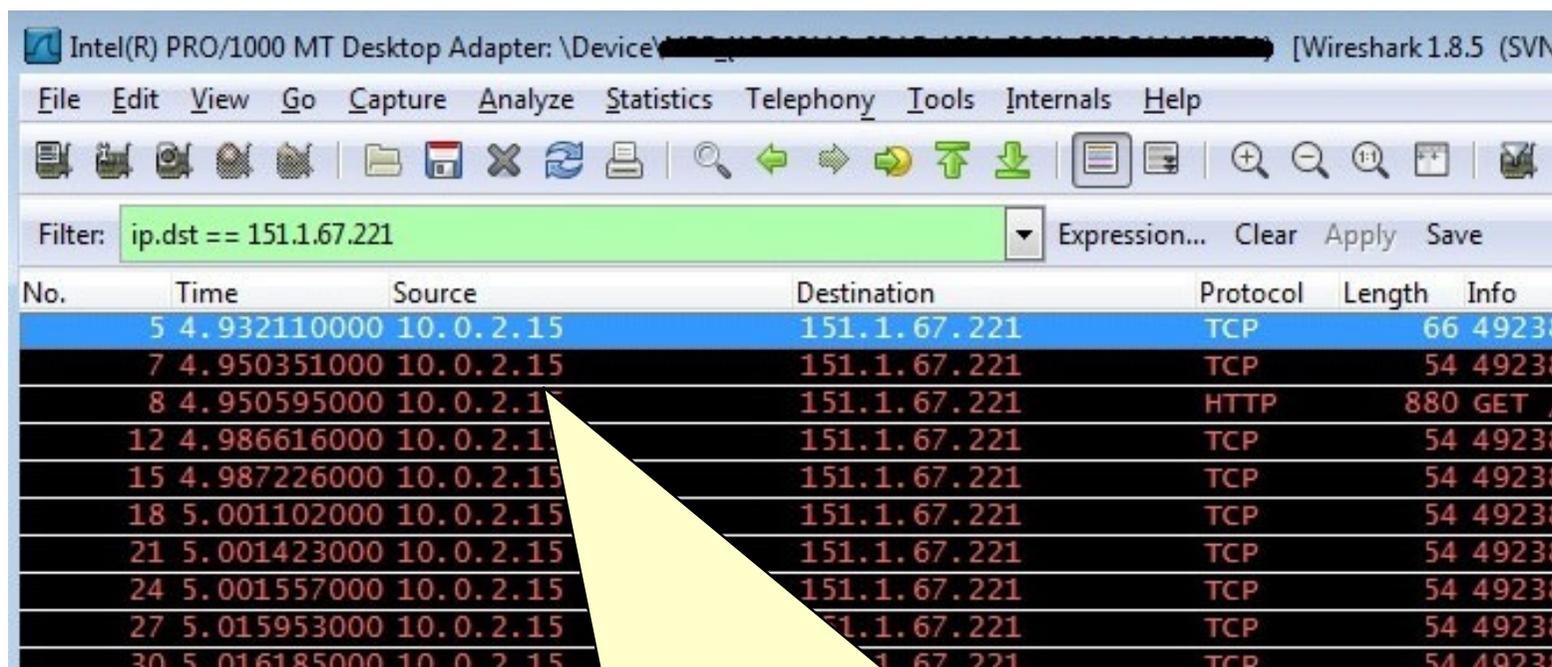
Filtri per visualizzazione - esempio

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



Filtri per visualizzazione - esempio

... ed applicando l'espressione ...



Intel(R) PRO/1000 MT Desktop Adapter: \Device\NPF{...} [Wireshark 1.8.5 (SVN...)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **ip.dst == 151.1.67.221** Expression... Clear Apply Save

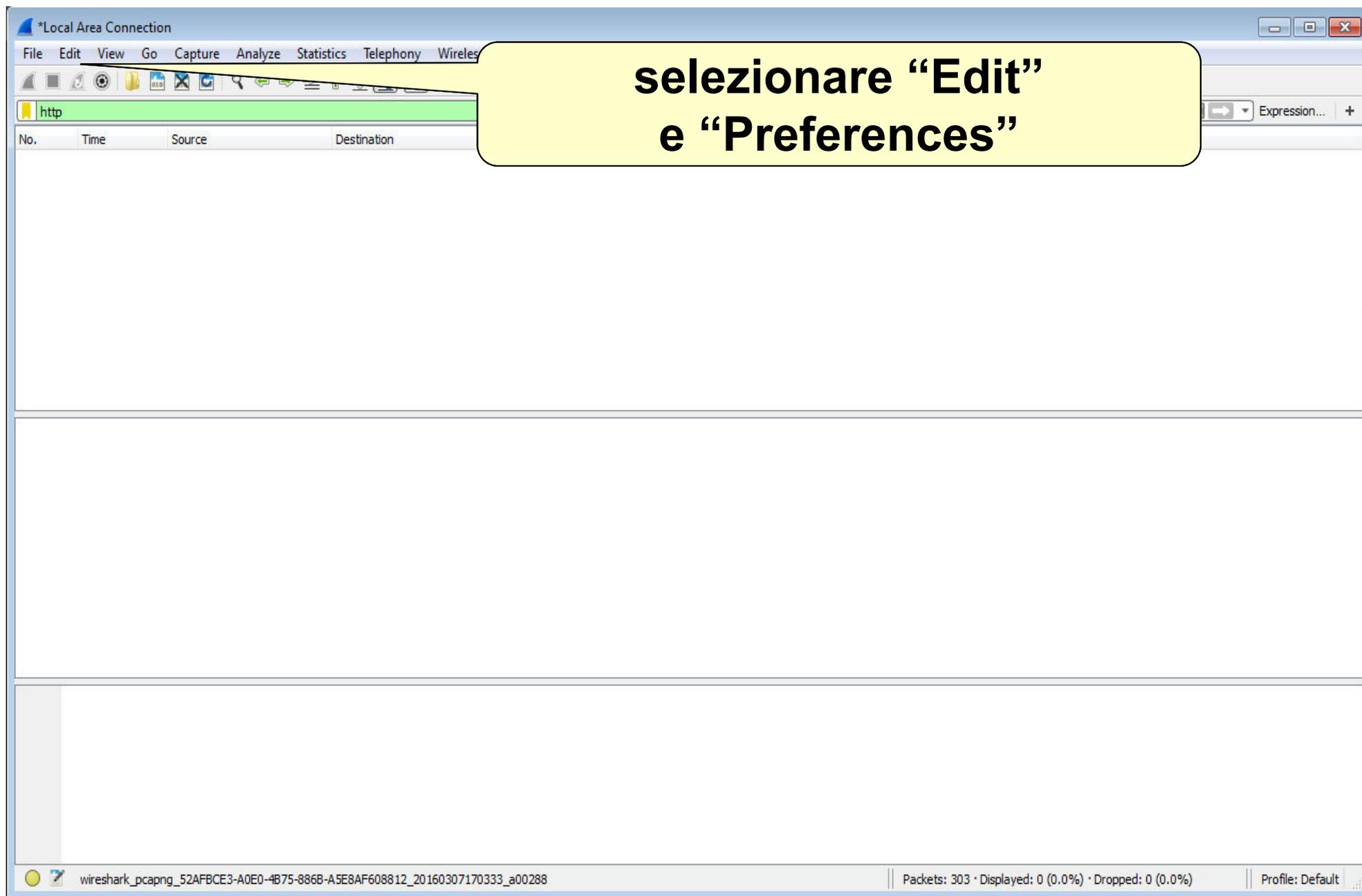
No.	Time	Source	Destination	Protocol	Length	Info
5	4.932110000	10.0.2.15	151.1.67.221	TCP	66	49230
7	4.950351000	10.0.2.15	151.1.67.221	TCP	54	49230
8	4.950595000	10.0.2.15	151.1.67.221	HTTP	880	GET
12	4.986616000	10.0.2.15	151.1.67.221	TCP	54	49230
15	4.987226000	10.0.2.15	151.1.67.221	TCP	54	49230
18	5.001102000	10.0.2.15	151.1.67.221	TCP	54	49230
21	5.001423000	10.0.2.15	151.1.67.221	TCP	54	49230
24	5.001557000	10.0.2.15	151.1.67.221	TCP	54	49230
27	5.015953000	10.0.2.15	151.1.67.221	TCP	54	49230
30	5.016185000	10.0.2.15	151.1.67.221	TCP	54	49230

pacchetti che soddisfano l'espressione

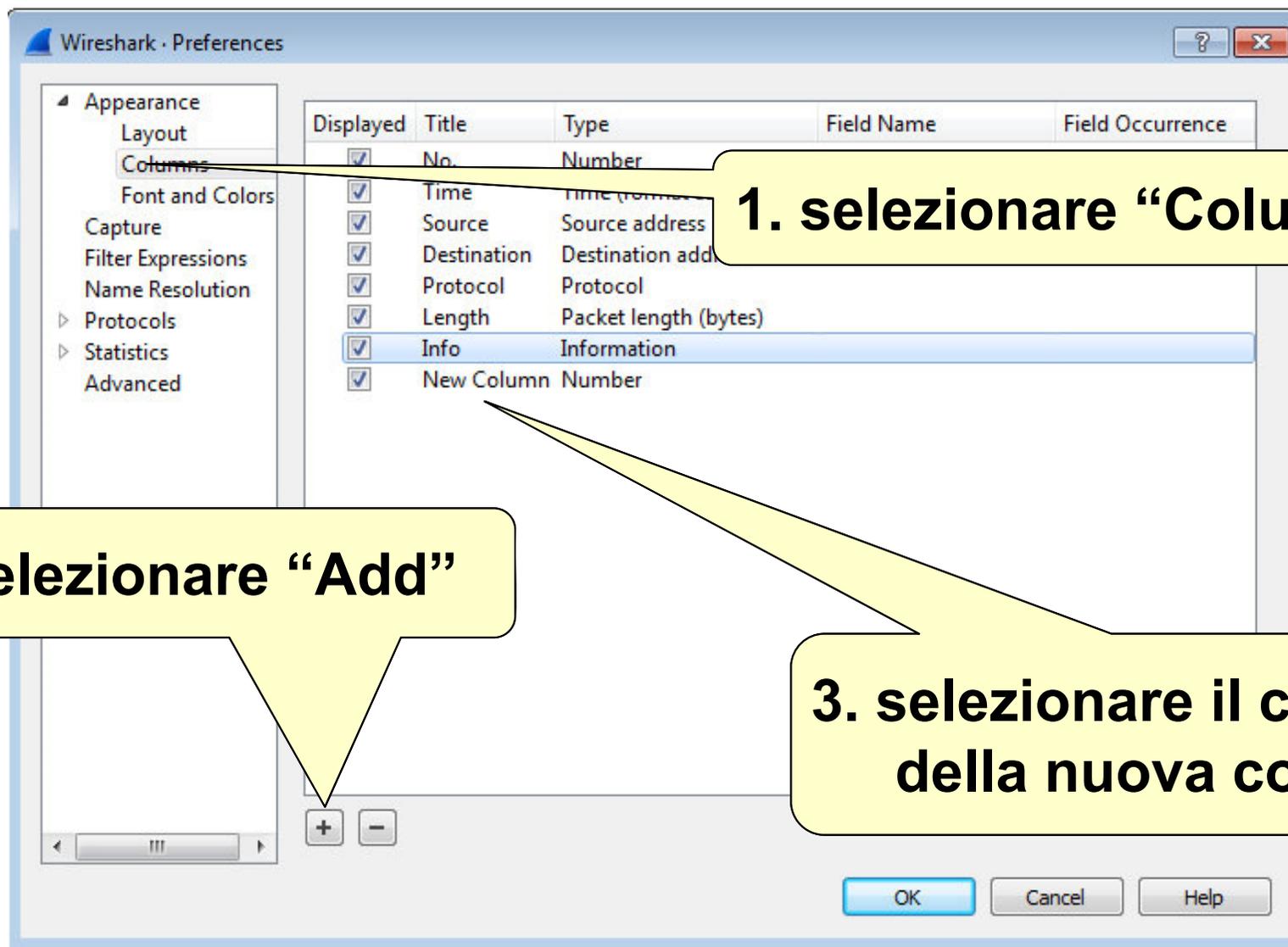
Visualizzare elementi aggiuntivi

- **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



1. selezionare "Columns"

2. selezionare "Add"

3. selezionare il contenuto della nuova colonna

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

Conversations: Intel(R) PRO/1000 MT Desktop Adapter: \Device\...

Ethernet: 3 | Fibre Channel | FDDI | IPv4: 19 | IPv6: 1 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 26 | Token Ring | UDP: 43 | USB | WLAN

IPv4 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

Name resolution Limit to display filter

Help Copy Follow Stream Close

Interfaccia Conversations

■ Statistics → Conversations

Conversations: Intel(R) PRO/1000 MT Desktop Adapter: \Device\NPF\{...}

Ethernet: 3 | Fibre Channel | FDDI | IPv4: 19 | IPv6: 1 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 26 | Token Ring | UDP: 43 | USB | WLAN

IPv4 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	200	11 676	410	322 660	4,482118000	8,0580	11591,98	320338,15
10.0.2.15	151.1.67.215	102	4 432	4	2 011	98	2 421	3,847066000	8,0580	6062,80	97902,36
10.0.2.15	151.1.67.231	243	9 432	9	2 011	234	2 421	3,847066000	8,0580	22626,76	205680,18
10.0.2.15	178.250.0.76	11	1 665	6	950	5	715	3,847066000	3,5546	2953,74	1930,45
10.0.2.15	93.184.220.20	11	1 665	6	950	5	715	3,847066000	3,5546	2044,13	2691,94
10.0.2.15	173.194.35.27	20	6 454	10	2 011	10	2 421	3,847066000	8,0580	5507,45	12167,89
10.0.2.15	212.58.244.61	11	1 762	6	879	5	883	3,847066000	3,5546	2508,49	2519,91
10.0.2.15	82.199.80.141	33	8 863	16	3 418	17	5 445	9,767100000	8,0580	11646,70	18553,62
10.0.2.15	195.22.200.25	32	13 557	13	1 100	19	12 457	9,966700000	8,0580	3449,96	39069,26
10.0.2.15	195.22.200.32	71	31 279	29	4 512	42	26 767	10,000000000	8,0580	16719,32	99185,76
10.0.2.15	54.239.158.155	11	1 970	6	607	5	1 363	3,847066000	1,1919	4074,26	9148,63
10.0.2.15	68.67.185.209	11	1 368	6	629	5	739	3,847066000	1,0705	4700,78	5522,85
10.0.2.15	68.67.185.184	14	3 438	7	2 011	7	1 427	3,847066000	8,0580	8439,16	23798,44
10.0.2.15	46.228.164.11	18	7 500	9	2 011	9	2 421	3,847066000	8,0580	452,23	65807,11
10.0.2.15	195.22.200.43	10	1 190	5	607	5	683	3,847066000	8,0580	292,85	19707,89
10.0.2.15	239.255.255.250	2	370	1	607	1	782	3,847066000	8,0580	782,61	N/A
10.0.2.2	10.0.2.15	1	20	0	0	1	20	3,847066000	8,0580	N/A	N/A

Apply as Filter | Prepare a Filter | Find Packet | Colorize Conversation

Selected | Not Selected | ... and Selected | ... or Selected | ... and not Selected | ... or not Selected

A → B | A ← B | A → Any | A ← Any | Any → B | Any ← B | Any → B

definizione assistita del filtro

Name resolution | Limit to display filter

Help | Copy | Follow Stream | Close