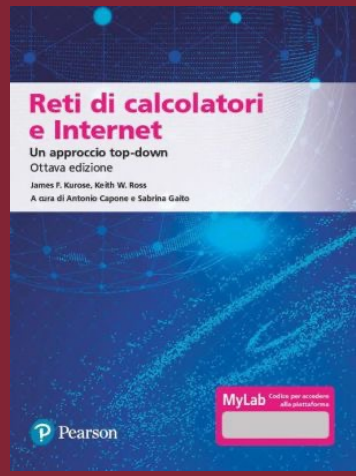
Reti di Elaboratori

Wireshark



SAPIENZA
UNIVERSITÀ DI ROMA

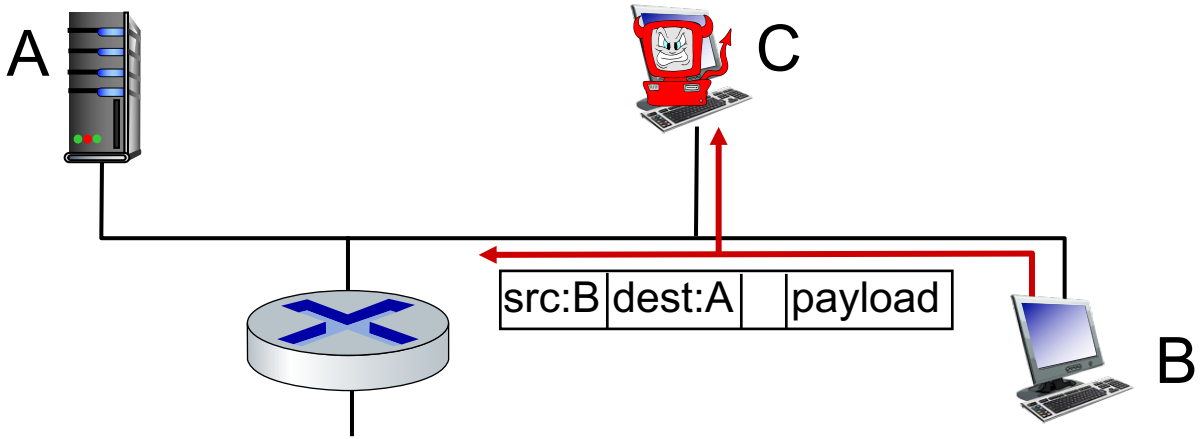
Alessandro Checco
alessandro.checco@uniroma1.it

Appendice

Attacchi alla rete: intercettazione di pacchetti

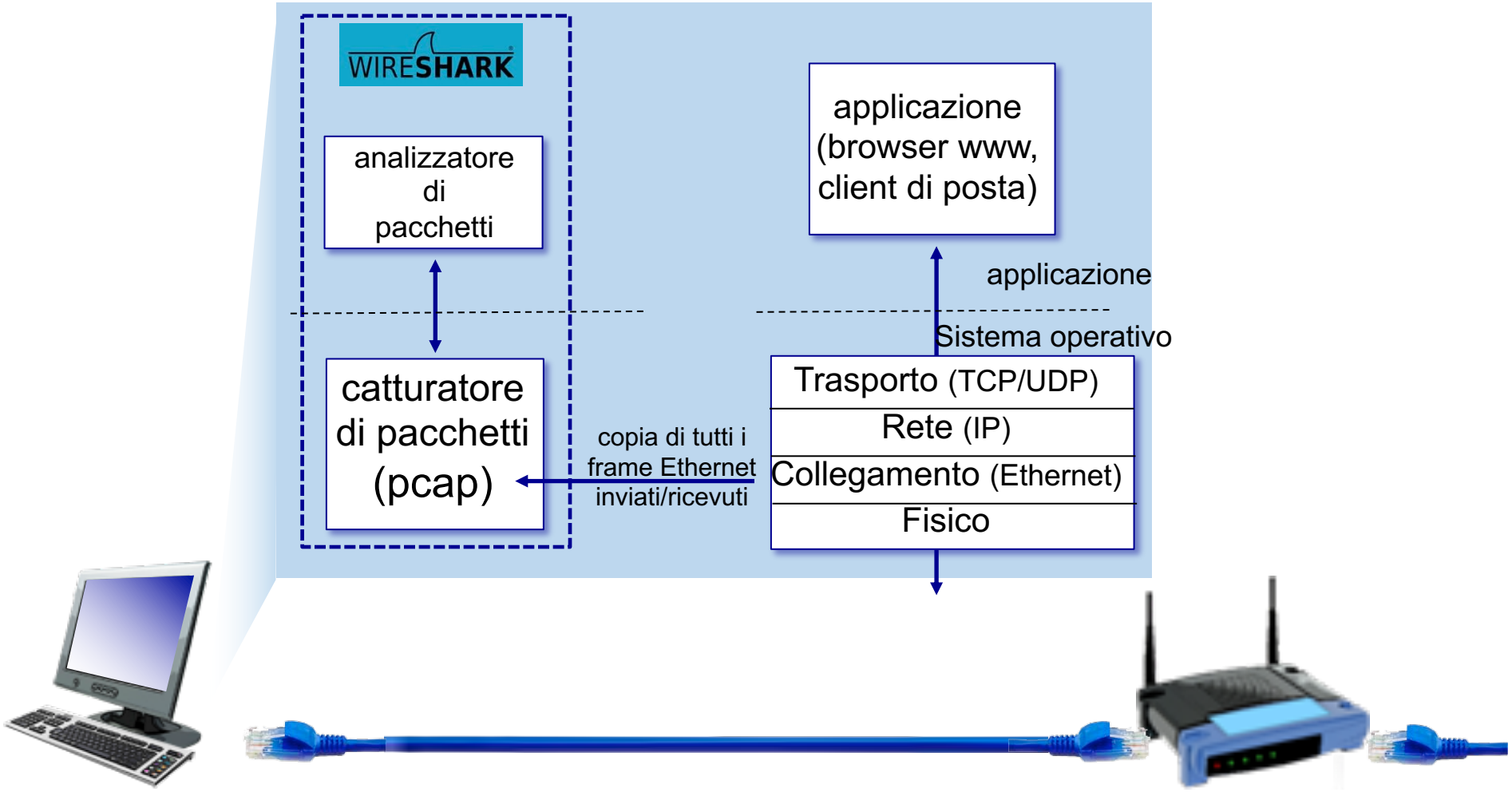
packet "sniffing"

- spesso via mezzi di trasmissione (Ethernet condivisa, wireless)
  - In alcuni casi tramite switch compromessi (ad es. attacchi governativi)
- l'interfaccia di rete malevola legge/registra tutti i pacchetti (ad esempio, comprese le password!) che passano



Il software Wireshark è uno sniffer di pacchetti (gratuito)

Wireshark

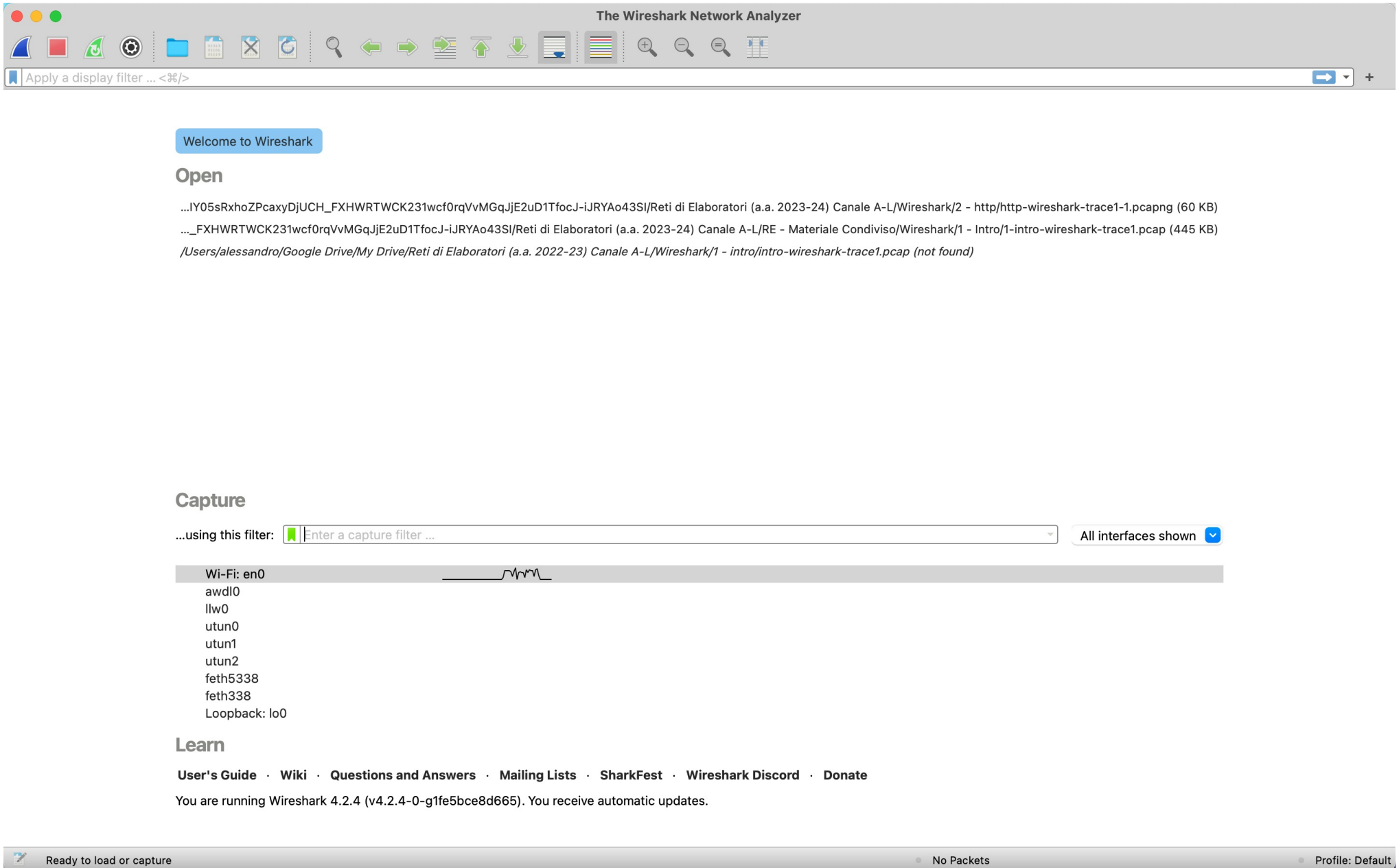

WIRESHARK
analizzatore di pacchetti
catturatore di pacchetti (pcap)
copia di tutti i frame Ethernet inviati/ricevuti
applicazione (browser www, client di posta)
applicazione
Sistema operativo
Trasporto (TCP/UDP)
Rete (IP)
Collegamento (Ethernet)
Fisico

Modalità di intercettazione (per IEEE 802)

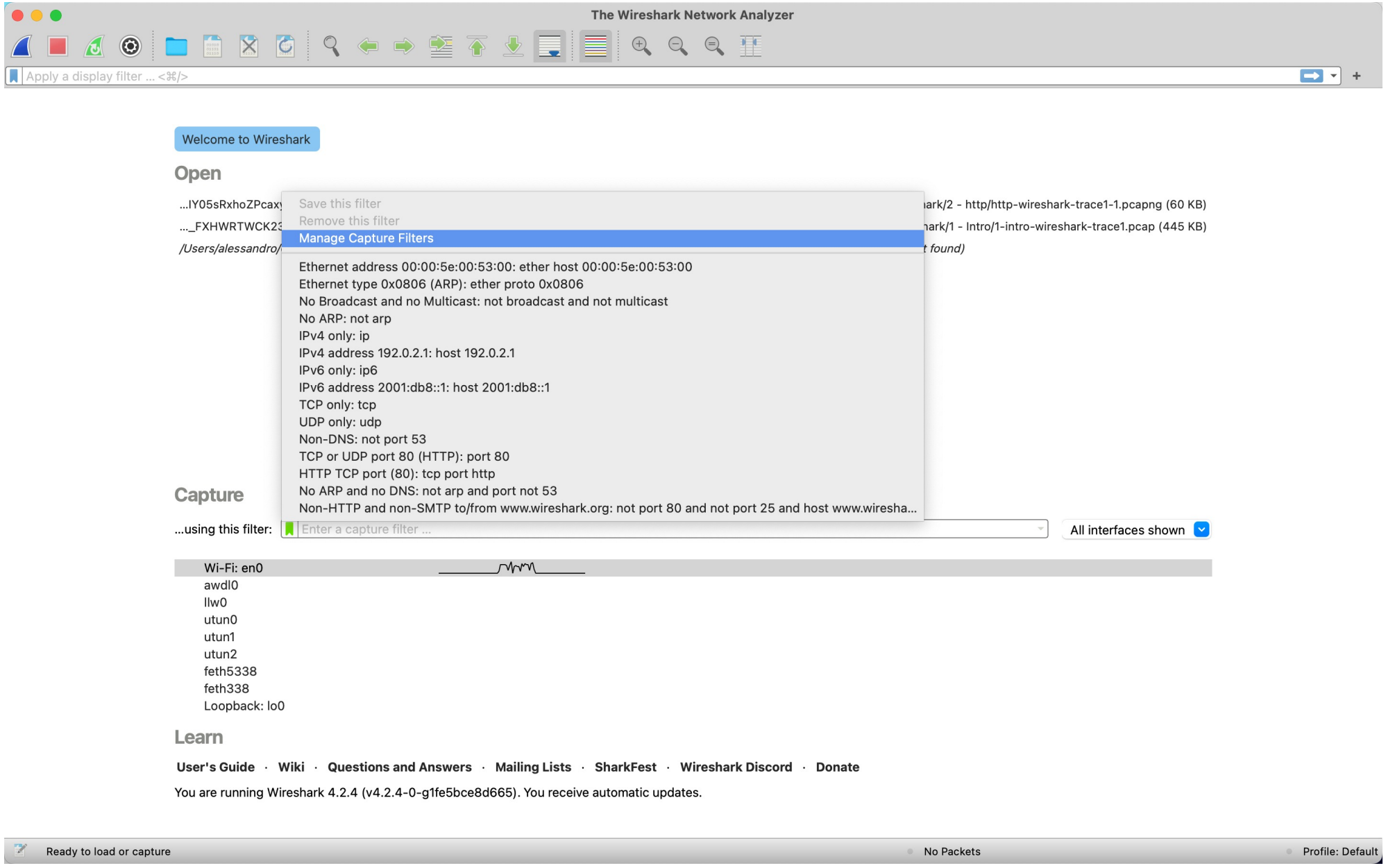
- Modalità di ascolto della scheda di rete
  - Normale: solo traffico destinato alla scheda di rete (identificata attraverso l'indirizzo MAC) o broadcast
  - Promiscuous (Monitor Mode)
    - traffico destinato ad altri nodi (anche altri MAC). Ad esempio traffico a/da altri nodi nella rete WiFi
    - può essere utile per il controllo del traffico di una rete
    - può essere illegale (anche penale!) se fatto a danno di terzi

Art. 617 quater codice penale: "Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi(2), ovvero le impedisce o le interrompe(3), è punito con la reclusione da un anno e sei mesi a cinque anni"

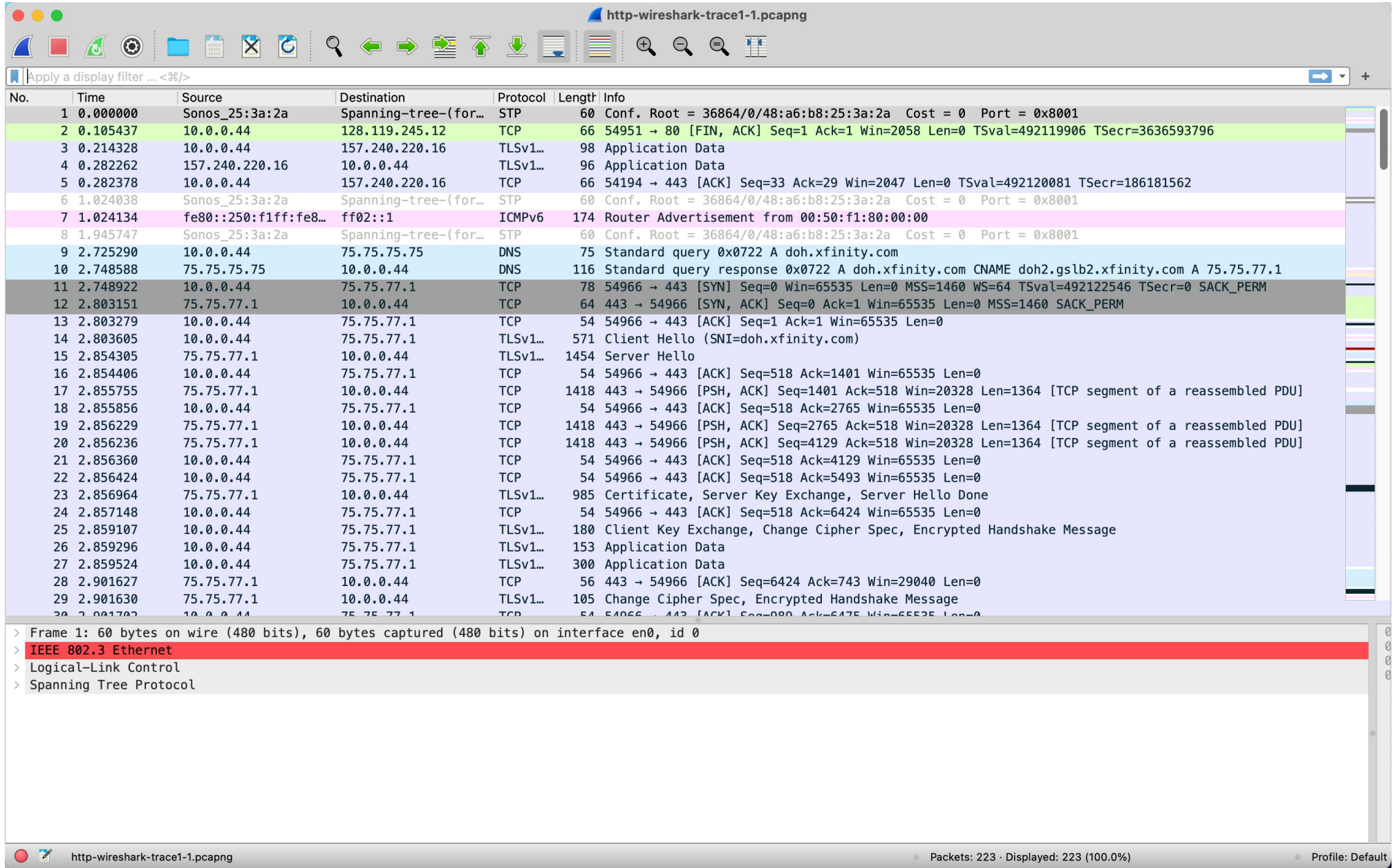
Interfaccia Iniziale



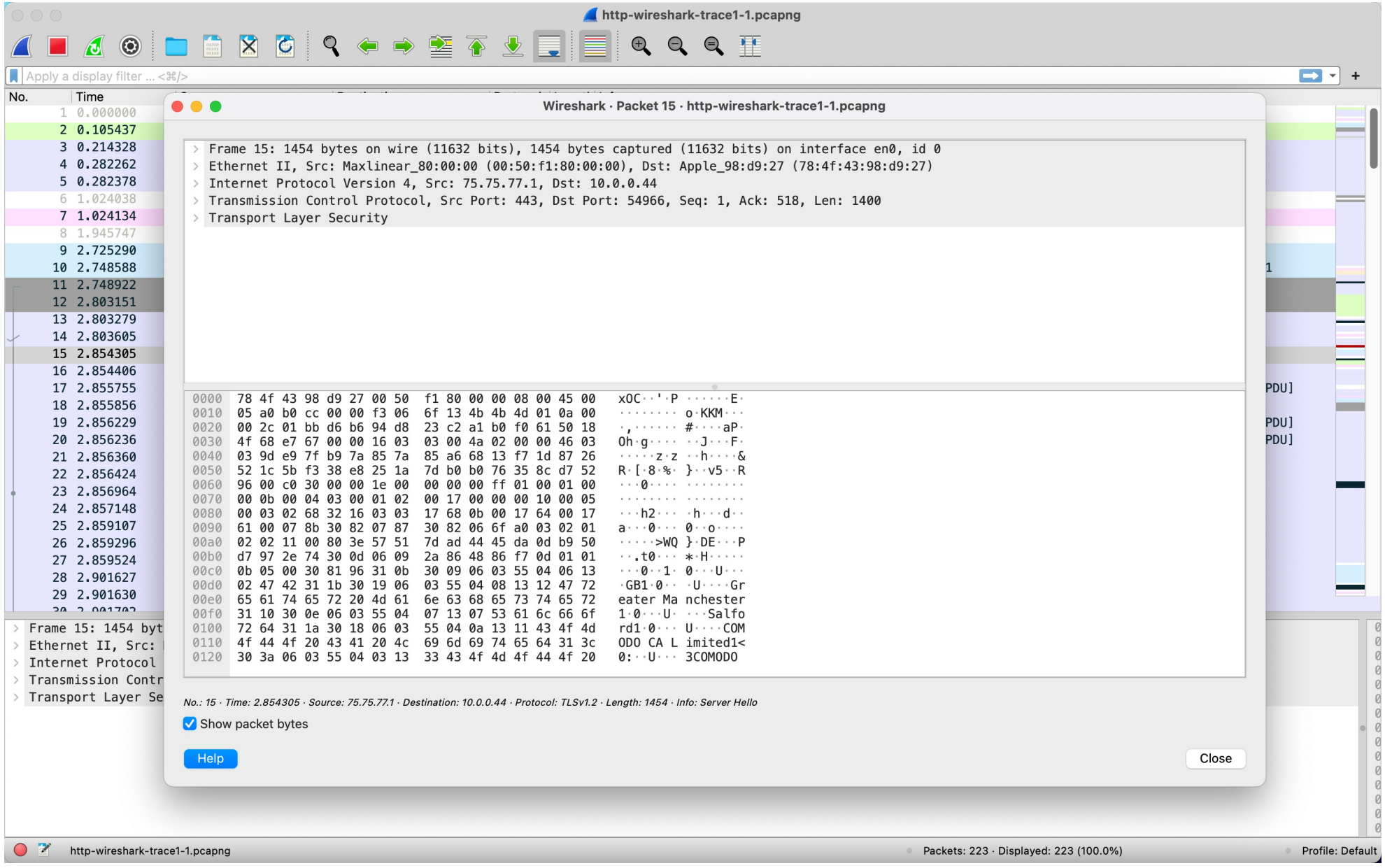
Filtri di cattura predefiniti



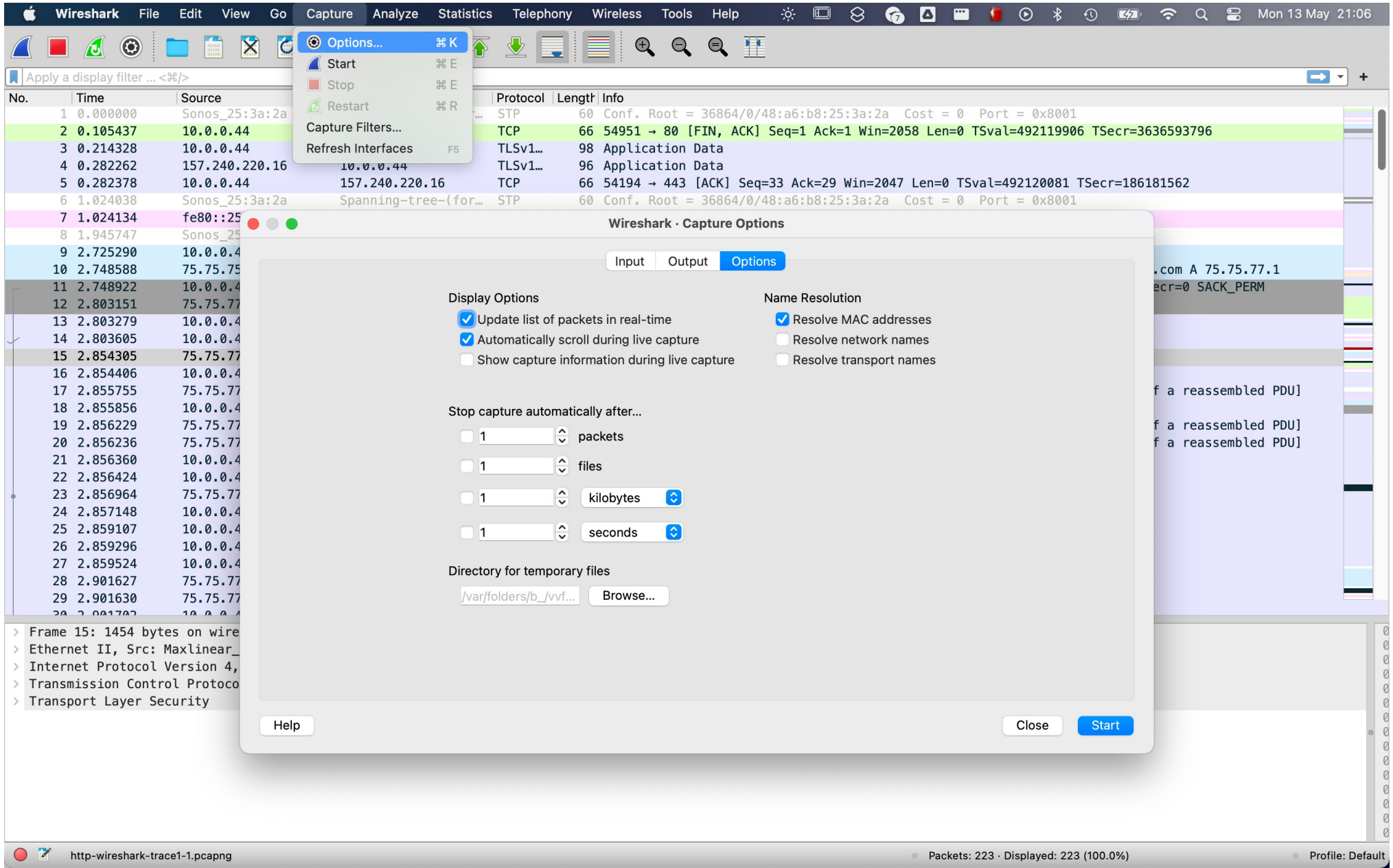
Interfaccia principale



Visualizzazione pacchetto



Opzioni di Cattura

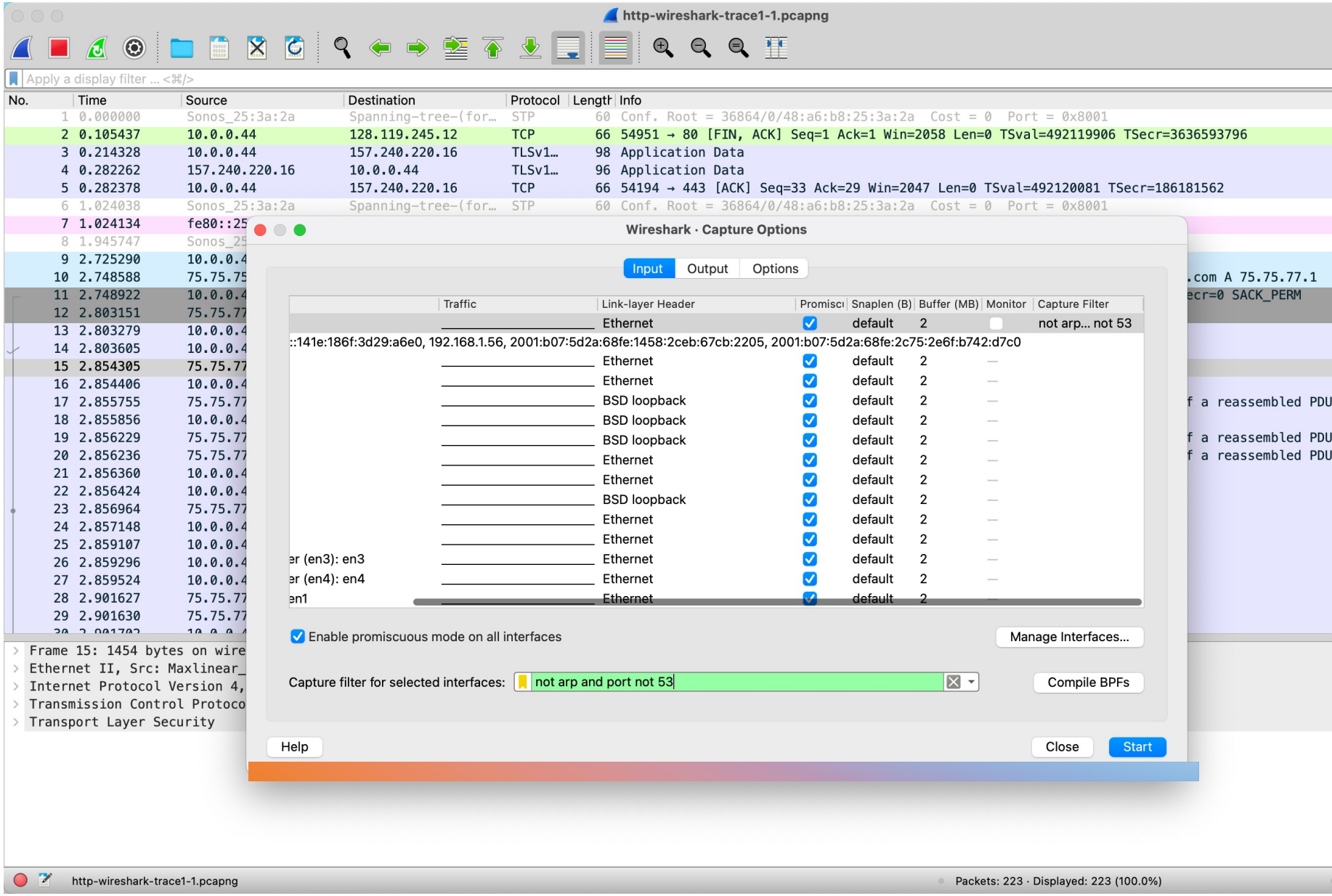


Filtri di Wireshark

- Applicabili prima o dopo l'intercettazione
- Per catturare solo il traffico d'interesse
  - può essere difficile mantenere tutto il traffico (cfr. NSA)
- Si possono specificare:
  - protocollo (UDP, TCP, ICMP, etc.)
  - contenuto dell'header
    - ad es. IP src, port
  - composizione con operatori logici
    - ad es. host 10.10.10.1 and not (port 80 or port 25)
- Doc: http://wiki.wireshark.org/CaptureFilters

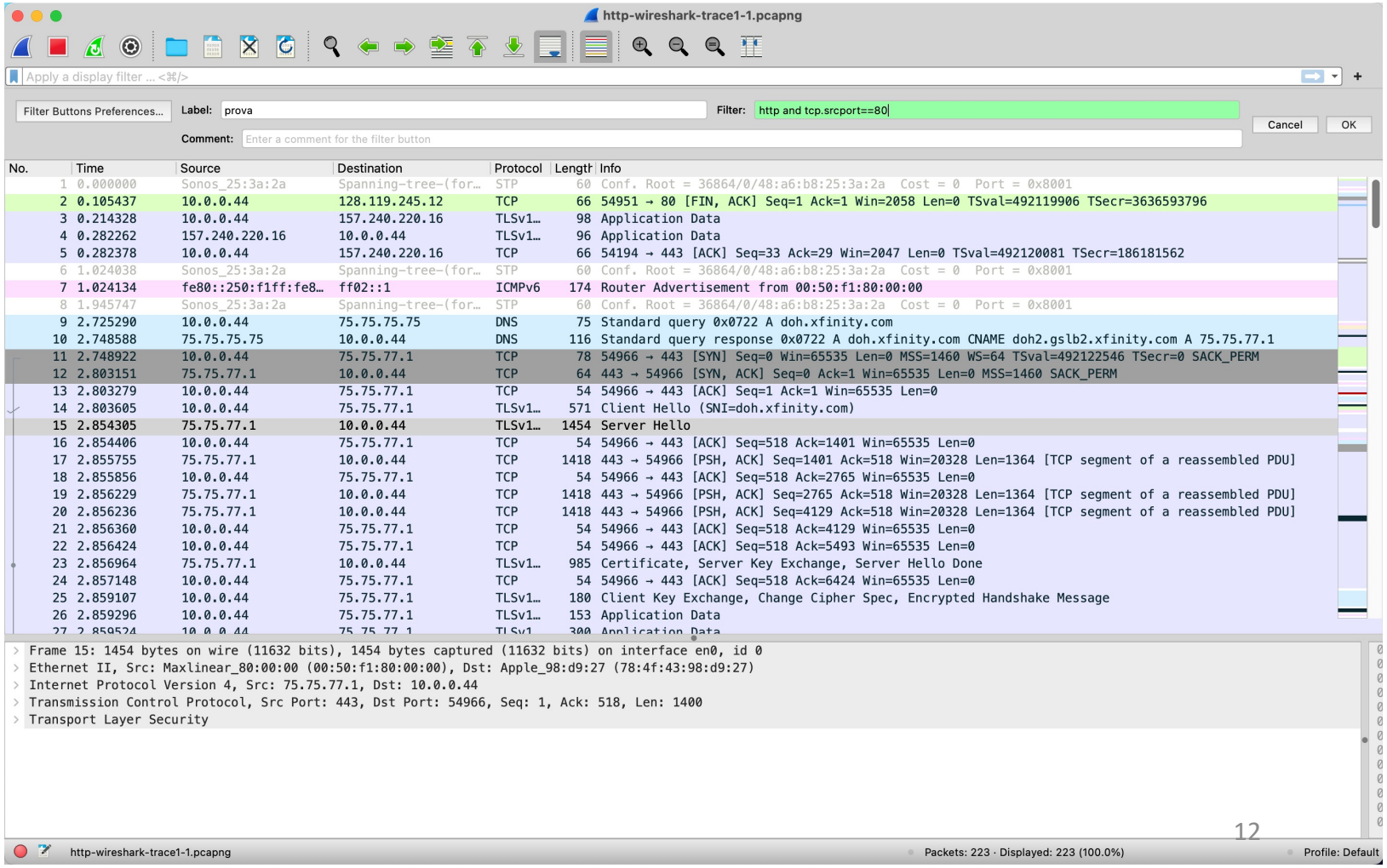
Esempio di filtro in input

- Corretto (in verde)
- viene compilato in un linguaggio usato dal motore di packet capture



Filtri per visualizzazione

- Si applicano a pacchetti già intercettati
- http://wiki.wireshark.org/DisplayFilters



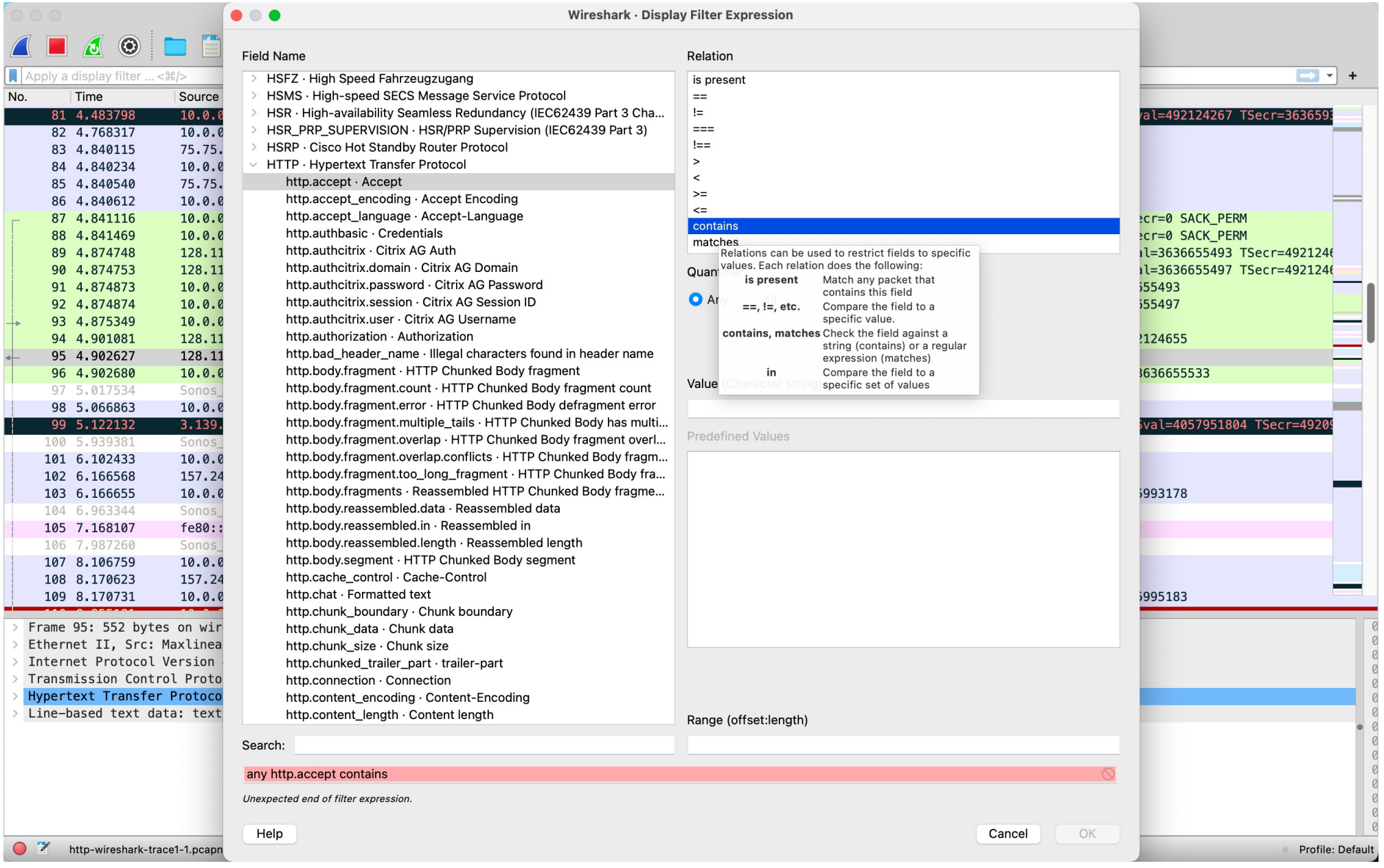
Sintassi

- Composti con operatori logici
  - and
  - or
  - not
- Regex
  - usato con "matches"
- Cliccando su un pacchetto si può usare come punto di partenza per un filtro

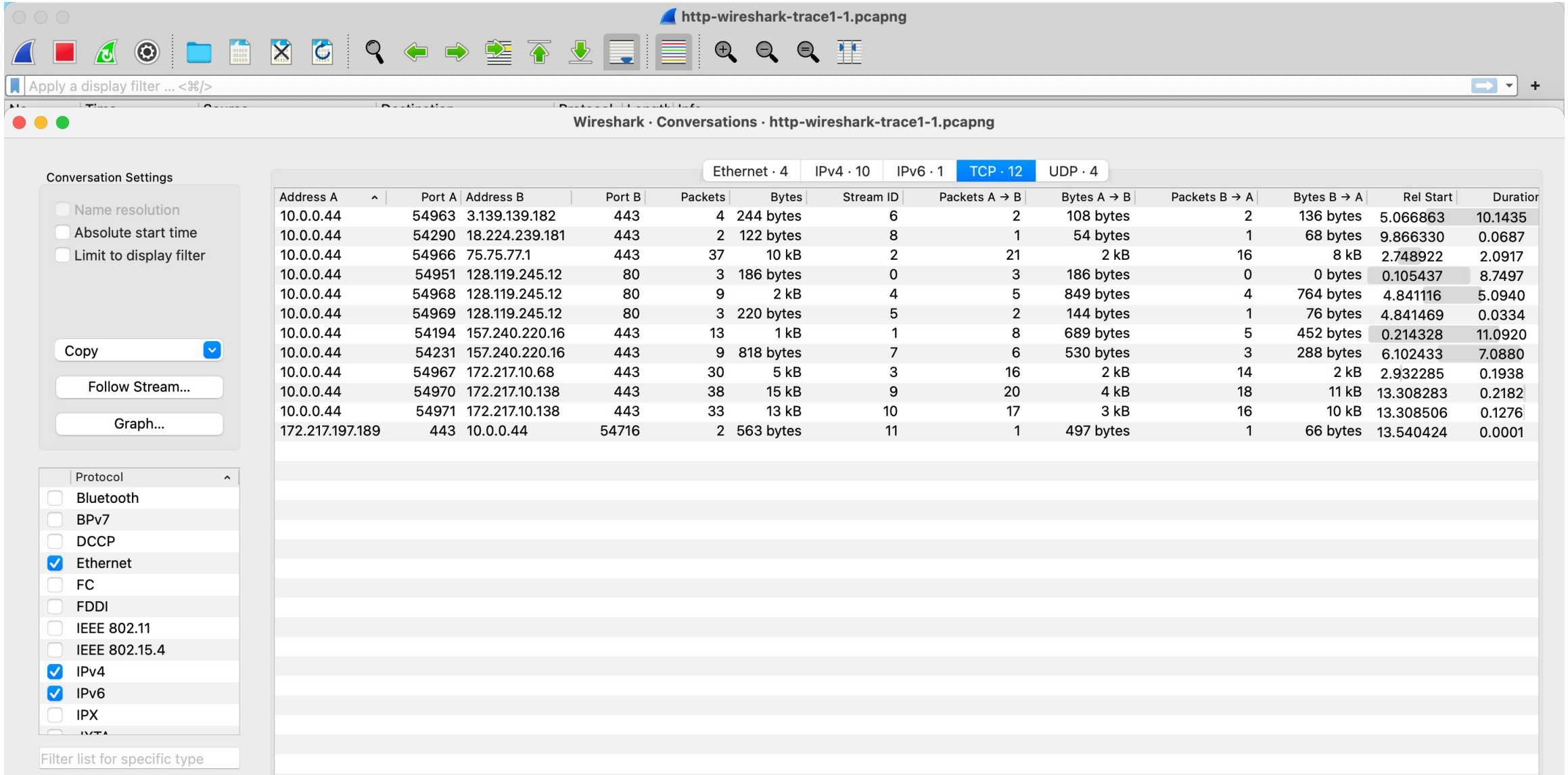
Esenpi di filtri

- `http.request and tcp.port==80` – Display all HTTP requests on port 80
- `http.request || http.response` – Display all HTTP request and responses.
- `ip.addr == 127.0.0.1` – Display all IP packets whose source or destination is localhost.
- `tcp.len < 100` – Display all TCP packets whose data length is less than 100 bytes.
- `http.request.uri matches "(gif)$"` - Display all HTTP requests in which the uri ends with “gif”.
- `dns.query.name == "www.google.com"` - Display all DNS queries for “www.google.com”.

Analyze/Display Filter Expressions



Statistics/Conversations



Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
10.0.0.44	54963	3.139.139.182	443	4	244 bytes	6	2	108 bytes	2	136 bytes	5.066863	10.1435
10.0.0.44	54290	18.224.239.181	443	2	122 bytes	8	1	54 bytes	1	68 bytes	9.866330	0.0687
10.0.0.44	54966	75.75.77.1	443	37	10 kB	2	21	2 kB	16	8 kB	2.748922	2.0917
10.0.0.44	54951	128.119.245.12	80	3	186 bytes	0	3	186 bytes	0	0 bytes	0.105437	8.7497
10.0.0.44	54968	128.119.245.12	80	9	2 kB	4	5	849 bytes	4	764 bytes	4.841116	5.0940
10.0.0.44	54969	128.119.245.12	80	3	220 bytes	5	2	144 bytes	1	76 bytes	4.841469	0.0334
10.0.0.44	54194	157.240.220.16	443	13	1 kB	1	8	689 bytes	5	452 bytes	0.214328	11.0920
10.0.0.44	54231	157.240.220.16	443	9	818 bytes	7	6	530 bytes	3	288 bytes	6.102433	7.0880
10.0.0.44	54967	172.217.10.68	443	30	5 kB	3	16	2 kB	14	2 kB	2.932285	0.1938
10.0.0.44	54970	172.217.10.138	443	38	15 kB	9	20	4 kB	18	11 kB	13.308283	0.2182
10.0.0.44	54971	172.217.10.138	443	33	13 kB	10	17	3 kB	16	10 kB	13.308506	0.1276
172.217.197.189	443	10.0.0.44	54716	2	563 bytes	11	1	497 bytes	1	66 bytes	13.540424	0.0001