

Reti di Elaboratori

Wireshark

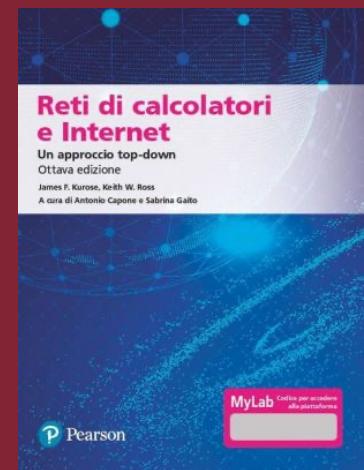


SAPIENZA
UNIVERSITÀ DI ROMA

Alessandro Checco

alessandro.checco@uniroma1.it

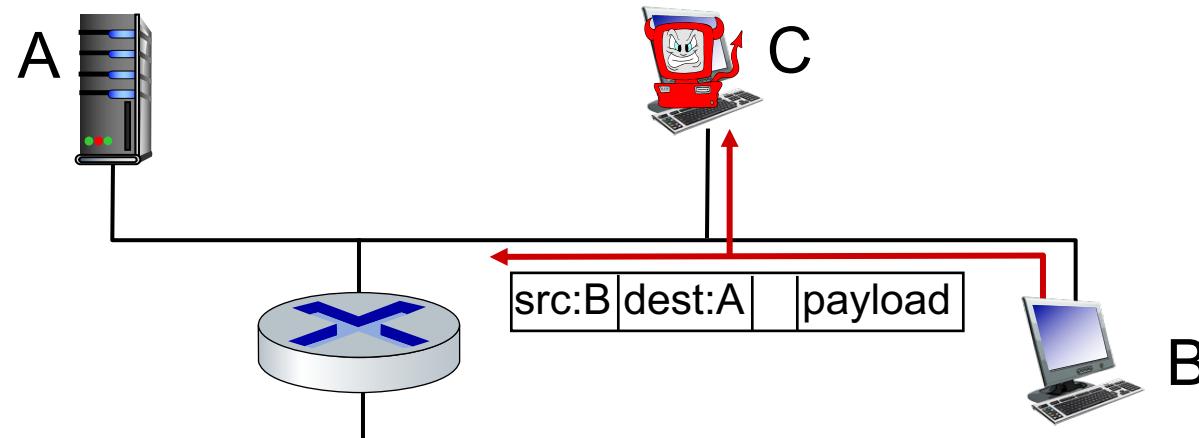
Appendice



Attacchi alla rete: intercettazione di pacchetti

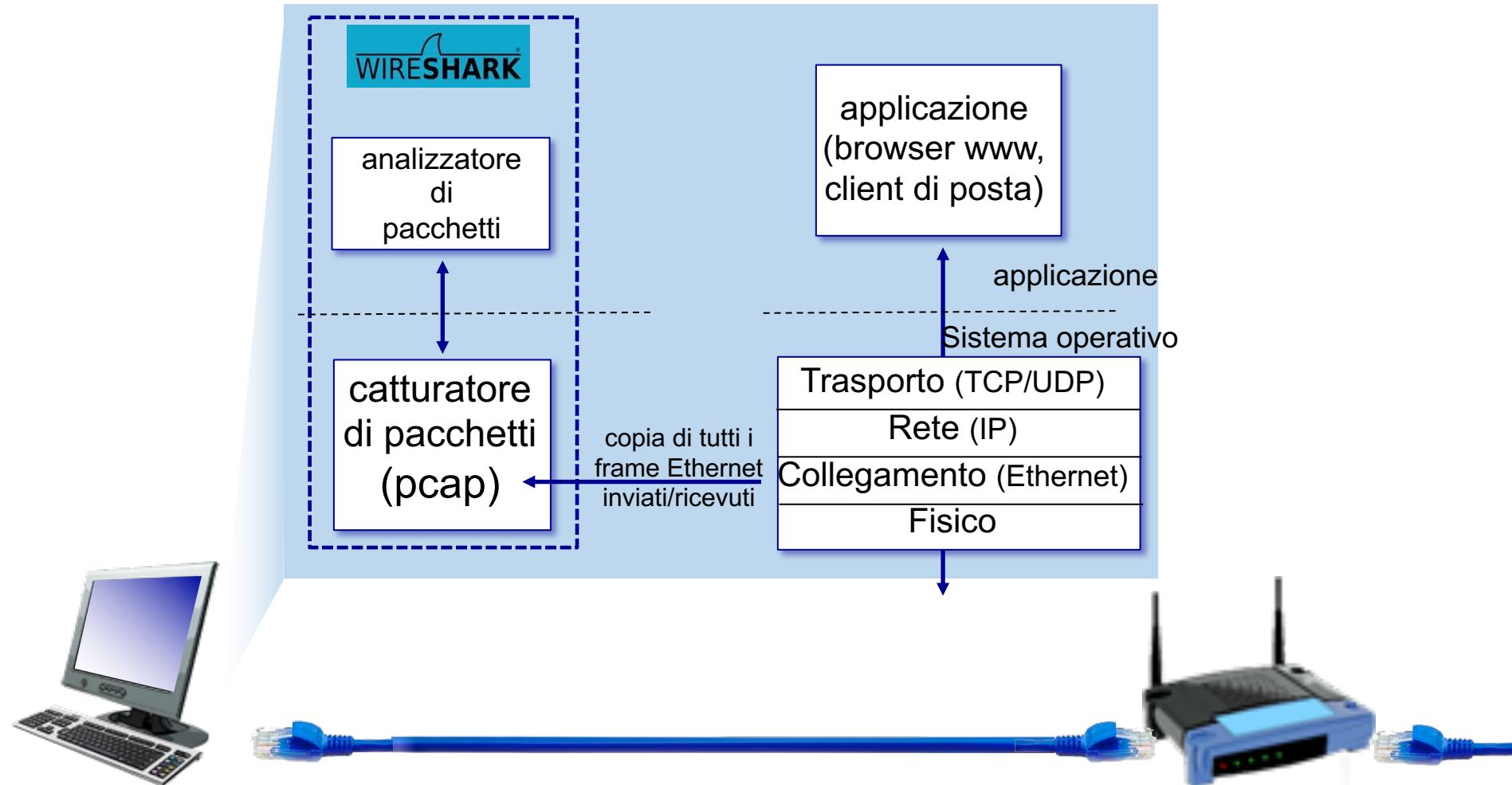
packet “sniffing”

- 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



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

The screenshot shows the initial interface of Wireshark, titled "The Wireshark Network Analyzer". The top bar includes standard OS X window controls (red, yellow, green) and application icons. Below the title is a toolbar with various icons for file operations, search, and analysis. A search bar at the top right contains the placeholder text "Apply a display filter ... <⌘>/".

Welcome to Wireshark

Open

- ...IY05sRxhoZPcaxyDjUCH_FXHWRTWCK231wcf0rqVvMGqJJE2uD1TfocJ-iJRYAo43SI/Reti di Elaboratori (a.a. 2023-24) Canale A-L/Wireshark/2 - http/http-wireshark-trace1-1.pcapng (60 KB)
- ..._FXHWRTWCK231wcf0rqVvMGqJJE2uD1TfocJ-iJRYAo43SI/Reti di Elaboratori (a.a. 2023-24) Canale A-L/RE - Materiale Condiviso/Wireshark/1 - Intro/1-intro-wireshark-trace1.pcap (445 KB)
- /Users/alessandro/Google Drive/My Drive/Reti di Elaboratori (a.a. 2022-23) Canale A-L/Wireshark/1 - intro/intro-wireshark-trace1.pcap (not found)

Capture

...using this filter: Enter a capture filter ... All interfaces shown

Wi-Fi: en0 Wlan

- awdl0
- llw0
- utun0
- utun1
- utun2
- feth5338
- feth338
- Loopback: lo0

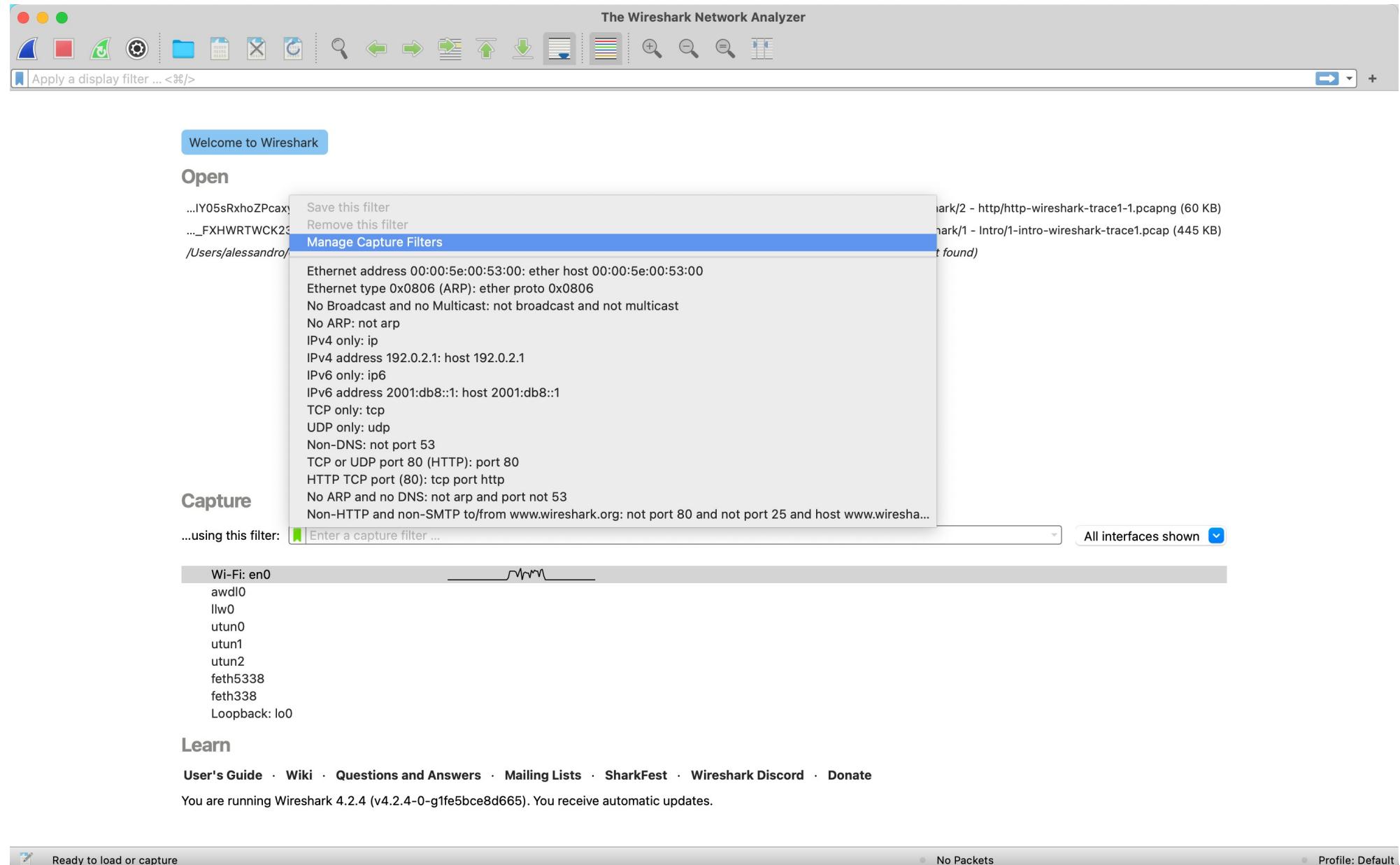
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.2.4 (v4.2.4-0-g1fe5bce8d665). You receive automatic updates.

Ready to load or capture No Packets Profile: Default

Filtri di cattura predefiniti



Interfaccia principale

http-wireshark-trace1-1.pcapng

Apply a display filter ... <%>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Sonos_25:3a:2a	Spanning-tree-(for...	STP	60	Conf. Root = 36864/0/48:a6:b8:25:3a:2a Cost = 0 Port = 0x8001
2	0.105437	10.0.0.44	128.119.245.12	TCP	66	54951 → 80 [FIN, ACK] Seq=1 Ack=1 Win=2058 Len=0 TSval=492119906 TSecr=3636593796
3	0.214328	10.0.0.44	157.240.220.16	TLSv1...	98	Application Data
4	0.282262	157.240.220.16	10.0.0.44	TLSv1...	96	Application Data
5	0.282378	10.0.0.44	157.240.220.16	TCP	66	54194 → 443 [ACK] Seq=33 Ack=29 Win=2047 Len=0 TSval=492120081 TSecr=186181562
6	1.024038	Sonos_25:3a:2a	Spanning-tree-(for...	STP	60	Conf. Root = 36864/0/48:a6:b8:25:3a:2a Cost = 0 Port = 0x8001
7	1.024134	fe80::250:f1ff:fe8...	ff02::1	ICMPv6	174	Router Advertisement from 00:50:f1:80:00:00
8	1.945747	Sonos_25:3a:2a	Spanning-tree-(for...	STP	60	Conf. Root = 36864/0/48:a6:b8:25:3a:2a Cost = 0 Port = 0x8001
9	2.725290	10.0.0.44	75.75.75.75	DNS	75	Standard query 0x0722 A doh.xfinity.com
10	2.748588	75.75.75.75	10.0.0.44	DNS	116	Standard query response 0x0722 A doh.xfinity.com CNAME doh2.gslb2.xfinity.com A 75.75.77.1
11	2.748922	10.0.0.44	75.75.77.1	TCP	78	54966 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=492122546 TSecr=0 SACK_PERM
12	2.803151	75.75.77.1	10.0.0.44	TCP	64	443 → 54966 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM
13	2.803279	10.0.0.44	75.75.77.1	TCP	54	54966 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
14	2.803605	10.0.0.44	75.75.77.1	TLSv1...	571	Client Hello (SNI=doh.xfinity.com)
15	2.854305	75.75.77.1	10.0.0.44	TLSv1...	1454	Server Hello
16	2.854406	10.0.0.44	75.75.77.1	TCP	54	54966 → 443 [ACK] Seq=518 Ack=1401 Win=65535 Len=0
17	2.855755	75.75.77.1	10.0.0.44	TCP	1418	443 → 54966 [PSH, ACK] Seq=1401 Ack=518 Win=20328 Len=1364 [TCP segment of a reassembled PDU]
18	2.855856	10.0.0.44	75.75.77.1	TCP	54	54966 → 443 [ACK] Seq=518 Ack=2765 Win=65535 Len=0
19	2.856229	75.75.77.1	10.0.0.44	TCP	1418	443 → 54966 [PSH, ACK] Seq=2765 Ack=518 Win=20328 Len=1364 [TCP segment of a reassembled PDU]
20	2.856236	75.75.77.1	10.0.0.44	TCP	1418	443 → 54966 [PSH, ACK] Seq=4129 Ack=518 Win=20328 Len=1364 [TCP segment of a reassembled PDU]
21	2.856360	10.0.0.44	75.75.77.1	TCP	54	54966 → 443 [ACK] Seq=518 Ack=4129 Win=65535 Len=0
22	2.856424	10.0.0.44	75.75.77.1	TCP	54	54966 → 443 [ACK] Seq=518 Ack=5493 Win=65535 Len=0
23	2.856964	75.75.77.1	10.0.0.44	TLSv1...	985	Certificate, Server Key Exchange, Server Hello Done
24	2.857148	10.0.0.44	75.75.77.1	TCP	54	54966 → 443 [ACK] Seq=518 Ack=6424 Win=65535 Len=0
25	2.859107	10.0.0.44	75.75.77.1	TLSv1...	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
26	2.859296	10.0.0.44	75.75.77.1	TLSv1...	153	Application Data
27	2.859524	10.0.0.44	75.75.77.1	TLSv1...	300	Application Data
28	2.901627	75.75.77.1	10.0.0.44	TCP	56	443 → 54966 [ACK] Seq=6424 Ack=743 Win=29040 Len=0
29	2.901630	75.75.77.1	10.0.0.44	TLSv1...	105	Change Cipher Spec, Encrypted Handshake Message
30	2.901702	10.0.0.44	75.75.77.1	TCP	51	E4066 → 112 [ACK] Seq=6424 Ack=6475 Win=65535 Len=0

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en0, id 0

> IEEE 802.3 Ethernet

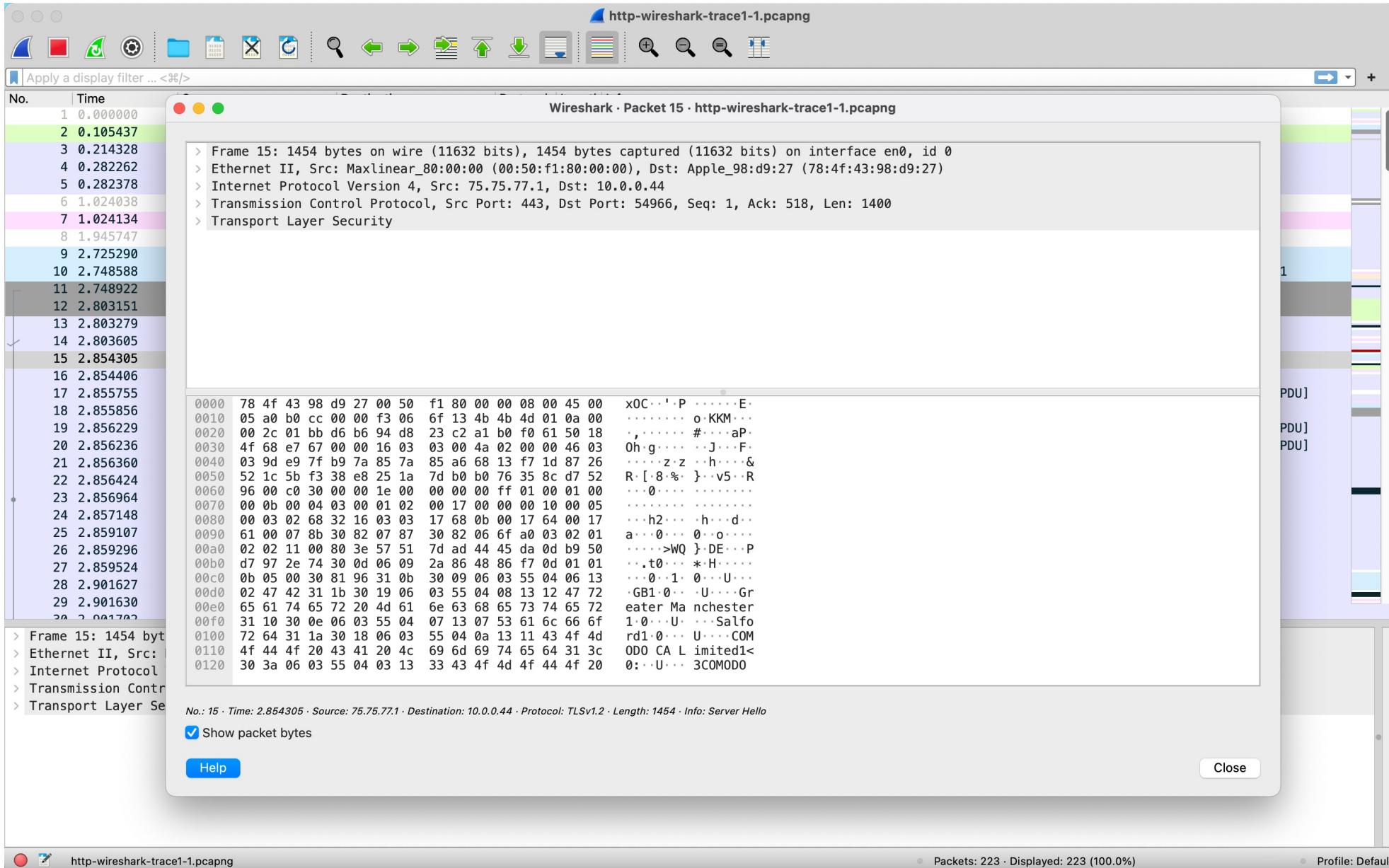
> Logical-Link Control

> Spanning Tree Protocol

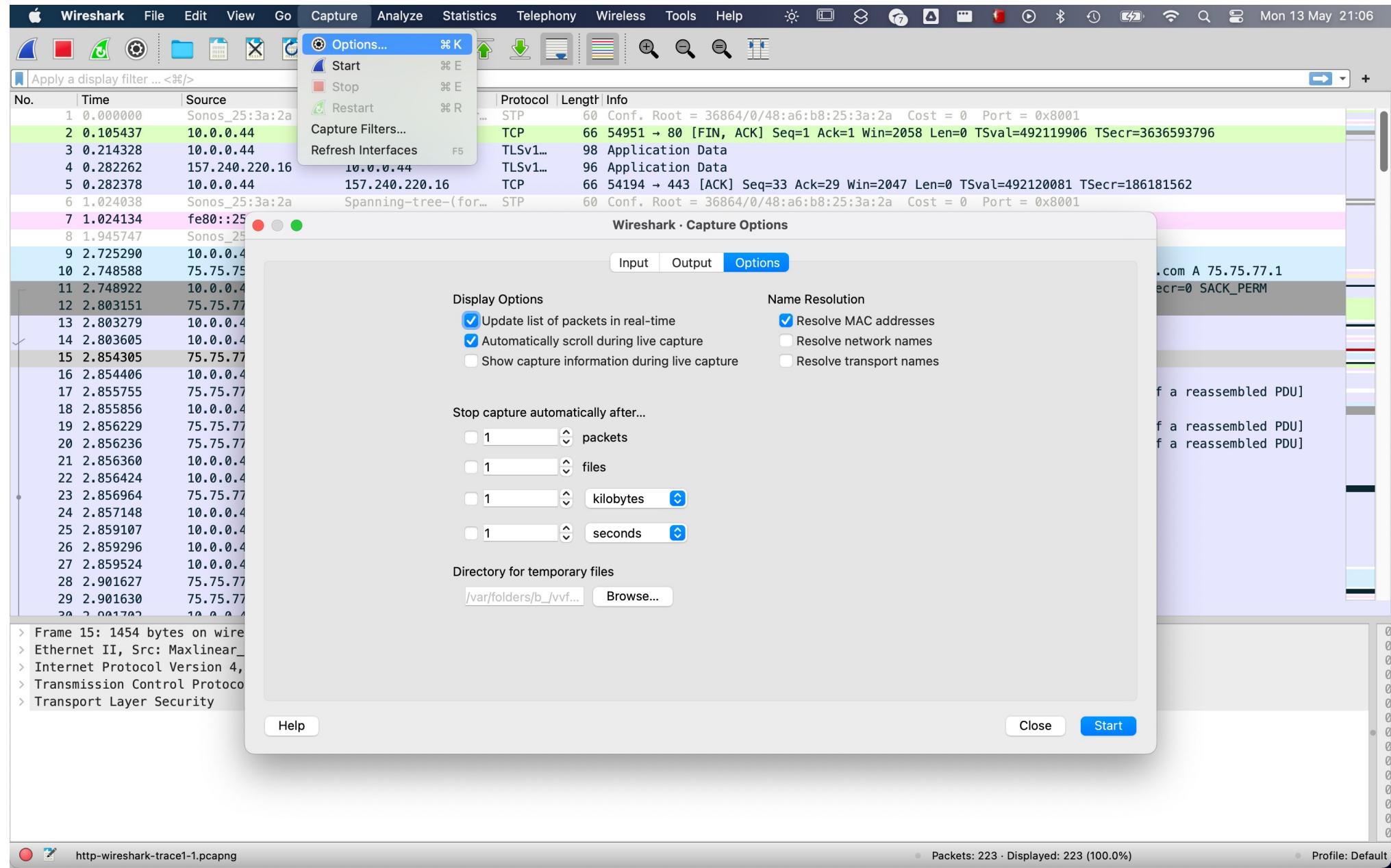
Packets: 223 · Displayed: 223 (100.0%)

Profile: Default

Visualizzazione pacchetto



Opzioni di Cattura

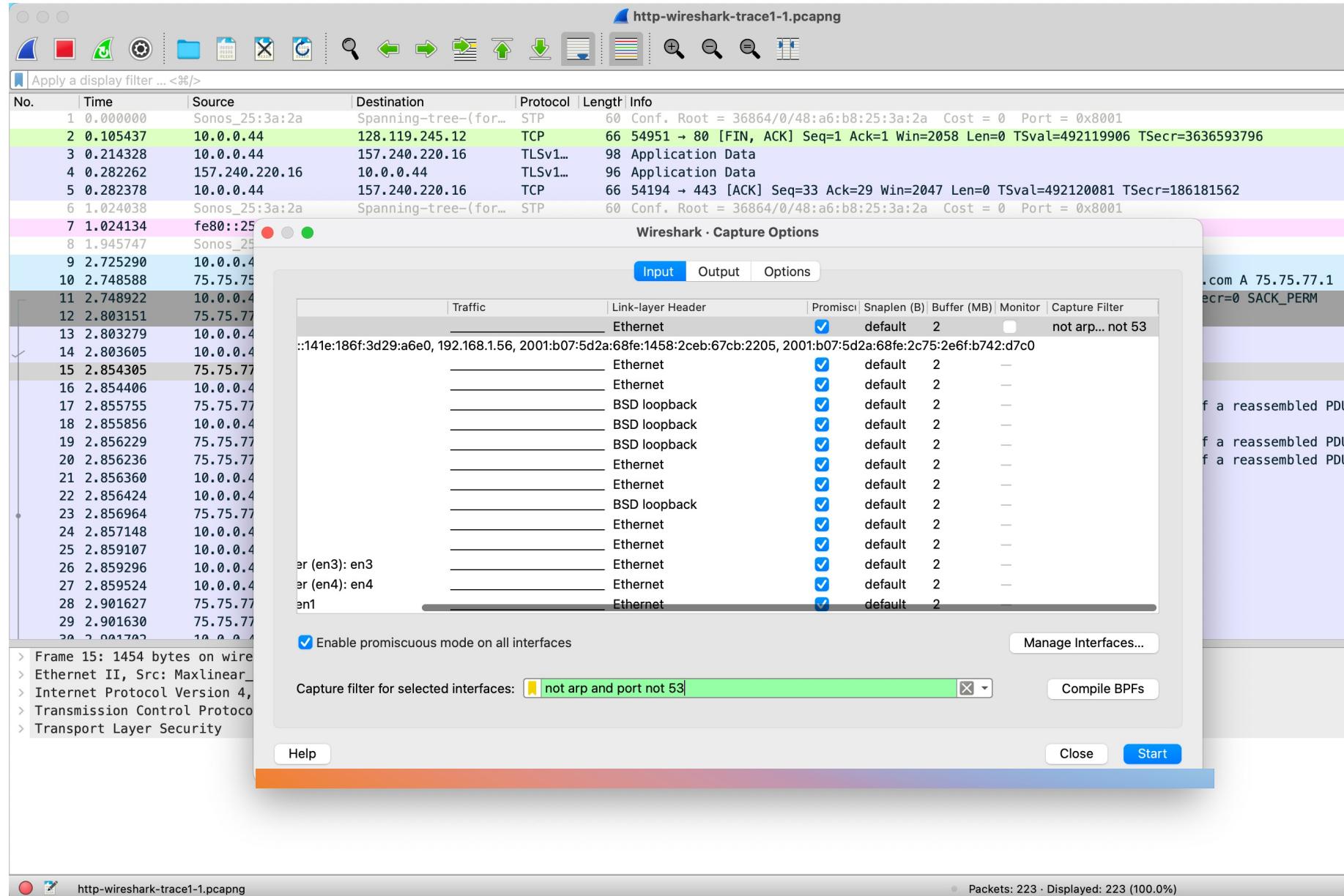


Filtri di Wireshark

- 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

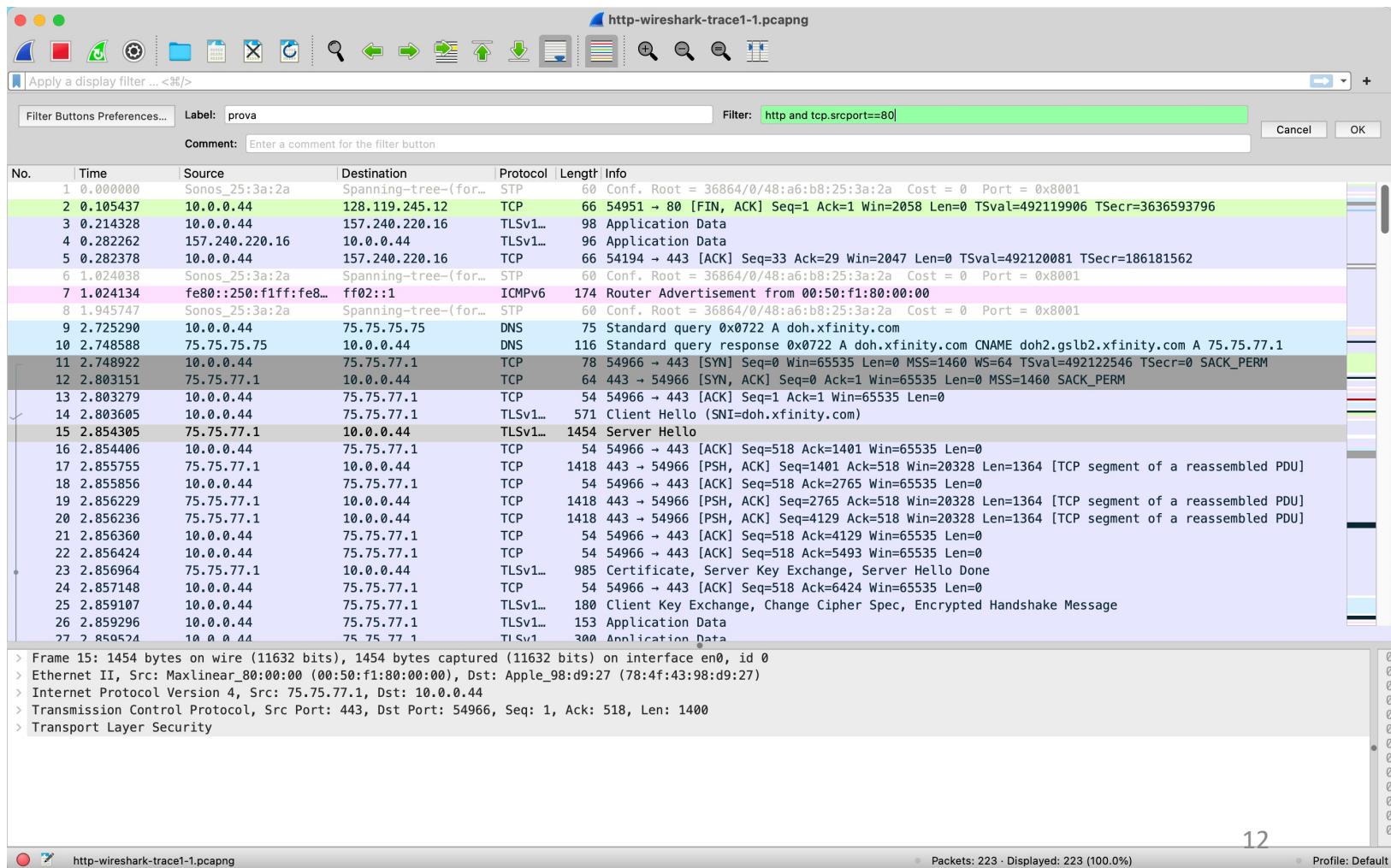
- Corretto (in verde)
 - viene compilato in un linguaggio usato dal motore di packet capture



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

Wireshark · Display Filter Expression

Field Name Relation

- > HSFZ · High Speed Fahrzeugzugang
- > HSMS · High-speed SECS Message Service Protocol
- > HSR · High-availability Seamless Redundancy (IEC62439 Part 3 Cha...
- > HSR_PRP_SUPERVISION · HSR/PRP Supervision (IEC62439 Part 3)
- > HSRP · Cisco Hot Standby Router Protocol
- > HTTP · Hypertext Transfer Protocol
 - http.accept · Accept
 - http.accept_encoding · Accept Encoding
 - http.accept_language · Accept-Language
 - http.authbasic · Credentials
 - http.authcitrix · Citrix AG Auth
 - http.authcitrix.domain · Citrix AG Domain
 - http.authcitrix.password · Citrix AG Password
 - http.authcitrix.session · Citrix AG Session ID
 - http.authcitrix.user · Citrix AG Username
 - http.authorization · Authorization
 - http.bad_header_name · Illegal characters found in header name
 - http.body.fragment · HTTP Chunked Body fragment
 - http.body.fragment.count · HTTP Chunked Body fragment count
 - http.body.fragment.error · HTTP Chunked Body defragment error
 - http.body.fragment.multiple_tails · HTTP Chunked Body has multi...
 - http.body.fragment.overlap · HTTP Chunked Body fragment overl...
 - http.body.fragment.overlap.conflicts · HTTP Chunked Body fragm...
 - http.body.fragment.too_long_fragment · HTTP Chunked Body fra...
 - http.body.fragments · Reassembled HTTP Chunked Body fragme...
 - http.body.reassembled.data · Reassembled data
 - http.body.reassembled.in · Reassembled in
 - http.body.reassembled.length · Reassembled length
 - http.body.segment · HTTP Chunked Body segment
 - http.cache_control · Cache-Control
 - http.chat · Formatted text
 - http.chunk_boundary · Chunk boundary
 - http.chunk_data · Chunk data
 - http.chunk_size · Chunk size
 - http.chunked_trailer_part · trailer-part
 - http.connection · Connection
 - http.content_encoding · Content-Encoding
 - http.content_length · Content length
- > Frame 95: 552 bytes on wire (4384 bits), 552 bytes captured (4384 bits) on interface wireless interface at 2012-01-11 10:00:00 UTC
- > Ethernet II, Src: Maxlinea [REDACTED] (08:00:27:00:00:00), Dst: Sonos [REDACTED] (08:00:27:00:00:01)
- > Internet Protocol Version 4, Src: 10.0.0.100, Dst: 10.0.0.101
- > Transmission Control Protocol, Src Port: 51213 (51213), Dst Port: 80 (80)
- > Hypertext Transfer Protocol
- > Line-based text data: text

is present
==
!=
===
!==
>
<
>=
=<
contains
matches

Relations can be used to restrict fields to specific values. Each relation does the following:

Quantifier Relation Description

Any is present Match any packet that contains this field

All ==, !=, etc. Compare the field to a specific value.

Some contains, matches Check the field against a string (contains) or a regular expression (matches)

in Compare the field to a specific set of values

Value (Character string)

Predefined Values

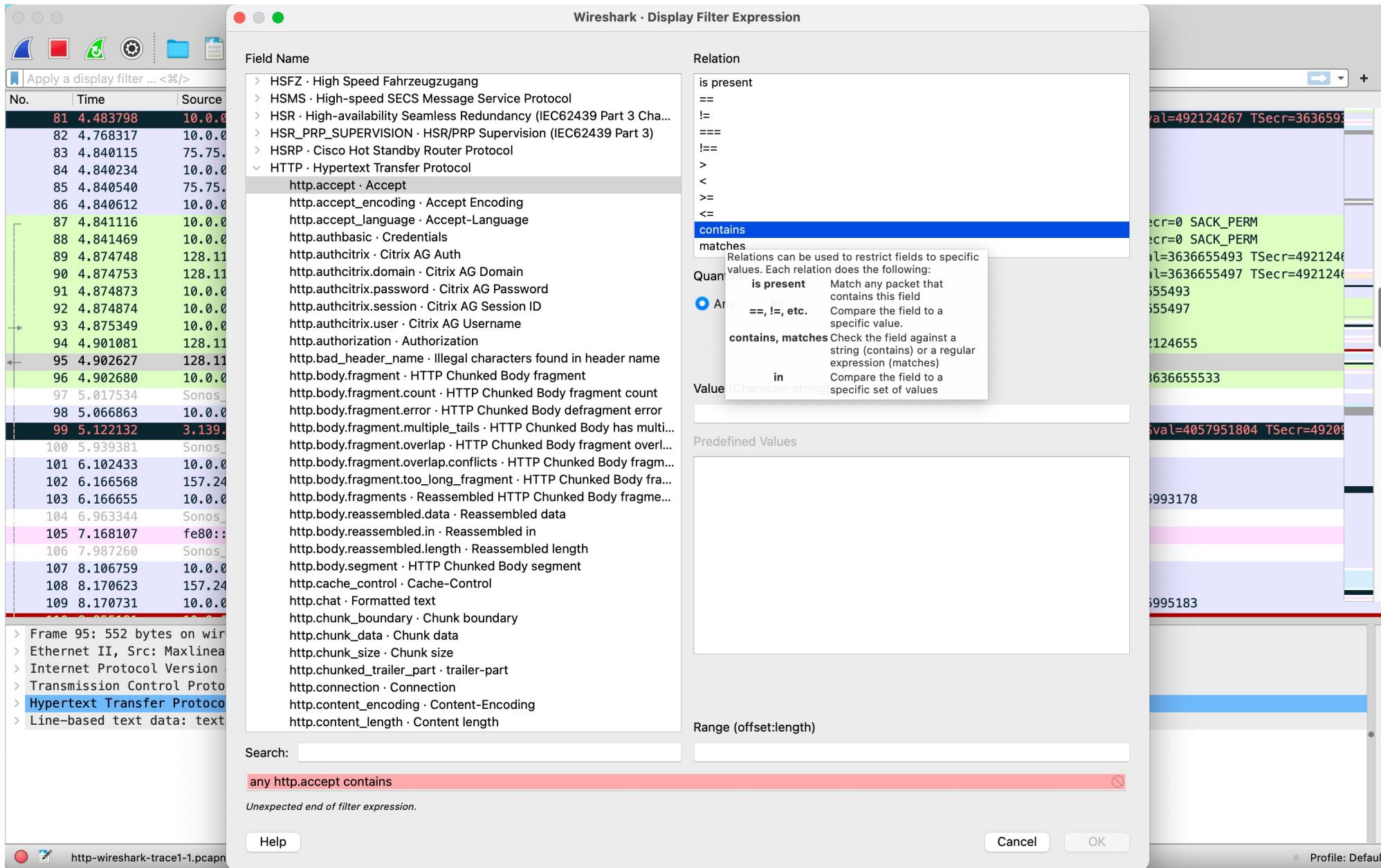
Range (offset:length)

Search: any http.accept contains

Unexpected end of filter expression.

Help Cancel OK

Profile: Default



Statistics/Conversations

http-wireshark-trace1-1.pcapng

Apply a display filter ... <%>

Wireshark · Conversations · http-wireshark-trace1-1.pcapng

Conversation Settings

- Name resolution
- Absolute start time
- Limit to display filter

Copy

Follow Stream...

Graph...

Protocol

- Bluetooth
- BPv7
- DCCP
- Ethernet
- FC
- FDDI
- IEEE 802.11
- IEEE 802.15.4
- IPv4
- IPv6
- IPX
- IXTA

Filter list for specific type

Ethernet · 4	IPv4 · 10	IPv6 · 1	TCP · 12	UDP · 4								
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