



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA
CAMPUS DI CESENA

Programmazione di Reti Analizzatore di Protocollo

Andrea Piroddi

Dipartimento di Informatica, Scienza e Ingegneria

ANALIZZATORE di PROTOCOLLO



ANALIZZATORE di PROTOCOLLO

#	LIVELLO	ESEMPI	DENOMINAZIONE PACCHETTO	IMPLEMENTAZIONE	INDIRIZZAMENTO
5	Applicazione	HTTP, FTP, DNS, TLS	Messaggio	SW	Nomi
4	Trasporto	TCP, UDP, SCTP	Segmento	SW	Porte
3	Rete	IP, {routing}	Datagramma	SW	Indirizzi IP
2	Collegamento	Ethernet	Frame	HW	Indirizzi MAC
1	Fisico		Bit	HW	



ANALIZZATORE di PROTOCOLLO

Descrizione livelli

Livello 2 (data link): il suo servizio per i livelli superiori è quello di instaurare un collegamento tra due punti contigui della rete libero da errori di trasmissione non segnalati.

Livello 3 (network): il suo compito è quello di inserire dei pacchetti nella rete in modo tale che questi viaggino verso una destinazione; il protocollo utilizzato è il IP.

Livello 4 (trasporto): permette a due entità di pari livello di portare avanti una conversazione; i protocolli utilizzati sono due: TCP orientato alla connessione e affidabile e l'altro l' UDP (User Datagram Protocol) che non è orientato alla connessione e inaffidabile.

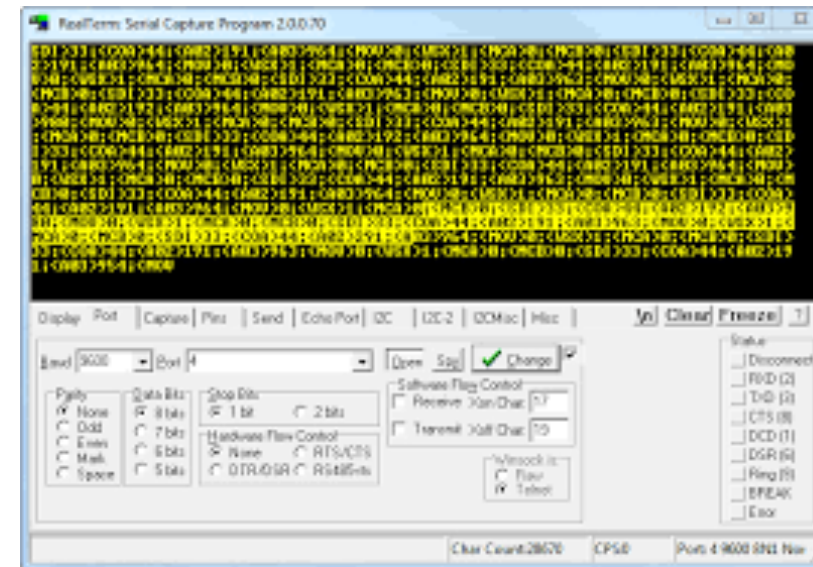
Livello 5 (applicazione): in questo livello fanno parte i diversi protocolli utilizzati dalle applicazioni degli utenti: terminale virtuale (TELNET), posta elettronica (SMTP), trasferimento archivi (FTP), web (HTML), ecc....



ANALIZZATORE di PROTOCOLLO

Un **Analizzatore di Protocollo** è un hardware o un software utilizzato per intercettare e catturare il traffico inviato su una rete.

Analizzatori di protocollo sono anche denominati Analizzatori di Rete o Analizzatori di Pacchetti.



ANALIZZATORE di PROTOCOLLO

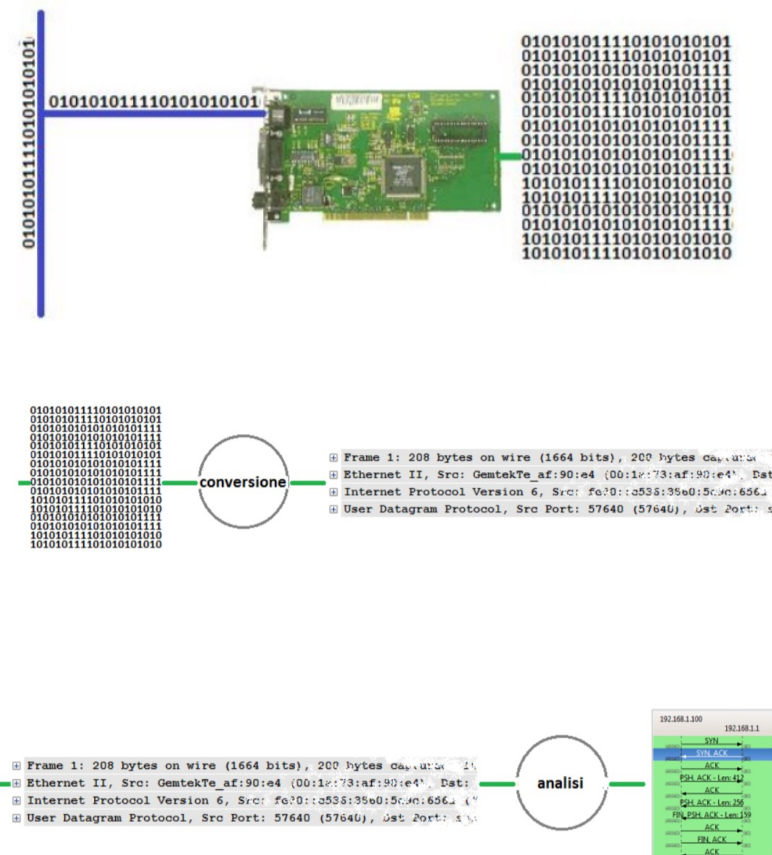
- Questo strumento, una volta catturati i Frames, li analizza in profondità decodificandoli e dissezionandoli. Fatto questo, è capace di mostrare il traffico di rete in una configurazione che sia leggibile e comprensibile dagli esseri umani. Questo permette agli utenti di comprendere quello che sta accadendo sulla rete.
- Si installa sopra un sistema operativo standard (SO) e utilizza per la cattura dei pacchetti le schede di interfaccia di rete (NIC - Network Interface Card) in modalità promiscua. Questa è una particolare modalità che permette di leggere tutto il traffico che transita in quel punto della rete, non solo quello diretto ad una specifica interfaccia. La modalità **promiscua** è l'opposto della modalità **non-promiscua** con cui funziona "normalmente" una NIC.
- Normalmente quando i pacchetti così formati vengono trasmessi sopra una rete, vengono inviati a "tutti gli ascoltatori" che sono in attesa sul segmento di rete, cioè a tutte le NIC di una LAN, essendo il mezzo in condivisione.
- Questa modalità di funzionamento viene definita **Broadcast**, cioè trasmissione di tutto a tutti.



ANALIZZATORE di PROTOCOLLO

Il processo di lavoro di un analizzatore di protocollo può essere suddiviso in tre fasi:

1. **Raccolta:** La prima fase comprende la selezione e il corretto posizionamento sulla rete dell'interfaccia di cattura in promiscuous mode. In questa modalità è possibile per l'interfaccia di cattura ascoltare tutto il traffico del particolare segmento di rete in cui è posizionata la sonda.
2. **Conversione:** In questa fase, i dati binari grezzi catturati sono convertiti in un formato comprensibile. In questo stato i dati catturati sono in una forma che consente di interpretarli solo ad un livello molto basso.
3. **Analisi:** Nella terza fase, l'analizzatore di protocollo prende i dati catturati sulla rete, verifica i protocolli basandosi sulle informazioni estratte e in base alle loro caratteristiche specifiche li analizza.



WIRESHARK



ANALIZZATORE di PROTOCOLLO - WIRESHARK

Ai link seguenti potete trovare il manuale di Wireshark e i pacchetti di installazione.


Manuale Wireshark:

<https://www.wireshark.org/download/docs/user-guide.pdf>

Download Pacchetto installativo:

<https://www.wireshark.org/download.html>

Stable Release (3.2.2)

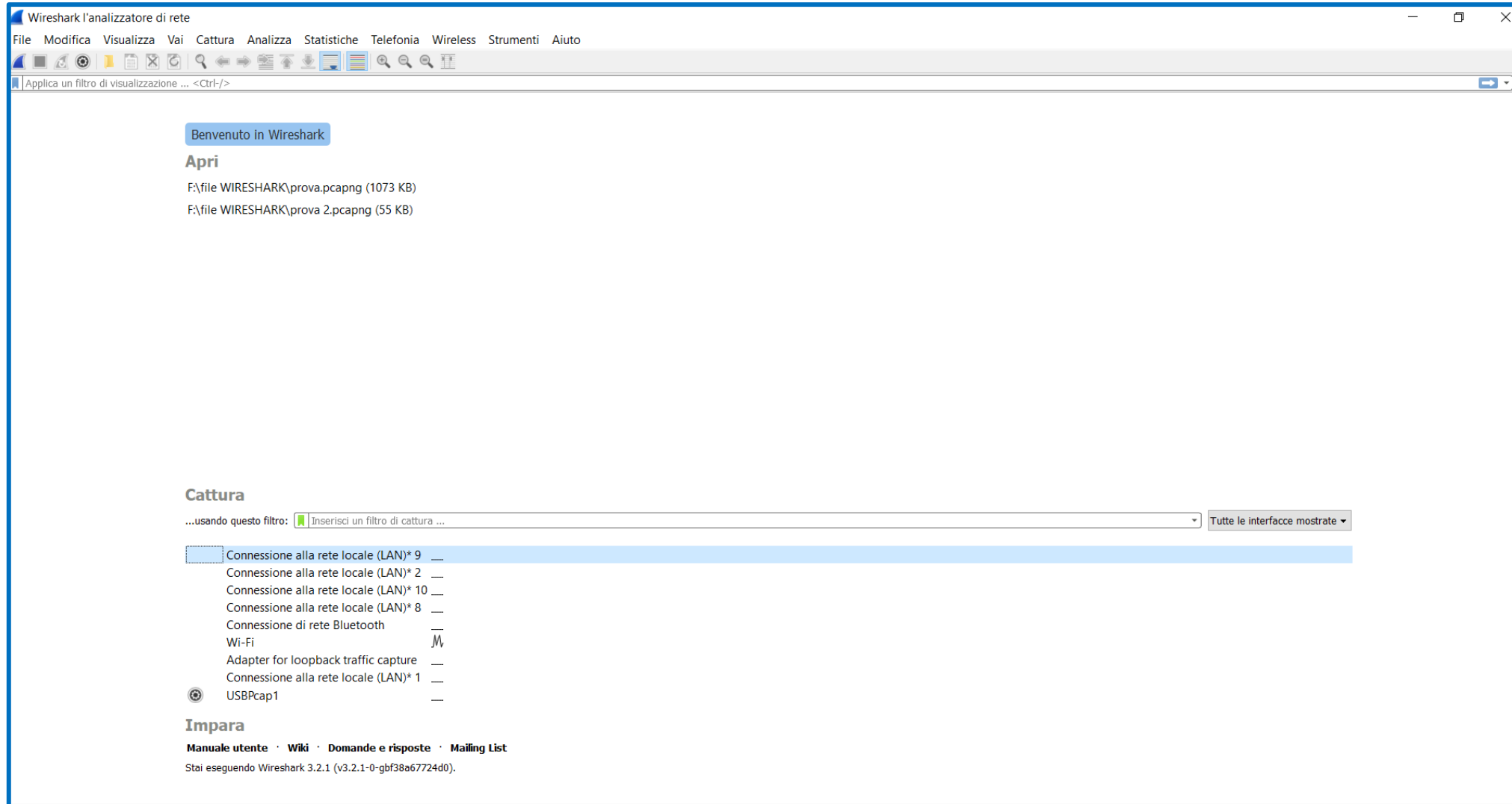
 Windows Installer (64-bit)
Windows Installer (32-bit)
Windows PortableApps® (32-bit)
macOS Intel 64-bit .dmg
Source Code

VENDOR / PLATFORM	SOURCES
Alpine / Alpine Linux	Standard package
Apple / macOS	Homebrew (Formula) MacPorts Fink
Arch Linux / Arch Linux	Standard package
Canonical / Ubuntu	Standard package Latest stable PPA
Debian / Debian GNU/Linux	Standard package
The FreeBSD Project / FreeBSD	Standard package
Gentoo Foundation / Gentoo Linux	Standard package
HP / HP-UX	Porting And Archive Centre for HP-UX
NetBSD Foundation / NetBSD	Standard package
Novell / openSUSE, SUSE Linux	Standard package
Offensive Security / Kali Linux	Standard package
PCLinuxOS / PCLinuxOS	Standard package
Red Hat / Fedora	Standard package
Red Hat / Red Hat Enterprise Linux	Standard package
Slackware Linux / Slackware	SlackBuilds.org
Oracle / Solaris 11	Standard package
* / *	The Written Word



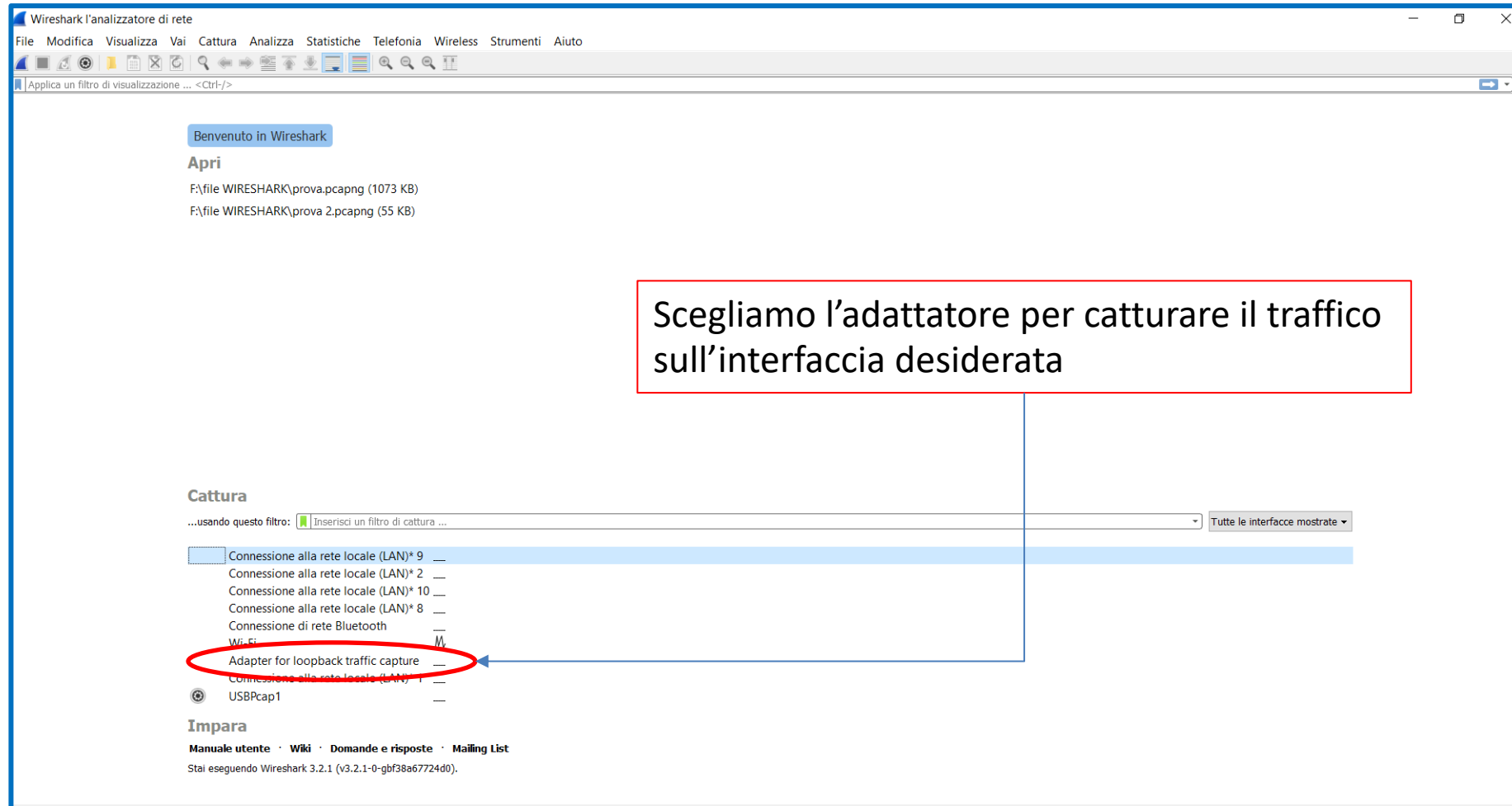
ANALIZZATORE di PROTOCOLLO - WIRESHARK

L'interfaccia grafica si presenta così:

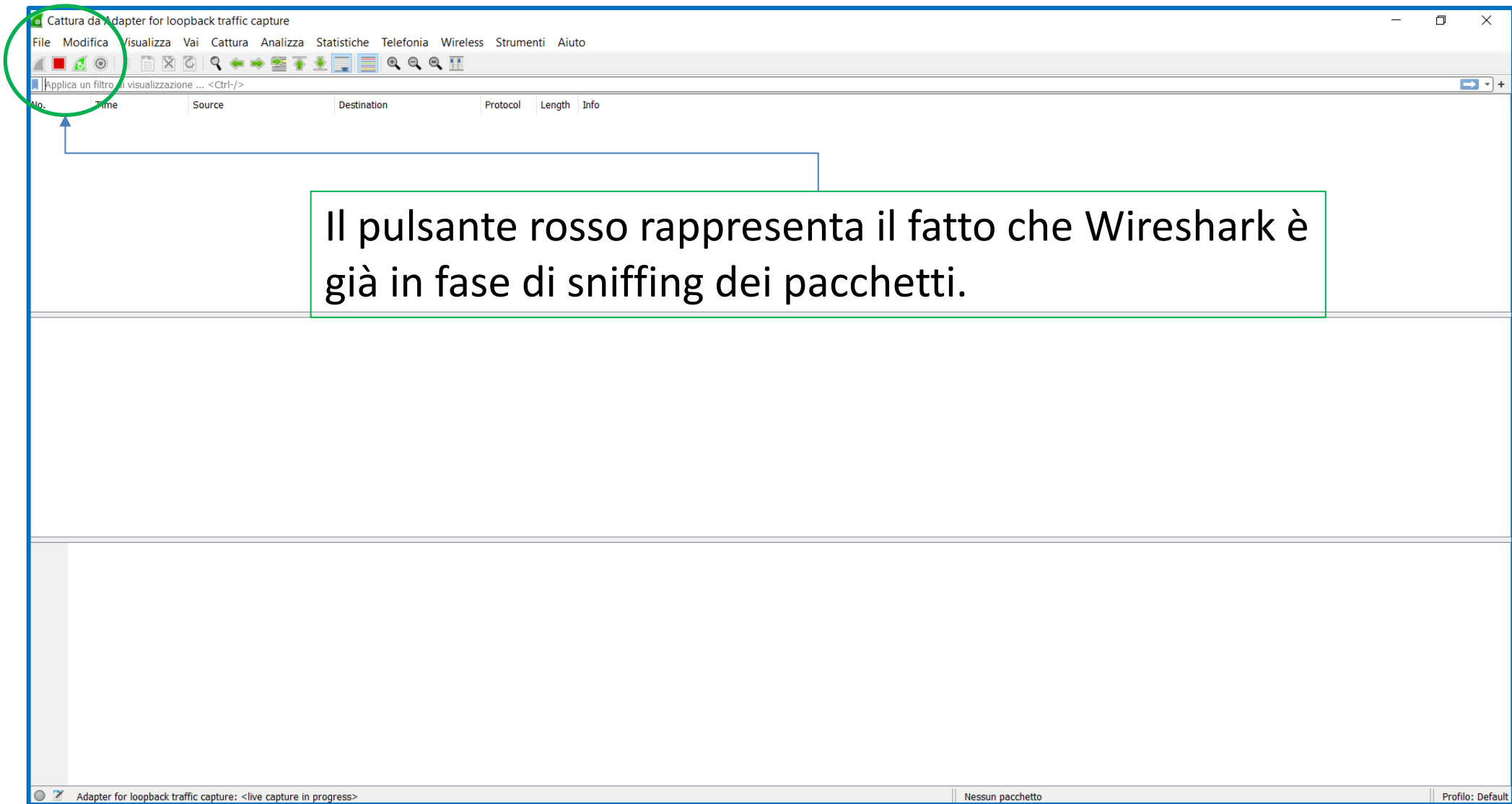


ANALIZZATORE di PROTOCOLLO - WIRESHARK

Selezionare l'interfaccia di rete su cui si vuole effettuare lo sniffing dei pacchetti



ANALIZZATORE di PROTOCOLLO - WIRESHARK



ANALIZZATORE di PROTOCOLLO - WIRESHARK

Wireshark è attivo e sta sniffando il traffico che proviene ed è destinato alla interfaccia selezionata.

Aprirete un browser e navigate con una sessione http verso un qualsiasi sito web.

http://www.brescianet.com/appunti/sistemi/http_protocol.htm

Comincerete a vedere nell'interfaccia di Wireshark alcune righe informative del tipo:

UDP_transaction.pcapng

File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonica Wireless Strumenti Aiuto

Applica un filtro di visualizzazione ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
109	196.550544	127.0.0.1	127.0.0.1	TCP	183	61873 → 61871 [PSH, ACK] Seq=144 Ack=5491 Win=2614272 Len=99
110	196.550617	127.0.0.1	127.0.0.1	TCP	84	61871 → 61873 [ACK] Seq=5491 Ack=243 Win=2619392 Len=0
111	196.563593	127.0.0.1	127.0.0.1	TCP	113	61871 → 61873 [PSH, ACK] Seq=5491 Ack=243 Win=2619392 Len=29
112	196.563651	127.0.0.1	127.0.0.1	TCP	84	61873 → 61871 [ACK] Seq=243 Ack=5520 Win=2614272 Len=0
113	196.564295	127.0.0.1	127.0.0.1	TCP	151	61873 → 61871 [PSH, ACK] Seq=243 Ack=5520 Win=2614272 Len=67
114	196.564353	127.0.0.1	127.0.0.1	TCP	84	61871 → 61873 [ACK] Seq=5520 Ack=310 Win=2619392 Len=0
115	196.568255	127.0.0.1	127.0.0.1	TCP	113	61871 → 61873 [PSH, ACK] Seq=5520 Ack=310 Win=2619392 Len=29
117	198.594922	127.0.0.1	127.0.0.1	UDP	83	54885 → 10000 Len=23
118	198.595261	127.0.0.1	127.0.0.1	TCP	103	61873 → 61871 [PSH, ACK] Seq=5520 Ack=5549 Win=2614016 Len=100
119	198.595418	127.0.0.1	127.0.0.1	TCP	173	61873 → 61871 [PSH, ACK] Seq=310 Ack=5549 Win=2614016 Len=89
120	198.595435	127.0.0.1	127.0.0.1	TCP	84	61871 → 61873 [ACK] Seq=5549 Ack=5520 Win=2614016 Len=0

> Frame 117: 83 bytes on wire (664 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{...}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

> User Datagram Protocol, Src Port: 54885, Dst Port: 10000

> Data (23 bytes)

0000 02 00 00 00 45 00 00 33 79 3a 00 00 80 11 00 00E..3 y:.....

0010 7f 00 00 01 7f 00 00 01 d6 65 27 10 00 1f da c5e.....

0020 51 75 65 73 74 6f 20 c3 a8 20 69 6c 20 63 6f 72 Questo - il cor

0030 73 6f 20 64 69 20 3f so di ?

Data (data.data), 23 byte

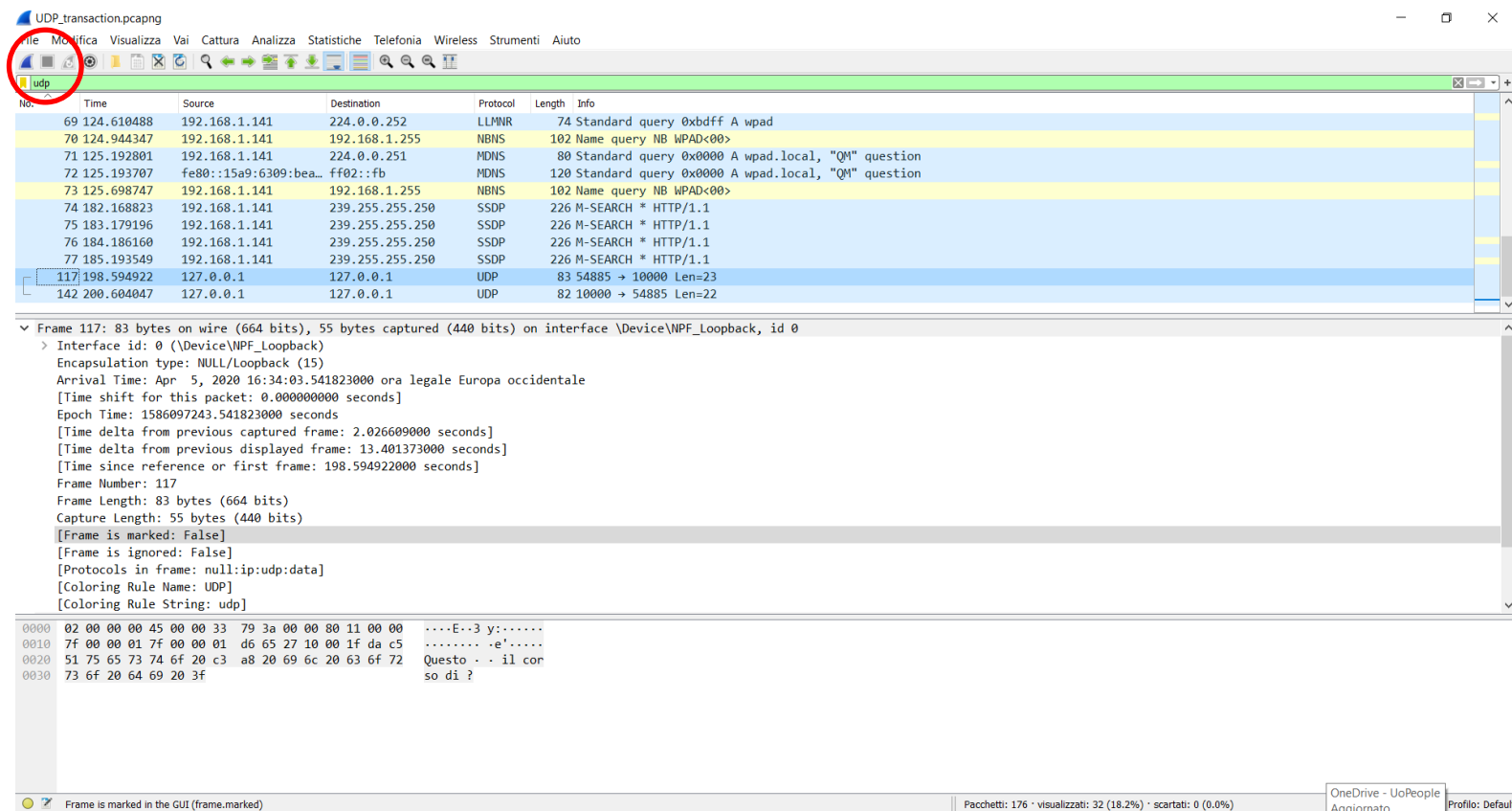
Pacchetti: 176 · visualizzati: 176 (100.0%) · scartati: 0 (0.0%)

Profilo: Default



ANALIZZATORE di PROTOCOLLO - WIRESHARK

Stoppiamo lo sniffing,
E salviamo il file in modo da averlo disponibile per successive analisi.



ANALIZZATORE di PROTOCOLLO - WIRESHARK

Applichiamo un filtro, per esempio traffico TCP

NOTA: stiamo solo filtrando la visualizzazione non stiamo filtrando il traffico catturato, cosa che invece è possibile fare utilizzando i filtri di cattura.

The screenshot shows the Wireshark interface with the following details:

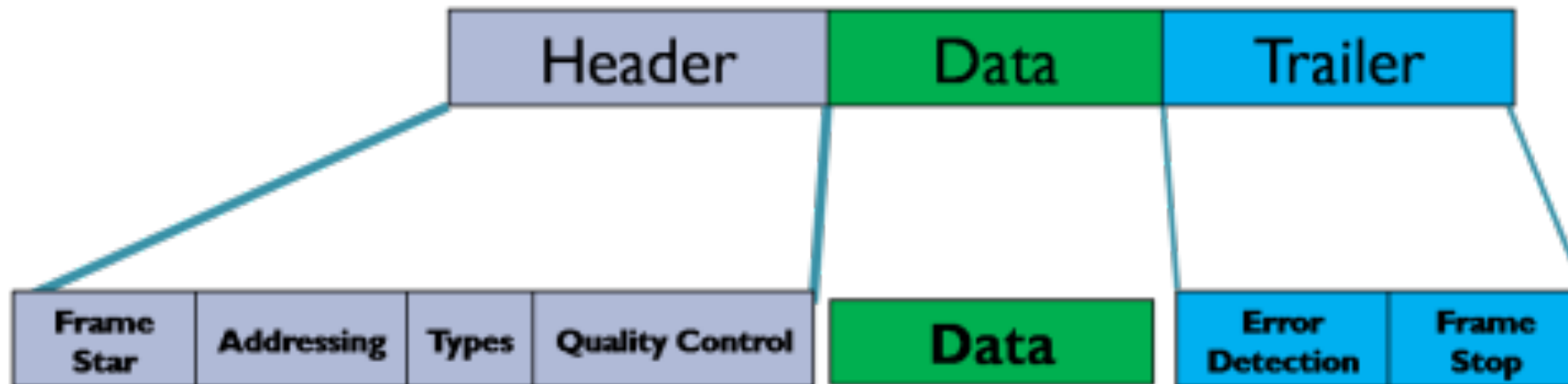
- Filter Bar:** A red circle highlights the 'udp' filter applied in the filter bar.
- Packet List:** A table of captured packets. Packet 117 is highlighted with a red box. It is a UDP packet from 198.59.49.22 to 127.0.0.1, length 83 bytes.
- Packet Details:** The details pane shows the structure of packet 117: Interface id: 0, Encapsulation type: NULL/Loopback (15), Arrival Time: Apr 5, 2020 16:34:03.541823000, Epoch Time: 1586097243.541823000, Frame Number: 117, Frame Length: 83 bytes (664 bits), Capture Length: 55 bytes (440 bits), [Frame is marked: False], [Frame is ignored: False], [Protocols in frame: null:ip:udp:data], [Coloring Rule Name: UDP], [Coloring Rule String: udp].
- Packet Bytes:** The bottom pane shows the raw bytes of the packet in hexadecimal and ASCII. The ASCII part shows the text 'Questo - il cor so di ?'.

Analizziamo la richiesta del client



ANALIZZATORE di PROTOCOLLO – WIRESHARK - FRAME

Il livello data link (Collegamento) si occupa di fornire ai livelli superiori una linea di comunicazione esente da errori di trasmissione non segnalati; per fare questo decompone i dati del mittente in pacchetti chiamati frame, composti da alcune centinaia o migliaia di byte, e li spedisce in sequenza attendendo eventualmente la conferma di avvenuta ricezione da parte del destinatario.



ANALIZZATORE di PROTOCOLLO – WIRESHARK - FRAME

(15) È un valore interno di Wireshark che rappresenta il particolare tipo di intestazione del livello di collegamento per il pacchetto in questione e i valori numerici possono differire da una versione all'altra.

▼ Frame 117: 83 bytes on wire (664 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{Loopback}, id 0

> Interface id: 0 (\Device\NPF Loopback)

Encapsulation type: NULL/Loopback (15)

Arrival Time: Apr 5, 2020 16:34:03.541823000 ora legale Europa occidentale
[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1586097243.541823000 seconds

[Time delta from previous captured frame: 2.026609000 seconds]
[Time delta from previous displayed frame: 2.026609000 seconds]
[Time since reference or first frame: 198.594922000 seconds]

Frame Number: 117

Frame Length: 83 bytes (664 bits)

Capture Length: 55 bytes (440 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: null:ip:udp:data]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

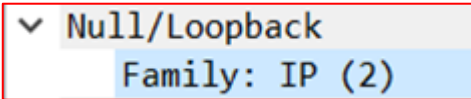
Epoch Time (noto anche come tempo UNIX) è il numero di secondi dal 1 ° gennaio 1970. Questo è ciò che è effettivamente memorizzato nel file .pcap o .pcapng. Gli altri formati di tempo in Wireshark sono conversioni del Epoch Time a scopo di visualizzazione.

Frame is Marked: False - Wireshark ci permette di "contrassegnare" una frame; vedete «Marca / Deseleziona pacchetto» nel menu "Modifica". "Il frame è contrassegnato: False" significa che il frame non è stato "contrassegnato".

Frame is Ignored: False - Wireshark ci permette anche di "ignorare" un pacchetto; se «Ignora/Considera Pacchetto» nel menu "Modifica". "Frame ignorato: False" significa che il frame non è stato "ignorato".



ANALIZZATORE di PROTOCOLLO – WIRESHARK - Networking



Il protocollo "**null**" è il protocollo a livello di collegamento utilizzato sull'interfaccia di loopback sulla maggior parte dei sistemi operativi BSD.

È chiamato impropriamente «**null**», in quanto l'intestazione del livello di collegamento non è «nulla»; l'intestazione del livello di collegamento è un numero intero di 4 byte, nell'ordine di byte nativo della macchina su cui viene acquisito il traffico, contenente un valore "famiglia di indirizzi" / "famiglia di protocollo" per il protocollo in esecuzione sul livello di collegamento, ad esempio AF_INET per IPv4 e AF_INET6 per IPv6. **AF_INET** è **2** su tutti i sistemi operativi basati su BSD (Berkeley Sockets - <http://www.on-time.com/rtos-32-docs/rtip-32/programming-manual/programming-with/berkeley-socket-api.htm>)



ANALIZZATORE di PROTOCOLLO – WIRESHARK - Networking

Il campo Identificazione è semplicemente un ID univoco applicato a ciascun pacchetto che un host invia su una determinata connessione. È generalmente utile solo se un pacchetto deve essere frammentato (diciamo da un router) - ogni frammento manterrà l'identificazione originale. Permette all'host ricevente di sapere come riassemblare i frammenti.

▼ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 51

Identification: 0x793a (31034)

> Flags: 0x0000

...0 0000 0000 0000 = Fragment offset: 0

Time to live: 128

Protocol: UDP (17)

Header checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source: 127.0.0.1

Destination: 127.0.0.1



ANALIZZATORE di PROTOCOLLO – WIRESHARK - TRASPORTO

✓ User Datagram Protocol, Src Port: 54885, Dst Port: 10000

Source Port: 54885

Destination Port: 10000

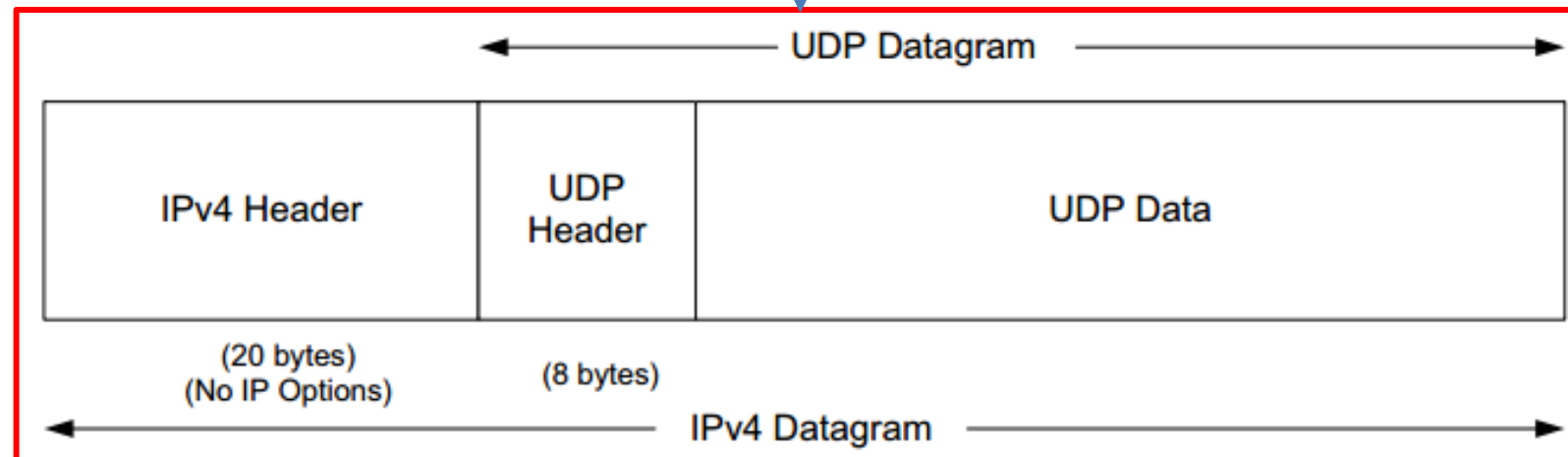
Length: 31

Checksum: 0xdac5 [unverified]

[Checksum Status: Unverified]

[Stream index: 9]

> [Timestamps]



ANALIZZATORE di PROTOCOLLO - WIRESHARK

UDP_transaction.pcapng

File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto

udp

No.	Time	Source	Destination	Protocol	Length	Info
69	124.610488	192.168.1.141	224.0.0.252	LLMNR	74	Standard query 0xbdf A wpad
70	124.944347	192.168.1.141	192.168.1.255	NBNS	102	Name query NB WPAD<00>
71	125.192801	192.168.1.141	224.0.0.251	MDNS	80	Standard query 0x0000 A wpad.local, "QM" question
72	125.193707	fe80::15a9:6309:bea...	ff02::fb	MDNS	120	Standard query 0x0000 A wpad.local, "QM" question
73	125.698747	192.168.1.141	192.168.1.255	NBNS	102	Name query NB WPAD<00>
74	182.168823	192.168.1.141	239.255.255.250	SSDP	226	M-SEARCH * HTTP/1.1
75	183.179196	192.168.1.141	239.255.255.250	SSDP	226	M-SEARCH * HTTP/1.1
76	184.186160	192.168.1.141	239.255.255.250	SSDP	226	M-SEARCH * HTTP/1.1
77	185.193549	192.168.1.141	239.255.255.250	SSDP	226	M-SEARCH * HTTP/1.1
117	108.504022	127.0.0.1	127.0.0.1	UDP	82	10000 → 54885 Len=22
142	200.604047	127.0.0.1	127.0.0.1	UDP	82	10000 → 54885 Len=22

> Frame 142: 82 bytes on wire (656 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{Loopback}, id 0

▼ Null/Loopback

Family: IP (2)

> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

> User Datagram Protocol, Src Port: 10000, Dst Port: 54885

> Data (22 bytes)

0000 02 00 00 00 45 00 00 32 79 53 00 00 80 11 00 00 ...E--2 yS.....
0010 7f 00 00 01 7f 00 00 01 27 10 d6 65 00 1e da ee'.e.....
0020 50 72 6f 67 72 61 6d 6d 61 7a 69 6f 6e 65 20 64 Programm azione d
0030 69 20 52 65 74 69 i Reti

Data (data.data), 22 byte

Pacchetti: 176 · visualizzati: 32 (18.2%) · scartati: 0 (0.0%)

Profilo: Default

Analizziamo la risposta del server



ANALIZZATORE di PROTOCOLLO - WIRESHARK

L	142	200.604047	127.0.0.1	127.0.0.1	UDP	82	10000 → 54885	Len=22									
> Frame 142: 82 bytes on wire (656 bits), 54 bytes captured (432 bits) on interface \Device\NPF_Loopback, id 0																	
v Null/Loopback																	
Family: IP (2)																	
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1																	
v User Datagram Protocol, Src Port: 10000, Dst Port: 54885																	
Source Port: 10000																	
Destination Port: 54885																	
Length: 30																	
Checksum: 0xdaee [unverified]																	
[Checksum Status: Unverified]																	
[Stream index: 9]																	
> [Timestamps]																	
v Data (22 bytes)																	
Data: 50726f6772616d6d617a696f6e652064692052657469																	
[Length: 22]																	
0000	02	00	00	00	45	00	00	32	79	53	00	00	80	11	00	00E..2 yS.....
0010	7f	00	00	01	7f	00	00	01	27	10	d6	65	00	1e	da	ee'.e....
0020	50	72	6f	67	72	61	6d	6d	61	7a	69	6f	6e	65	20	64	Programm azione d
0030	69	20	52	65	74	69											i Reti

