



# Corso di Digital Forensics

CdLM in Informatica

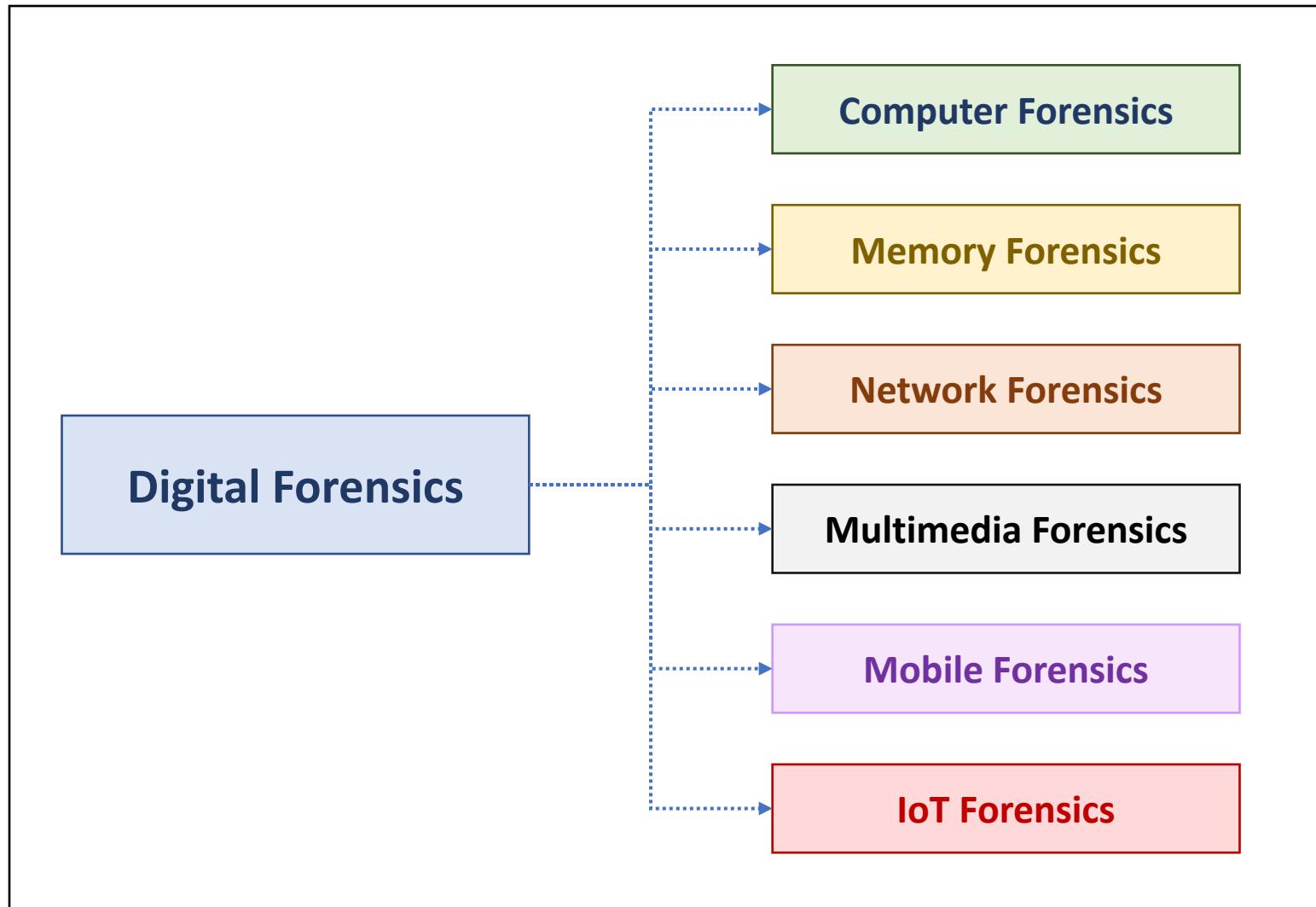
Università degli Studi di Salerno

Docente: Ugo Fiore

6 – Network Forensics

# Network Forensics

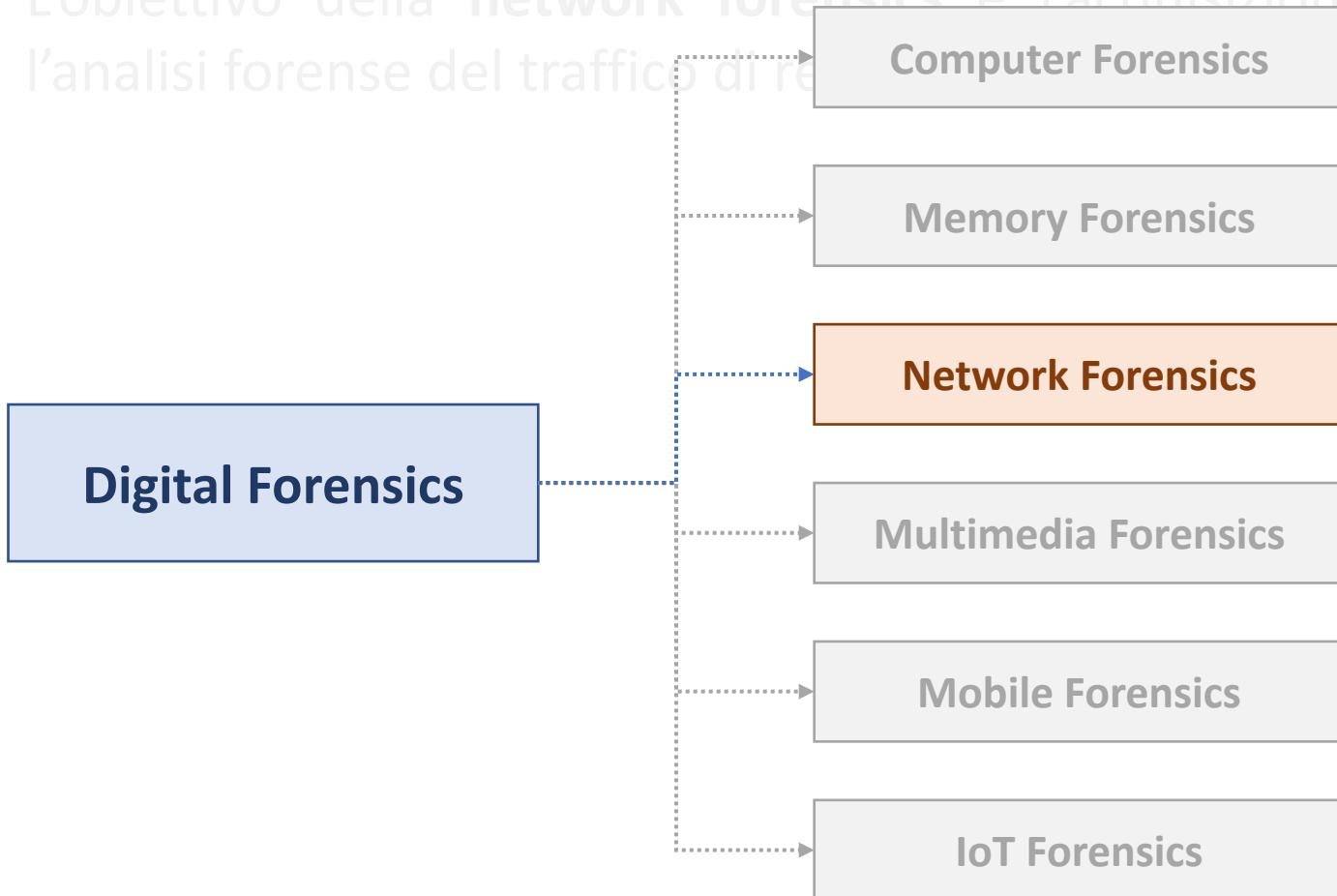
## Caratteristiche | 1/3



# Network Forensics

## Caratteristiche | 2/3

- L'obiettivo della network forensics è l'acquisizione e l'analisi forense del traffico di rete.



# Network Forensics

## Caratteristiche | 3/3

- La **network forensics** è un ramo della digital forensics
- Si occupa degli **aspetti forensi** riguardanti le reti (computer, apparati di rete, ecc.)
- Principalmente, la network forensics viene eseguita sui live system
  - Viene acquisito il traffico *raw*, prodotto dalle interfacce di rete di un dispositivo informatico
    - Pacchetti, eventuali log, ecc.
  - Tale traffico viene poi analizzato

# Il tool Xplico

# Il tool Xplico

## Caratteristiche | 1/3

- **Xplico** è un tool Open Source che permette l'**analisi forense di traffico di rete**
- L'**acquisizione del traffico di rete** può essere eseguita mediante **Xplico stesso** o mediante tool esterni (ad esempio, **Wireshark**, **Ettercap**, ecc.)
  - **NOTA:** Wireshark ed Ettercap sono direttamente disponibili in Kali Linux e Parrot Linux
- Xplico permette di analizzare file che contengono acquisizioni di rete, i quali hanno generalmente estensione **.pcap (packet capture)**
- Ulteriori caratteristiche possono ed informazioni su Xplico possono essere reperite al seguente link:
  - <https://www.xplico.org/>

# Il tool Xplico

## Caratteristiche | 1/3

*Maggiori dettagli nelle prossime slide...*

*l'analisi*

- Xplico è un tool forense di traffico di rete.
- **L'acquisizione del traffico di rete** può essere eseguita mediante **Xplico stesso** o mediante tool esterni (ad esempio, **Wireshark**, **Ettercap**, ecc.)
  - NOTA: Wireshark ed Ettercap sono direttamente disponibili in Kali Linux e Parrot Linux
- Xplico permette di analizzare file che contengono acquisizioni di rete, i quali hanno generalmente estensione .pcap (**packet caputre**)
- Ulteriori caratteristiche possano ed informazioni su Xplico possono essere reperite al seguente link:
  - <https://www.xplico.org/>

# Il tool Xplico

## Caratteristiche | 2/3

- Tantissimi protocolli di rete sono supportati da Xplico, fra cui:
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
  - Hypertext Transfer Protocol (HTTP)
  - File Transfer Protocol (FTP)
  - Internet Message Access Protocol (IMAP)
  - Simple Mail Transfer Protocol (SMTP)
  - Post Office Protocol (POP3)
  - Ecc.
- Fornisce una interfaccia intuitiva e web-based

# Il tool Xplico

## Caratteristiche | 3/3



All'interno del traffico di rete  
possiamo trovare **tracce molto utili**  
**per le indagini**, ad esempio:

[Indirizzi Web di Siti Visitati](#)

[Contenuto di E-mail](#)

[Chat di Social Network](#)

[Pacchetti VoIP](#)

[File Stampati](#)



# Il tool Xplico

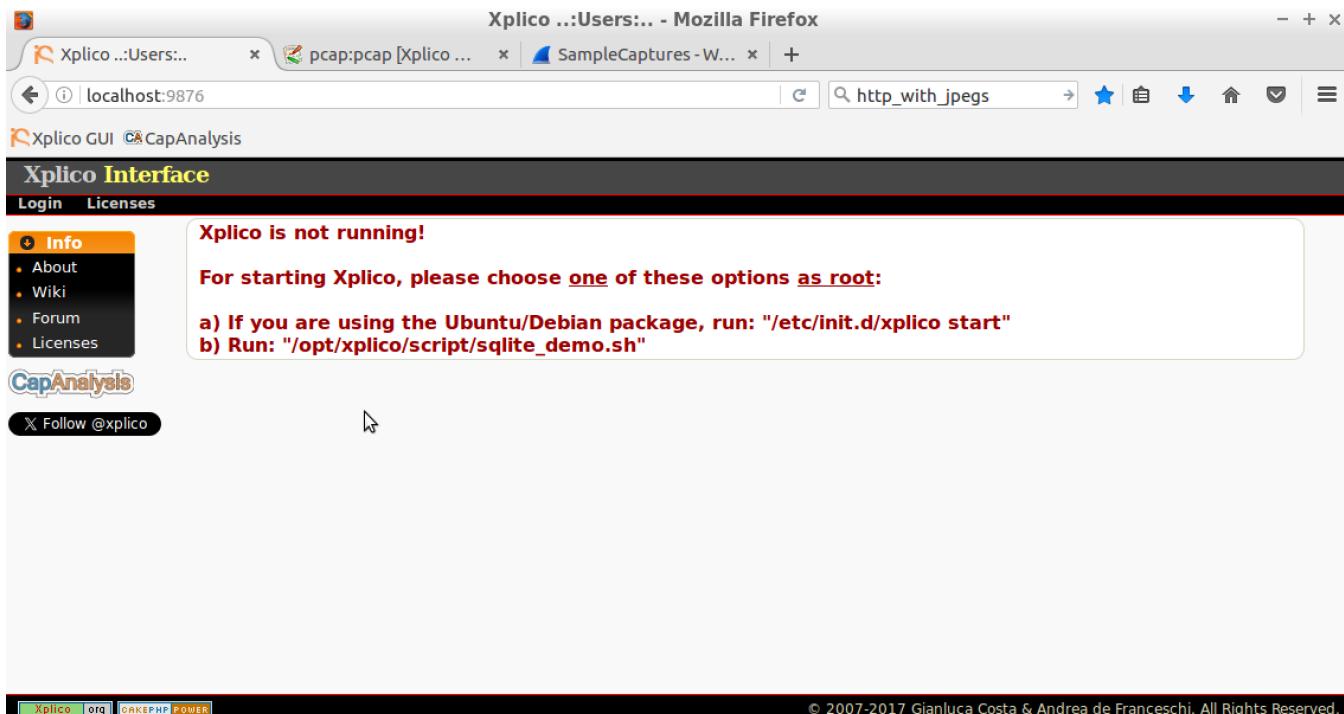
## Installazione e avvio | 1/3

- Xplico non è installato di default su Kali Linux
- L'installazione non è semplice su alcune architetture
- Un modo conveniente per usare Xplico è attivare la macchina virtuale Lubuntu\_xplico\_1.2\_64bit , scaricabile all'indirizzo  
<https://sourceforge.net/projects/xplico/files/VirtualBox%20images/>

# Il tool Xplico

## Installazione e avvio | 2/3

- Accedere all'URL [localhost:9876](http://localhost:9876)



# Il tool Xplico

## Installazione e avvio | 3/3

- Eseguire (come root o con sudo) il comando

```
service xplico start
```

# Il tool Xplico

## File per gli Esempi di Utilizzo

- Per gli esempi di utilizzo delle prossime slide, verranno utilizzati tre file, in formato PCAP
- I file PCAP memorizzano traffico di rete, acquisito precedentemente
- Utilizzeremo i seguenti tre file:
  1. xplico.org\_sample\_capture\_web\_must\_use\_xplico\_nc.cfg.pcap
  2. freeswitch4560\_tosipphone\_ok.pcap
  3. smtp.pcap

**NOTA:** I file sono gratuitamente scaricabili (link nelle prossime slide)

# Il tool Xplico

## File per gli Esempi di Utilizzo

- Per gli esempi di utilizzo delle prossime slide, verranno utilizzati tre file, in formato PCAP
- I file PCAP memorizzano traffico di rete, acquisito precedentemente
- Utilizzeremo i seguenti tre file:

1. `xplico.org_sample_capture_web_must_use_xplico_nc.cfg.pcap`
2. `freeswitch4560_tosipphone_ok.pcap`

3. `smtp.pcap`

- <http://wiki.xplico.org/doku.php?id=pcap:pcap>

HTTP (web)

SIP example 1 (thanks to <http://www.wireshark.org/>)



# Il tool Xplico

## File per gli Esempi di Utilizzo

- Per gli esempi di utilizzo delle prossime slide, verranno utilizzati tre file, in formato PCAP
- I file PCAP memorizzano traffico di rete, acquisito precedentemente
- Utilizzeremo i seguenti tre file:
  1. xplico.org\_sample\_capture\_web\_must\_use\_xplico\_nc.cfg.pcap
  2. freeswitch4560\_tosipphone\_ok.pcap

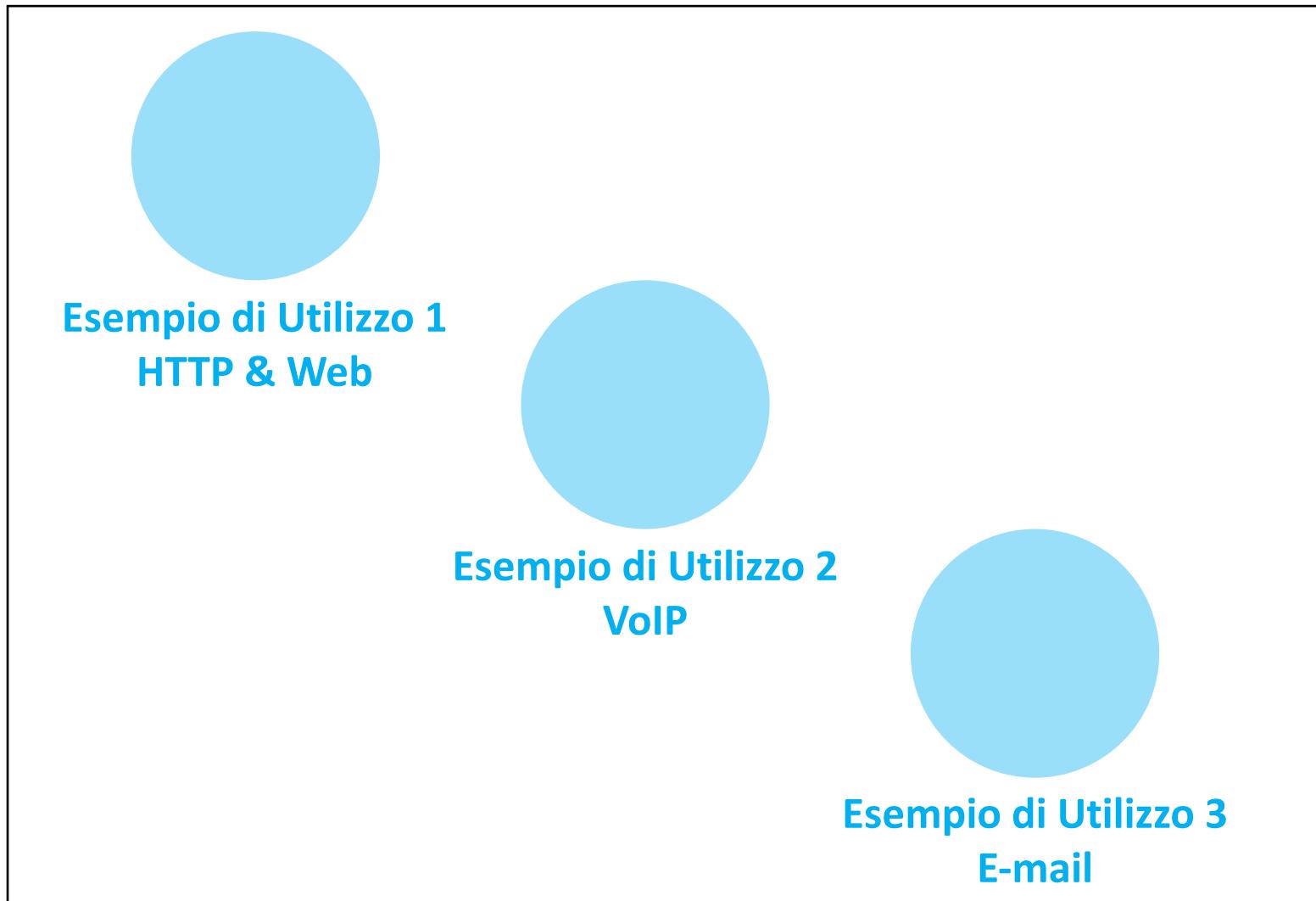
### 3. smtp.pcap

- <https://wiki.wireshark.org/SampleCaptures>



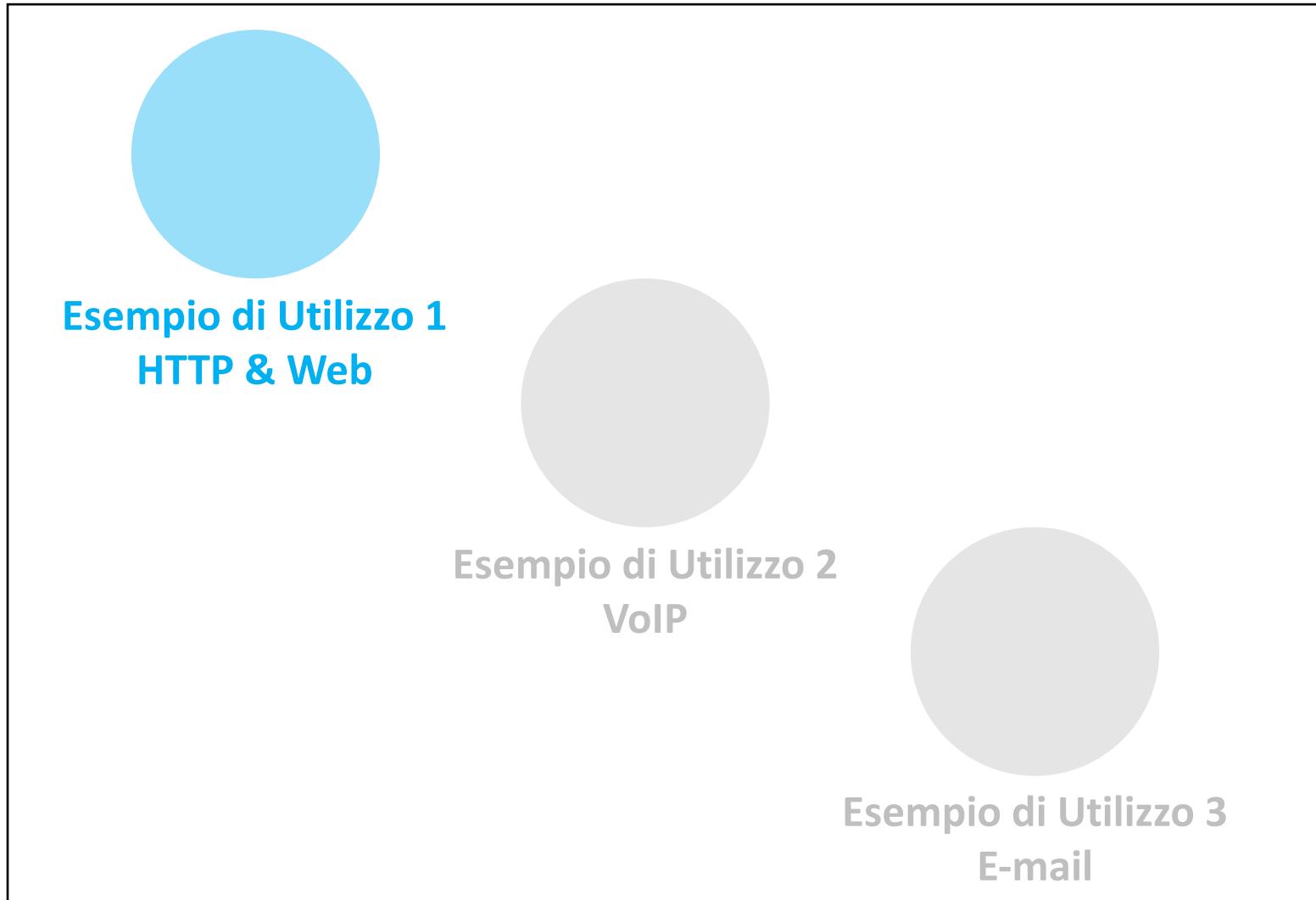
# Il tool Xplico

## Esempi di Utilizzo



# Il tool Xplico

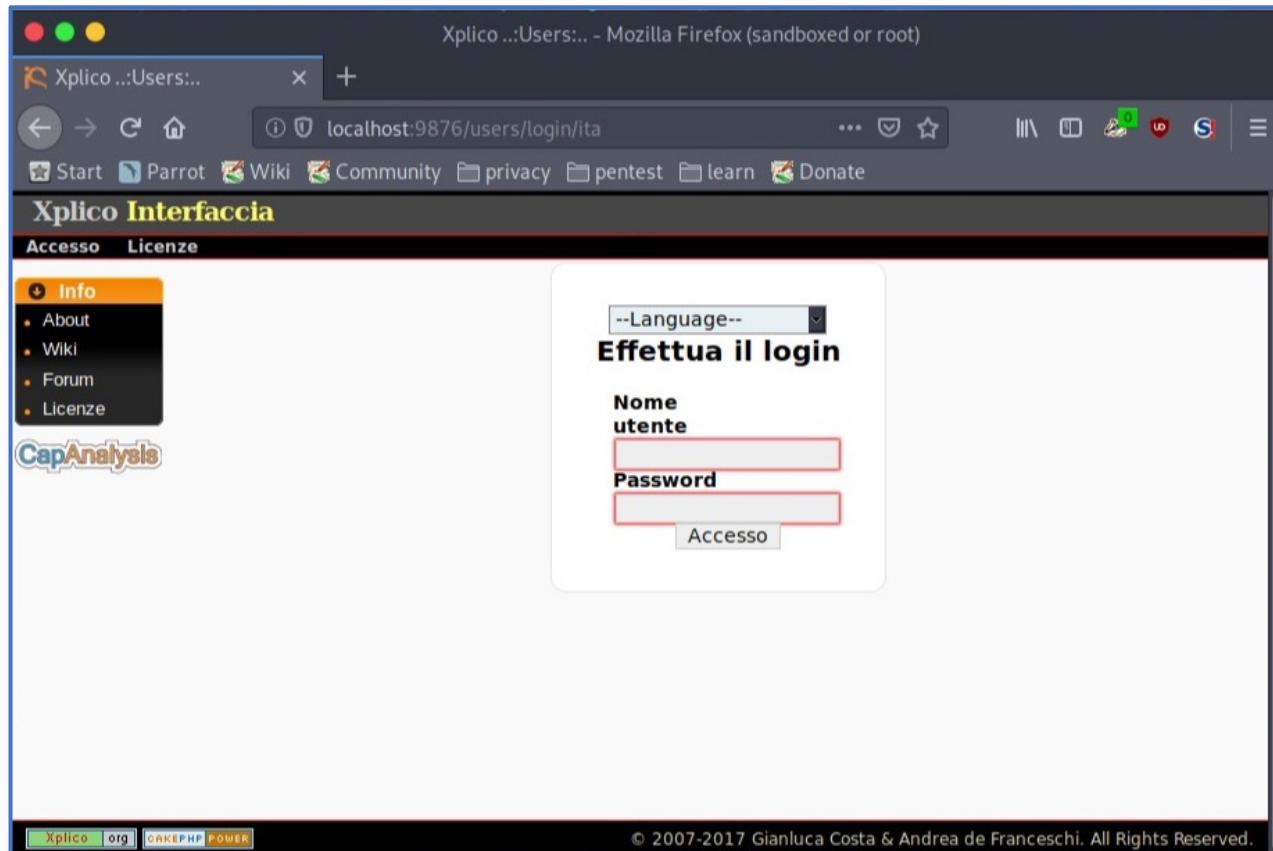
## Esempi di Utilizzo



# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 1/24

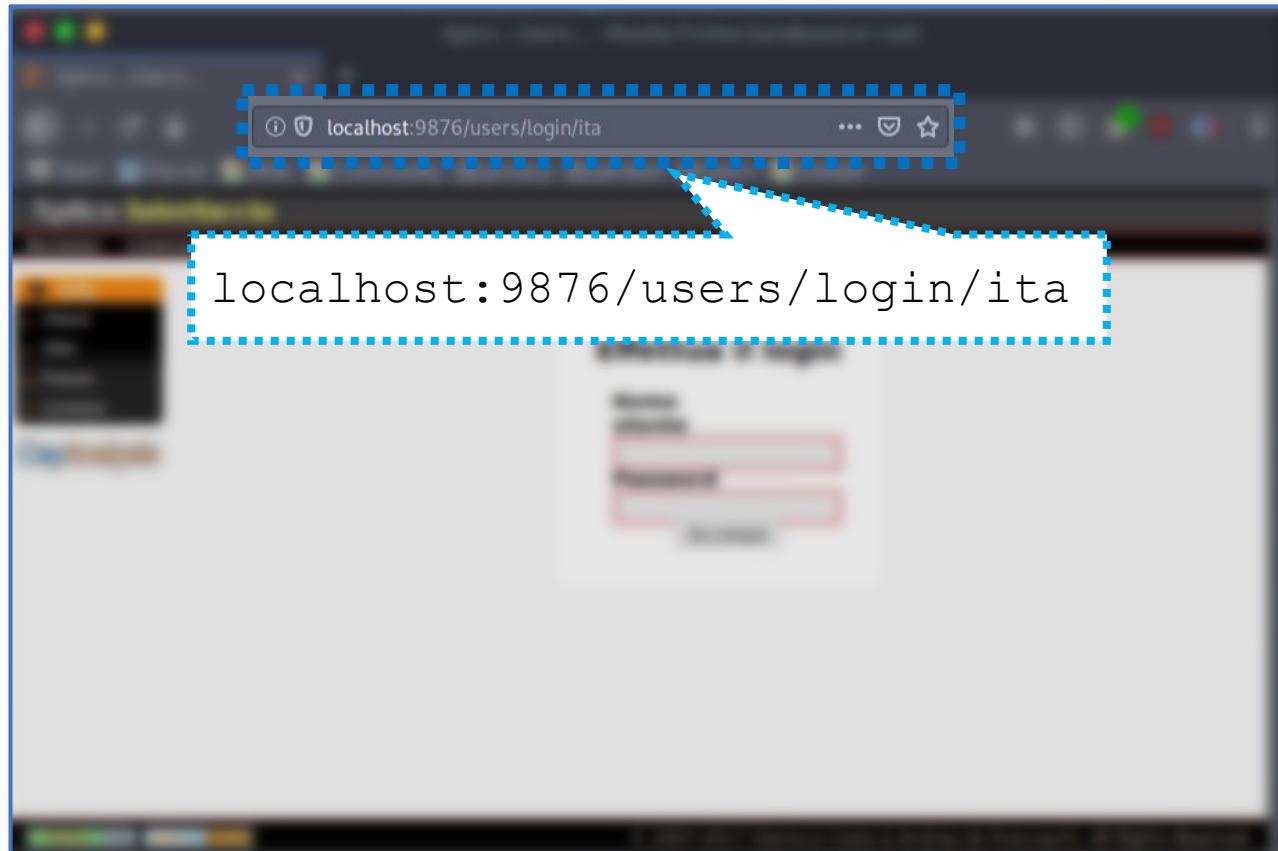
- *Schermata di Avvio di Xplico*



# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 1/24

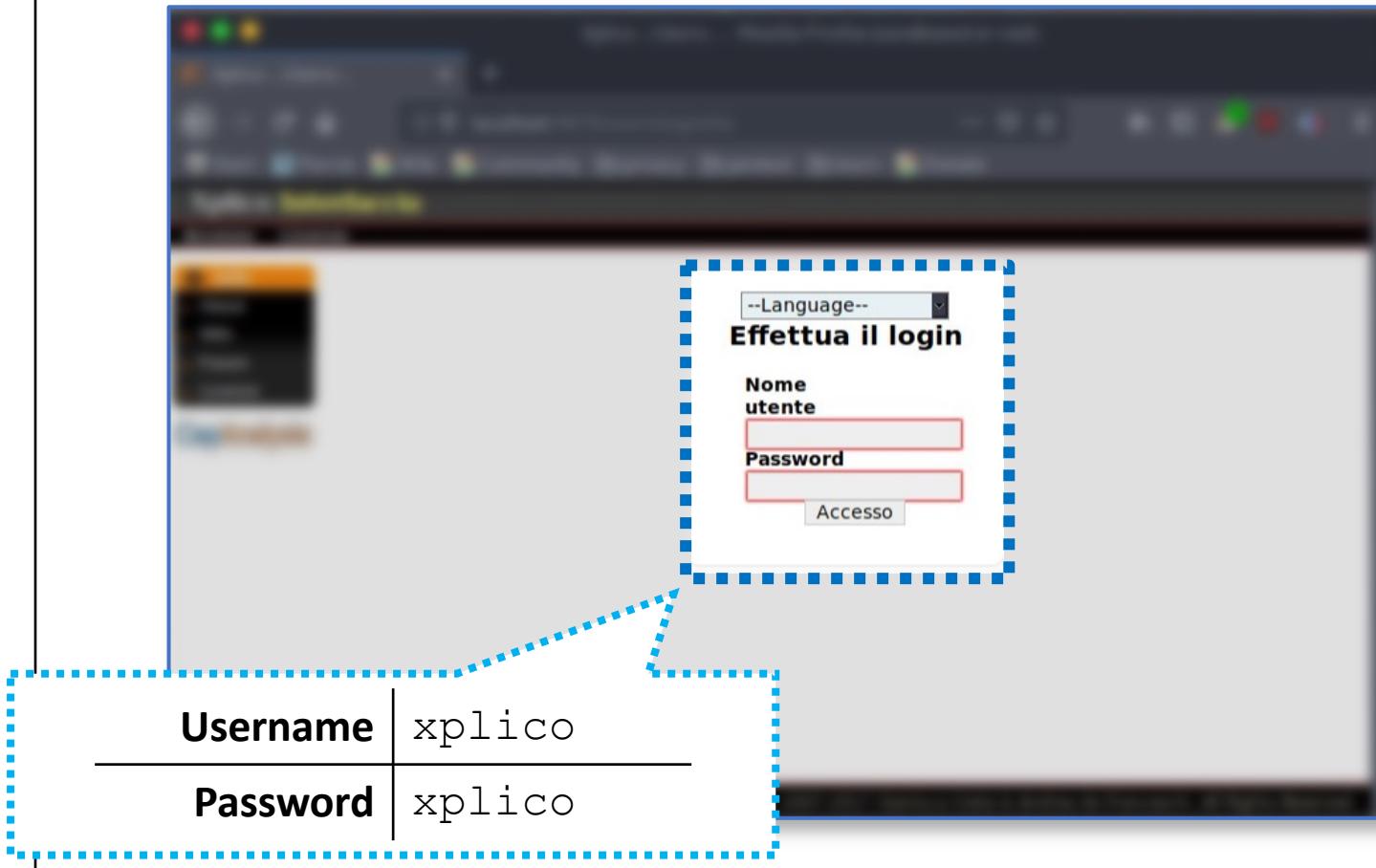
- *Schermata di Avvio di Xplico*



# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 1/24

- *Schermata di Avvio di Xplico*



# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 2/24

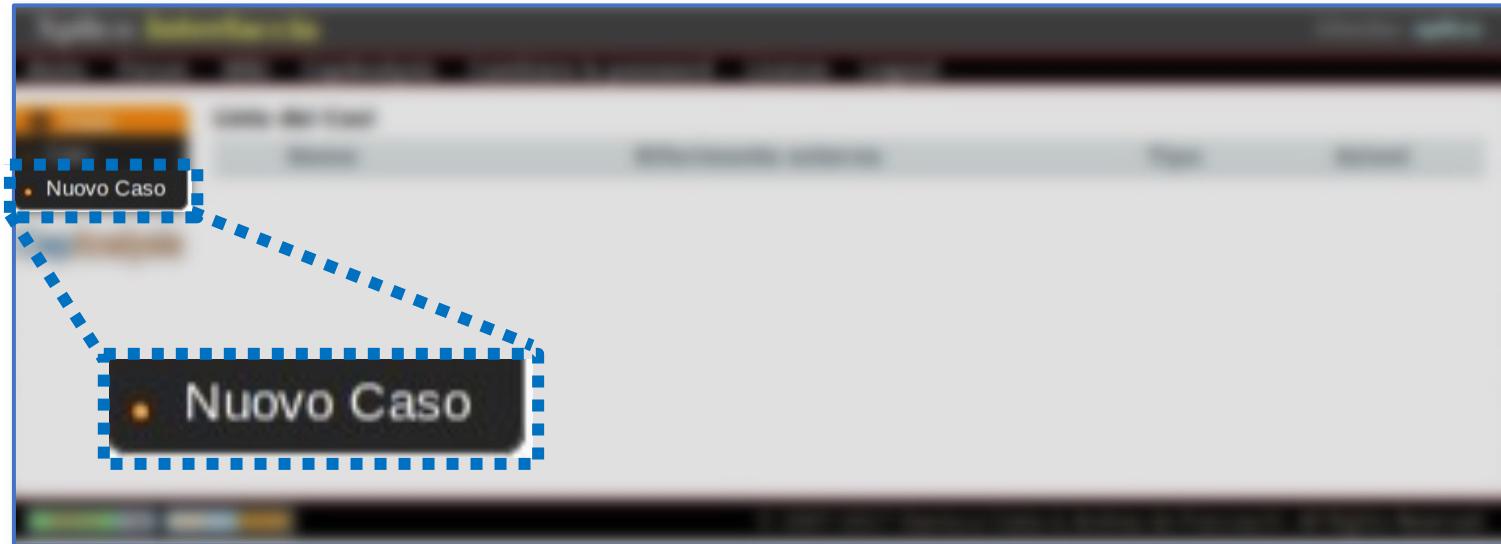
- *Schermata di Xplico dopo il login*

The screenshot shows the Xplico Interface login page. The title bar reads "Xplico Interfaccia" and "Utente: xplico". The menu bar includes links for Aiuto, Forum, Wiki, CapAnalysis, Cambiare la password, Licenze, and Logout. A sidebar on the left has a "Caso" tab selected, showing options for "Casi" and "Nuovo Caso". The main area is titled "Lista dei Casi" and displays columns for Nome, Riferimento esterno, Tipo, and Azioni. At the bottom left is a "CapAnalysis" logo, and at the bottom right is copyright information: "© 2007-2017 Gianluca Costa & Andrea de Franceschi. All Rights Reserved." Logos for "Xplico.org" and "ONKEPHP POWER" are also present at the bottom.

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 3/24

- Creiamo un nuovo caso, cliccando sul link «**Nuovo Caso**», nel *menu a sinistra*



# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 4/24

- Verrà proposta una schermata in cui vengono richieste le seguenti informazioni
  - La metodologia di acquisizione
    - File con dati di rete, precedentemente acquisiti (file con estensione .pcap)
    - Acquisizione diretta del traffico, mediante Xplico, dall'interfaccia di rete
  - Il nome del caso
  - Eventuali riferimenti esterni

Dati da:

**File pcap**     **Interfaccia di rete**

**Nome del Caso**

**Riferimento esterno**

**Crea**

A screenshot of a software interface titled "Dati da:" (Data from). It contains two radio buttons: one selected for "File pcap" and one unselected for "Interfaccia di rete" (Network Interface). Below these are two input fields: "Nome del Caso" (Case Name) and "Riferimento esterno" (External Reference), each with a corresponding text input box. At the bottom is a blue "Crea" (Create) button.

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 5/24

Dati da:

File pcap    Interfaccia di rete

Nome del Caso

Riferimento esterno

- Specifichiamo la metodologia di acquisizione dei dati (nell'esempio, mediante file .pcap), il **nome del caso** (nell'esempio CasoXplico) ed un eventuale **riferimento esterno** (non specificato, nell'esempio)

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 5/24

Dati da:

File pcap     Interfaccia di rete

Nome del Caso

Riferimento esterno

**Crea**

- Specifichiamo la metodologia di acquisizione dei dati (nell'esempio, mediante file .pcap), il **nome del caso** (nell'esempio CasoXplico) ed un eventuale **riferimento esterno** (non specificato, nell'esempio)
- Clicchiamo sul tasto «**Crea**», per creare il nuovo caso, e proseguire, nell'analisi

Nome del Caso

Riferimento esterno

**Crea**

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 6/24

**Il caso è stato creato**

**Lista dei Casi**

Nome	Riferimento esterno	Tipo	Azioni
CasoXplico		File	Elimina

- Al passo successivo, Xplico ci informerà sulla **corretta creazione del caso**, denominato CasoXplico

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 6/24

**Il caso è stato creato**

**Lista dei Casi**

Nome	Riferimento esterno	Tipo	Azioni
CasoXplico		File	Elimina

- Al passo successivo, Xplico ci informerà sulla **corretta creazione del caso**, denominato CasoXplico
- Selezionando il caso, cliccandoci sopra, sarà possibile creare una **nuova sessione** di analisi

**Elenco delle sessioni, riferite al Caso: CasoXplico**

Nome	Ora d'inizio	Ora di fine	Stato	Azioni

# Il tool Xplico

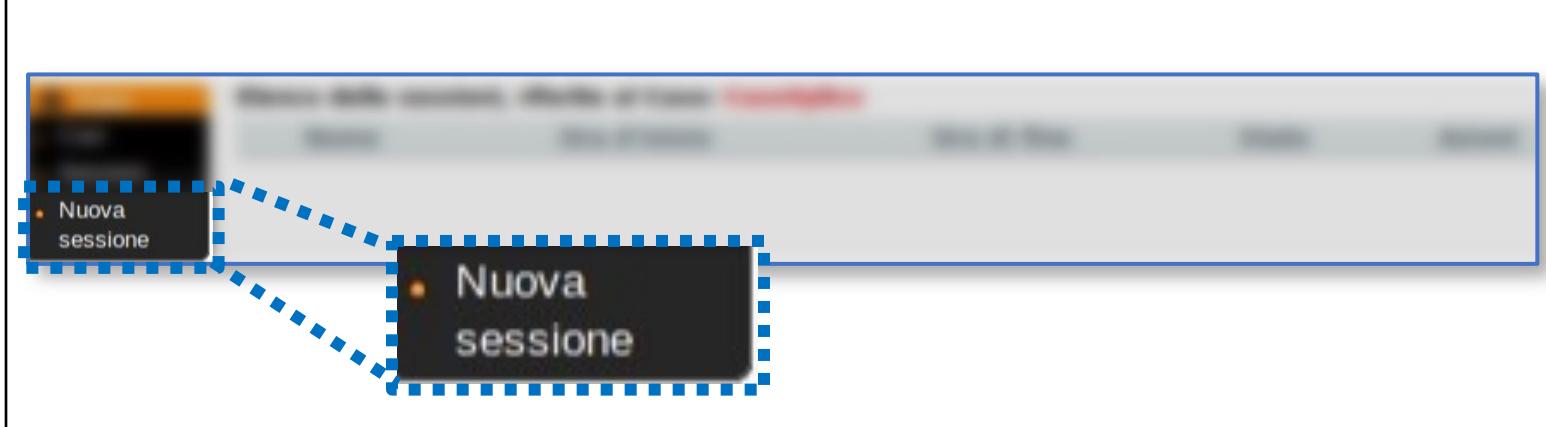
## Esempio di Utilizzo 1 | HTTP & Web | 6/24

Il caso è stato creato

**Lista dei Casi**

Nome	Riferimento esterno	Tipo	Azioni
CasoXplico		File	Elimina

- Al passo successivo, Xplico ci informerà sulla **corretta creazione del caso**, denominato CasoXplico
- Selezionando il caso, cliccandoci sopra, sarà possibile creare una **nuova sessione** di analisi, cliccando su «Nuova sessione»



The screenshot shows a blurred Xplico interface. In the bottom-left corner, there is a dark rectangular button with a white border containing the text "Nuova sessione". This button is highlighted with a blue dashed rectangular box. A dashed blue arrow points from the text "Nuova sessione" in the previous slide's list to this highlighted button.

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 7/24

- *Schermata creazione Nuova sessione*
  - Richiesto inserimento del nome della sessione (**Session Name**), nell'esempio `HTTP_WEB`

The screenshot shows a dialog box titled "Nuova sessione" (New Session). It contains a single input field labeled "Nome della Sessione" (Session Name) with the value "HTTP\_WEB" entered. Below the input field is a "Crea" (Create) button.

Nuova sessione	
Nome della Sessione	HTTP_WEB
<input type="button" value="Crea"/>	

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 7/24

- *Schermata creazione Nuova sessione*
  - Richiesto inserimento del nome della sessione (**Session Name**), nell'esempio `HTTP_WEB`

The screenshot illustrates the process of creating a new session in the Xplico tool. It consists of two main parts:

- Top Panel:** Shows a blurred list of sessions. A blue dashed box highlights the "Crea" (Create) button, which is also highlighted by a blue dotted arrow pointing downwards.
- Bottom Panel:** Displays a success message: "La sessione è stata creata" (The session has been created). Below it is a table titled "Elenco delle sessioni, riferite al Caso: CasoXplico". The table has columns: Nome, Ora d'inizio, Ora di fine, Stato, and Azioni. A single row is present: "HTTPWEB" in the Nome column, with "EMPTY" in the Stato column.

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 8/24

The screenshot shows the Xplico main interface with a session analysis for 'HTTPWEB'. A blue dashed arrow points from the top left, where the session name 'HTTPWEB' is displayed, down to the main interface. The main interface has a green header bar with the title 'Sessione dei dati' and a yellow header bar with the title 'Pcap set'. The 'Sessione dei dati' section shows the following details:

Caso e Sessione	CasoXplico -> HTTPWEB
Cap. Ora inizio	---
Cap. Ora di fine	---
Stato	EMPTY
Host	---

The 'Pcap set' section shows:

- PCAP-over-IP TCP port: 30001.
- Aggiungi nuovo file pcap.
- Browse... No file selected.
- Elabora
- Lista di tutti i file pcap.**

The main interface is divided into several sections with green headers:

- HTTP**:
  - Post 0
  - Get 0
  - Video 0
  - Immagini 0
- MMS**:
  - Numero 0
  - Contenuto 0
  - Video 0
  - Immagini 0
- E-mail**:
  - Ricevute 0
  - Inviate 0
  - Non lette 0/0
- FTP - TFTP - HTTP di file**:
  - Conessioni 0 - 0
  - Scaricato 0 - 0
  - Caricato 0 - 0
  - HTTP 0
- Web Mail**:
  - Totale 0
  - Ricevute 0
  - Inviate 0
- Facebook Chat / Paltalk**:
  - Utenti 0
  - Chat 0/0
- IRC/Paltalk Exp/Msn/Yahoo!**:
  - Server 0
  - Canali 0/0/0
- Dns - Arp - ICMPv6**:
  - DNS res 0
  - ARP/ICMPv6 0/0
- RTP / VoIP**:
  - Video 0
  - Audio 0
- NNTP**:
  - Gruppi 0
  - Articoli 0
- Feed & Printed files**:
  - Numero 0
  - Pdf 0
- WhatsApp**:
  - Connection 0
- Telnet / Syslog**:
  - Conessioni 0/0
- SIP**:
  - Chiamate 0
- Sconosc.**:
  - Testi 0/0
  - Dig 0

# Il tool Xplico

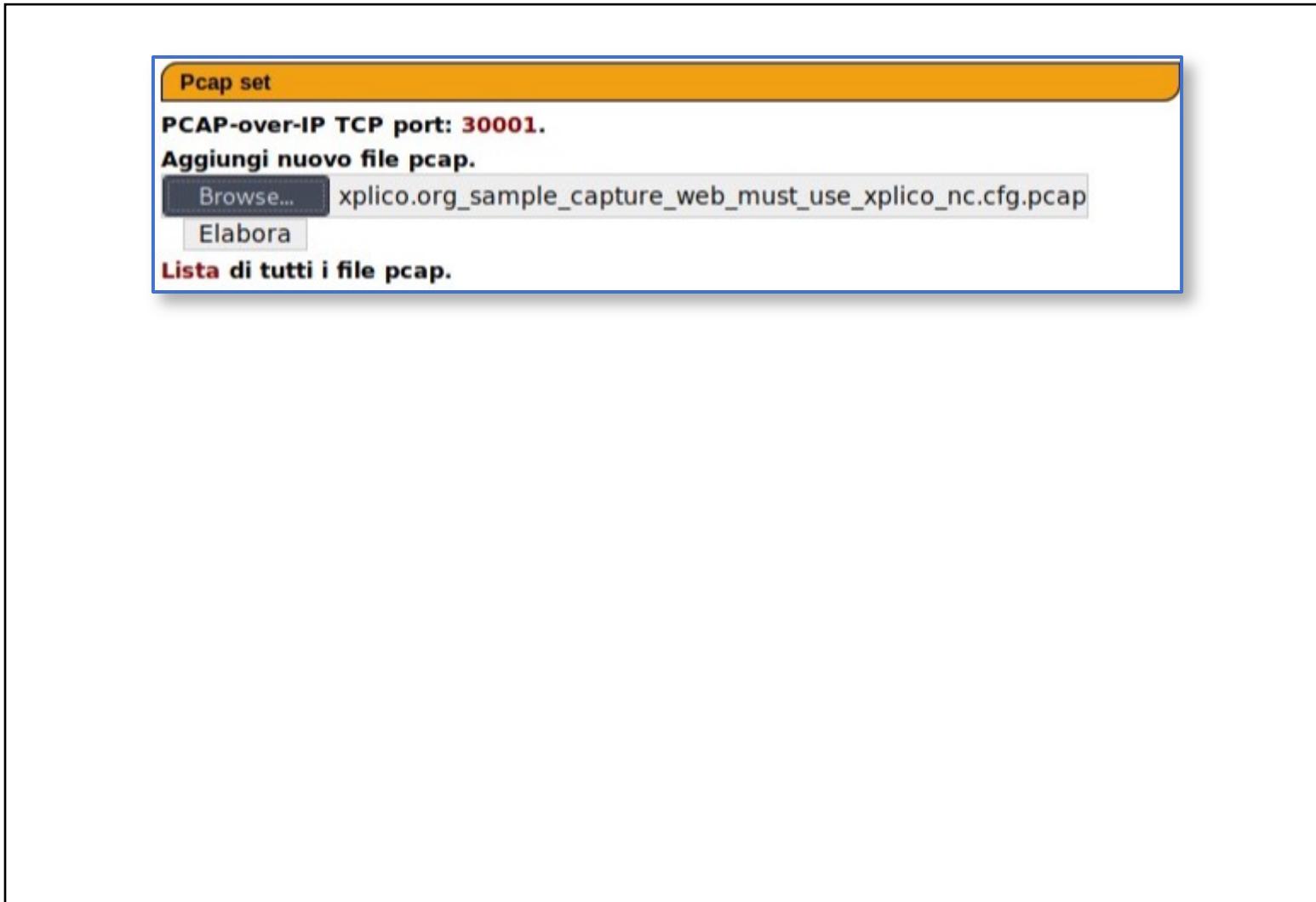
## Esempio di Utilizzo 1 | HTTP & Web | 8/24

The screenshot shows the Xplico interface. At the top, there is a header bar with the text "Pcap set" and "PCAP-over-IP TCP port: 30001". Below this, there is a message "Aggiungi nuovo file pcap." with a "Browse..." button and a "No file selected." message. There is also an "Elabora" button. A red dashed box highlights the "Aggiungi nuovo file pcap." section. To the right of this box is a magnifying glass icon. Below this header is a section titled "Lista di tutti i file pcap." which is also highlighted by a red dashed box.

The bottom half of the screenshot shows a blurred list of network captures, each represented by a row of green and grey bars. A blue rectangular box highlights this list area.

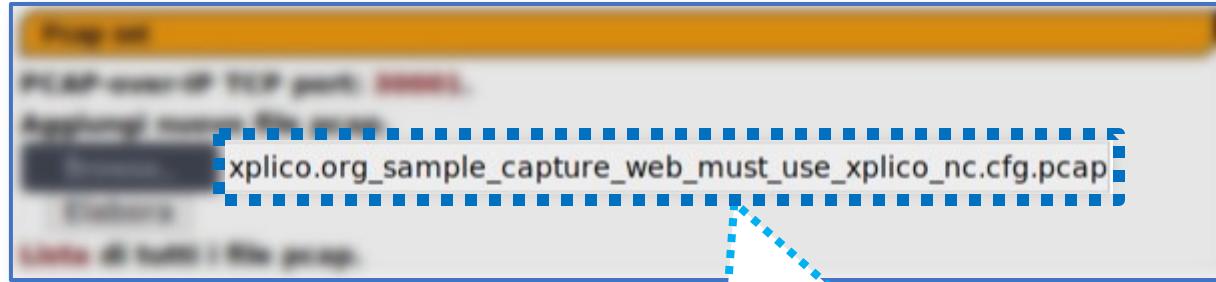
# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 9/24



# Il tool Xplico

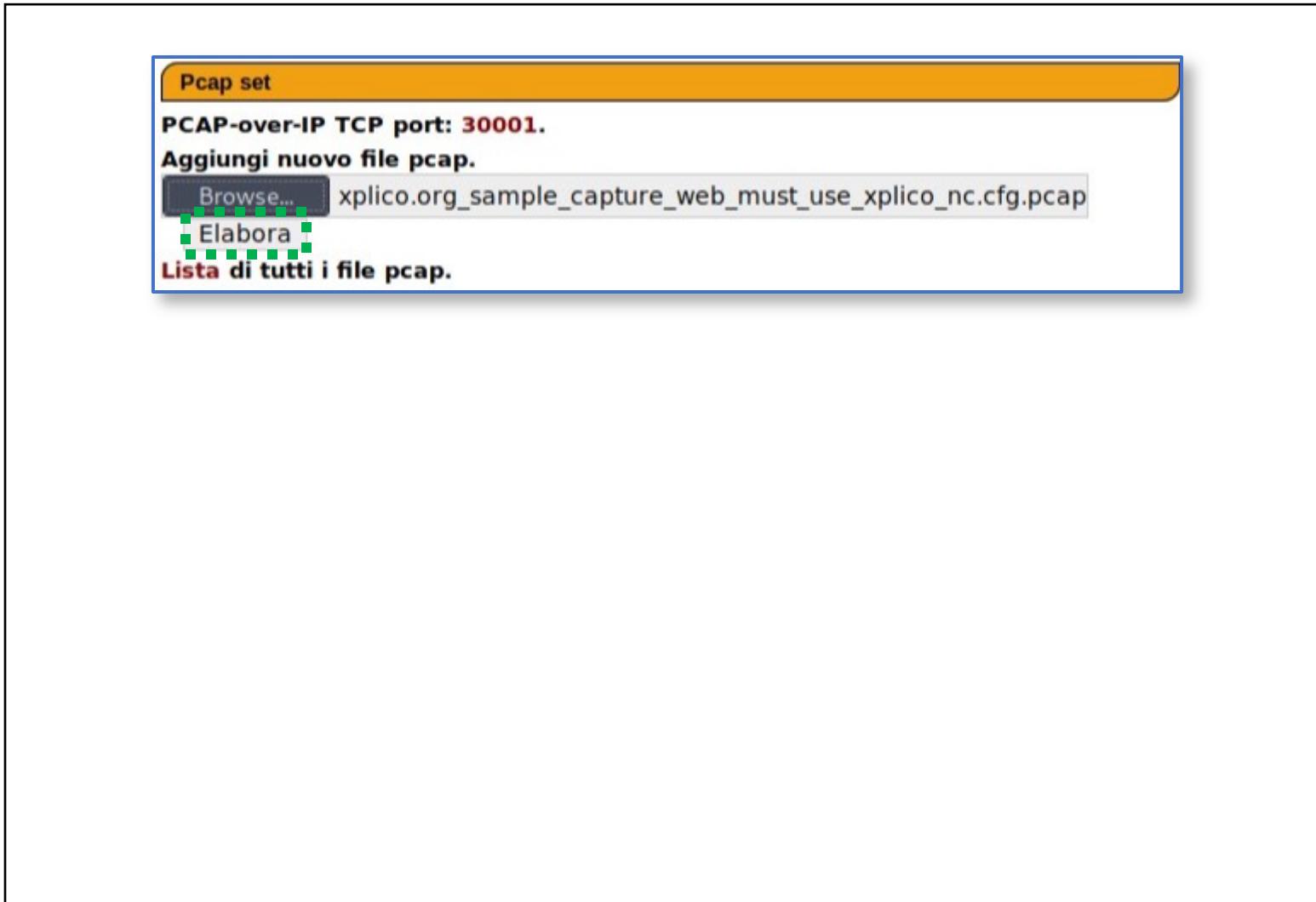
## Esempio di Utilizzo 1 | HTTP & Web | 9/24



In questo esempio, utilizzeremo il file, denominato  
xplico.org\_sample\_capture\_web\_must\_use\_x  
plico\_nc.cfg.pcap

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 10/24



# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 10/24

The screenshot shows the Xplico interface in two main sections:

**Top Section (Pcap set):**

- PCAP-over-IP TCP port: **30001**.
- Aggiungi nuovo file pcap.
- Browse... xplico.org\_sample\_capture\_web\_must\_use\_xplico\_nc.cfg.pcap
- Elabora** (button highlighted with a green box)
- Lista di tutti i file pcap.

**Bottom Section (Sessione dei dati):**

- File caricato, attendere iniziare la decodifica ...
- Gears icon on the left.
- Hourglass icon on the right.
- Sessione dei dati
- Caso e Sessione: CasoXplico -> HTTPWEB
- Cap. Ora inizio: 2009-12-09 17:42:17
- Cap. Ora di fine: 2009-12-09 17:42:50
- Stato: DECODING
- Host: ---

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 10/24

The screenshot illustrates the workflow of the Xplico tool. It starts with the "Pcap set" screen, where a PCAP file is loaded and the "Elabora" button is highlighted with a green box and arrow. This leads to the "Elaborazione Terminata" (Analysis Completed) screen, which displays a summary of network traffic and specific application statistics.

**Pcap set**

PCAP-over-IP TCP port: 30001.  
Aggiungi nuovo file pcap.

Browse... xplico.org\_sample\_capture\_web\_must\_use\_xplico\_nc.cfg.pcap  
Elabora

**Lista di tutti i file pcap.**

**Elaborazione Terminata**

**Sessione dei dati**

Caso e Sessione CasoXplico -> HTTPWEB  
Cap. Ora inizio 2009-12-09 17:42:17  
Cap. Ora di fine 2009-12-09 17:42:50  
Stato DECODING COMPLETED  
Host Filtra

**HTTP**

Post	0
Get	0
Video	0
Immagini	0

**MMS**

Numero	0
Contenuto	0
Video	0
Immagini	0

**E-mail**

Ricevute	0
Inviate	0
Non lette	0/0

**FTP - TFTP - HTTP di file**

Connessioni	0 - 0
Scaricato	0 - 0
Caricato	0 - 0
HTTP	0

**Web Mail**

Totale	0
Ricevute	0
Inviate	0

**Facebook Chat / Paitalk**

Utenti	0
Chat	0/0

**IRC/Paitalk Exp/Msn/Yahoo!**

Server	0
Canali	0/0/0/0

**Dns - Arp - ICMPv6**

DNS res	0
ARP/ICMPv6	0/0

**RTP / VoIP**

Video	0
Audio	0

**NNTP**

Gruppi	0
Articoli	0

**Feed & Printed files**

Numero	0
Pdf	0

**WhatsApp**

Connection	0
------------	---

**Telnet / Syslog**

Connessioni	0/0
-------------	-----

**SIP**

Chiamate	0
----------	---

**Sconosciuti**

Testi	5/18
Dig	9

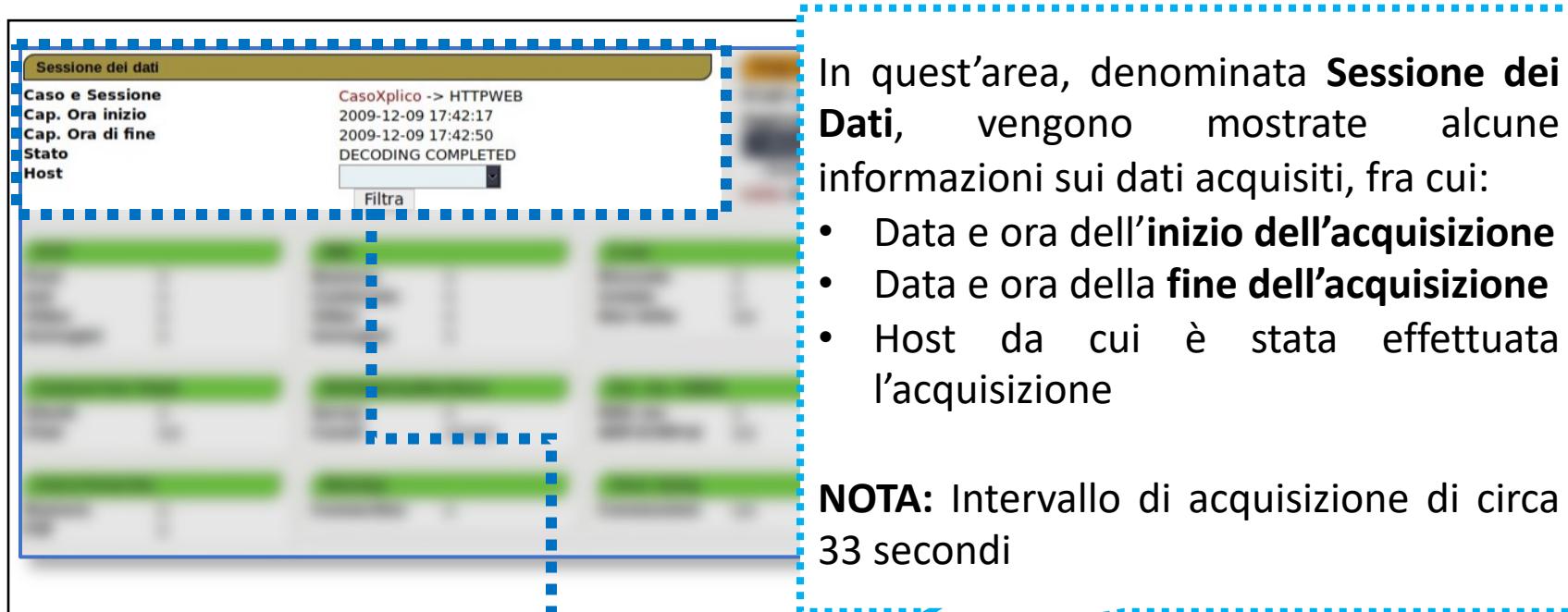
# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 12/24

In quest'area, denominata **Sessione dei Dati**, vengono mostrate alcune informazioni sui dati acquisiti, fra cui:

- Data e ora dell'**inizio dell'acquisizione**
- Data e ora della **fine dell'acquisizione**
- Host da cui è stata effettuata l'acquisizione

**NOTA:** Intervallo di acquisizione di circa 33 secondi



**Sessione dei dati**

**Caso e Sessione** CasoXplico -> HTTPWEB  
**Cap. Ora inizio** 2009-12-09 17:42:17  
**Cap. Ora di fine** 2009-12-09 17:42:50  
**Stato** DECODING COMPLETED  
**Host**

Filtra



# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 11/24

The screenshot shows a summary dashboard from the Xplico tool. It is organized into a grid of boxes, each representing a different protocol or category. The categories include:

- HTTP:** Post 0, Get 0, Video 0, Immagini 0.
- MMS:** Numero 0, Contenuto 0, Video 0, Immagini 0.
- E-mail:** Ricevute 0, Inviate 0, Non lette 0/0.
- FTP - TFTP - HTTP di file:** Connessioni 0 - 0, Scaricato 0 - 0, Caricato 0 - 0, HTTP 0.
- Web Mail:** Totale 0, Ricevute 0, Inviate 0.
- Facebook Chat / Paltalk:** Utenti 0, Chat 0/0.
- IRC/Paltalk Exp/Msn/Yahoo!** Server 0, Canali 0/0/0/0.
- Dns - Arp - ICMPv6:** DNS res 0, ARP/ICMPv6 0/0.
- RTP / VoIP:** Video 0, Audio 0.
- NNTP:** Gruppi 0, Articoli 0.
- Feed & Printed files:** Numero 0, Pdf 0.
- WhatsApp:** Connection 0.
- Telnet / Syslog:** Connessioni 0/0.
- SIP:** Chiamate 0.
- Sconosc.** Testi Dig 5/18 9.

**Sezione riepilogativa** in cui viene riportato il numero di «artefatti», suddivisi per tipologia, individuati nella fase di analisi di Xplico  
(maggiori dettagli su alcune sezioni, nelle prossime slide)

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 13/24

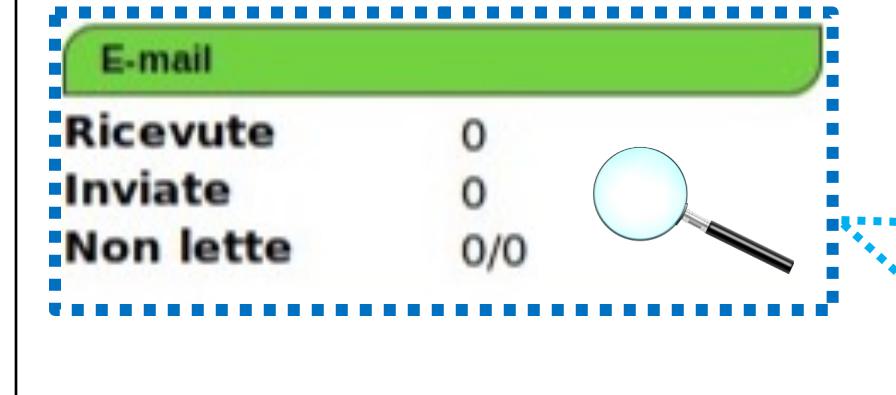
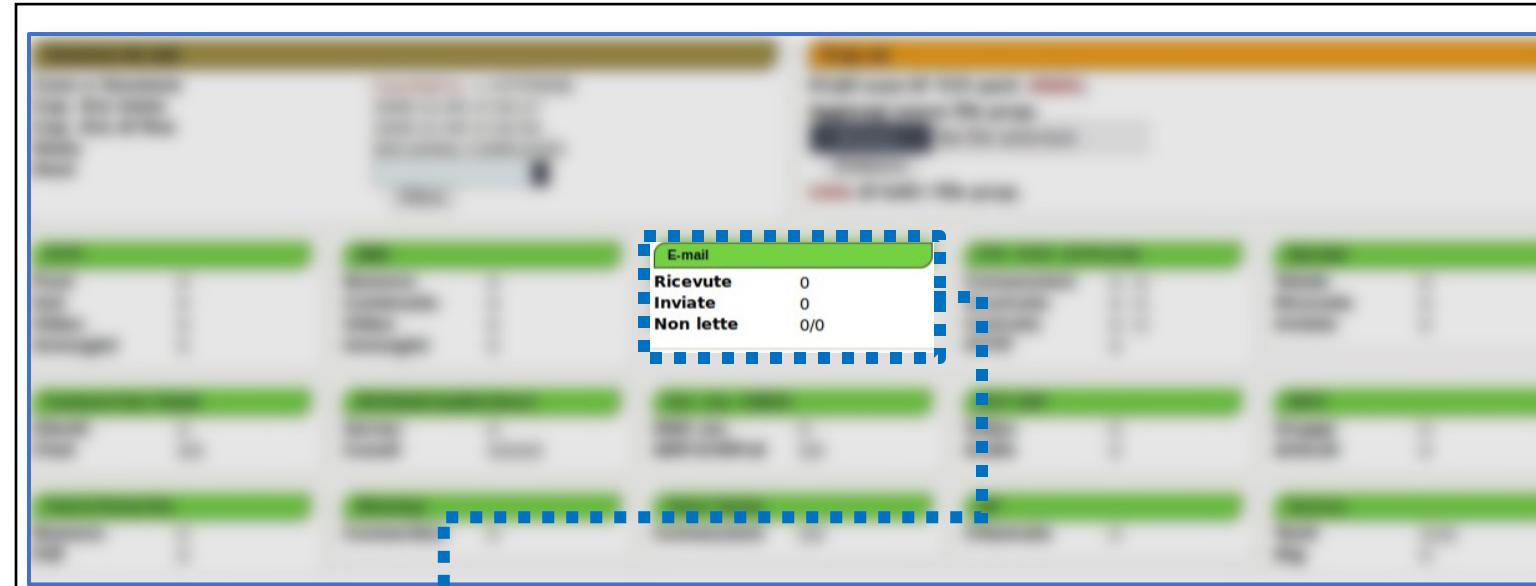
The image shows two screenshots of the Xplico tool's interface. The top screenshot displays a list of network packets with a focus on the 'HTTP' section. The bottom screenshot is a zoomed-in view of the 'HTTP' section, showing statistics for Post, Get, Video, and Immagini requests, all with a value of 0. A magnifying glass icon is positioned next to the bottom screenshot.

Nella **sezione HTTP**, viene riportato il **numero di pacchetti POST**, il numero di pacchetti GET, il numero di pacchetti relativi ad **immagini e video** (nell'esempio, non è stato individuato nessun pacchetto di questo tipo)

HTTP	
Post	0
Get	0
Video	0
Immagini	0

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 14/24



Nella sezione E-mail, Xplico riporta il numero di e-mail ricevute, inviate e non lette, individuate nel traffico analizzato (nell'esempio, non è stata rilevata alcuna e-mail)

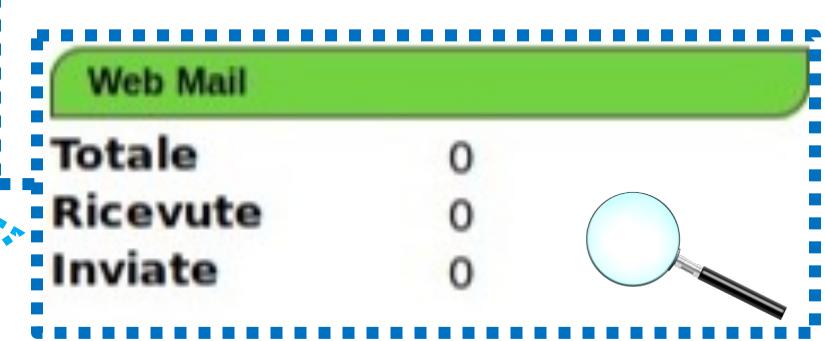
# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 15/24

The screenshot shows a list of items under the 'Web Mail' section. A summary statistics panel on the right indicates:

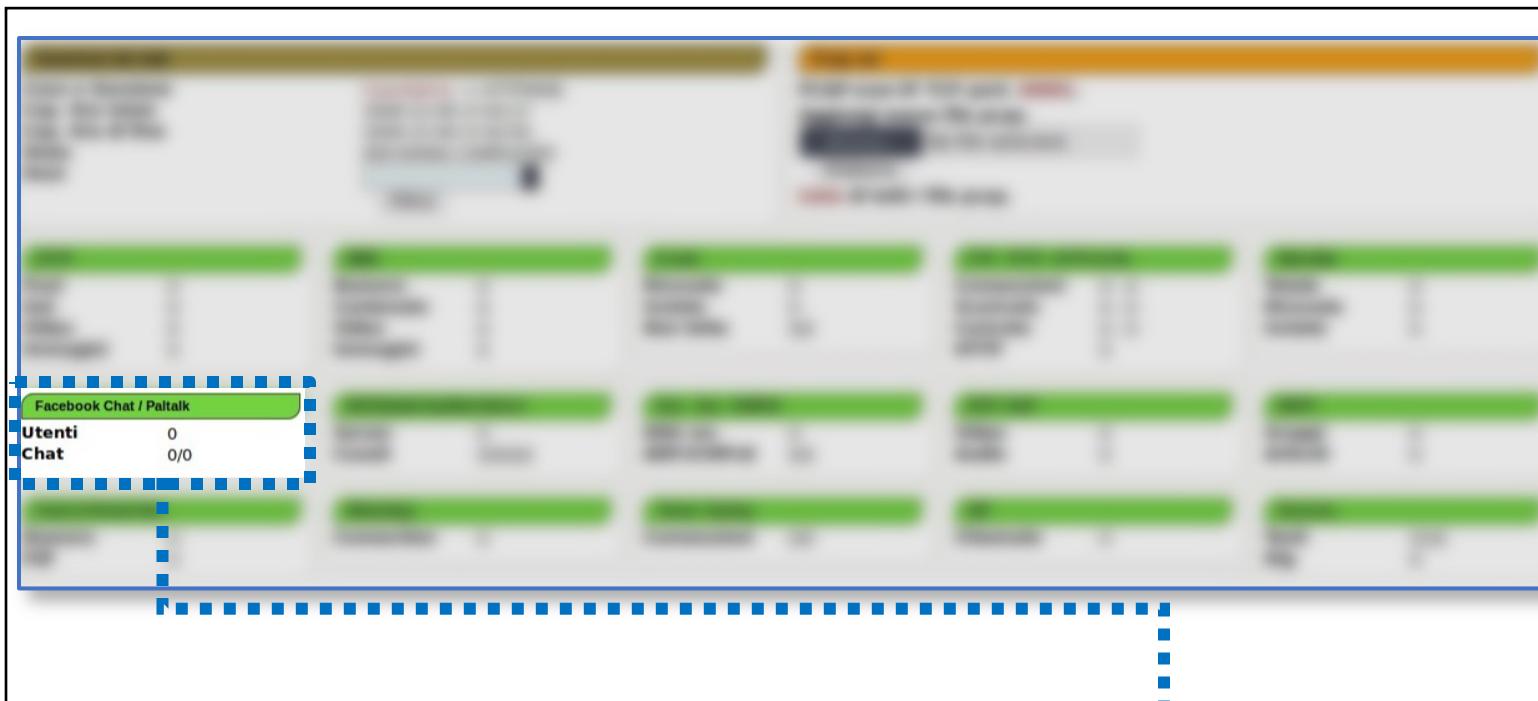
Web Mail	
Totale	0
Ricevute	0
Inviate	0

Nella sezione **Web Mail**, viene indicato il **numero di e-mail** (gestite mediante client Web) **ricevute, inviate e non lette**, individuate nel traffico analizzato (nell'esempio, non è stata rilevata alcuna e-mail)



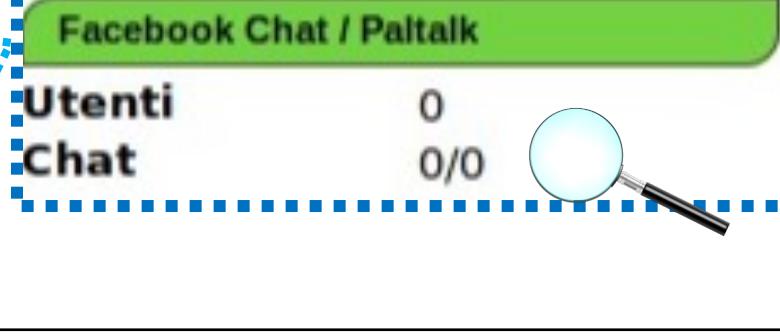
# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 16/24



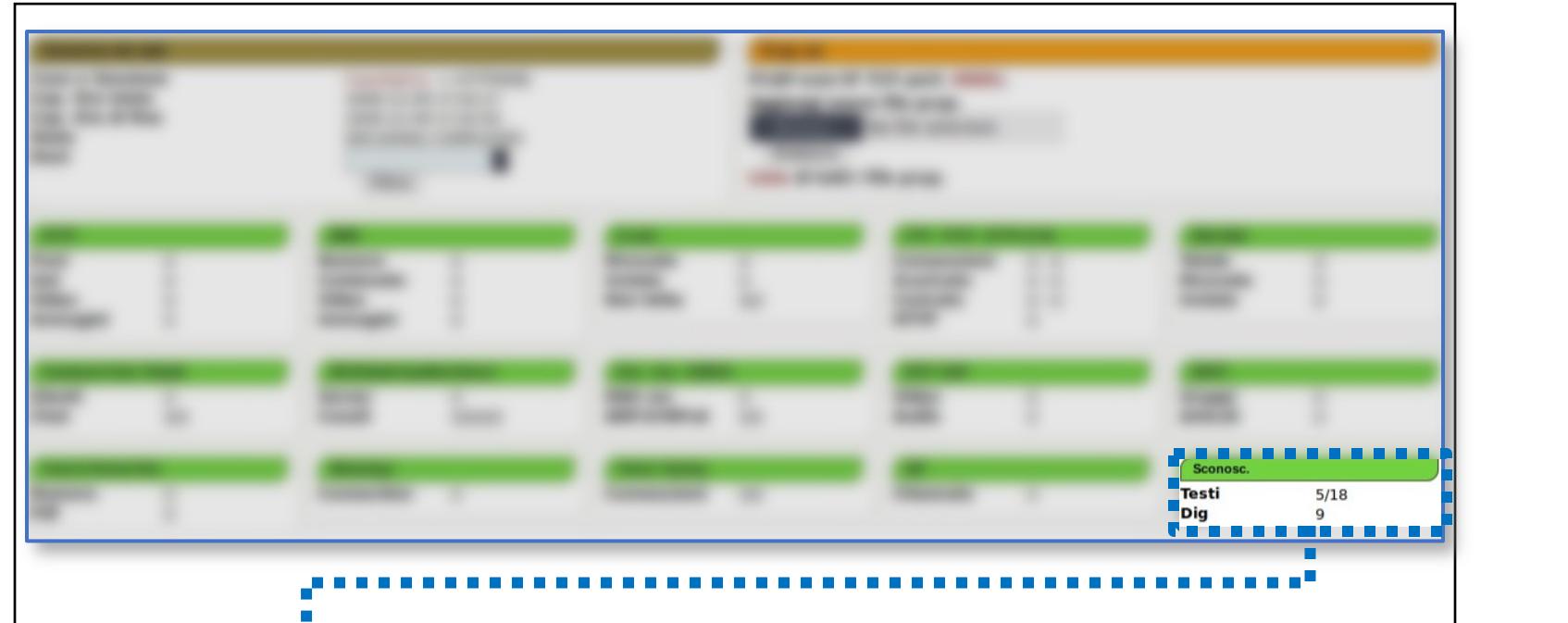
The screenshot shows a list of network traffic items. One item is highlighted with a blue dashed box. This item is from the 'Facebook Chat / Paltalk' section and shows 0 users and 0/0 chat instances.

Come intuibile dal nome, nella sezione **Facebook Chat/Paltalk**, vengono riportate le statistiche relative alla **chat di Facebook** (ed alla chat **Paltalk**) ed ai **relativi utenti identificati** (nell'esempio, non è stata individuata alcuna informazione)



# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 17/24



The screenshot shows the Xplico interface. At the top, there's a blurred list of network captures. In the bottom right corner of the main window, a specific capture is highlighted with a green bar containing the text "Sconosc.", "Testi", "Dig", "5/18", and "9". A magnifying glass icon is positioned next to this bar. A blue dotted line box encloses this information, which is then expanded into a larger blue dotted line box containing explanatory text.

**Sconosc.**,  
**Testi** 5/18  
**Dig** 9

In questa sezione, denominata **Sconosc.**, vengono riportate le statistiche in relazione ad artefatti/oggetti sconosciuti (*non decodificati*)

Nello specifico, sono stati identificati diversi artefatti **testuali** ed oggetti denominati **Dig**

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 18/24

The screenshot shows the Xplico interface with the following details:

- Sessione dei dati:**
  - Caso e Sessione: CasoXplico -> HTTPWEB
  - Cap. Ora inizio: 2009-12-09 17:42:17
  - Cap. Ora di fine: 2009-12-09 17:42:50
  - Stato: DECODING COMPLETED
  - Host: (dropdown menu)
  - Filtra: button
- Pcap set:**
  - PCAP-over-IP TCP port: 30001.
  - Add new pcap file.
  - Browse... No file selected.
  - Elabora button
  - List of all pcap files.
- Summary Statistics:**

Protocollo	Conteggio
HTTP	0
Post	0
Get	0
Video	0
Immagini	0
MMS	0
Numero	0
Contenuto	0
Video	0
Immagini	0
E-mail	0
Ricevute	0
Inviate	0
Non lette	0/0
FTP - TFTP - HTTP di file	0 - 0
Conessioni	0 - 0
Scaricato	0 - 0
Caricato	0 - 0
HTTP	0
Web Mail	0
Totali	0
Ricevute	0
Inviate	0
- Protocollo Specifico:**
  - Facebook Chat / Paltalk: Utenti 0, Chat 0/0
  - IRC/Paltalk Exp/Msn/Yahoo!: Server 0, Canali 0/0/0
  - Dns - Arp - ICMPv6: DNS res 0, ARP/ICMPv6 0/0
  - RTP / VoIP: Video 0, Audio 0
  - NNTP: Gruppi 0, Articoli 0
  - Feed & Printed files: Numero 0, Pdf 0
  - WhatsApp: Connection 0
  - Telnet / Syslog: Conessioni 0/0
  - SIP: Chiamate 0
  - Sconosc.:
    - Testi: 5/18
    - Dig: 9

**OSSERVAZIONE IMPORTANTE**

La sezione **Sconosc.** è l'unica che presenta degli artefatti, pertanto, è necessario approfondire

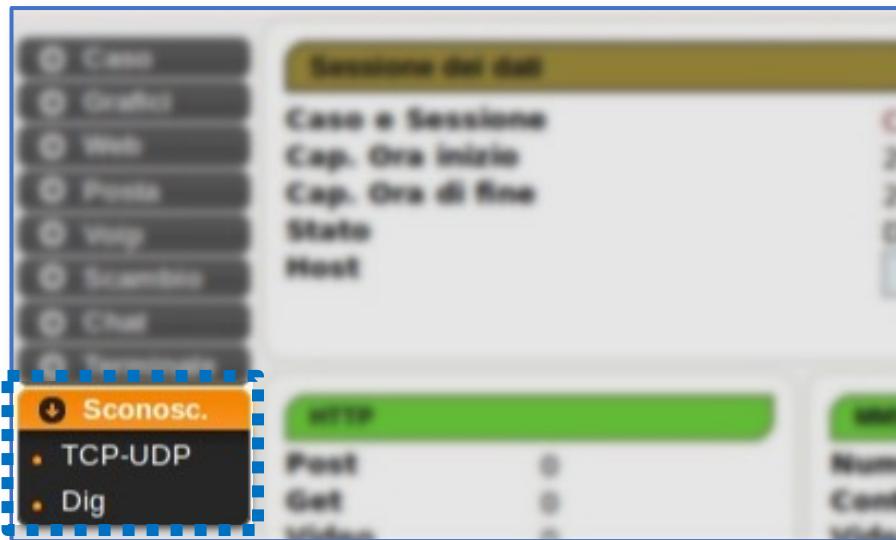
**Sconosc.**

Testi	5/18
Dig	9

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 19/24

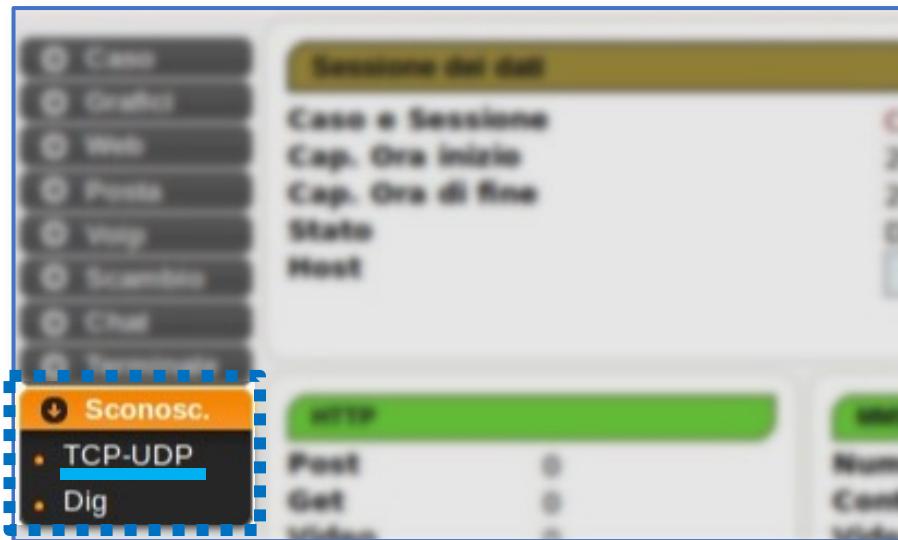
- È possibile approfondire gli artefatti sconosciuti, dal relativo menu a sinistra (sezione **Sconosc.**), mediante i seguenti link:
  - TCP-UDP
  - Dig



# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 19/24

- È possibile approfondire gli artefatti sconosciuti, dal relativo menu a sinistra (sezione **Sconosc.**), mediante i seguenti link:
  - **TCP-UDP**
  - Dig



# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 20/24

- Schermata TCP-UDP della sezione Sconosci.

Ricerca	Andare					
Data	Destinazione	Porto	Protocollo	Durata [s]	Dimensioni [byte]	Info
2009-12-09 17:42:47	<b>74.125.77.100</b>	80	Google	0	1190	<a href="#">Info.xml</a>
2009-12-09 17:42:44	<b>75.119.219.154</b>	80	HTTP	6	5763	<a href="#">Info.xml</a>
2009-12-09 17:42:39	<b>67.205.49.173</b>	80	HTTP	10	1065	<a href="#">Info.xml</a>
2009-12-09 17:42:39	<b>67.205.49.173</b>	80	HTTP	10	1041	<a href="#">Info.xml</a>
2009-12-09 17:42:39	<b>67.205.49.173</b>	80	HTTP	10	3723	<a href="#">Info.xml</a>
2009-12-09 17:42:36	<b>67.205.49.173</b>	80	HTTP	4	25182	<a href="#">Info.xml</a>
2009-12-09 17:42:36	<b>67.205.49.173</b>	80	HTTP	13	15419	<a href="#">Info.xml</a>
2009-12-09 17:42:36	<b>67.205.49.173</b>	80	HTTP	13	29258	<a href="#">Info.xml</a>
2009-12-09 17:42:33	<b>67.205.49.173</b>	80	HTTP	6	8381	<a href="#">Info.xml</a>
2009-12-09 17:42:28	<b>67.205.51.26</b>	80	HTTP	6	810	<a href="#">Info.xml</a>
2009-12-09 17:42:27	<b>195.37.77.138</b>	80	HTTP	7	6436	<a href="#">Info.xml</a>
2009-12-09 17:42:27	<b>216.34.181.71</b>	80	HTTP	7	3204	<a href="#">Info.xml</a>
2009-12-09 17:42:22	<b>67.205.51.26</b>	80	HTTP	6	39856	<a href="#">Info.xml</a>
2009-12-09 17:42:20	<b>67.205.51.26</b>	80	HTTP	8	13702	<a href="#">Info.xml</a>
2009-12-09 17:42:20	<b>67.205.51.26</b>	80	HTTP	8	10795	<a href="#">Info.xml</a>
2009-12-09 17:42:20	<b>67.205.51.26</b>	80	HTTP	8	15386	<a href="#">Info.xml</a>
Precedente	1   2 1 of 2			Prossimo		

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 20/24

- *Schermata TCP-UDP della sezione Sconosc.*

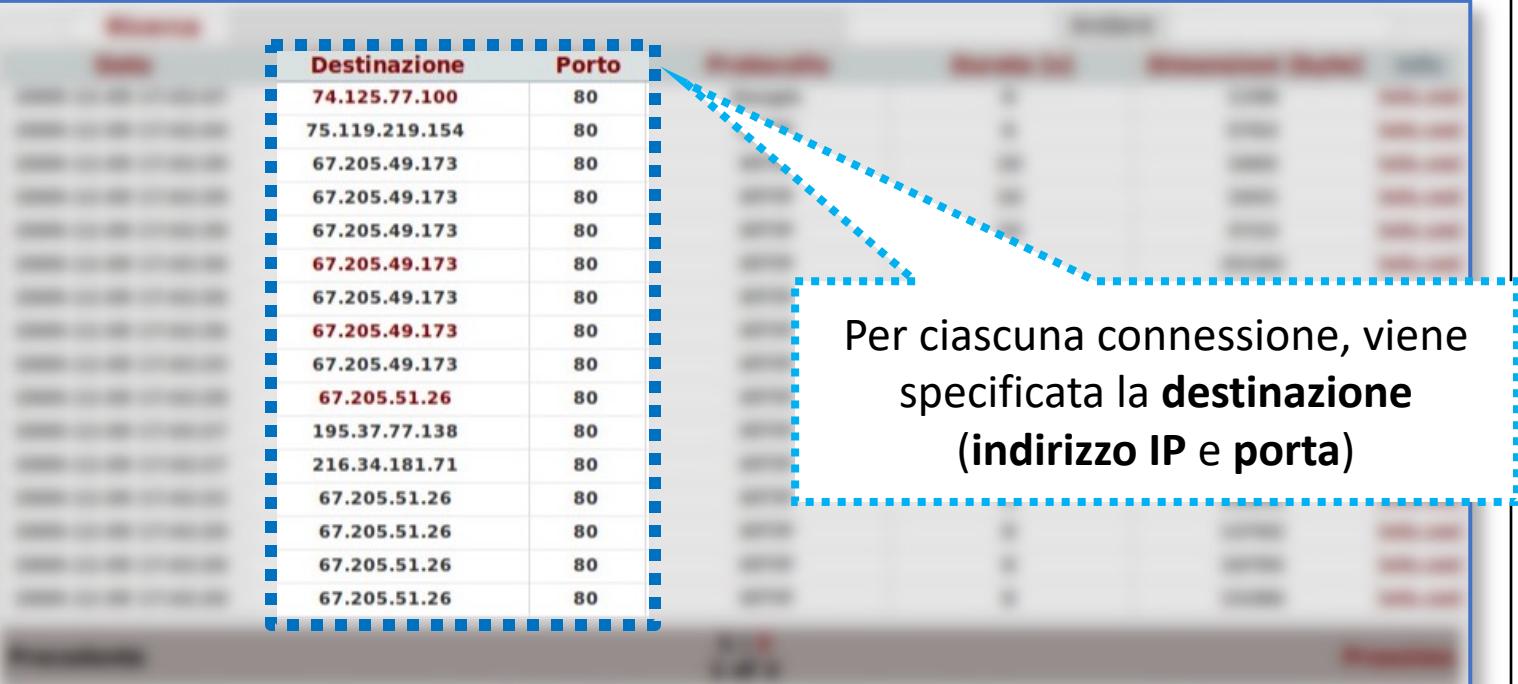
Data
2009-12-09 17:42:47
2009-12-09 17:42:44
2009-12-09 17:42:39
2009-12-09 17:42:39
2009-12-09 17:42:39
2009-12-09 17:42:36
2009-12-09 17:42:36
2009-12-09 17:42:36
2009-12-09 17:42:33
2009-12-09 17:42:28
2009-12-09 17:42:27
2009-12-09 17:42:27
2009-12-09 17:42:22
2009-12-09 17:42:20
2009-12-09 17:42:20
2009-12-09 17:42:20

Viene esplicitata la **data** e l'**ora**, in cui ha avuto luogo una certa connessione (riportata sulla riga)

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 20/24

- *Schermata TCP-UDP della sezione Sconosc.*



Per ciascuna connessione, viene specificata la **destinazione** (indirizzo IP e porta)

Destinazione	Porto
74.125.77.100	80
75.119.219.154	80
67.205.49.173	80
67.205.49.173	80
67.205.49.173	80
<b>67.205.49.173</b>	80
67.205.49.173	80
<b>67.205.49.173</b>	80
67.205.49.173	80
<b>67.205.51.26</b>	80
195.37.77.138	80
216.34.181.71	80
67.205.51.26	80
67.205.51.26	80
67.205.51.26	80
67.205.51.26	80

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 20/24

- Schermata TCP-UDP della sezione Sconosci.

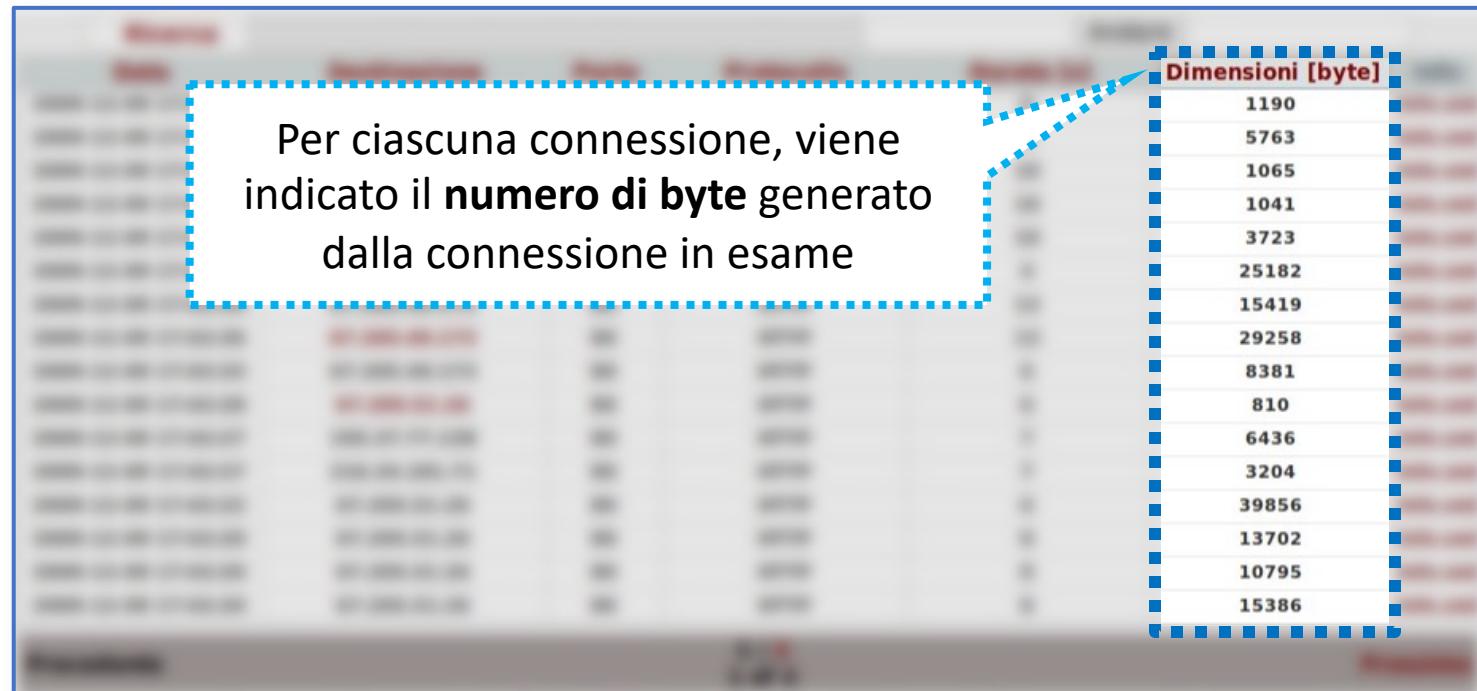
Per ciascuna connessione, viene esplicitato il **protocollo** e la **durata** (espressa in secondi)

Protocollo	Durata [s]
Google	0
HTTP	6
HTTP	10
HTTP	10
HTTP	10
HTTP	4
HTTP	13
HTTP	13
HTTP	6
HTTP	6
HTTP	7
HTTP	7
HTTP	6
HTTP	8
HTTP	8
HTTP	8

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 20/24

- *Schermata TCP-UDP della sezione Sconosci.*



# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 20/24

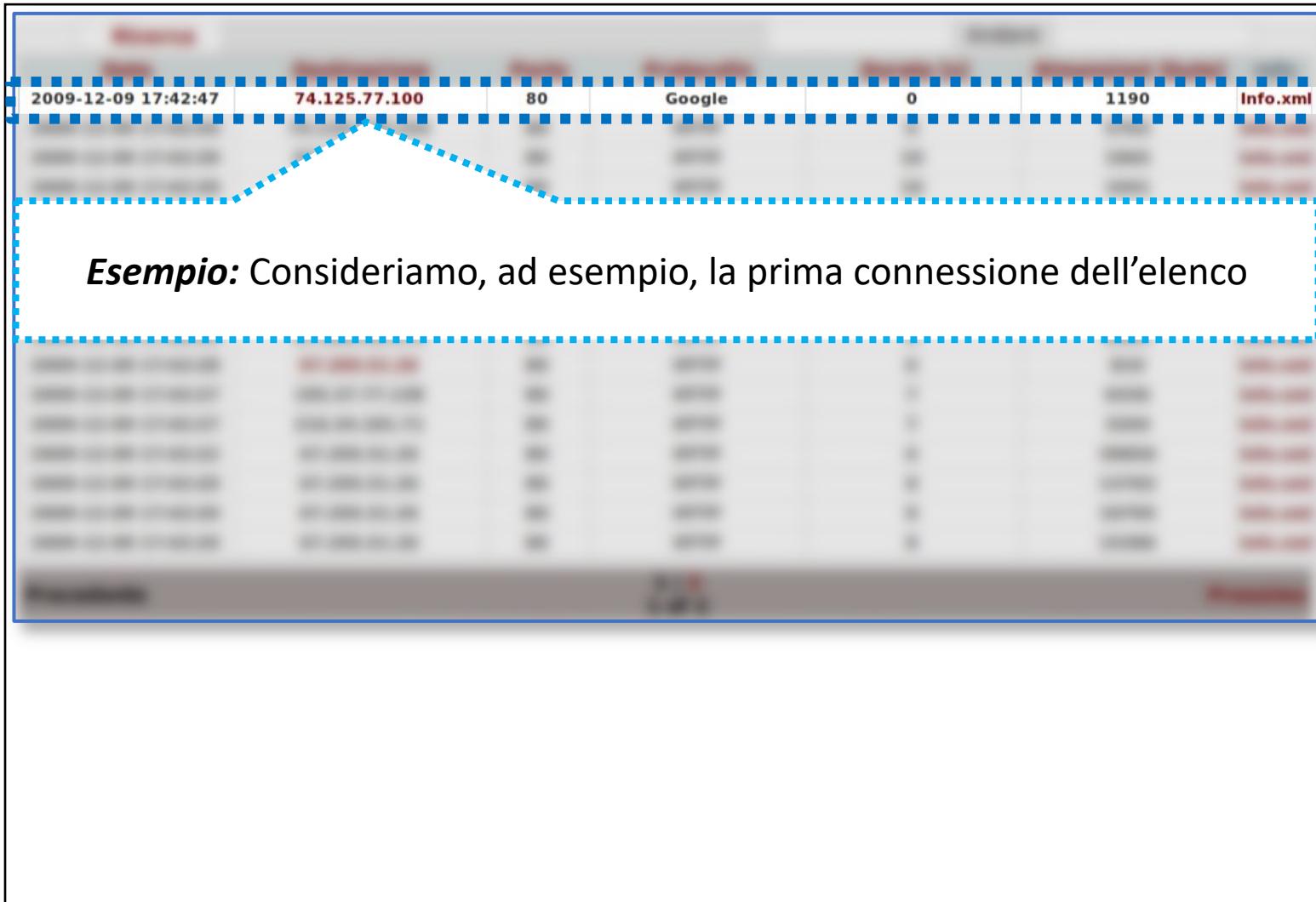
### OSSERVAZIONE

È possibile osservare che, per alcune connessioni, l'**indirizzo IP di destinazione** è evidenziato in **rosso scuro** ed è cliccabile, per ottenere **ulteriori dettagli** in merito alla connessione

Ricerca	Andare					
Data	Destinazione	Porto	Protocollo	Durata [s]	Dimensioni [byte]	Info
2009-12-09 17:42:47	74.125.77.100	80	Google	0	1190	<a href="#">Info.xml</a>
2009-12-09 17:42:44	75.119.219.154	80	HTTP	6	5763	<a href="#">Info.xml</a>
2009-12-09 17:42:39	67.205.49.173	80	HTTP	10	1065	<a href="#">Info.xml</a>
2009-12-09 17:42:39	67.205.49.173	80	HTTP	10	1041	<a href="#">Info.xml</a>
2009-12-09 17:42:39	67.205.49.173	80	HTTP	10	3723	<a href="#">Info.xml</a>
2009-12-09 17:42:36	67.205.49.173	80	HTTP	4	25182	<a href="#">Info.xml</a>
2009-12-09 17:42:36	67.205.49.173	80	HTTP	13	15419	<a href="#">Info.xml</a>
2009-12-09 17:42:36	67.205.49.173	80	HTTP	13	29258	<a href="#">Info.xml</a>
2009-12-09 17:42:33	67.205.49.173	80	HTTP	6	8381	<a href="#">Info.xml</a>
2009-12-09 17:42:28	67.205.51.26	80	HTTP	6	810	<a href="#">Info.xml</a>
2009-12-09 17:42:27	195.37.77.138	80	HTTP	7	6436	<a href="#">Info.xml</a>
2009-12-09 17:42:27	216.34.181.71	80	HTTP	7	3204	<a href="#">Info.xml</a>
2009-12-09 17:42:22	67.205.51.26	80	HTTP	6	39856	<a href="#">Info.xml</a>
2009-12-09 17:42:20	67.205.51.26	80	HTTP	8	13702	<a href="#">Info.xml</a>
2009-12-09 17:42:20	67.205.51.26	80	HTTP	8	10795	<a href="#">Info.xml</a>
2009-12-09 17:42:20	67.205.51.26	80	HTTP	8	15386	<a href="#">Info.xml</a>
Precedente	1   2 1 of 2			Prossimo		

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 21/24



# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 21/24

The screenshot shows a network traffic analysis interface. At the top, there's a header with various fields: timestamp (2009-12-09 17:42:47), source IP (74.125.77.100), destination port (80), destination host (Google), sequence number (0), acknowledgement number (1190), and file name (Info.xml). Below this, a list of network connections is shown, with the first connection highlighted by a blue dashed box. A larger blue dashed box encloses the detailed view of the selected connection.

**Esempio:** Cliccando sul link relativo all'indirizzo IP di destinazione (ovvero 74.125.77.100) della prima connessione, verrà scaricato un file testuale con il contenuto del/dei pacchetto/i

HTTP/1.1 200 OK	10	100
Date: Wed, 09 Dec 2009 17:42:46 GMT	10	372
Content-Length: 35	4	251
Pragma: no-cache	13	154
Cache-Control: private, no-cache, no-cache=Set-Cookie, proxy-revalidate	13	292
Expires: Wed, 19 Apr 2000 11:43:00 GMT	6	838
Last-Modified: Wed, 21 Jan 2004 19:50:30 GMT	6	81
Content-Type: image/gif	7	643
Server: Golfe	7	320
X-XSS-Protection: 0	6	398
GIF89a,D; [root@parrot]-[~]		

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 21/24

The screenshot shows the Xplico interface. At the top, a timeline displays a single connection between '2009-12-09 17:42:47' and '2009-12-09 17:42:47'. The connection details are: Source IP 74.125.77.100, Destination Port 80, Application Google, Duration 0, and File Info.xml. A blue dashed box highlights the first connection entry. Below the timeline, a detailed packet view is shown. The first packet is highlighted with a blue border and contains the text: 'HTTP/1.1 200 OK'. A callout box points to this packet with the text: 'Si tratta di una **risposta HTTP**, ad una richiesta, soddisfatta correttamente (Codice: 200 OK)'. The background of the packet view shows other blurred network traffic.

**Esempio:** Cliccando sul link relativo all'indirizzo IP di destinazione (ovvero 74.125.77.100) della prima connessione, verrà scaricato un file testuale con il contenuto del/dei pacchetto/i

Si tratta di una **risposta HTTP**, ad una richiesta, soddisfatta correttamente  
(Codice: 200 OK)

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 21/24

The screenshot shows a network traffic analysis interface. At the top, there's a header with various fields: timestamp (2009-12-09 17:42:47), source IP (74.125.77.100), destination port (80), source port (0), destination IP (1190), and file name (Info.xml). Below this, a list of network connections is visible. A specific connection is highlighted with a blue dashed box. A callout bubble points from this box to a detailed view of the packet content.

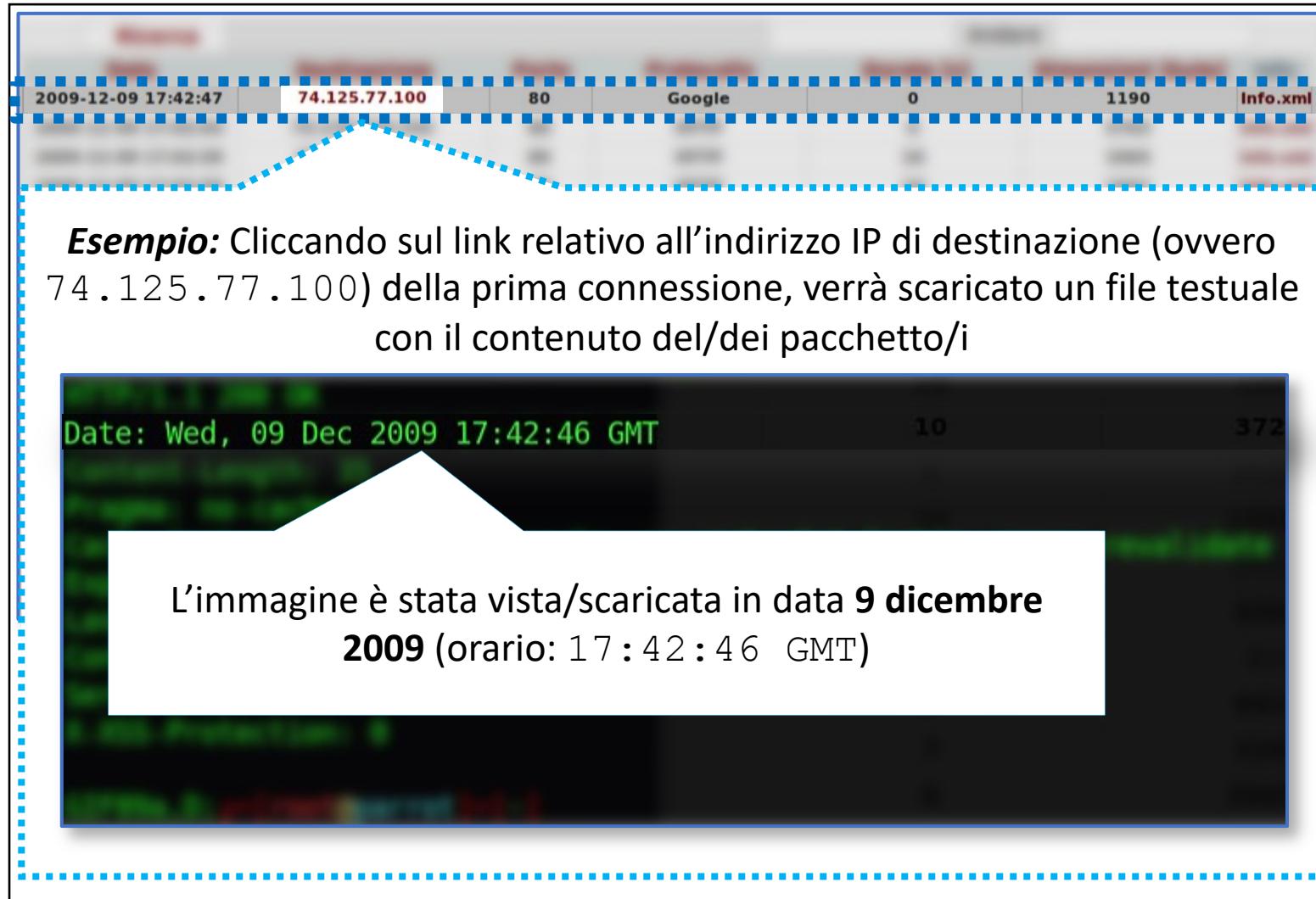
**Esempio:** Cliccando sul link relativo all'indirizzo IP di destinazione (ovvero 74.125.77.100) della prima connessione, verrà scaricato un file testuale con il contenuto del/dei pacchetto/i

All'interno del corpo della risposta è presente una immagine GIF, come si evince dal campo Content-Type uguale a `image/gif`)

Content-Type: `image/gif`

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 21/24



The screenshot shows a network traffic analysis interface. At the top, a timeline bar displays various connections with their start times, IP addresses, ports, and protocols. One connection is highlighted with a red box, showing details such as the source IP (74.125.77.100), destination port (80), protocol (Google), and file size (1190). A dashed blue line connects this connection to a detailed view below.

**Esempio:** Cliccando sul link relativo all'indirizzo IP di destinazione (ovvero 74.125.77.100) della prima connessione, verrà scaricato un file testuale con il contenuto del/dei pacchetto/i

Date: Wed, 09 Dec 2009 17:42:46 GMT

L'immagine è stata vista/scaricata in data **9 dicembre 2009** (orario: 17 : 42 : 46 GMT)

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 21/24



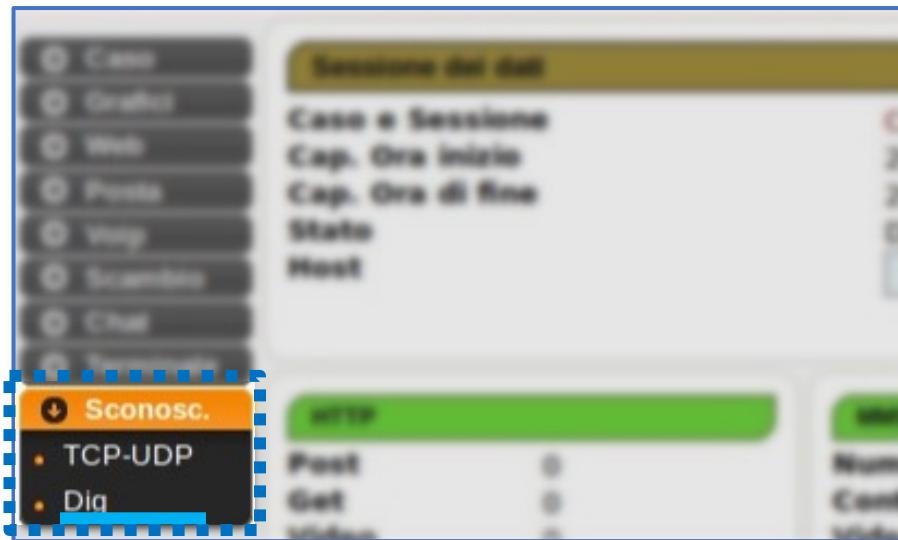
**Esempio:** Cliccando poi sul link **info.xml** e su **pcap**, si aprirà una pagina contenente ancora **altri dettagli** in relazione alla connessione in esame

```
--- Decoding info: stream 0 ---  
tcp  
  tcp.srcport 34342  
  tcp.dstport 80  
  tcp.cnt 1  
  tcp.lost 0  
  tcp.syn 0  
ip  
  ip.proto 6  
  ip.src 172.26.0.4  
  ip.dst 74.125.77.100  
  ip.offset 14  
eth  
  eth.src 00:16:e6:54:c8:97  
  eth.type 2048  
pol  
  pol.layer1 1  
  pol.count 621  
  pol.offset 375247  
  pol.file /opt/xplico/pol_1/sol_1/decode  
  /xplico.org_sample_capture_web_must_use_xplico_nc.cfg.pcap  
  pol.sesid 1  
  pol.polid 1
```

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 22/24

- È possibile approfondire gli artefatti sconosciuti, dal relativo menu a sinistra (sezione **Sconosc.**), mediante i seguenti link:
  - TCP-UDP
  - Dig



# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 23/24

- *Schermata Dig della sezione Sconosc.*

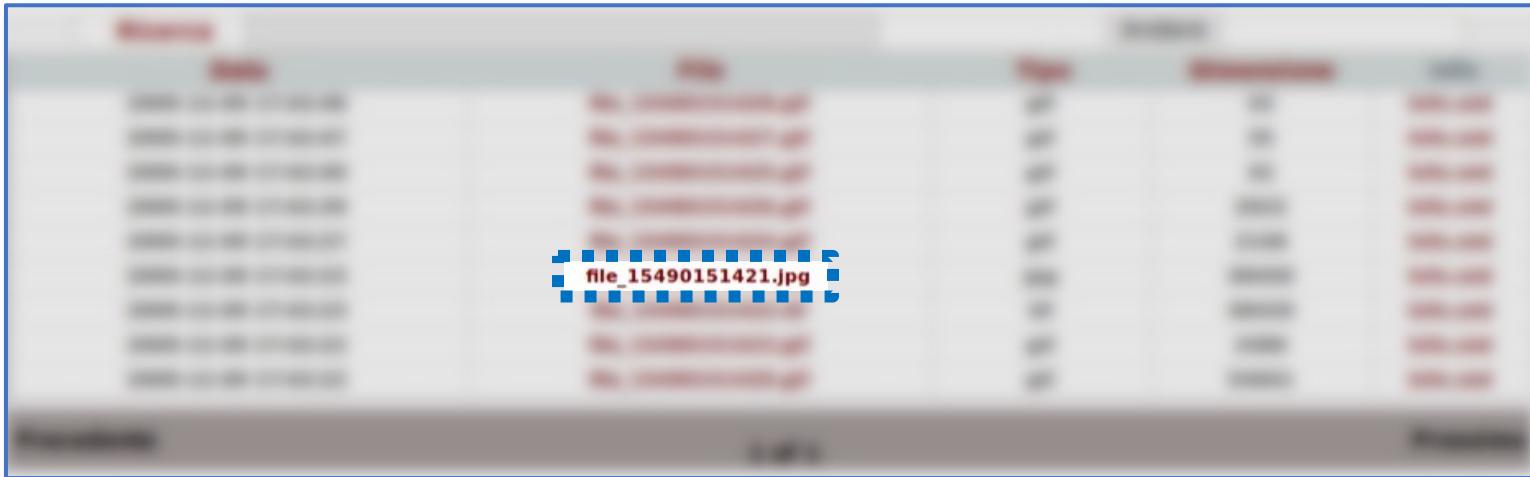
Ricerca	Andare			
Data	File	Tipo	Dimensione	Info
2009-12-09 17:42:48	file_15490151428.gif	gif	43	Info.xml
2009-12-09 17:42:47	file_15490151427.gif	gif	35	Info.xml
2009-12-09 17:42:40	file_15490151425.gif	gif	42	Info.xml
2009-12-09 17:42:39	file_15490151426.gif	gif	2022	Info.xml
2009-12-09 17:42:27	file_15490151424.gif	gif	2148	Info.xml
2009-12-09 17:42:23	file_15490151421.jpg	jpg	48450	Info.xml
2009-12-09 17:42:23	file_15490151422.tif	tif	48420	Info.xml
2009-12-09 17:42:22	file_15490151423.gif	gif	2480	Info.xml
2009-12-09 17:42:22	file_15490151420.gif	gif	54661	Info.xml
Precedente	1 of 1			Prossimo

- Vengono riportati diversi artefatti
  - Nello specifico, si tratta di immagini nei formati .gif, .tif e .jpg
  - In questo caso, è possibile visionare ciascun artefatto, cliccandone il nome del file, evidenziato in **rosso scuro**

# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 24/24

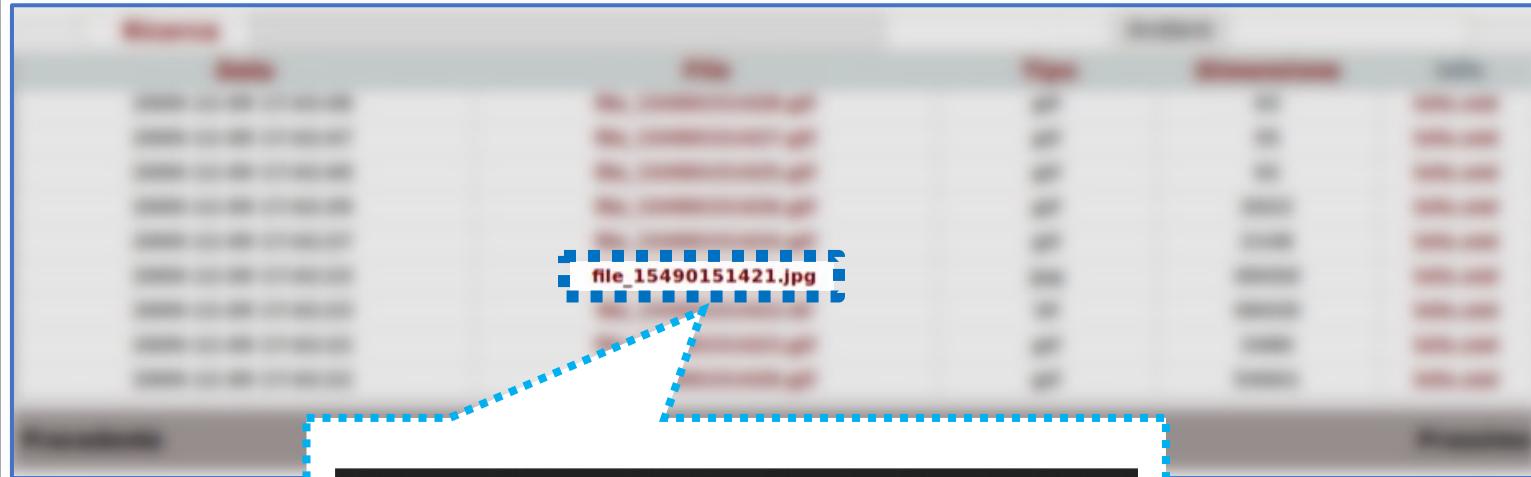
- *Schermata Dig della sezione Sconosc.*



# Il tool Xplico

## Esempio di Utilizzo 1 | HTTP & Web | 24/24

- *Schermata Dig della sezione Sconosci.*



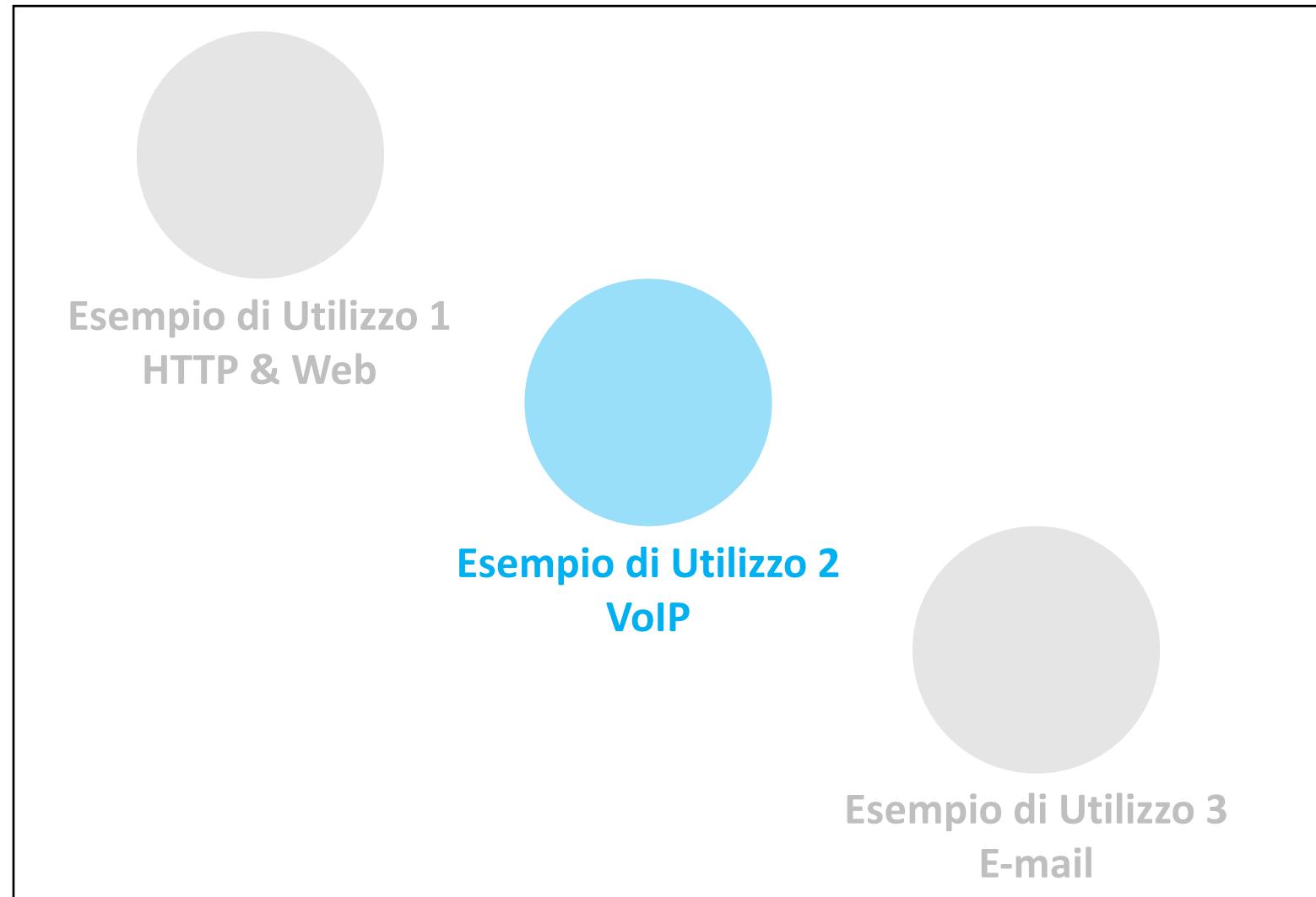
# Il tool Xplico

## Configurazione

- I file di configurazione di xplico, nella versione grafica, sono nella directory /opt/xplico/cfg
- Volendo usare la configurazione «nocheck», richiamata nel nome del file di cattura, va modificato il file xplico\_install\_lite.cfg riportando in esso le differenze tra i file xplico\_cli.nc e xplico\_cli.cfg

# Il tool Xplico

## Esempi di Utilizzo



# Il tool Xplico

## Il Servizio VoIP | Caratteristiche e Idee Base | 1/12

- Voice over IP (VoIP) definisce un insieme di protocolli
- Il segnale analogico, prodotto dalla **voce**, viene convertito in un segnale digitale, il quale viene **incapsulato in pacchetti**
  - Ciò permette di effettuare chiamate telefoniche, mediante le infrastrutture di rete



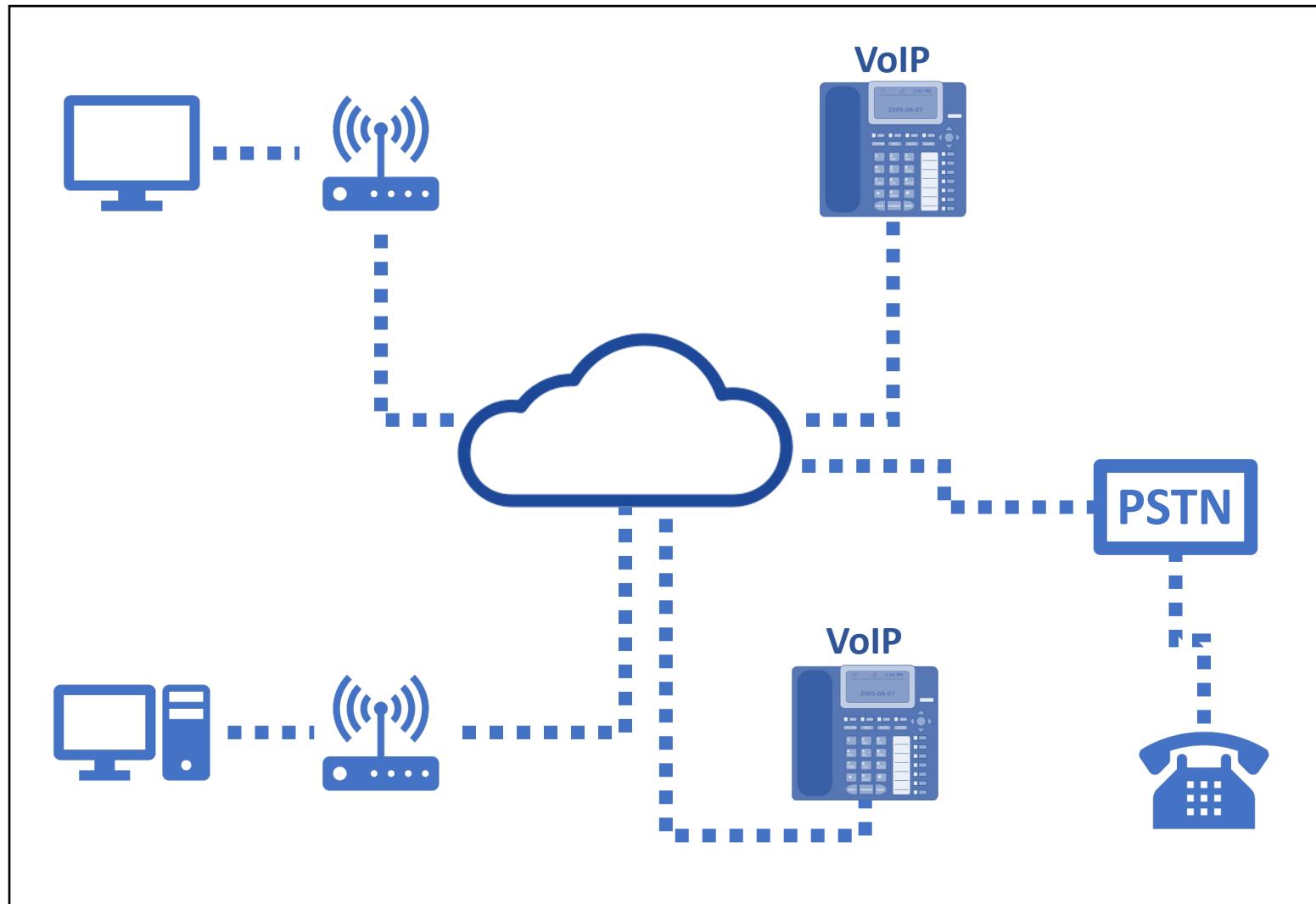
# Il tool Xplico

## Il Servizio VoIP | Caratteristiche e Idee Base | 2/12

- La comunicazione mediante VoIP è:
  - **Real-time**
  - **Bi-direzionale**
- Alcuni servizi VoIP permettono di effettuare chiamate telefoniche anche verso telefoni fissi e cellulari
  - Le linee telefoniche sono generalmente su rete **PSTN (Public Switched Telephone Network)**

# Il tool Xplico

## Il Servizio VoIP | Caratteristiche e Idee Base | 2/12



# Il tool Xplico

## Il Servizio VoIP | Vantaggi | 4/12



**Risparmio Economico**

**Meno Costi Hardware  
(Chiamate anche via PC)**

**Utilizzo Efficiente della Banda**

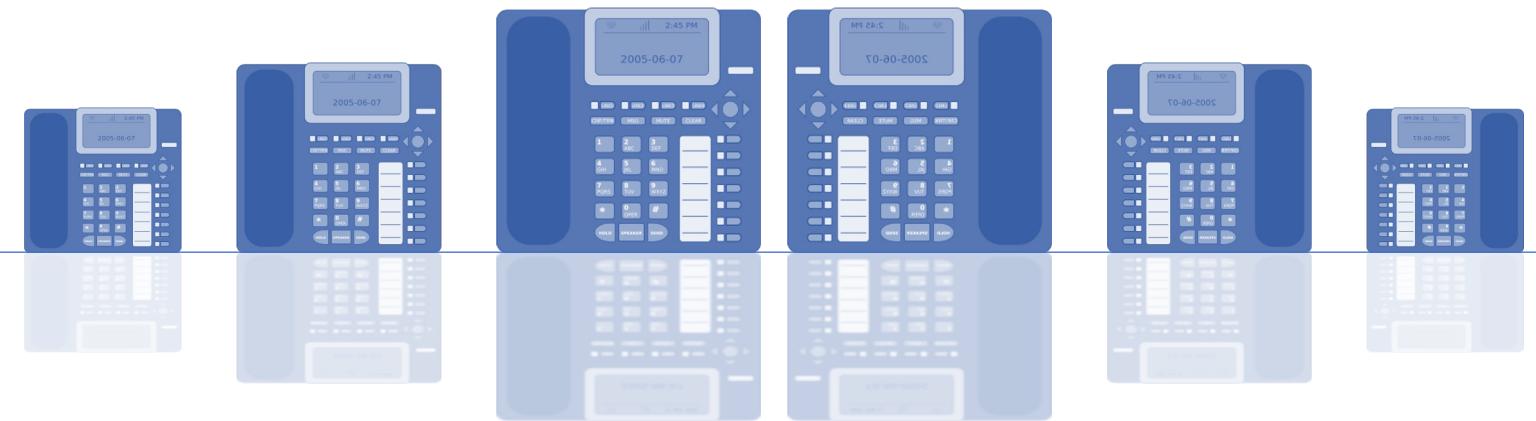
**Ulteriori Servizi  
(Trasferimento immagini, ecc.)**

# Il tool Xplico

## Il Servizio VoIP | 5/12

Una telefonata VoIP si articola in due fasi principali:

1. Setup
2. Flusso Audio

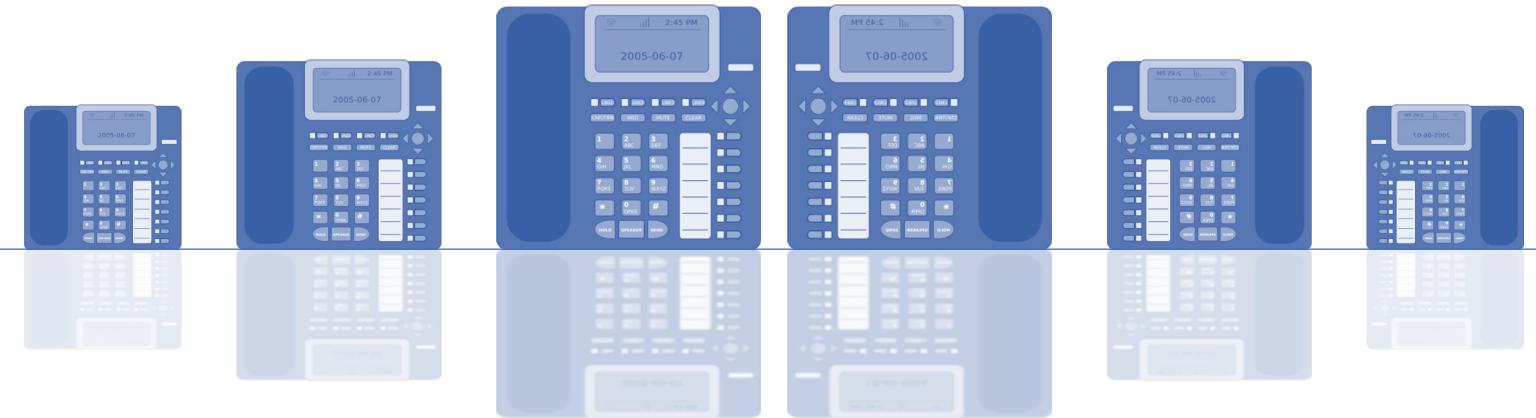


# Il tool Xplico

## Il Servizio VoIP | 5/12

Una telefonata VoIP si articola in due fasi principali:

1. Setup
2. Flusso Audio

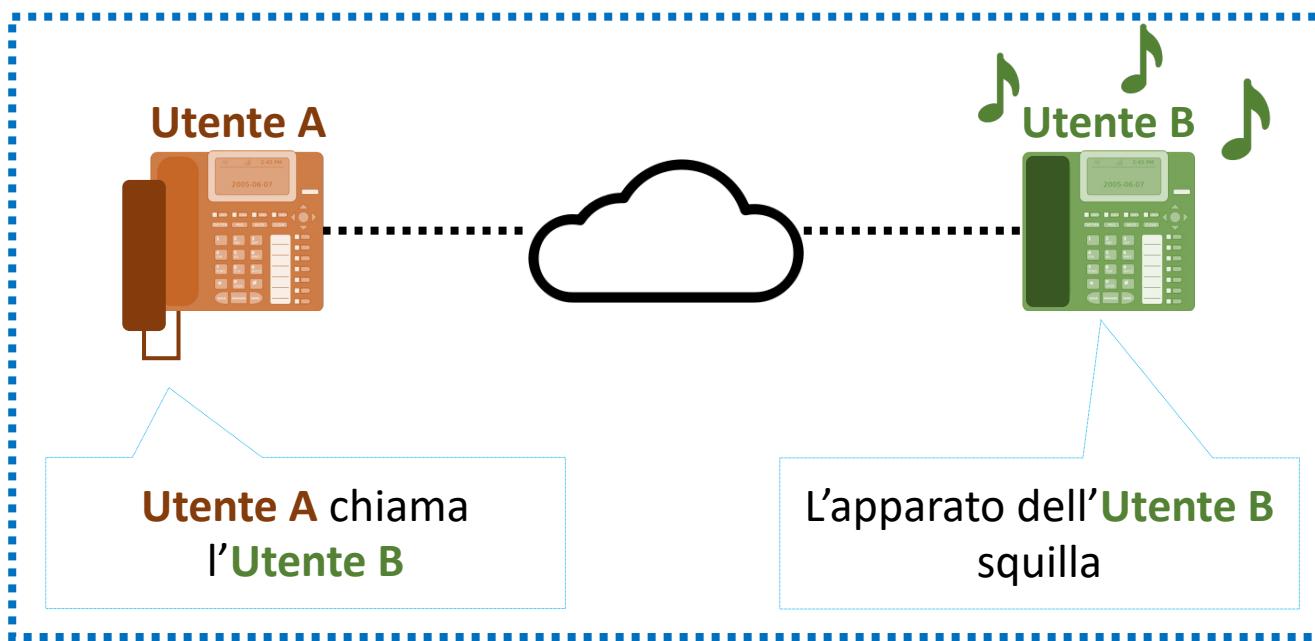


# Il tool Xplico

## Il Servizio VoIP | 6/12

### Setup | Idee Base

- Nella fase di setup, viene instaurata una **sessione**: il **chiamante** cerca di contattare il **chiamato**, mediante le varie infrastrutture di rete (router, gateway, ecc.)
- In questa fase può essere utilizzato uno dei seguenti protocolli: **H.323, SIP (Session Initiation Protocol)**, ecc.

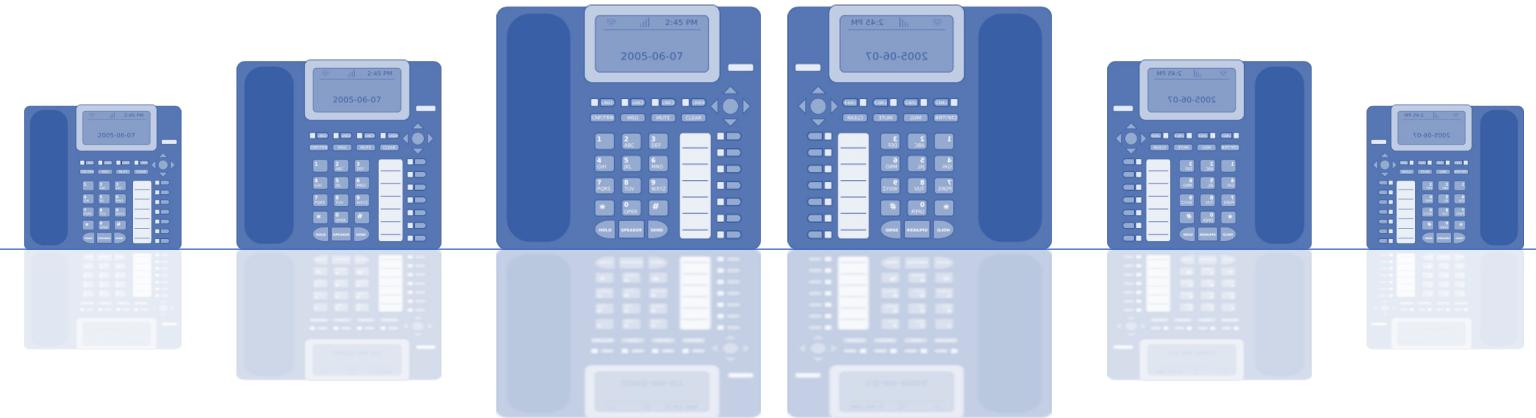


# Il tool Xplico

## Il Servizio VoIP | 7/12

Una telefonata VoIP si articola in due fasi principali:

1. Setup
2. Flusso Audio



# Il tool Xplico

## Il Servizio VoIP | 8/12

### Flusso Audio | Idee Base

- Se **chiamante** e **chiamato** hanno accettato la **sessione**, (instaurata nella fase di setup), viene **avviato il flusso audio** (ovvero, la telefonata)
  - Ad esempio, il **chiamato** può accettare la sessione, rispondendo al telefono
- Il protocollo utilizzato è tipicamente **RTP (Real-Time Protocol)**



### *Caratteristiche del Protocollo SIP (Cenni) | 1/2*

- Il protocollo SIP (Session Initiation Protocol) permette di **iniziare, modificare e terminare sessioni** per:
  - **Chiamate** telefoniche
  - **Conferenze** con più flussi multimediali (ad esempio, conferenze telefoniche)
  - Ecc.

### *Caratteristiche del Protocollo SIP (Cenni) | 2/2*

- Con il protocollo SIP, l'**identificativo** (telefonico) è **associato all'utente**, non al terminale
  - Analogia con l'e-mail (associata all'utente)
  - L'identificativo è nel formato Uniform Resource Identifier (URI)
    - *Esempi*
      - **sip:rpizzolante@unisa.it**
      - **sip:+39089546445454@gateway.com**
      - **sip:pincopallino@1.2.3.4**
- Protocollo di tipo client-server con scambio di **messaggi testuali**
  - Analogia con il protocollo HTTP

### *Alcune Funzionalità del Protocollo SIP (Cenni)*

- *Creazione della sessione*
  - Instaurare la sessione per una chiamata, impostando adeguati parametri, ecc.
- *Gestione di una sessione*
  - Trasferimento di una sessione
  - Modifiche ai parametri della sessione
  - Invocazione dei servizi

### Aspetti Forensi del servizio VoIP

- Il traffico di rete generato dal servizio VoIP può essere una **importante risorsa** per gli investigatori forensi
- È possibile individuare tracce di comunicazione, ad esempio:
  - Data e ora
  - Durata della comunicazione
  - Identificativo del chiamato (chiamate in uscita)
  - Identificativo del chiamante (chiamate in entrata)
  - Ecc.

# Il tool Xplico

## Esempio di Utilizzo 2 | VoIP | 1/12

- Creiamo una **nuova sessione** relativa al caso, precedentemente creato, denominato CasoXplico, cliccando su «**Nuova sessione**»

Elenco delle sessioni, riferite al Caso: CasoXplico				
	Nome	Ora d'inizio	Ora di fine	Stato
	HTTPWEB	2009-12-09 17:42:17	2009-12-09 17:42:50	DECODING COMPLETED

- Specifichiamo un **nome** per la sessione appena creata (nell'esempio, è stata denominata SIP)

The dialog box has a title 'Nuova sessione'. It contains a label 'Nome della Sessione' followed by a text input field containing 'SIP'. At the bottom is a blue 'Crea' button.

# Il tool Xplico

## Esempio di Utilizzo 2 | VoIP | 2/12

The screenshot shows the Xplico interface. At the top, there is a search bar and a 'Crea' button highlighted with a blue dashed border. A large blue arrow points downwards from this button to a message box at the bottom. The message box contains the text 'La sessione è stata creata'. Below this, a table titled 'Elenco delle sessioni, riferite al Caso: CasoXplico' is displayed. The table has columns: Nome, Ora d'inizio, Ora di fine, Stato, and Azioni. It lists two sessions: 'SIP' (empty) and 'HTTPWEB' (Decoding Completed). The 'HTTPWEB' row has an 'Elimina' (Delete) link in the 'Azioni' column.

Nome	Ora d'inizio	Ora di fine	Stato	Azioni
SIP	---	---	EMPTY	
HTTPWEB	2009-12-09 17:42:17	2009-12-09 17:42:50	DECODING COMPLETED	Elimina

- La nuova sessione è stata correttamente creata ed è mostrata nella lista delle sessioni, relative al caso CasoXplico

# Il tool Xplico

## Esempio di Utilizzo 2 | VoIP | 3/12

The screenshot shows the Xplico interface with a focus on a SIP session. A blue dashed box highlights the "SIP" entry in the top navigation bar. A large blue arrow points down from this bar to the main content area.

**Sessione dei dati**

Caso e Sessione	CasoXplico -> SIP
Cap. Ora inizio	---
Cap. Ora di fine	---
Stato	EMPTY
Host	---

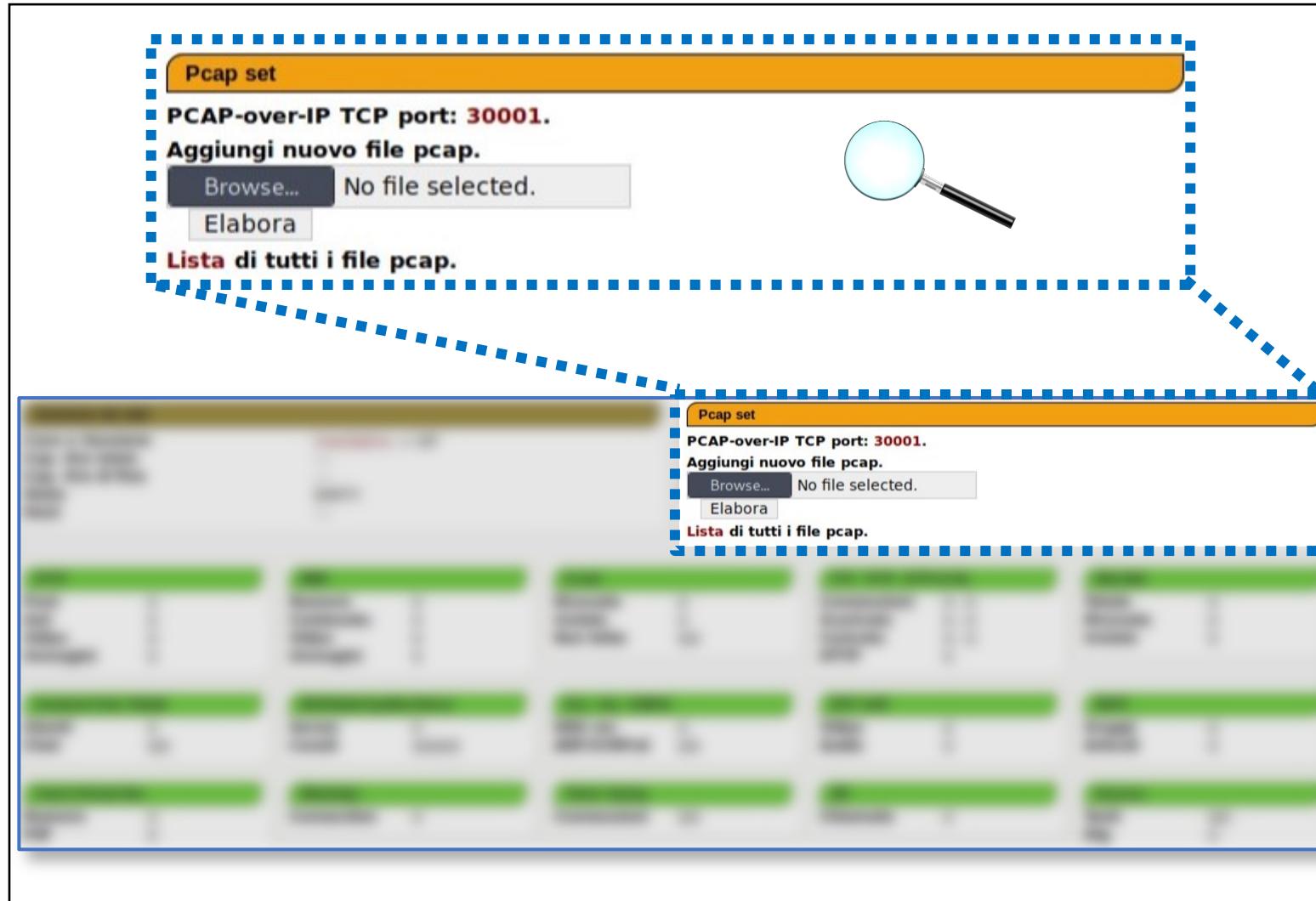
**Pcap set**

PCAP-over-IP TCP port: 30001.  
Aggiungi nuovo file pcap.  
Browse... No file selected.  
Elabora  
Lista di tutti i file pcap.

<b>HTTP</b>	<b>MMS</b>	<b>E-mail</b>	<b>FTP - TFTP - HTTP di file</b>	<b>Web Mail</b>
<b>Post</b> 0	<b>Numero</b> 0	<b>Ricevute</b> 0	<b>Connessioni</b> 0 - 0	<b>Totale</b> 0
<b>Get</b> 0	<b>Contenuto</b> 0	<b>Inviate</b> 0	<b>Scaricato</b> 0 - 0	<b>Ricevute</b> 0
<b>Video</b> 0	<b>Video</b> 0	<b>Non lette</b> 0/0	<b>Caricato</b> 0 - 0	<b>Inviate</b> 0
<b>Immagini</b> 0	<b>Immagini</b> 0		<b>HTTP</b> 0	
<b>Facebook Chat / Paitalk</b>				
<b>Utenti</b> 0	<b>IRC/Paitalk Exp/Msn/Yahoo!</b>	<b>Dns - Arp - ICMPv6</b>	<b>RTP / VoIP</b>	<b>NNTP</b>
<b>Chat</b> 0/0	<b>Server</b> 0	<b>DNS res</b> 0	<b>Video</b> 0	<b>Gruppi</b> 0
	<b>Canali</b> 0/0/0	<b>ARP/ICMPv6</b> 0/0	<b>Audio</b> 0	<b>Articoli</b> 0
<b>Feed &amp; Printed files</b>				
<b>Numero</b> 0	<b>WhatsApp</b>	<b>Telnet / Syslog</b>	<b>SIP</b>	<b>Sconosc.</b>
<b>Pdf</b> 0	<b>Connection</b> 0	<b>Connessioni</b> 0/0	<b>Chiamate</b> 0	<b>Testi</b> 0/0
				<b>Dig</b> 0

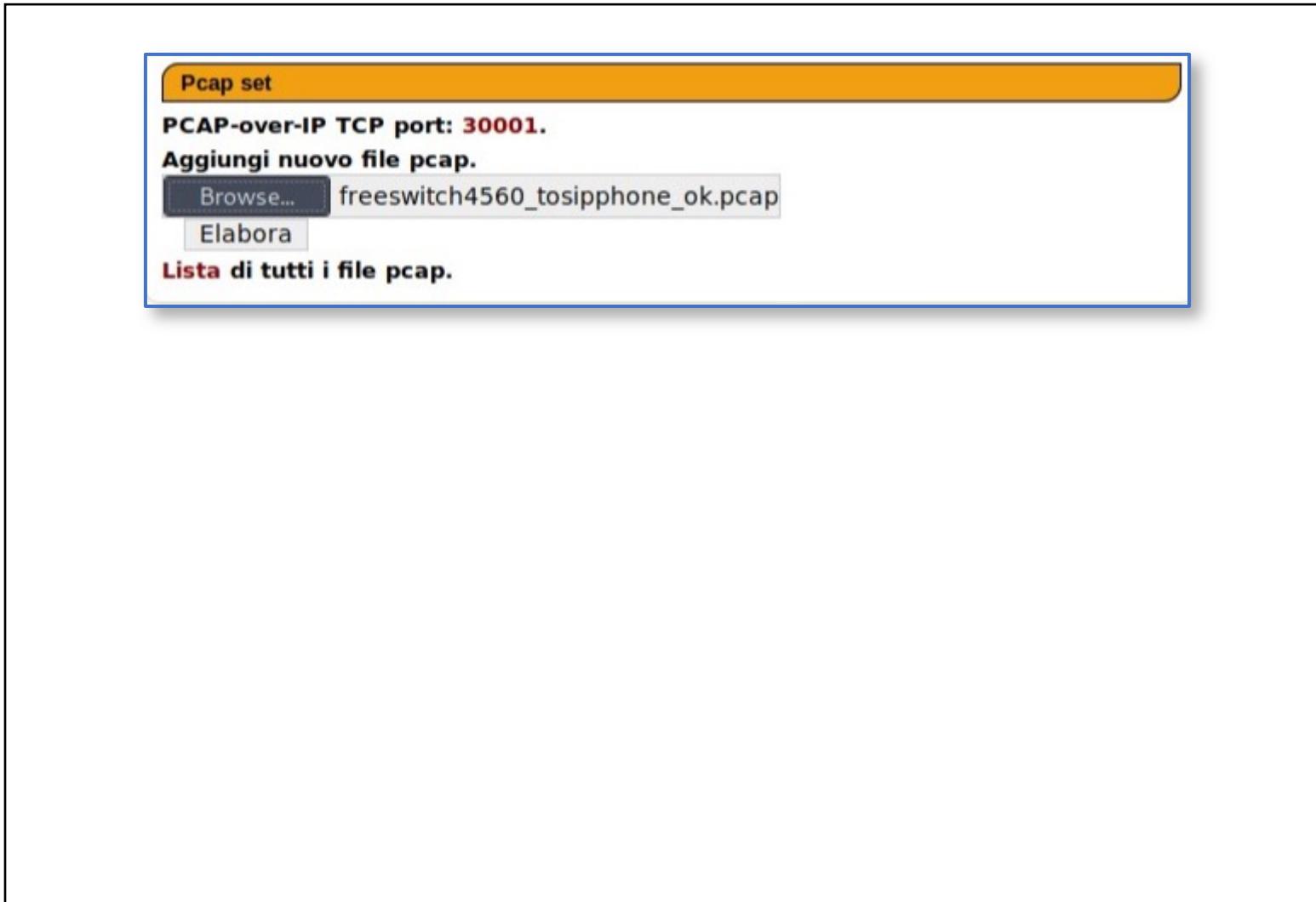
# Il tool Xplico

## Esempio di Utilizzo 2 | VoIP | 3/12



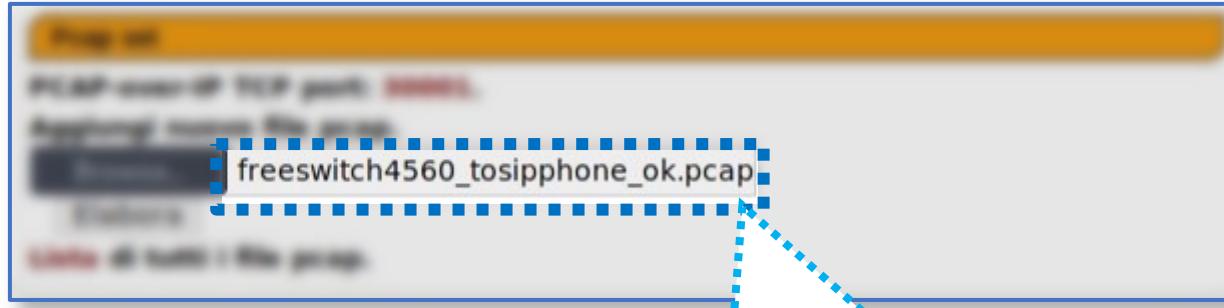
# Il tool Xplico

## Esempio di Utilizzo 2 | VoIP | 4/12



# Il tool Xplico

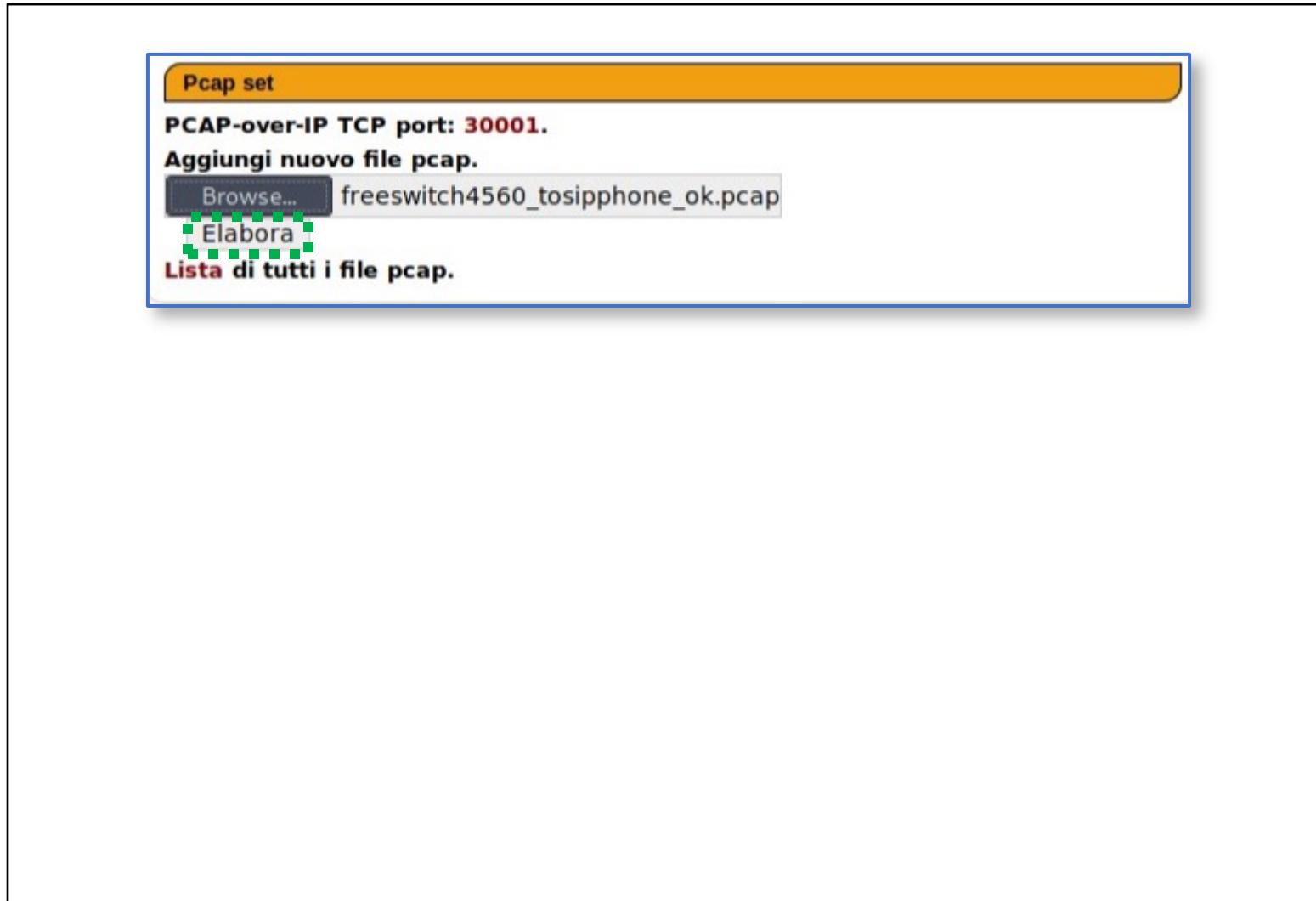
## Esempio di Utilizzo 2 | VoIP | 4/12



In questo esempio, utilizzeremo il file, denominato  
`freeswitch4560_tosipphone_ok.pcap`

# Il tool Xplico

## Esempio di Utilizzo 2 | VoIP | 5/12



# Il tool Xplico

## Esempio di Utilizzo 2 | VoIP | 5/12

Pcap set

PCAP-over-IP TCP port: 30001.

Aggiungi nuovo file pcap.

Browse... freeswitch4560\_tosipphone\_ok.pcap

Elabora

Lista di tutti i file pcap.

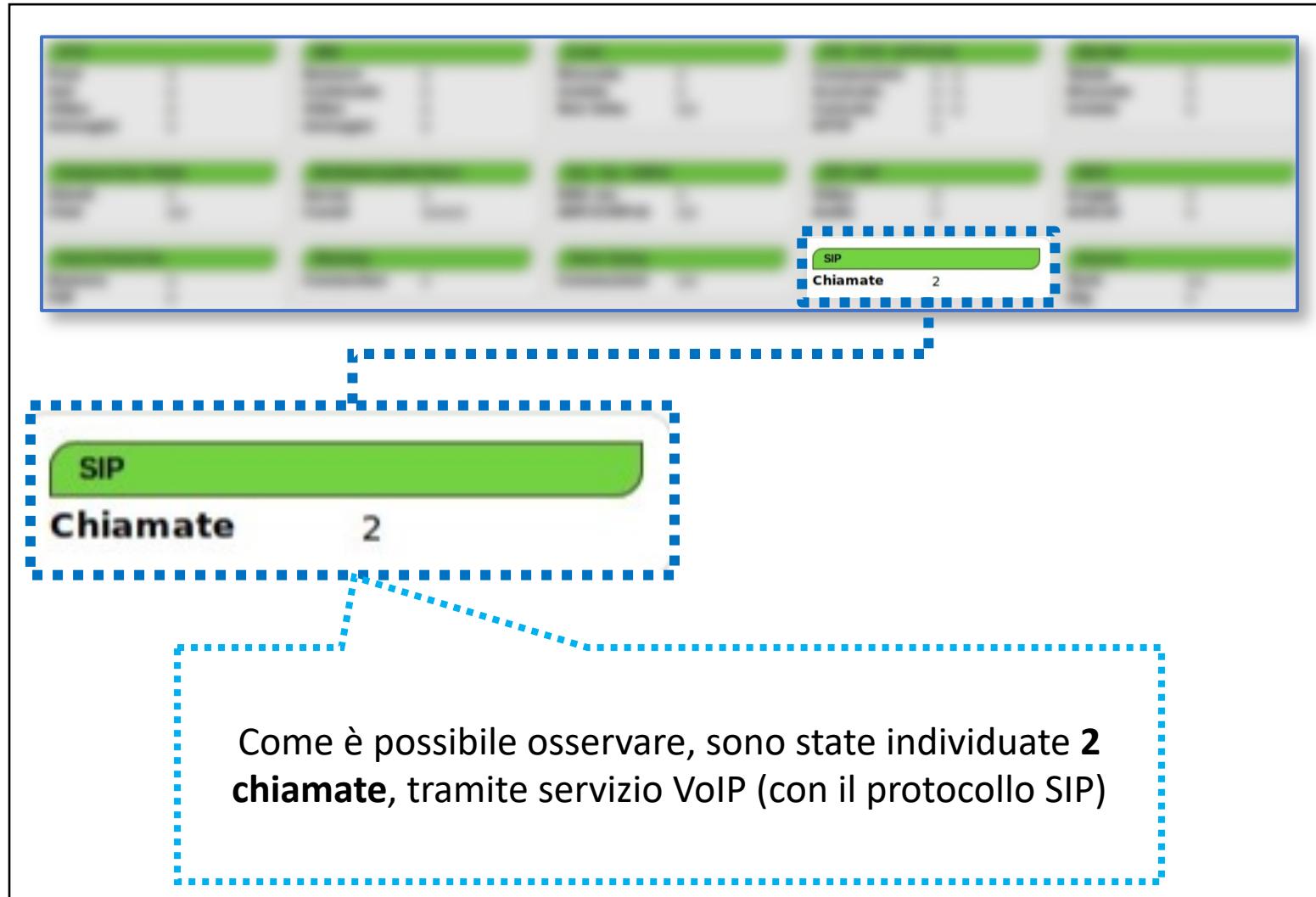


### Sessione Riepilogativa

<b>HTTP</b> Post 0 Get 0 Video 0 Immagini 0	<b>MMS</b> Numero 0 Contenuto 0 Video 0 Immagini 0	<b>E-mail</b> Ricevute 0 Inviate 0 Non lette 0/0	<b>FTP - TFTP - HTTP di file</b> Conessioni 0 - 0 Scaricato 0 - 0 Caricato 0 - 0 HTTP 0	<b>Web Mail</b> Totale 0 Ricevute 0 Inviate 0
<b>Facebook Chat / Paitalk</b> Utenti 0 Chat 0/0	<b>IRC/Paitalk Exp/Msn/Yahoo!</b> Server 0 Canali 0/0/0	<b>Dns - Arp - ICMPv6</b> DNS res 0 ARP/ICMPv6 0/0	<b>RTP / VoIP</b> Video 0 Audio 0	<b>NTP</b> Gruppi 0 Articoli 0
<b>Feed &amp; Printed files</b> Numero 0 Pdf 0	<b>WhatsApp</b> Connection 0	<b>Telnet / Syslog</b> Conessioni 0/0	<b>SIP</b> Chiamate 2	<b>Sconosciuti</b> Testi 0/1 Dig 0

# Il tool Xplico

## Esempio di Utilizzo 2 | VoIP | 6/12



# Il tool Xplico

## Esempio di Utilizzo 2 | VoIP | 7/12

- Per ottenere ulteriori informazioni in merito alle chiamate individuate, è possibile cliccare sul link **SIP**, dal relativo menu a sinistra (sezione **VoIP**)



# Il tool Xplico

## Esempio di Utilizzo 2 | VoIP | 8/12

- *Schermata SIP della sezione VoIP*

Cerca:		Andare	
Data	Da	A	Durata
2007-10-31 12:14:23	"FreeSwitch" <sip:5555551212@192.168.1.111>	<sip:6580@192.168.1.12>	0:0:0
2007-10-31 12:14:23	"FreeSwitch" <sip:5555551212@192.168.1.111>	<sip:6580@192.168.1.12>	0:0:19

# Il tool Xplico

## Esempio di Utilizzo 2 | VoIP | 8/12

- Schermata SIP della sezione VoIP

Cerca:		Andare	
Data	Da	A	Durata
2007-10-31 12:14:23	"FreeSwitch" <sip:5555551212@192.168.1.111>	<sip:6580@192.168.1.12>	0:0:0
2007-10-31 12:14:23	"FreeSwitch" <sip:5555551212@192.168.1.111>	<sip:6580@192.168.1.12>	0:0:19

### OSSERVAZIONE IMPORTANTE

Sono state effettuate **due chiamate** da "**FreeSwitch**" <sip:**5555551212**@192.168.1.111> (colonna denominata **Da**) a <sip:**6580**@192.168.1.12> (colonna denominata **A**) della durata rispettivamente di **0 secondi** e **19 secondi** (entrambe le comunicazioni sono state effettuate alle ore **12:14:23** del giorno **31/10/2007**, come si evince dalla colonna **Data**)

# Il tool Xplico

## Esempio di Utilizzo 2 | VoIP | 9/12

- *Schermata SIP della sezione VoIP*

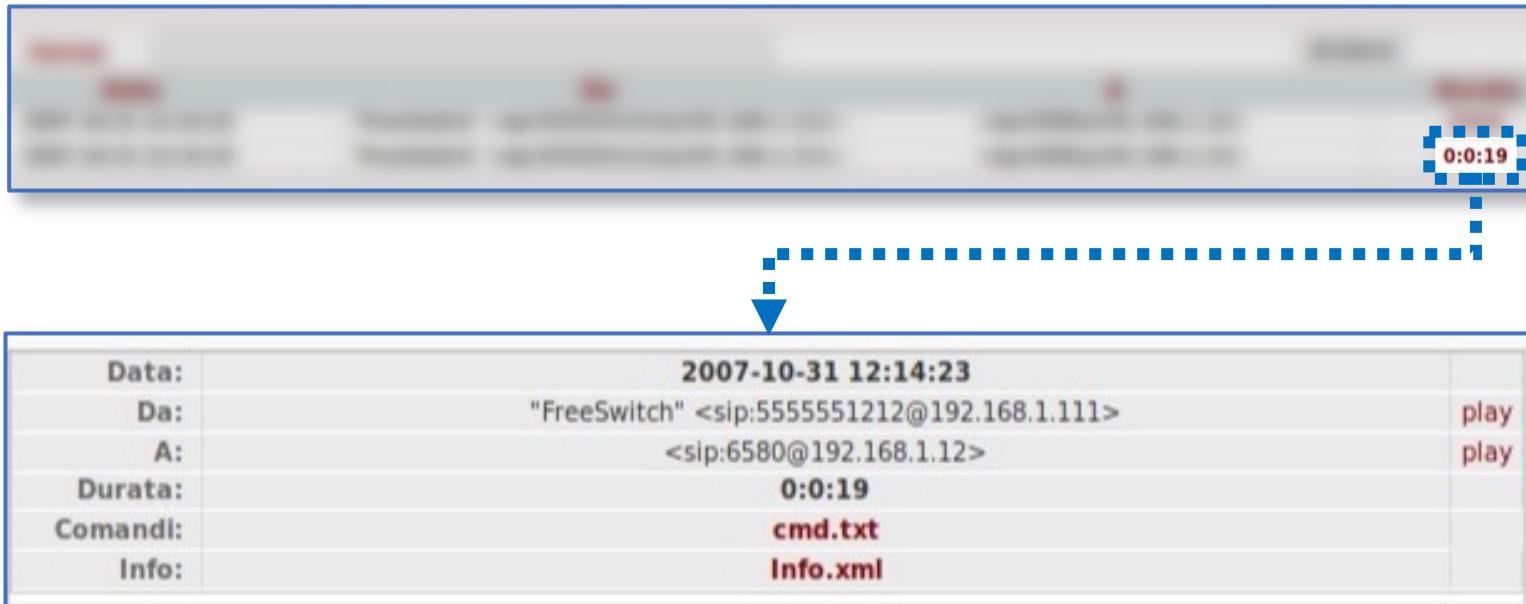


- Cliccando sulla **durata** (evidenziata in **rosso scuro**), è possibile ottenere maggiori informazioni

# Il tool Xplico

## Esempio di Utilizzo 2 | VoIP | 10/12

- *Schermata SIP della sezione VoIP*



Data:	2007-10-31 12:14:23
Da:	"FreeSwitch" <sip:5555551212@192.168.1.111>
A:	<sip:6580@192.168.1.12>
Durata:	0:0:19
Comandi:	<a href="#">cmd.txt</a>
Info:	<a href="#">Info.xml</a>

- Cliccando su **cmd.txt** è possibile visionare il contenuto di alcuni **pacchetti** del protocollo SIP, all'interno dei quali potrebbero esservi **informazioni utili all'investigatore**

# Il tool Xplico

## Esempio di Utilizzo 2 | VoIP | 11/12

- Schermata SIP della sezione VoIP



```
SIP/2.0 180 Ringing
Call-ID: a83ec57b-024d-122b-2780-39a48cb53b8d
CSeq: 90798095 INVITE
From: "FreeSwitch" <sip:5555551212@192.168.1.111>;tag=NZcQcBB9gXt5K
To: <sip:6580@192.168.1.12>;tag=cbc95aff6448a9
Via: SIP/2.0/UDP 192.168.1.111;branch=z9hG4bKN5DyctFHeef8m;rport
Content-Length: 0
Contact: tel sip <sip:6580@192.168.1.12:5060;transport=udp>
User-Agent: optiPoint 400 standard

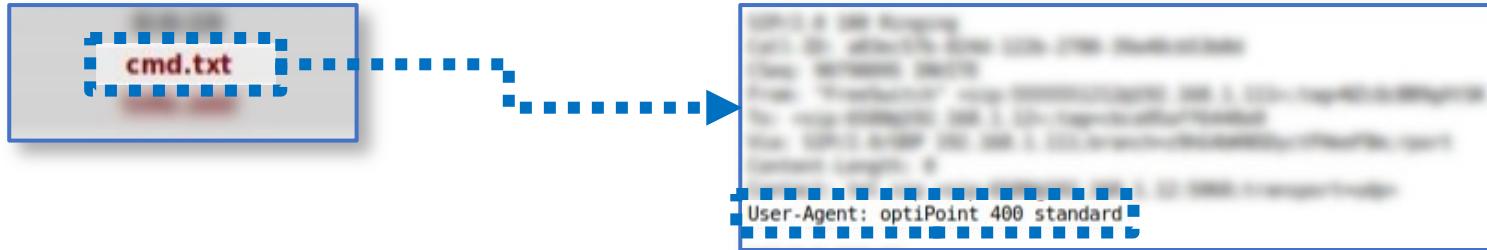
SIP/2.0 200 OK
Call-ID: a83ec57b-024d-122b-2780-39a48cb53b8d
CSeq: 90798095 INVITE
From: "FreeSwitch" <sip:5555551212@192.168.1.111>;tag=NZcQcBB9gXt5K
To: <sip:6580@192.168.1.12>;tag=cbc95aff6448a9
Via: SIP/2.0/UDP 192.168.1.111;branch=z9hG4bKN5DyctFHeef8m;rport
Content-Length: 186
Content-Type: application/sdp
Supported: replaces
Contact: tel sip <sip:6580@192.168.1.12:5060;transport=udp>
User-Agent: optiPoint 400 standard

v=0
o=MxSIP 0 1468182247 IN IP4 192.168.1.12
s=SIP Call
c=IN IP4 192.168.1.12
t=0 0
m=audio 5010 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=ptime:20
BYE sip:mod_sofia@192.168.1.111:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.12:5060;branch=z9hG4bKf4ecb0721
Max-Forwards: 70
To: "FreeSwitch" <sip:5555551212@192.168.1.111>;tag=NZcQcBB9gXt5K
From: <sip:6580@192.168.1.12>;tag=cbc95aff6448a9;epid=SC23351B
Call-ID: a83ec57b-024d-122b-2780-39a48cb53b8d
CSeq: 1041945456 BYE
Supported: timer
Content-Length: 0
Supported: replaces
User-Agent: optiPoint 400 standard
```

# Il tool Xplico

## Esempio di Utilizzo 2 | VoIP | 12/12

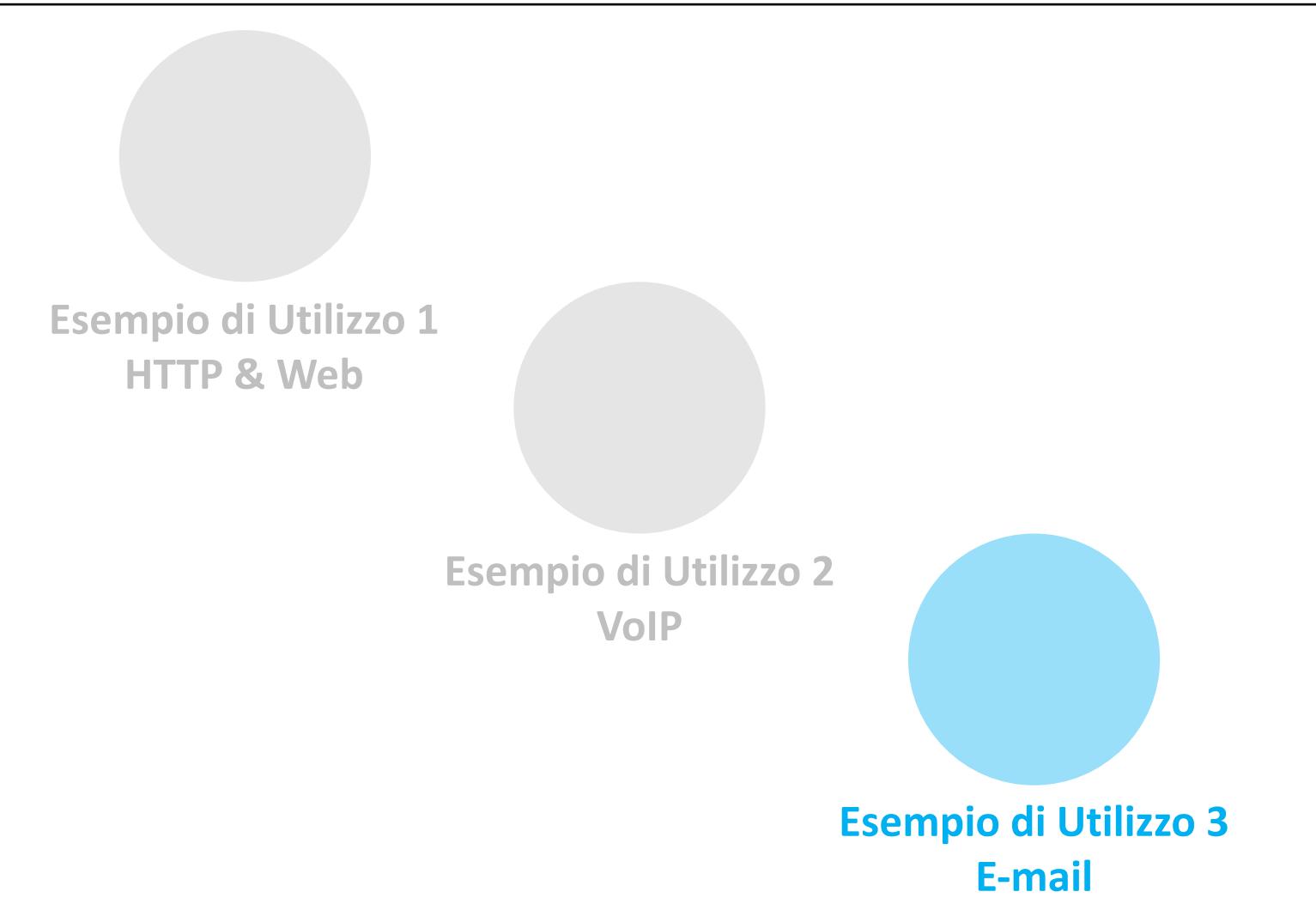
- Schermata SIP della sezione VoIP



**Esempio:** Tramite il valore del campo User-Agent, nei pacchetti SIP, è possibile individuare il modello (o i modelli) degli apparati che hanno effettuato la comunicazione (nell'esempio, si tratta di un Siemens OptiPoint 400 Standard)

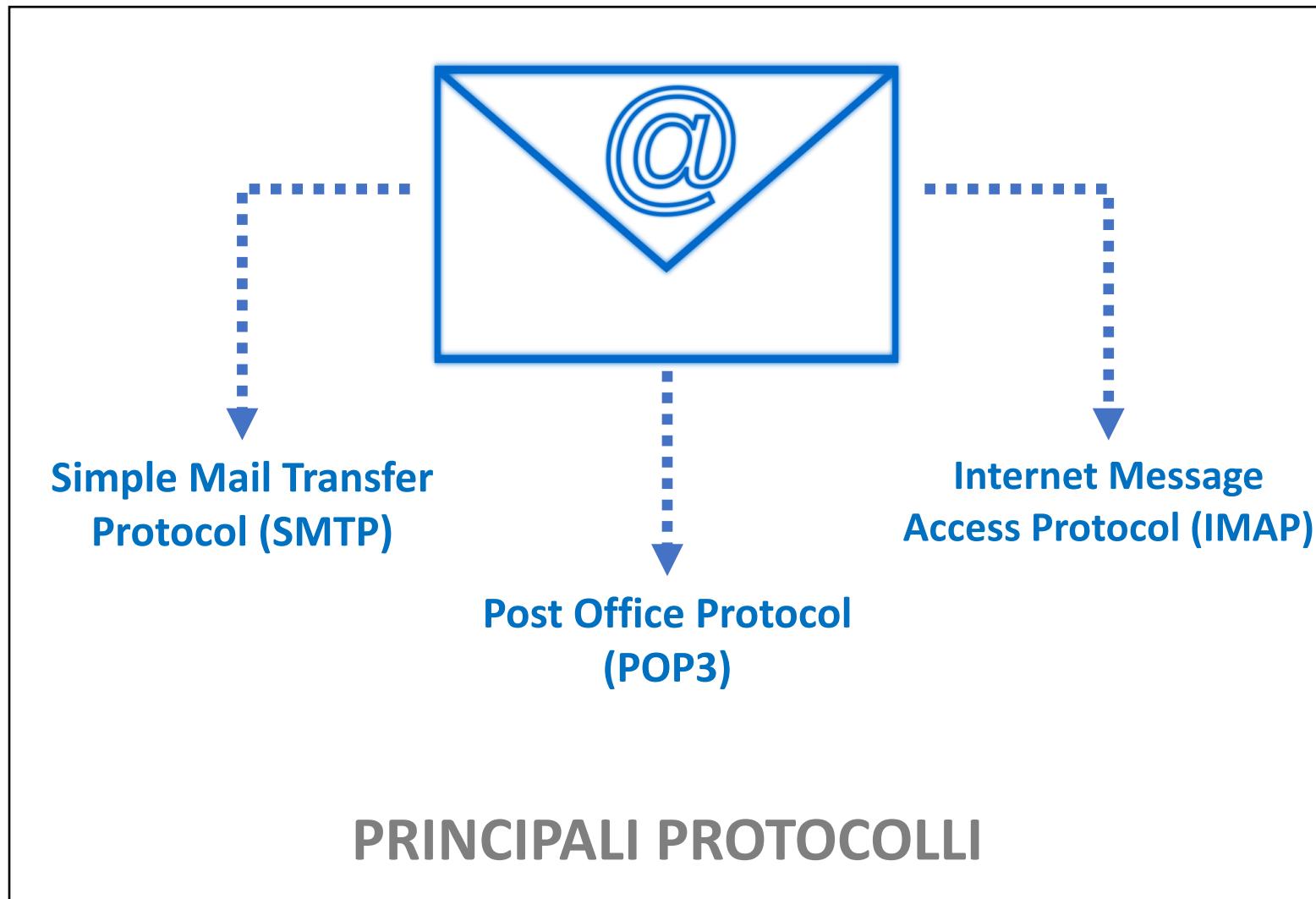
# Il tool Xplico

## Esempi di Utilizzo



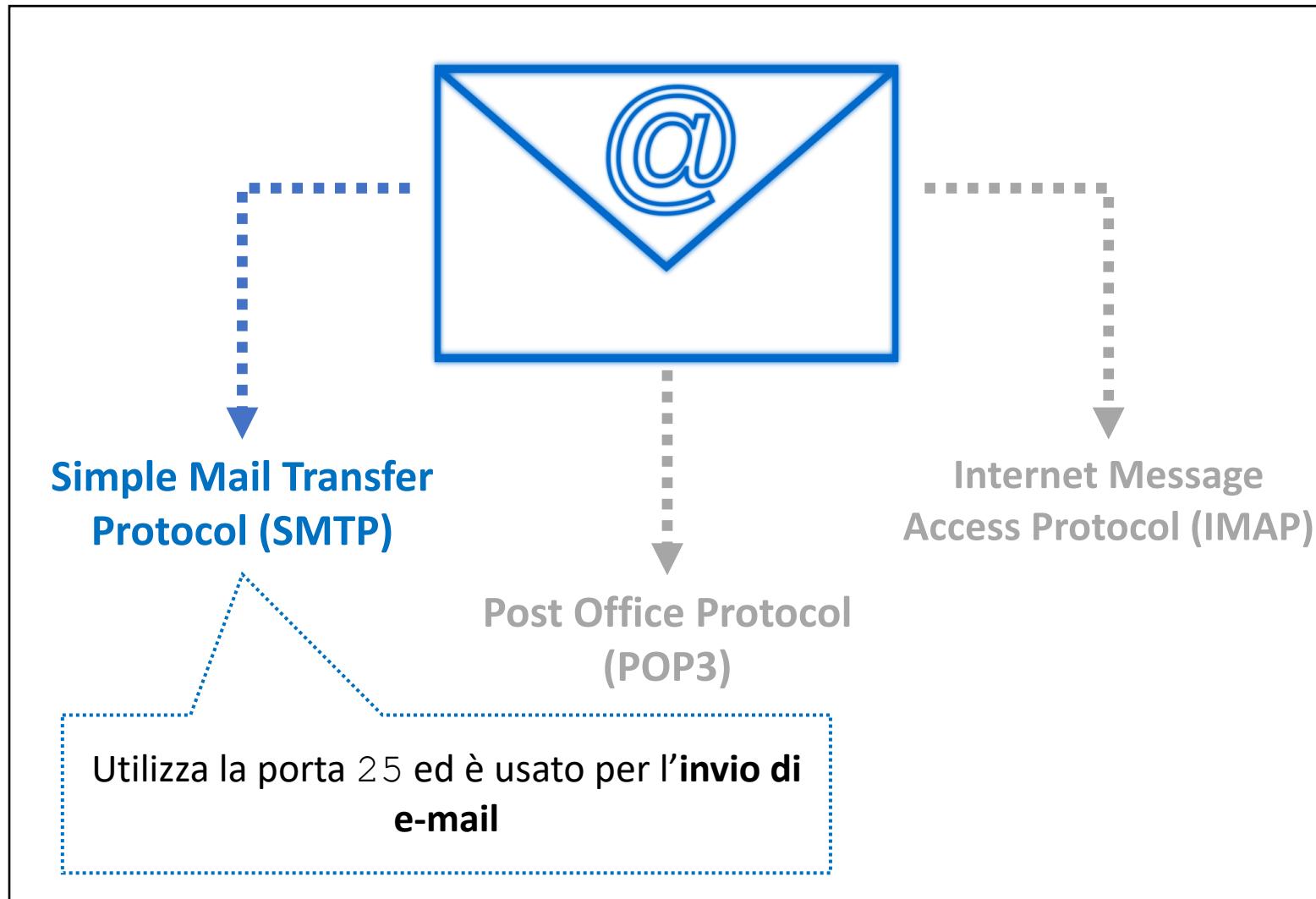
# Il tool Xplico

## Protocolli E-mail | 1/3



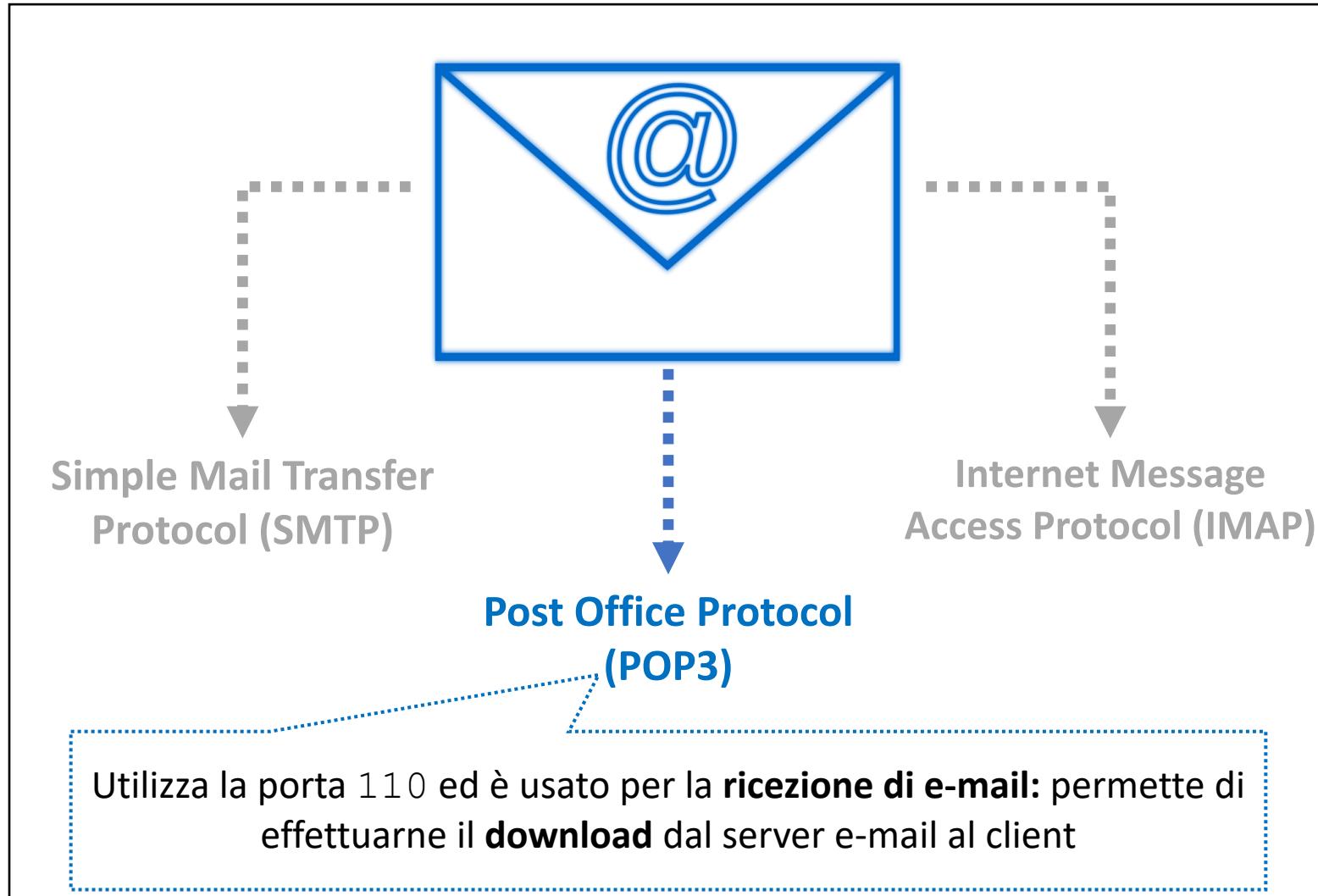
# Il tool Xplico

## Protocolli E-mail | 1/3



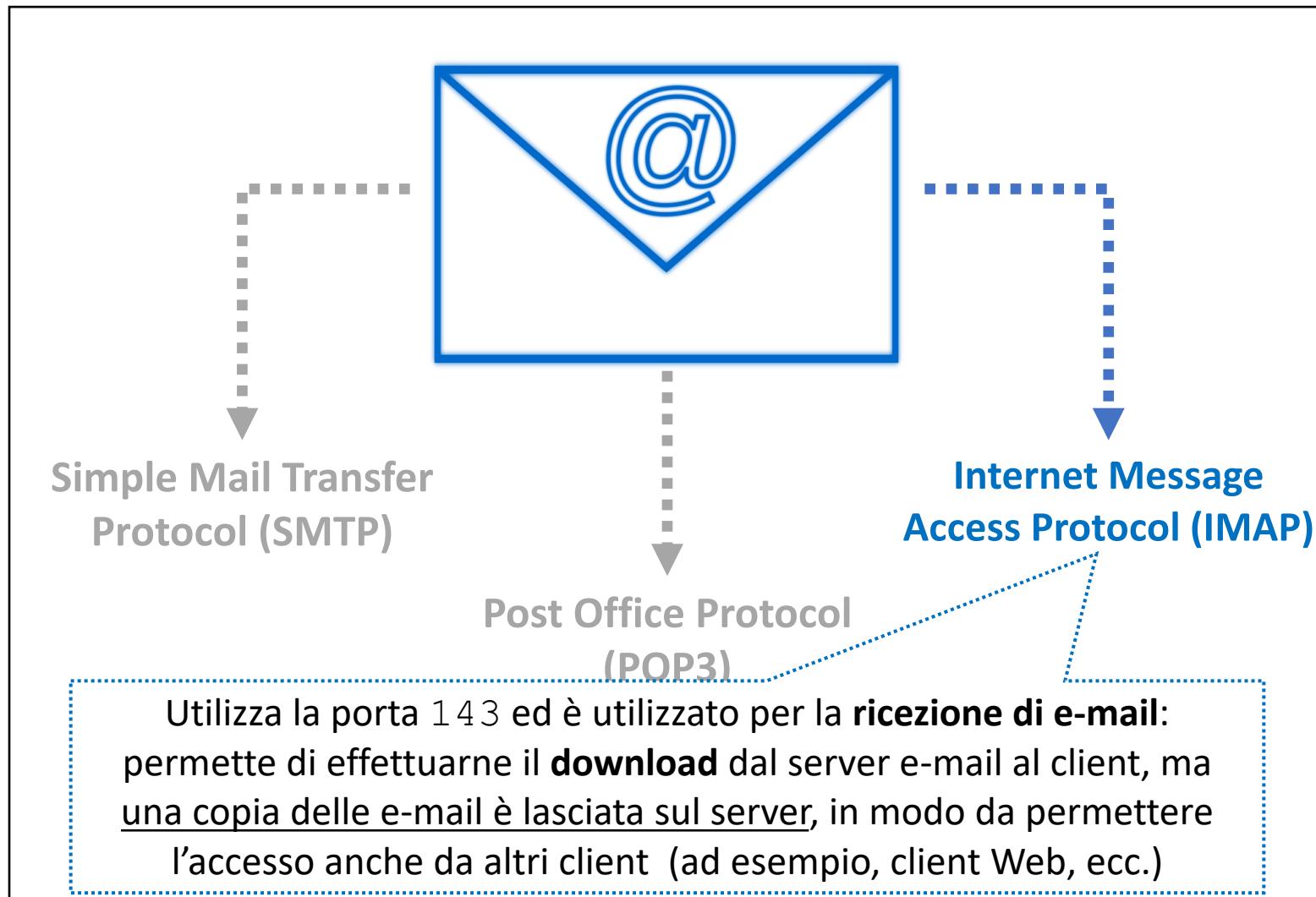
# Il tool Xplico

## Protocolli E-mail | 2/3



# Il tool Xplico

## Protocolli E-mail | 3/3



# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 1/12

- Creiamo una **nuova sessione** relativa al caso precedentemente creato, denominato CasoXplico, cliccando su «**Nuova sessione**»

Elenco delle sessioni, riferite al Caso: CasoXplico					
	Nome	Ora d'inizio	Ora di fine	Stato	Azioni
	SIP	2007-10-31 12:14:23	2007-10-31 12:14:44	DECODING COMPLETED	
	HTTPWEB	2009-12-09 17:42:17	2009-12-09 17:42:50	DECODING COMPLETED	Elimina

- Specifichiamo un **nome** per la sessione appena creata (nell'esempio, è stata denominata SMTP\_Email)

**Nuova sessione**

Nome della Sessione

# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 2/12

The screenshot shows the Xplico interface. At the top, there is a blue header bar with the text "Nuova sessione". Below it, a form has "Nome della Sessione" set to "SMTP\_Email" and a "Crea" button. A dashed blue arrow points from this form down to a second, lower window. This second window has a red header bar with the text "La sessione è stata creata". Below it, a message says "Elenco delle sessioni, riferite al Caso: CasoXplico". A table lists one session:

Nome	Ora d'inizio	Ora di fine	Stato	Azioni
SMTPEmail	---	---	EMPTY	

- La nuova sessione è stata correttamente creata ed è mostrata nella lista delle sessioni, relative al caso CasoXplico

# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 3/12

The screenshot shows the Xplico interface with a blue dashed box highlighting the "SMTPEmail" session. A large blue arrow points down from this session to the main statistics panel.

**Sessione dei dati**

Caso e Sessione	CasoXplico -> SMTPEmail
Cap. Ora inizio	---
Cap. Ora di fine	---
Stato	EMPTY
Host	---

**Pcap set**

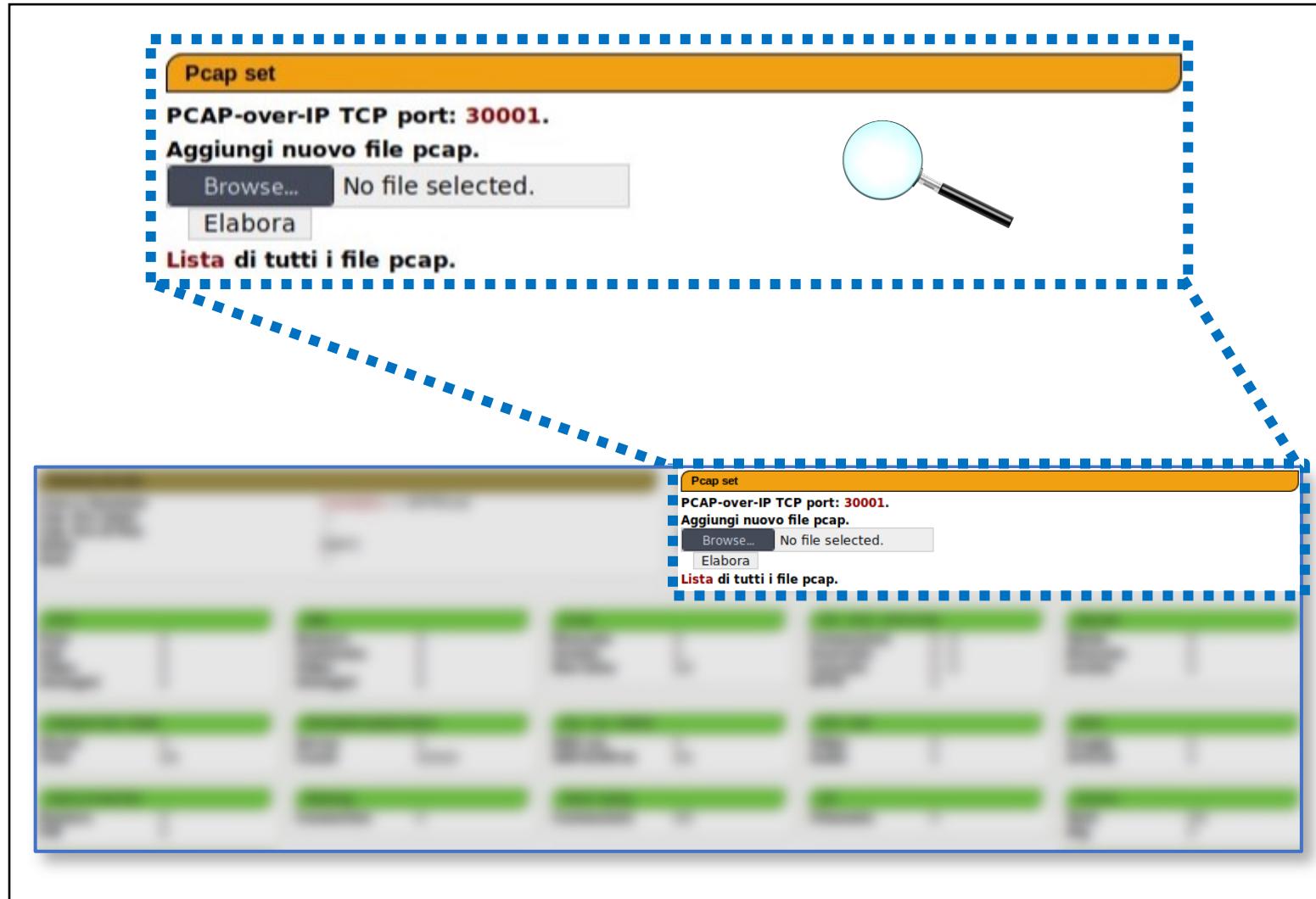
PCAP-over-IP TCP port: 30001.  
Aggiungi nuovo file pcap.  
Browse... No file selected.  
Elabora  
Lista di tutti i file pcap.

**Protocol Statistics (Summary)**

<b>HTTP</b>	<b>MMS</b>	<b>E-mail</b>	<b>FTP - TFTP - HTTP di file</b>	<b>Web Mail</b>
Post 0	Numero 0	Ricevute 0	Connessioni 0 - 0	Total 0
Get 0	Contenuto 0	Inviate 0	Scaricato 0 - 0	Ricevute 0
Video 0	Video 0	Non lette 0/0	Caricato 0 - 0	Inviate 0
Immagini 0	Immagini 0		HTTP 0	
<b>Facebook Chat / Paltalk</b>				
Utenti 0	Server 0	Dns - Arp - ICMPv6 0	RTP / VoIP 0	Nntp 0
Chat 0/0	Canali 0/0/0	DNS res 0	Video 0	Gruppi 0
<b>IRC/Paltalk Exp/Msn/Yahoo!</b>				
Numero 0	Connection 0	ARP/ICMPv6 0/0	Audio 0	Articoli 0
Pdf 0				
<b>Feed &amp; Printed files</b>				
Numero 0		Telnet / Syslog 0/0	SIP 0	Sconosc. 0/0
Pdf 0		Connessioni 0/0	Chiamate 0	Testi 0
				Dig 0

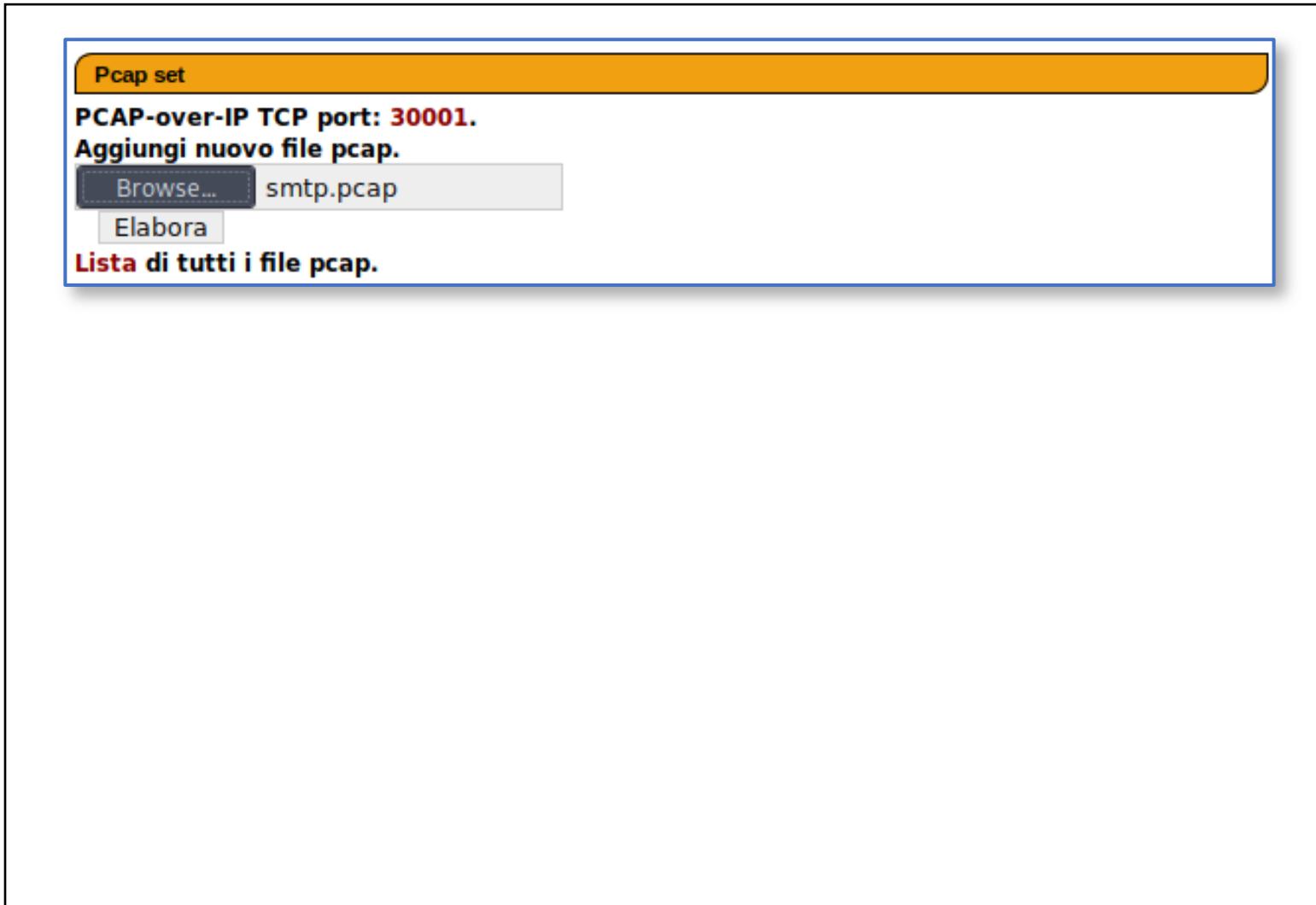
# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 3/12



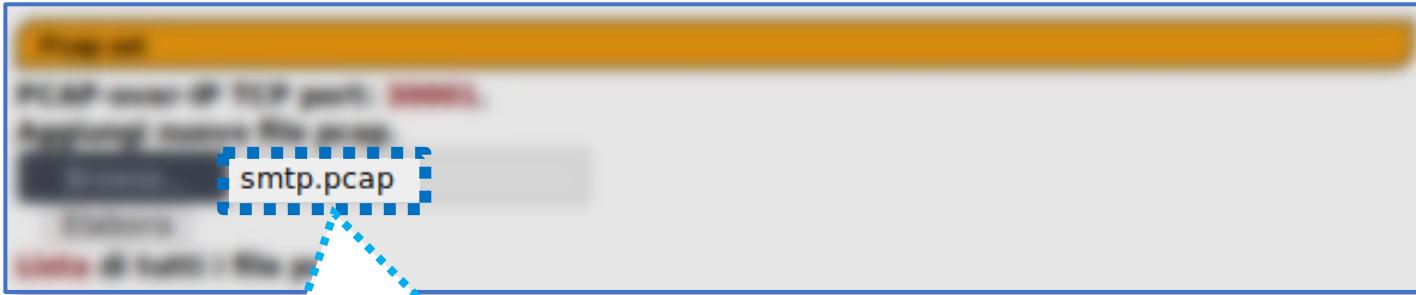
# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 4/12



# Il tool Xplico

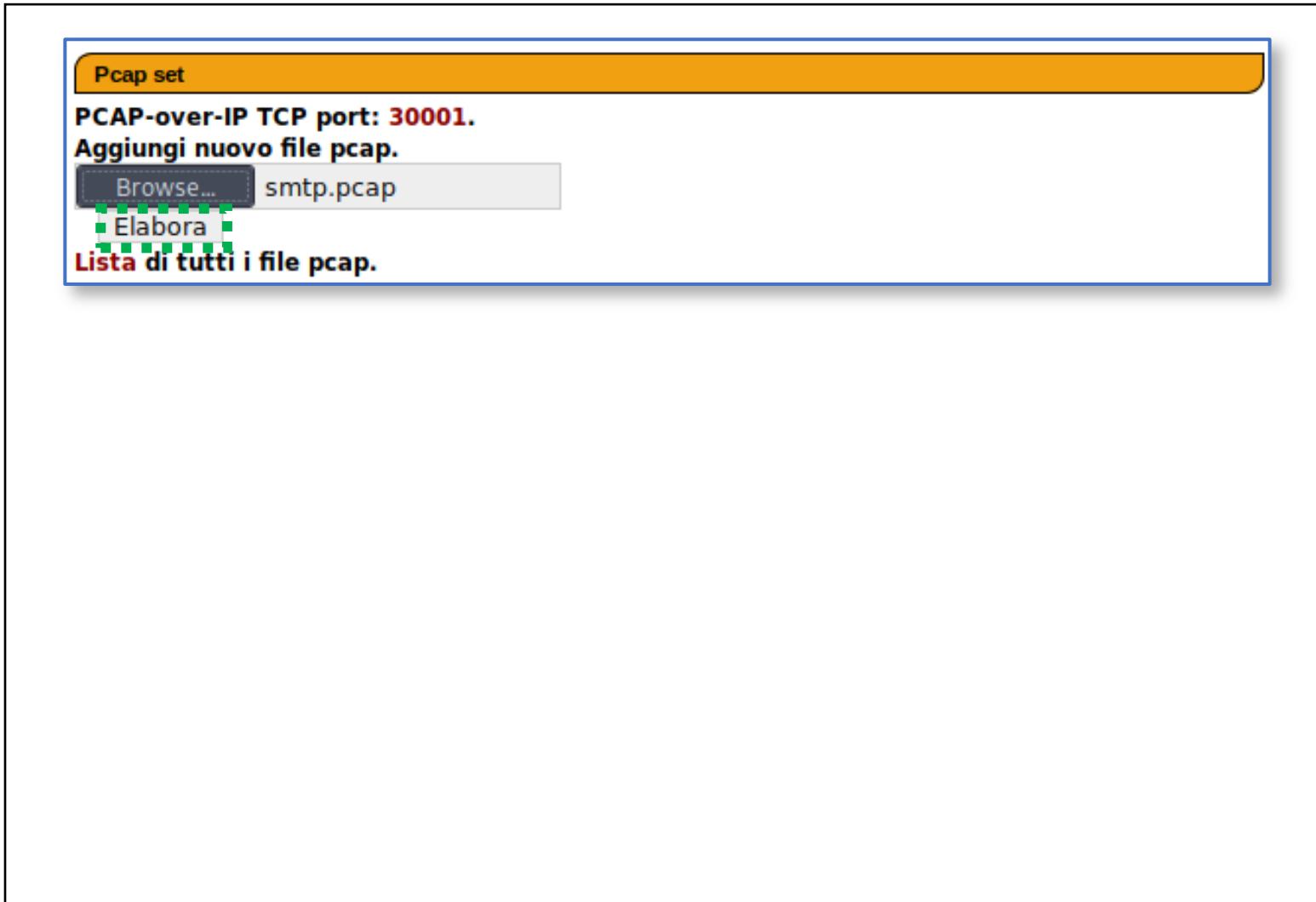
## Esempio di Utilizzo 3 | E-mail | 4/12



In questo esempio, utilizzeremo il file, denominato smtp.pcap

# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 5/12



# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 5/12

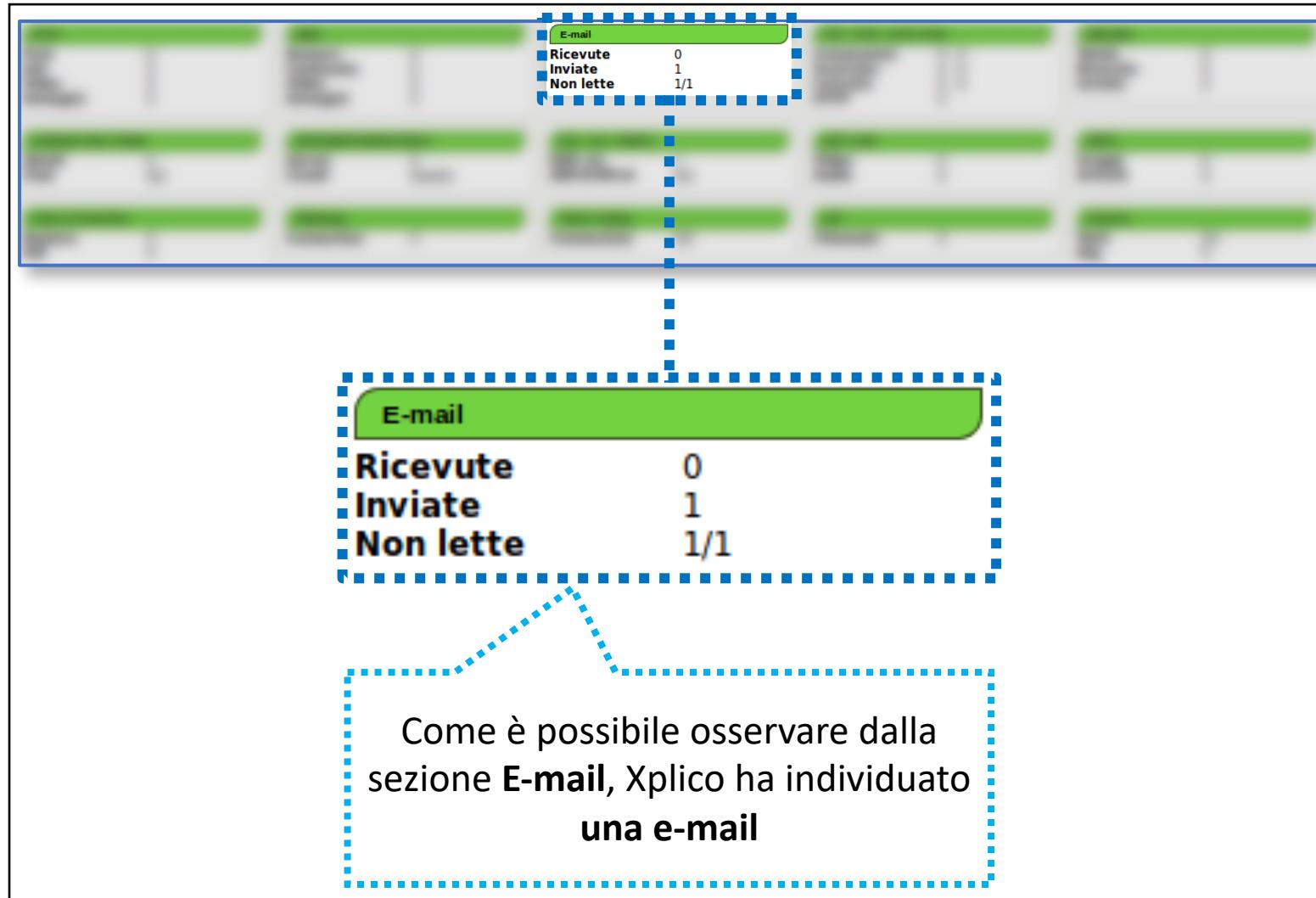
Pcap set  
PCAP-over-IP TCP port: 30001.  
Aggiungi nuovo file pcap.  
Browse... smtp.pcap  
Elabora  
Lista di tutti i file pcap.

Sessione Riepilogativa

HTTP	MMS	E-mail	FTP - TFTP - HTTP di file	Web Mail
Post 0 Get 0 Video 0 Immagini 0	Numero 0 Contenuto 0 Video 0 Immagini 0	Ricevute 0 Inviate 1 Non lette 1/1	Connessioni 0 - 0 Scaricato 0 - 0 Caricato 0 - 0 HTTP 0	Totale 0 Ricevute 0 Inviate 0
Facebook Chat / Paltalk	IRC/Paltalk Exp/Msn/Yahoo!	Dns - Arp - ICMPv6	RTP / VoIP	NNTP
Utenti Chat 0/0	Server Canali 0/0/0	DNS res 1 ARP/ICMPv6 0/0	Video 0 Audio 0	Gruppi Articoli 0
Feed & Printed files	WhatsApp	Telnet / Syslog	SIP	Sconosciuti
Numero 0 Pdf 0	Connection 0	Connessioni 0/0	Chiamate 0	Testi Dig 0/1

# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 6/12



The screenshot shows the Xplico interface with a focus on the 'E-mail' section. The main pane displays a list of files or messages, with one item highlighted. A callout box provides a detailed view of the 'E-mail' statistics:

E-mail	
Ricevute	0
Inviate	1
Non lette	1/1

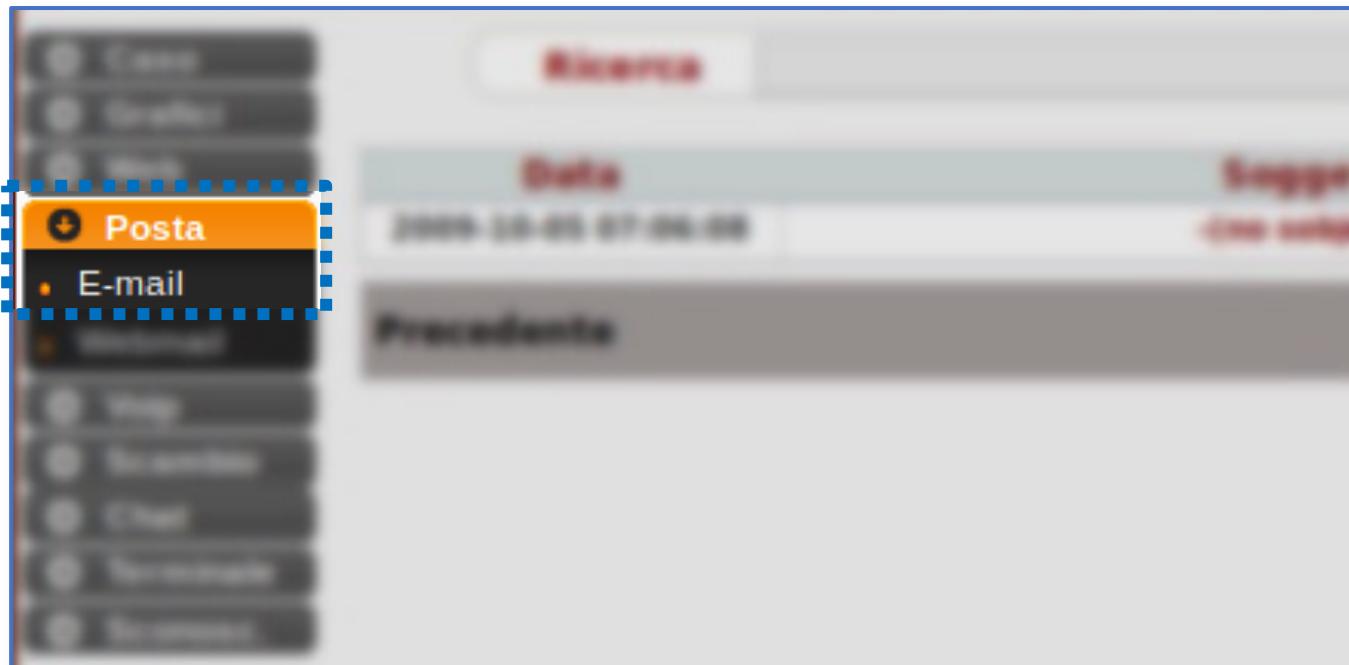
A callout box at the bottom right contains the following text:

Come è possibile osservare dalla sezione **E-mail**, Xplico ha individuato una e-mail

# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 7/12

- Per ottenere ulteriori informazioni in merito alla e-mail non letta, individuata da Xplico, è possibile cliccare sul link **E-mail**, dal relativo menu a sinistra (sezione **Posta**)



# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 8/12

- *Schermata E-mail della sezione Posta*

Data	Soggetto	Mittente	Ricevitore	Dimensio	Rilevanza (?)
2009-10-05 07:06:08	-(no subject)-	gurpartap@patriots.in	raj_deol2002in@yahoo.co.in	14544	
Precedente		1 of 1			Prossimo

# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 8/12

- *Schermata E-mail della sezione Posta*

Data	Soggetto	Mittente	Ricevitore	Dimensio	Rilevanza (?)
2009-10-05 07:06:08	-(no subject)-	gurpartap@patriots.in	raj_deol2002in@yahoo.co.in	14544	
Precedente		1 of 1			Prossimo

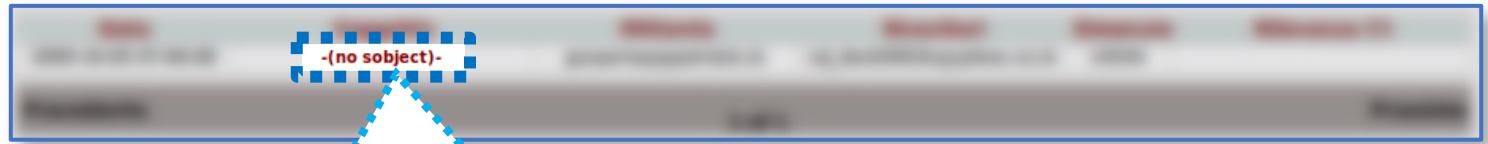
### OSSERVAZIONE IMPORTANTE

È stata individuata **una e-mail** (dove non è stato specificato l'oggetto), inviata da gurpartap@patriots.in (colonna **Mittente**) a raj\_deol2002in@yahoo.co.in (colonna **Ricevitore**), avente dimensione, in termini di byte, pari a 14544

# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 9/12

- *Schermata E-mail della sezione Posta*

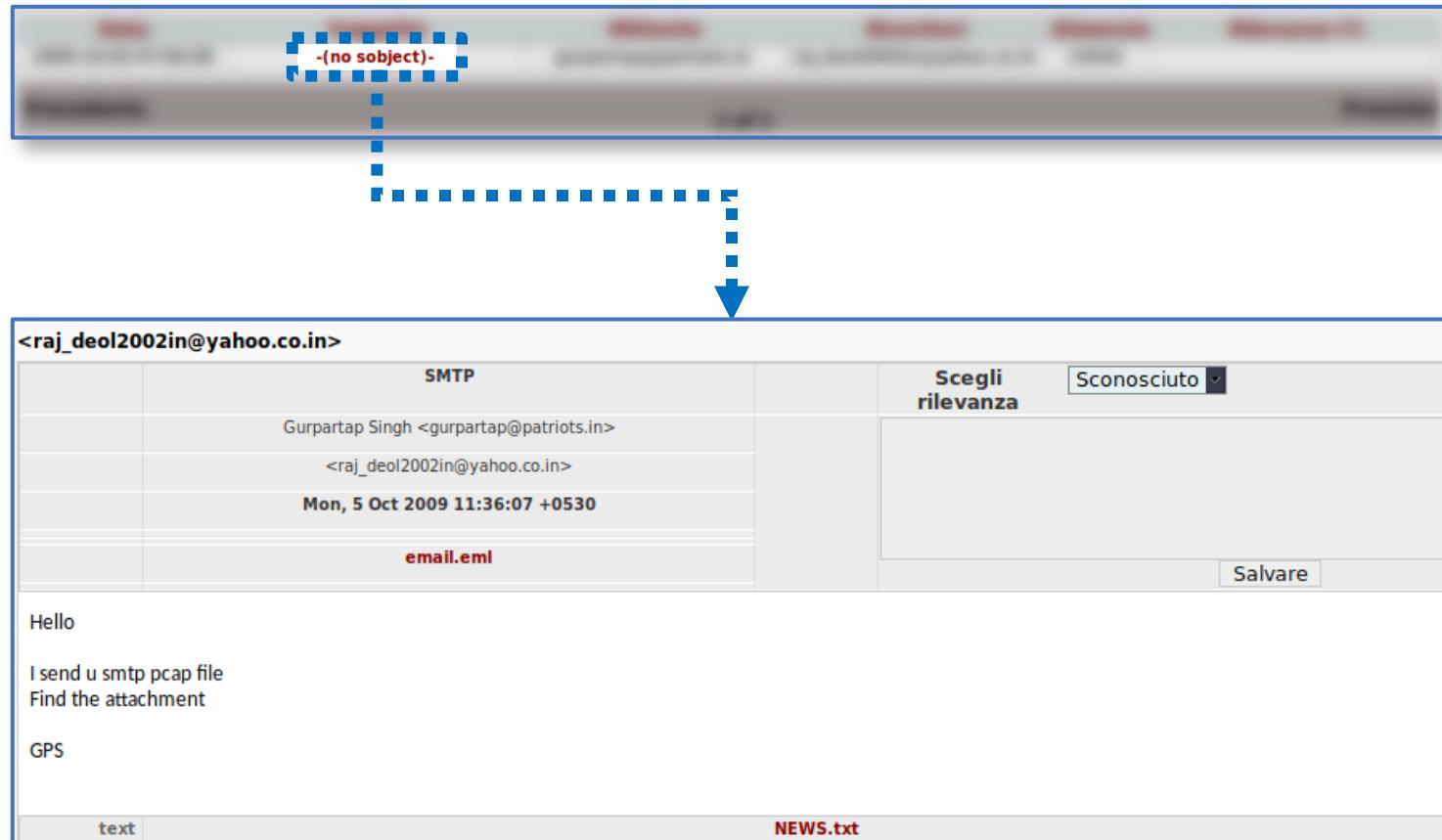


Cliccando sull'oggetto dell'email (denominato – (no subject) –), evidenziato in **rosso scuro**, è possibile visionare il contenuto della e-mail

# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 10/12

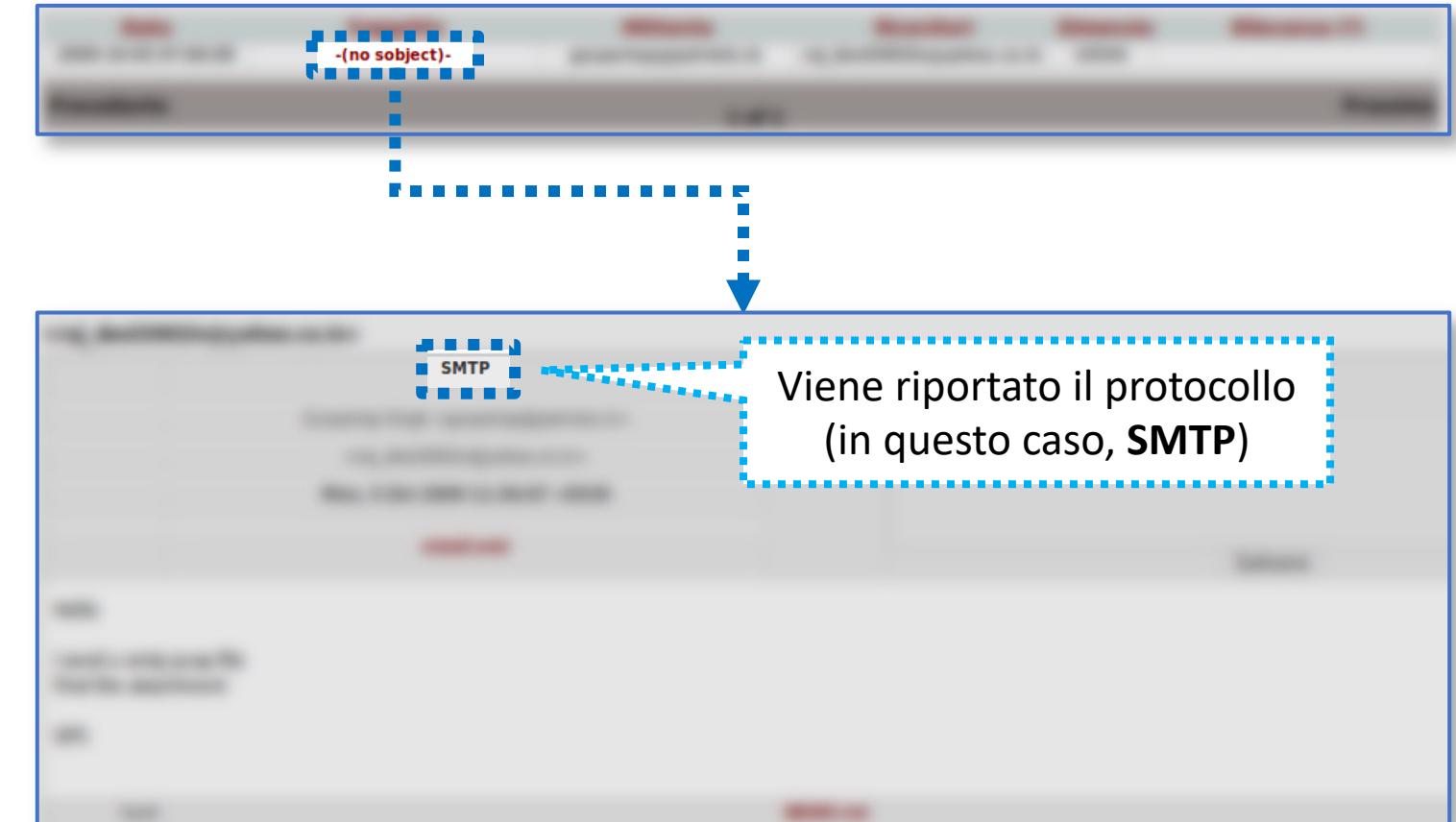
- *Schermata E-mail della sezione Posta*



# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 10/12

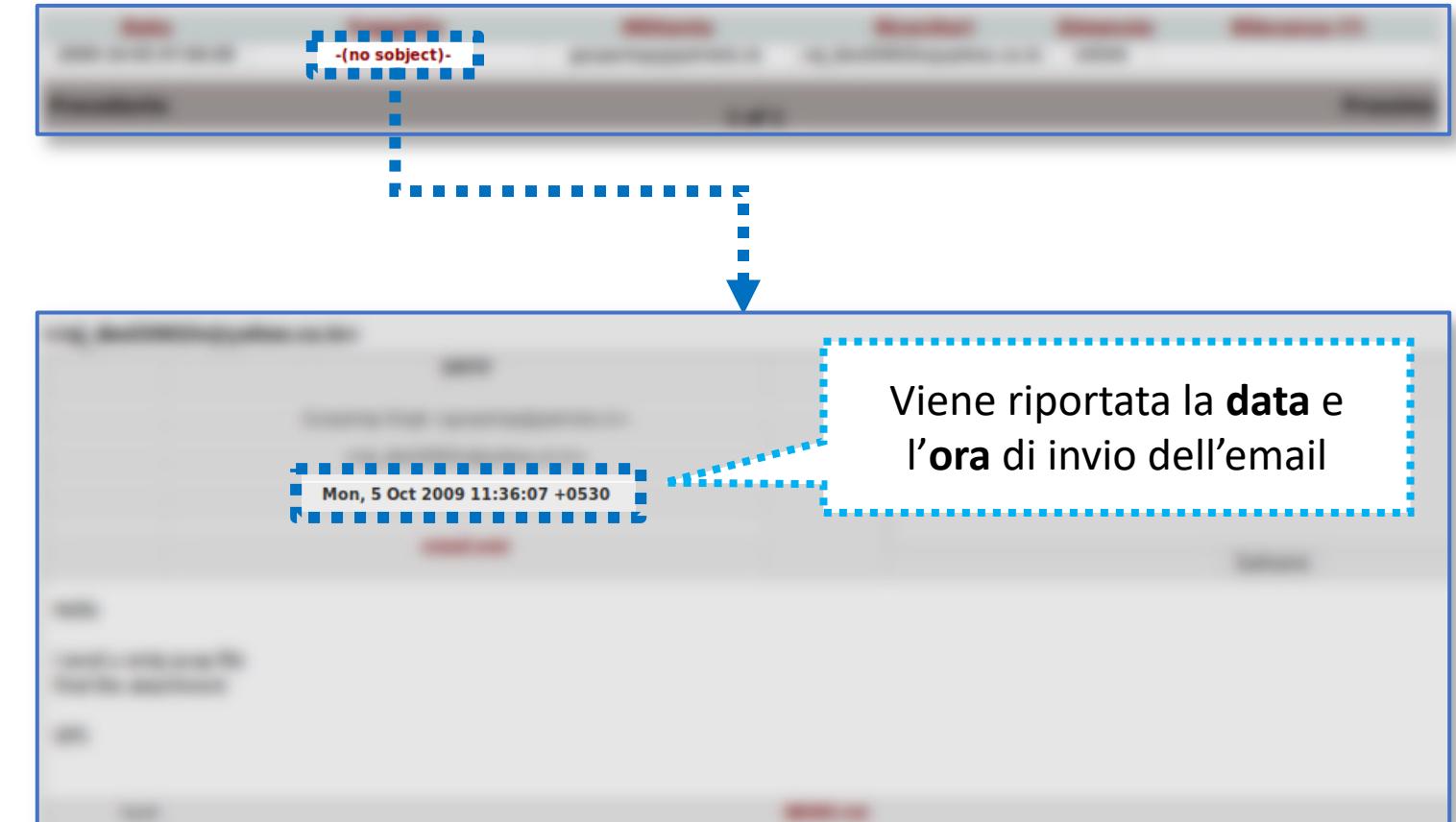
- *Schermata E-mail della sezione Posta*



# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 10/12

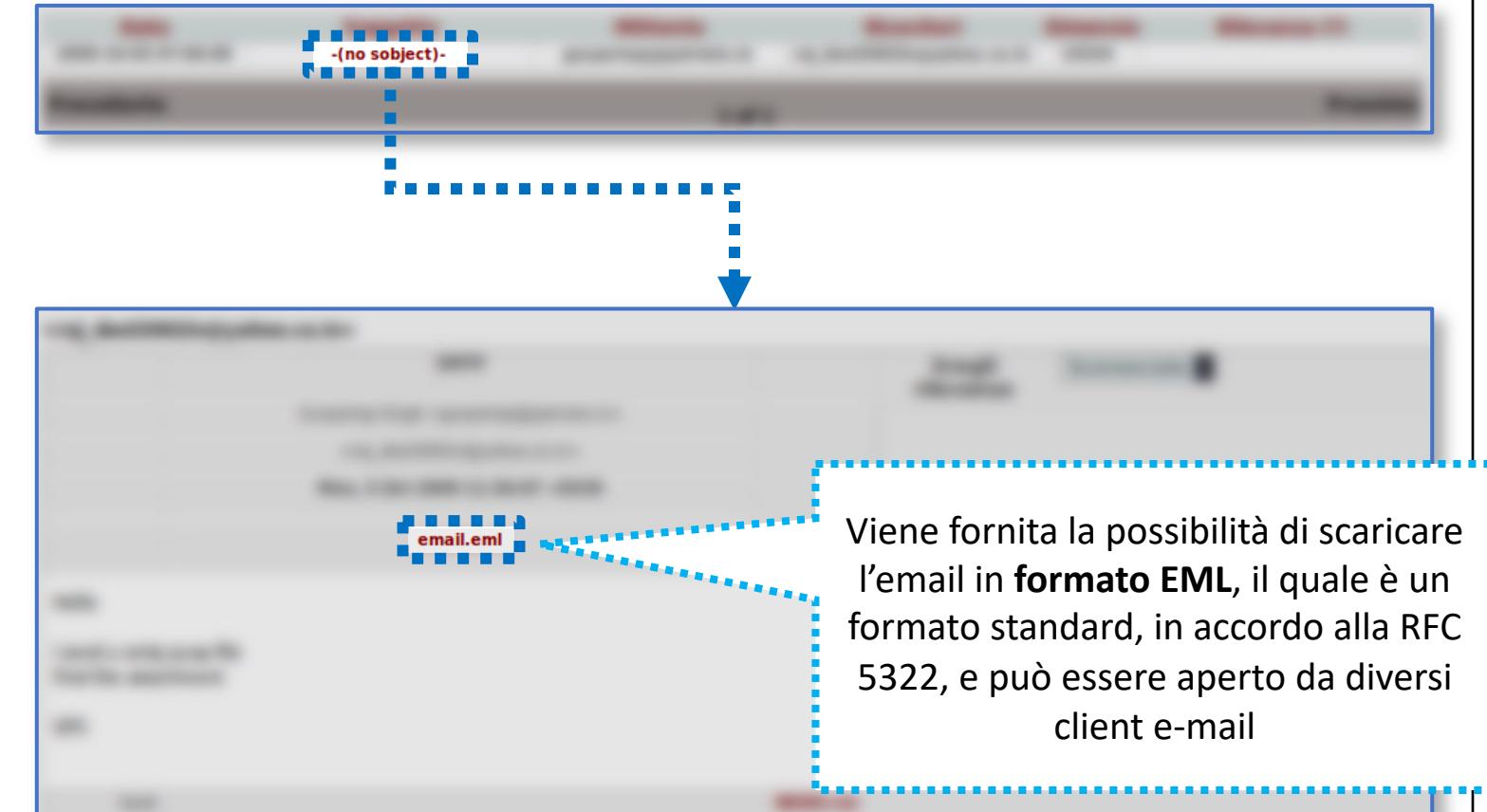
- *Schermata E-mail della sezione Posta*



# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 10/12

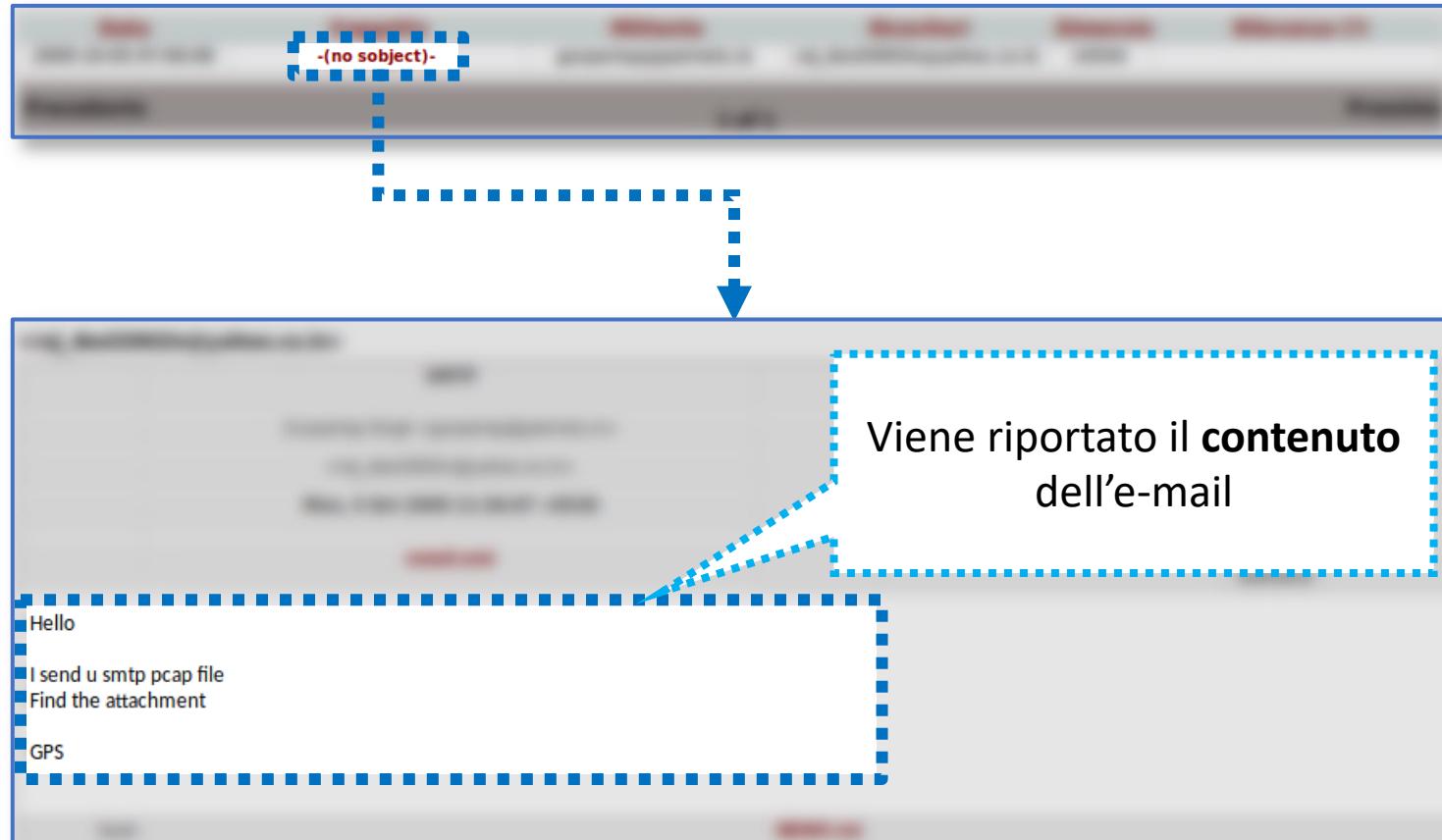
- *Schermata E-mail della sezione Posta*



# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 11/12

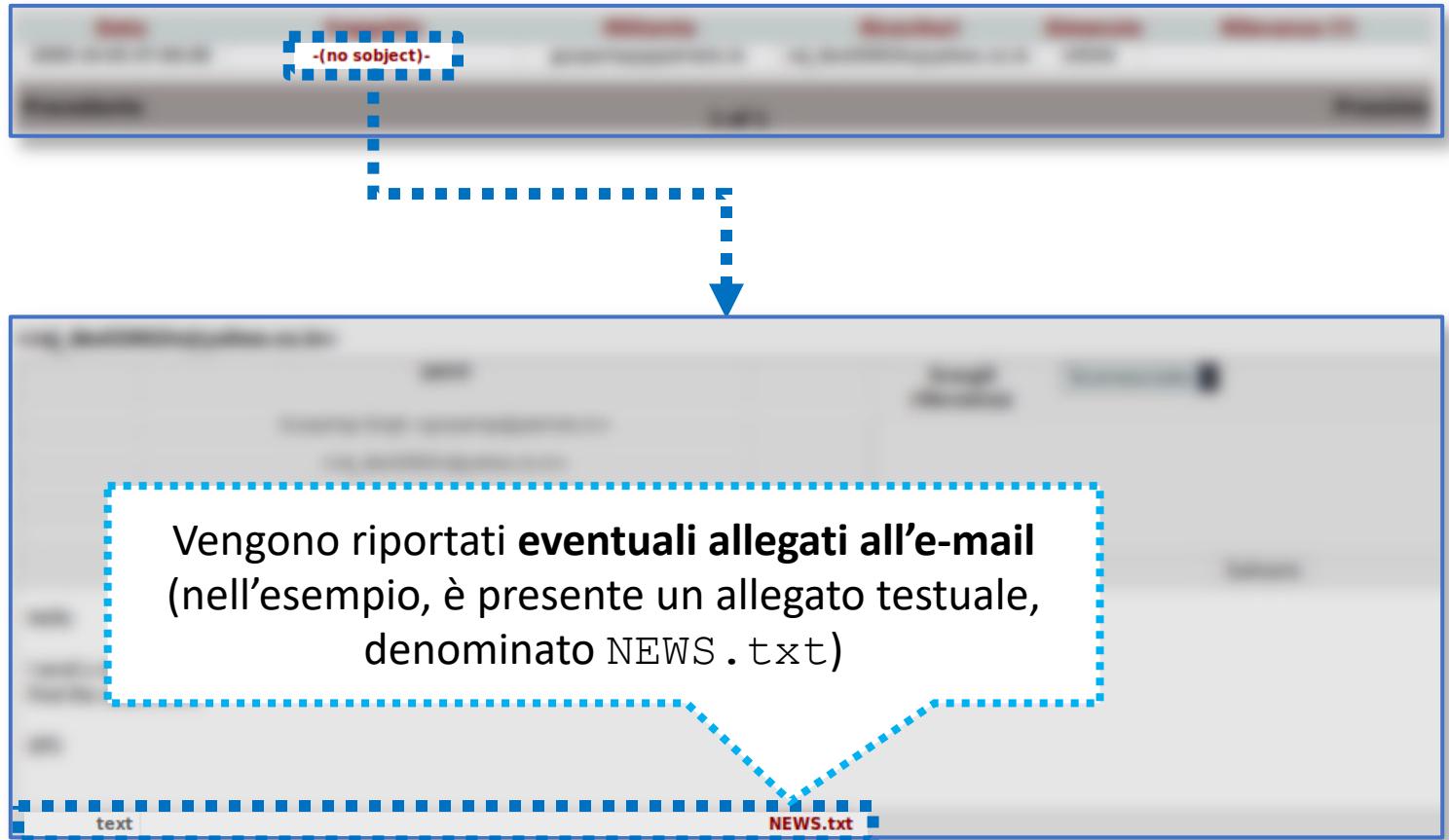
- *Schermata E-mail della sezione Posta*



# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 11/12

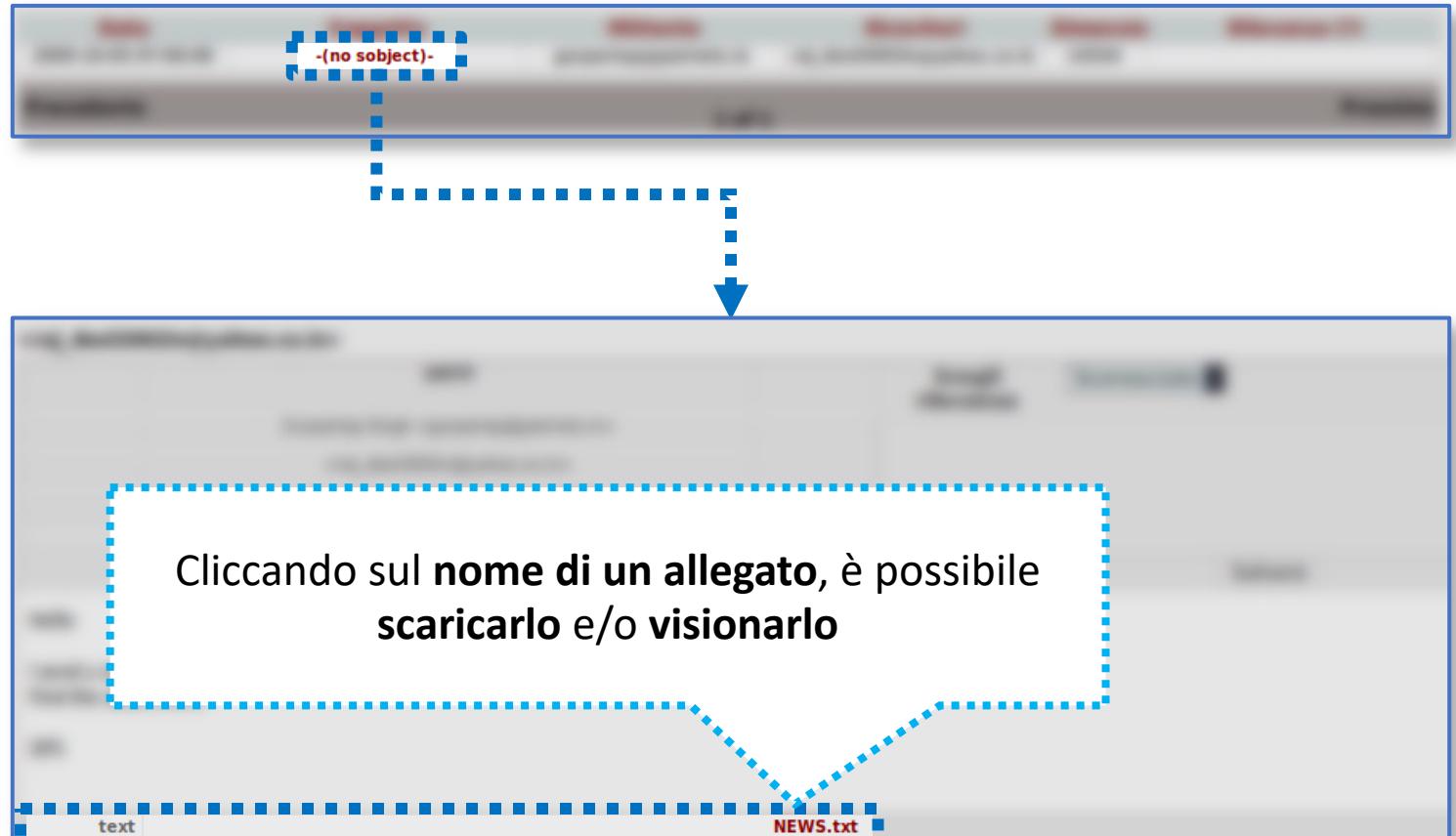
- *Schermata E-mail della sezione Posta*



# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 11/12

- *Schermata E-mail della sezione Posta*



# Il tool Xplico

## Esempio di Utilizzo 3 | E-mail | 12/12

### Contenuto (Parziale) dell'allegato NEWS.txt

```
Version 4.9.9.1
* Many bug fixes
* Improved editor

Version 4.9.9.0
* Support for latest Mingw compiler system builds
* Bug fixes

Version 4.9.8.9
* New code tooltip display
* Improved Indent/Unindent and Remove Comment
* Improved automatic indent
* Added support for the "interface" keyword
* WebUpdate should now report installation problems from PackMan
* New splash screen and association icons
* Improved installer
* Many bug fixes

Version 4.9.8.7
* Added support for GCC > 3.2
* Debug variables are now resent during next debug session
* Watched Variables not in correct context are now kept and updated when it is needed
* Added new compiler/linker options:
  - Strip executable
  - Generate instructions for a specific machine (i386, i486, i586, i686, pentium, pentium-mmx, pentiumpro, pentium2, pentium3, pentium4, k6, k6-2, k6-3, athlon, athlon-tbird, athlon-4, athlon-xp, athlon-mp, winchip-c6, winchip2, k8, c3 and c3-2)
  - Enable use of processor specific built-in functions (mmmx, sse, sse2, pni, 3dnow)
* "Default" button in Compiler Options is back
* Error messages parsing improved
* Bug fixes
```

NEWS.txt

# Acquisizione Traffico di Rete | Wireshark

# Acquisizione Traffico di Rete con Wireshark

## Caratteristiche di Wireshark | 1/2

- Wireshark è uno *sniffer* (letteralmente, *annusatore*) di traffico di rete
  - Open-Source e con una GUI user-friendly
  - Disponibile per **diversi sistemi operativi**:
    - Microsoft Windows, Apple macOS/OS X, Linux (già installato su Kali Linux e Parrot Linux)
    - È in grado di catturare il traffico di rete, in **modalità promiscua**
    - Permette anche di effettuare alcune analisi sul traffico di rete acquisito
  - Ulteriori caratteristiche e dettagli:
    - <https://www.wireshark.org>

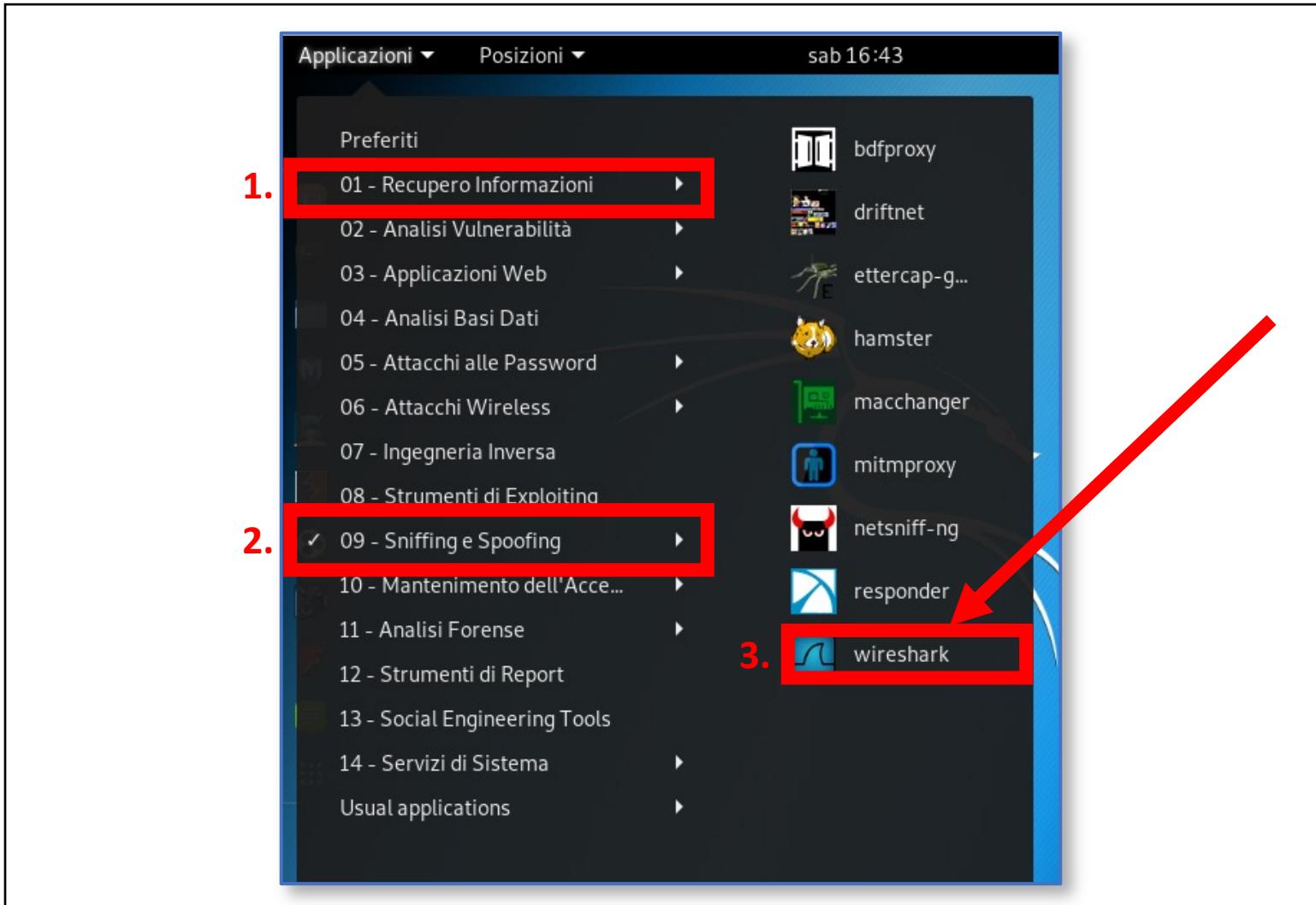
# Acquisizione Traffico di Rete con Wireshark

## Caratteristiche di Wireshark | 1/2

- Wireshark è uno *sniffer* (letteralmente, *annusatore*) di traffico di rete
  - Open-Source e con una GUI user-friendly
  - Disponibile per diversi sistemi operativi:
    - Microsoft Windows, Apple macOS/OS X, Linux (già installato su Kali Linux e Parrot Linux)
  - È in grado di catturare il traffico di rete, in **modalità promiscua**
  - Permette anche di effettuare alcune analisi sul traffico acquisito
- Nella **modalità promiscua**, tutto il traffico osservato, da una interfaccia, viene passato alla CPU (si tratta di una modalità di controllo) ed è quindi possibile memorizzarlo

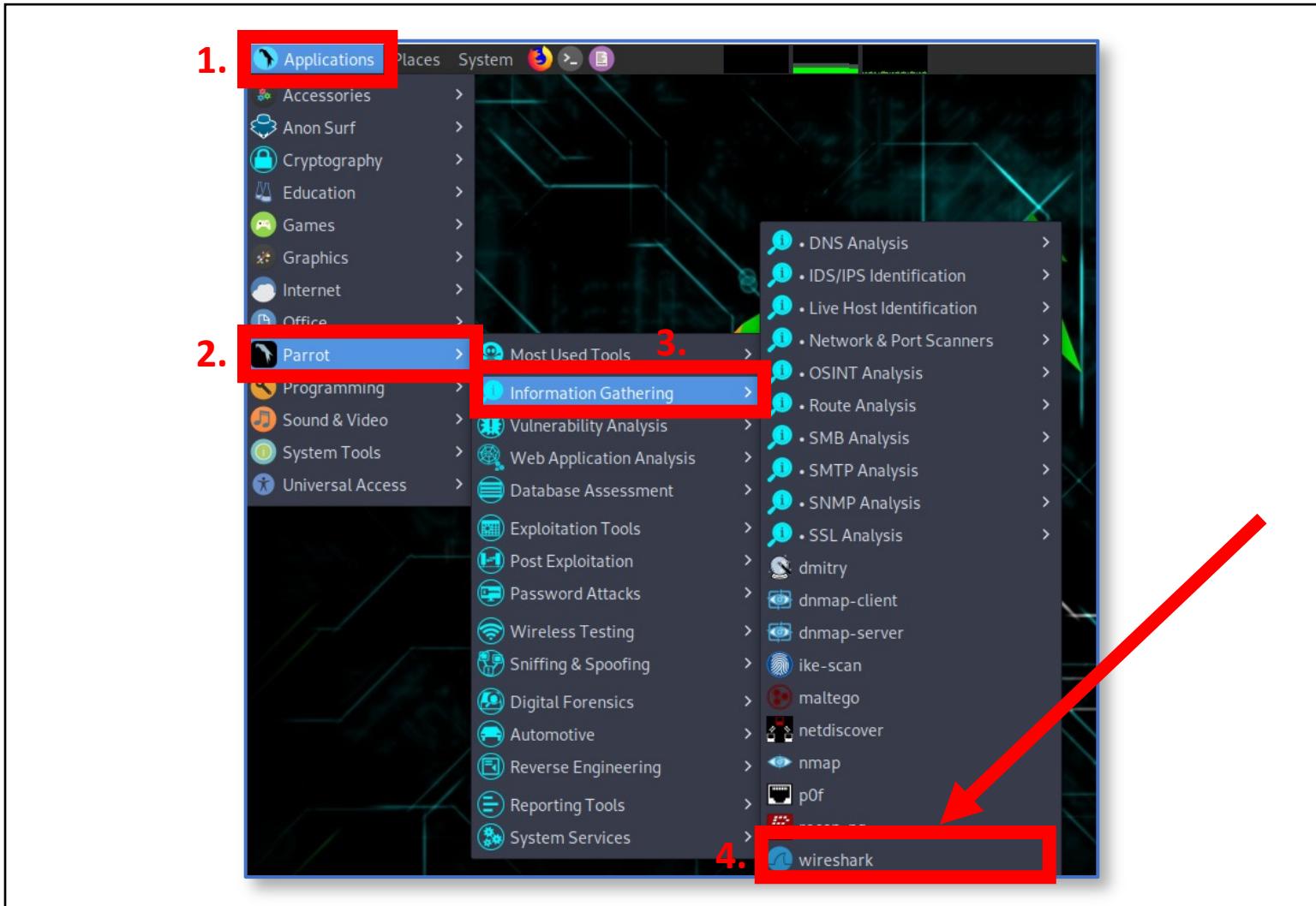
# Acquisizione Traffico di Rete con Wireshark

## Avvio del tool | Kali Linux | 1/2



# Acquisizione Traffico di Rete con Wireshark

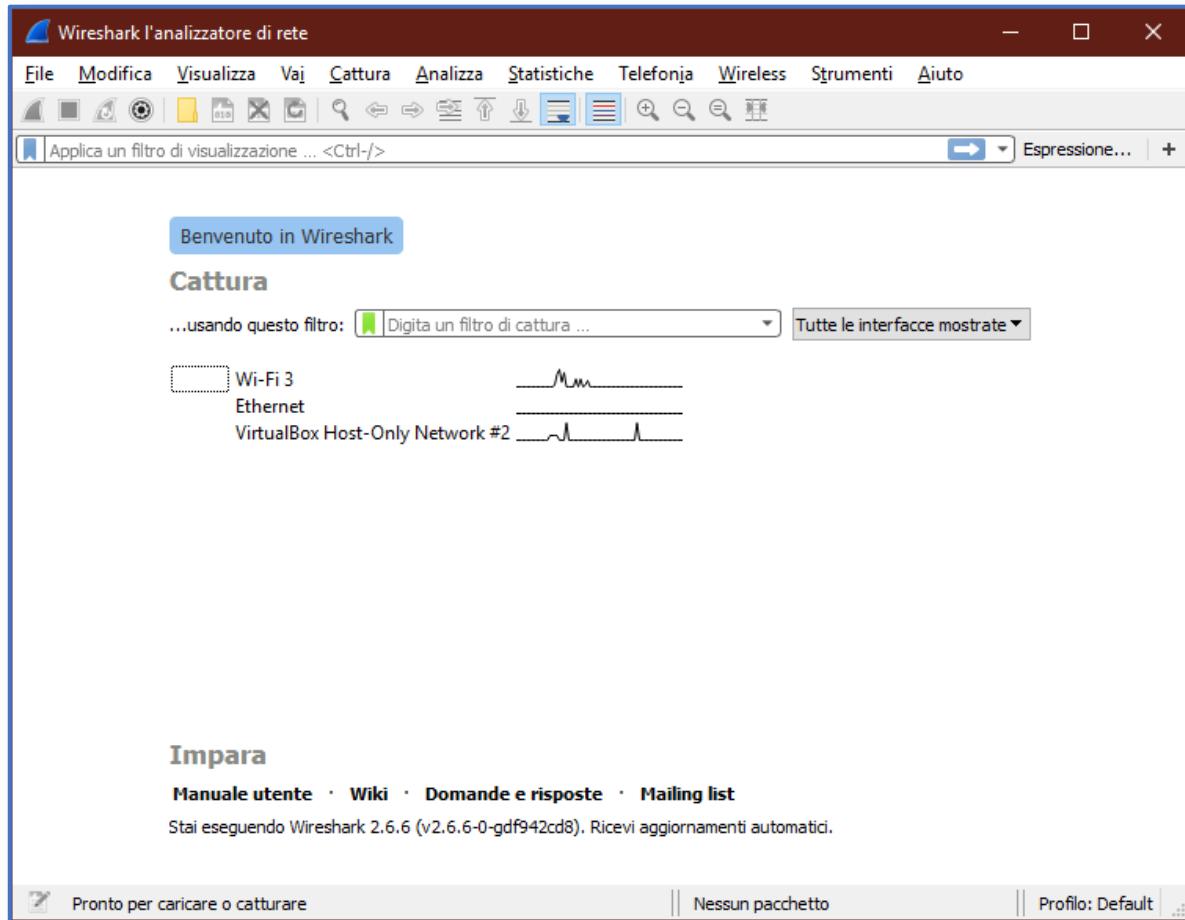
## Avvio del tool | Parrot Linux | 2/2



# Acquisizione Traffico di Rete con Wireshark

## Interfaccia Utente | 1/9

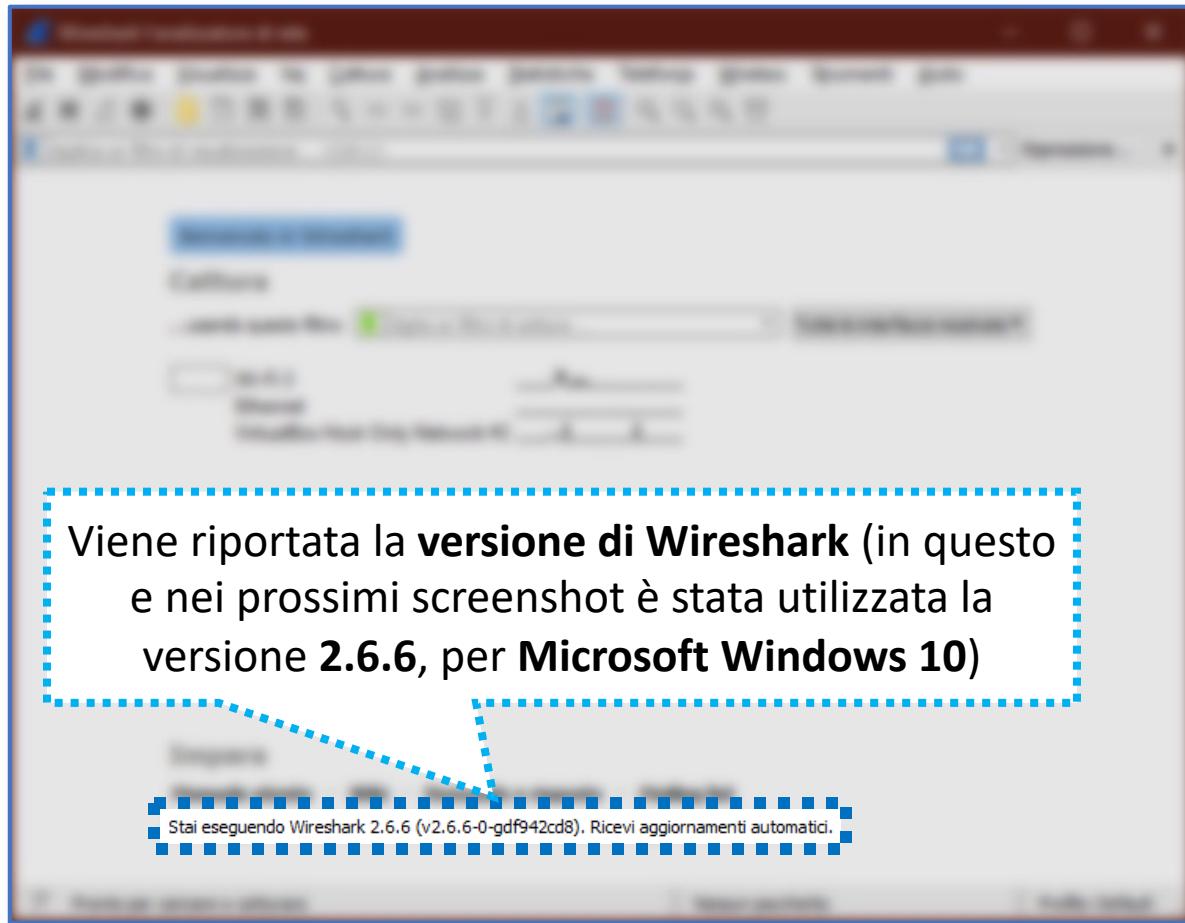
- *Schermata Iniziale di Wireshark*



# Acquisizione Traffico di Rete con Wireshark

## Interfaccia Utente | 1/9

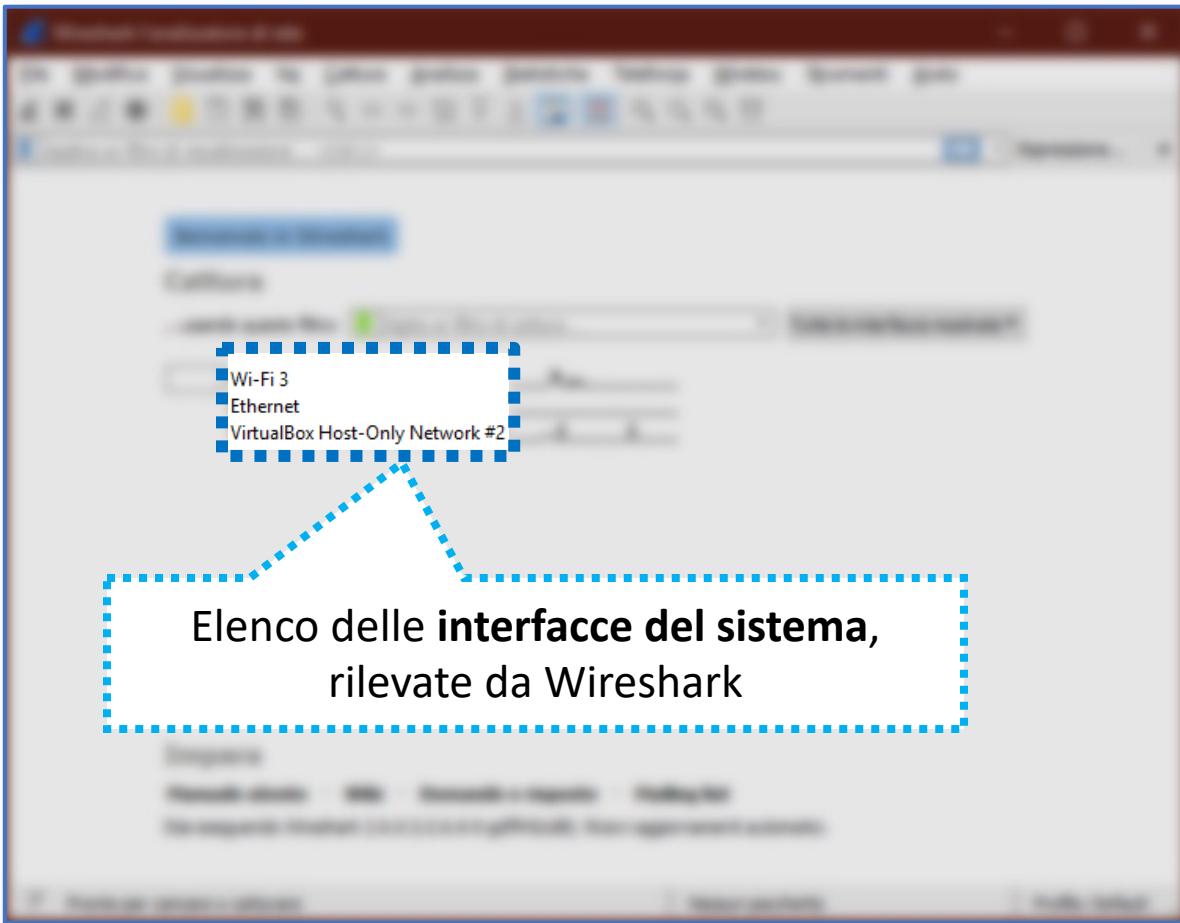
- *Schermata Iniziale di Wireshark*



# Acquisizione Traffico di Rete con Wireshark

## Interfaccia Utente | 1/9

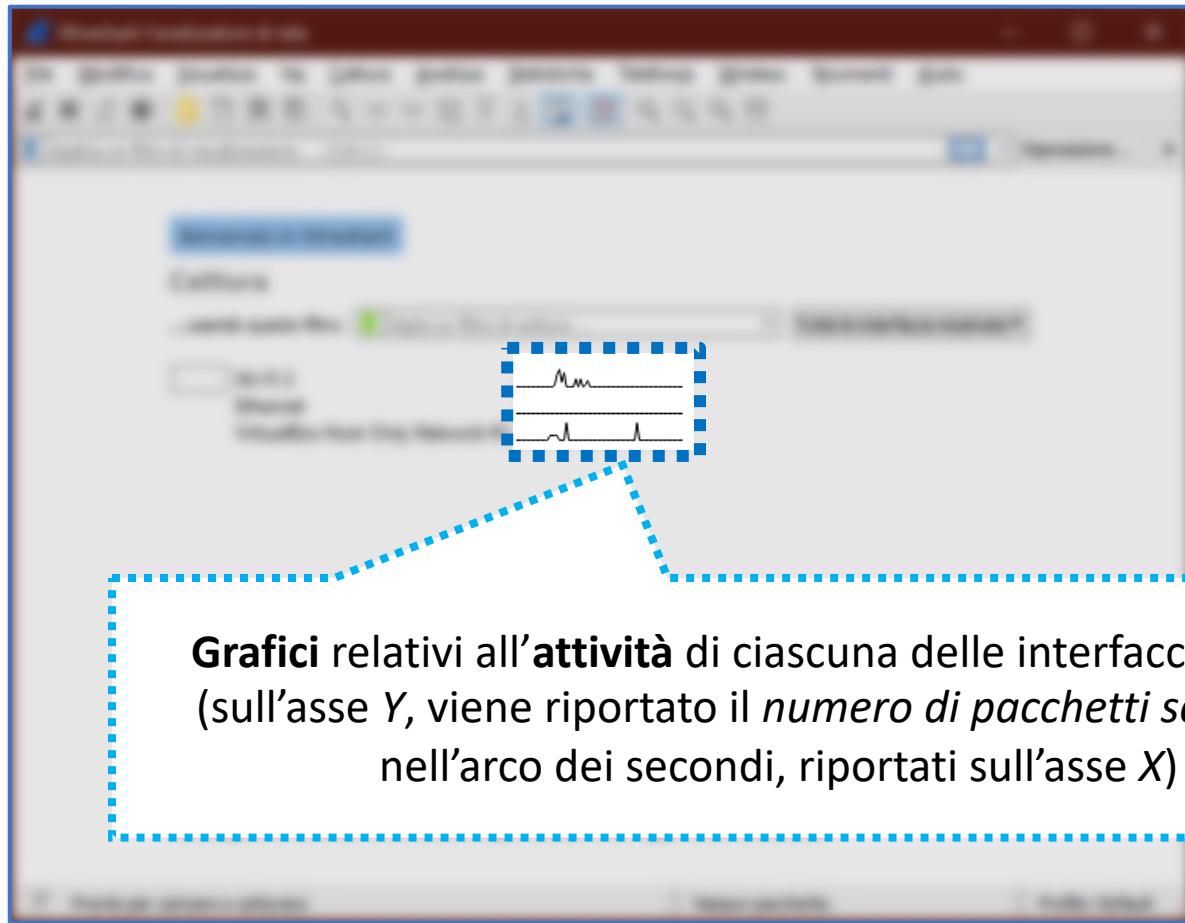
- *Schermata Iniziale di Wireshark*



# Acquisizione Traffico di Rete con Wireshark

## Interfaccia Utente | 1/9

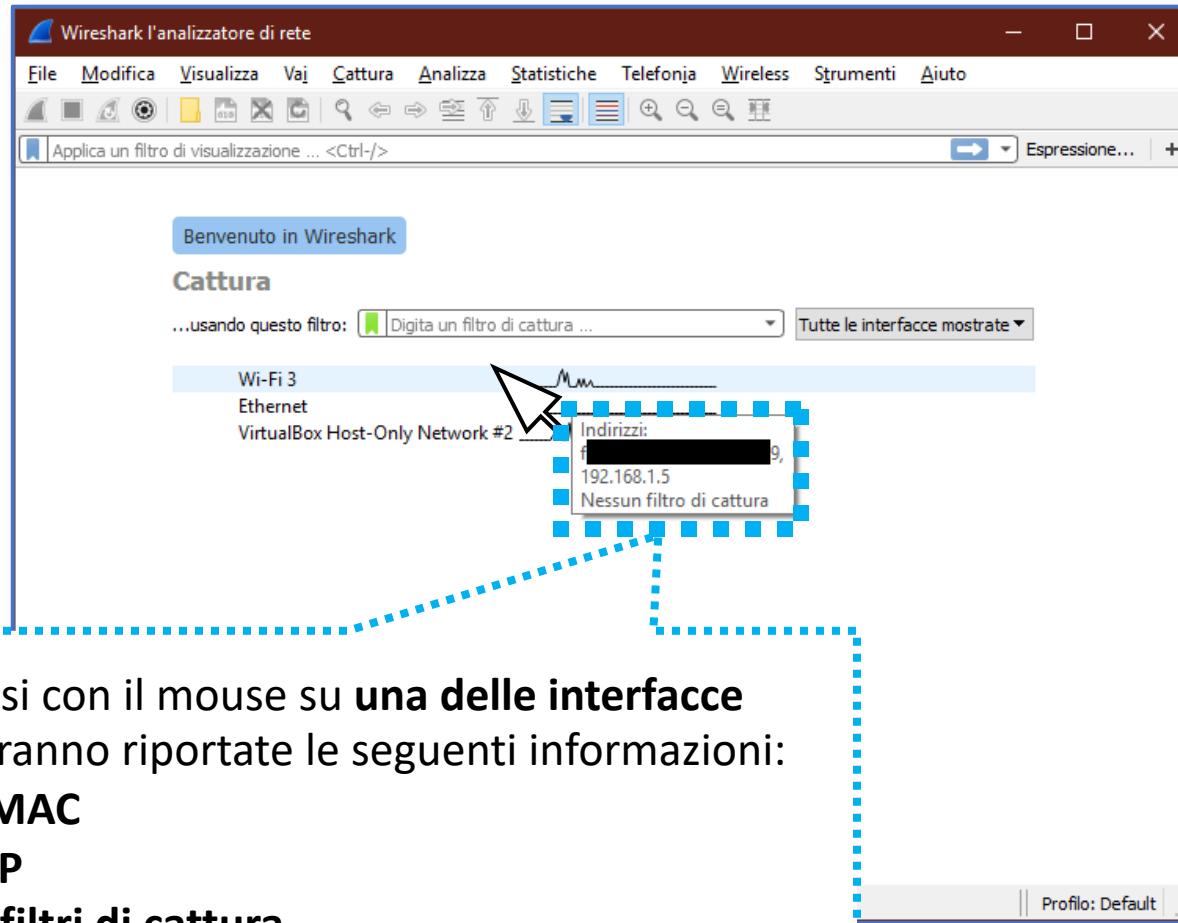
- *Schermata Iniziale di Wireshark*



# Acquisizione Traffico di Rete con Wireshark

## Interfaccia Utente | 2/9

- *Schermata Iniziale di Wireshark*



Soffermandosì con il mouse su **una delle interfacce disponibili**, verranno riportate le seguenti informazioni:

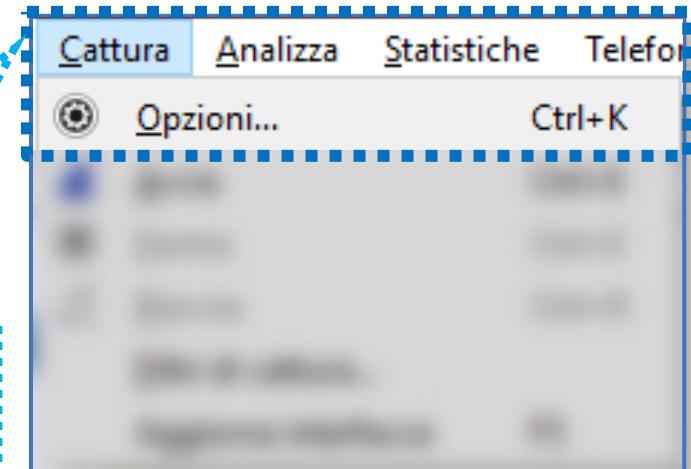
- Indirizzo MAC
- Indirizzo IP
- Eventuali filtri di cattura

# Acquisizione Traffico di Rete con Wireshark

## Interfaccia Utente | 3/9

- *Opzioni di Cattura* | 1/4

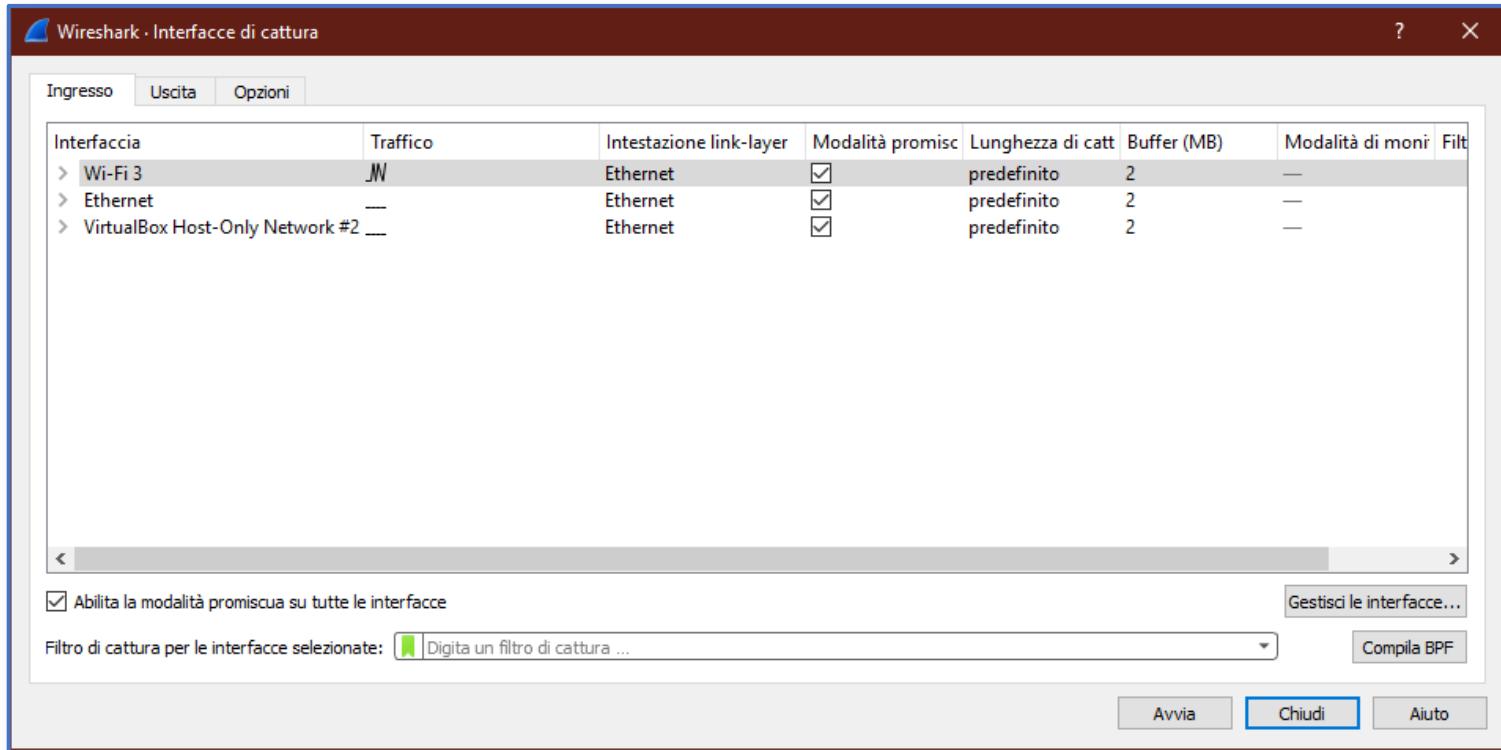
È possibile definire diverse opzioni per quanto riguarda l'acquisizione del traffico di rete, cliccando su **Opzioni...**, dal menu **Cattura**



# Acquisizione Traffico di Rete con Wireshark

## Interfaccia Utente | 4/9

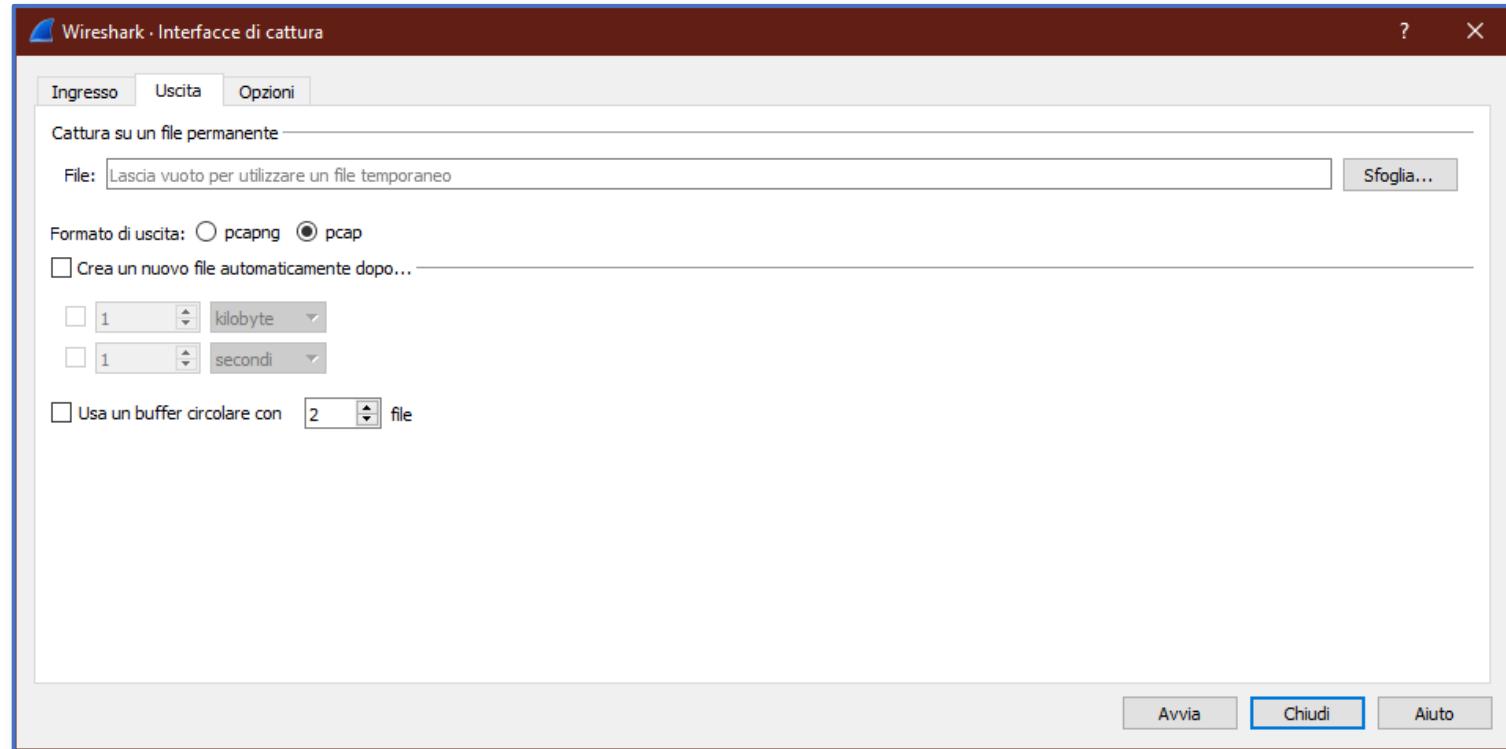
- *Opzioni di Cattura | 2/4 | Tab Ingresso*



# Acquisizione Traffico di Rete con Wireshark

## Interfaccia Utente | 5/9

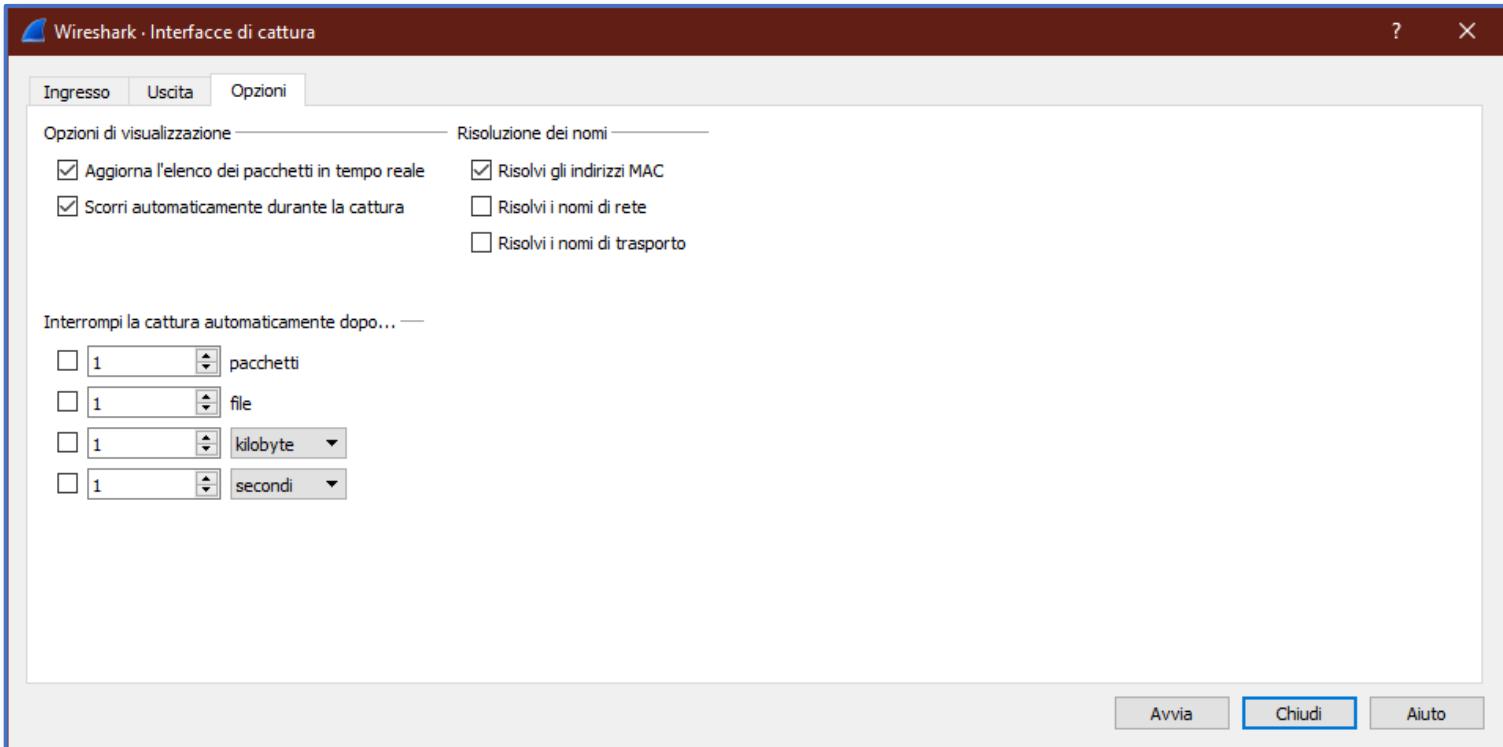
- *Opzioni di Cattura* | 3/4 | Tab Uscita



# Acquisizione Traffico di Rete con Wireshark

## Interfaccia Utente | 6/9

- *Opzioni di Cattura | 4/4 | Tab Opzioni*



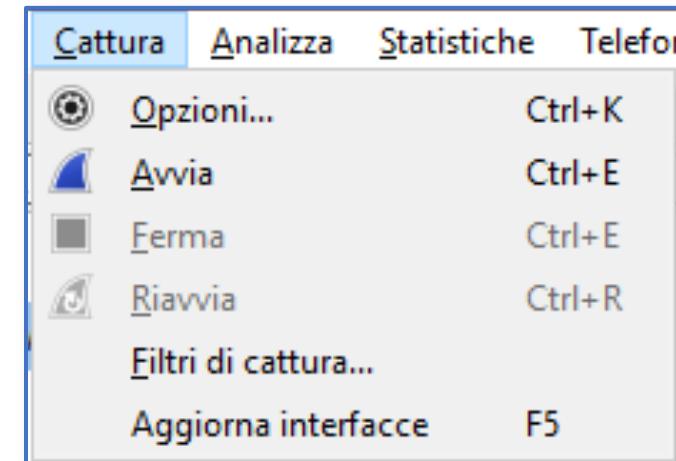
# Acquisizione Traffico di Rete con Wireshark

## Interfaccia Utente | 7/9

- *Filtri di Cattura* | 1/4

Wireshark permette la definizione di **filtre** per l'acquisizione del traffico

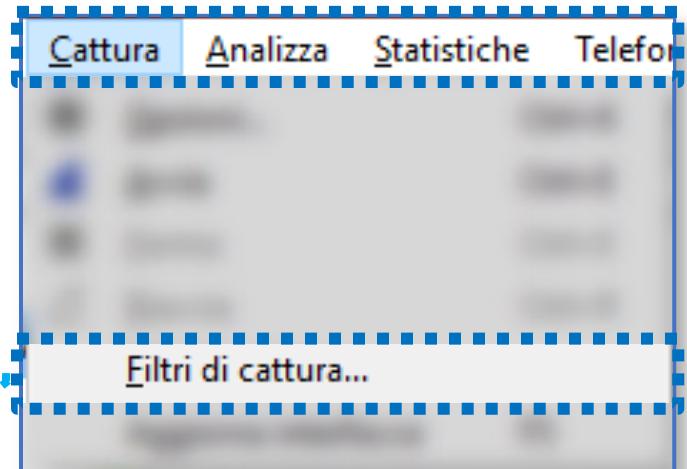
Ad esempio, acquisizione di pacchetti di determinati protocolli, da determinati host, ecc.



# Acquisizione Traffico di Rete con Wireshark

## Interfaccia Utente | 7/9

- *Filtri di Cattura | 1/4*

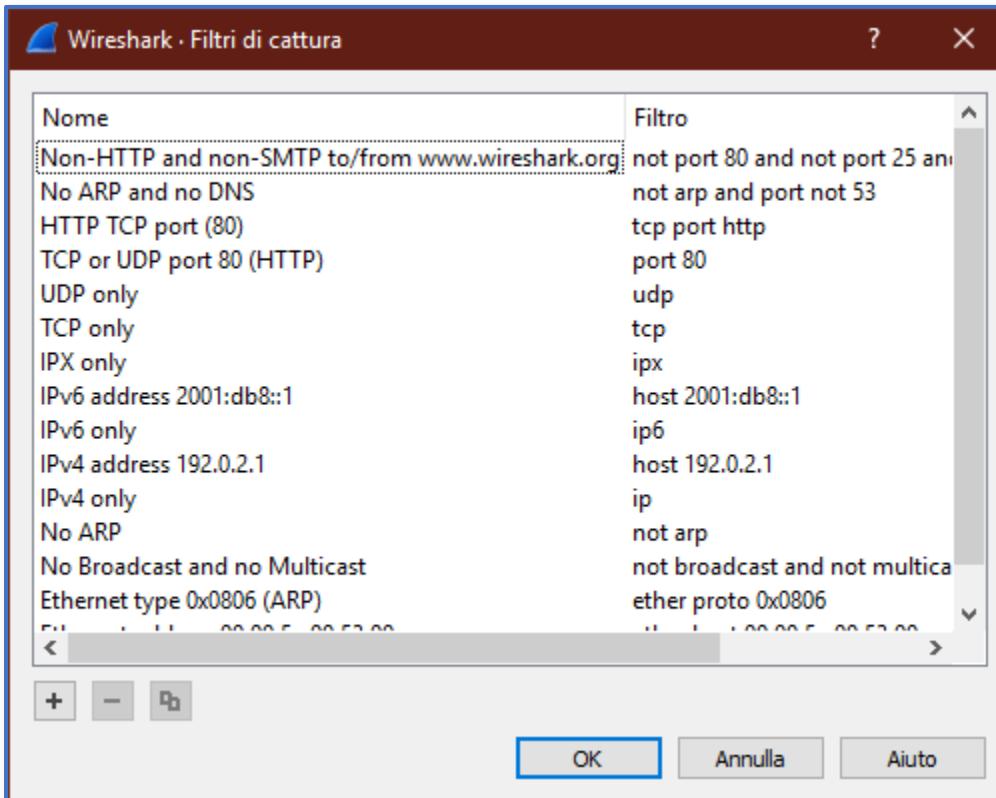


Cliccare sulla voce **Filtri di Cattura...**,  
dal menu **Cattura**, per aprire il  
relativo pannello

# Acquisizione Traffico di Rete con Wireshark

## Interfaccia Utente | 8/9

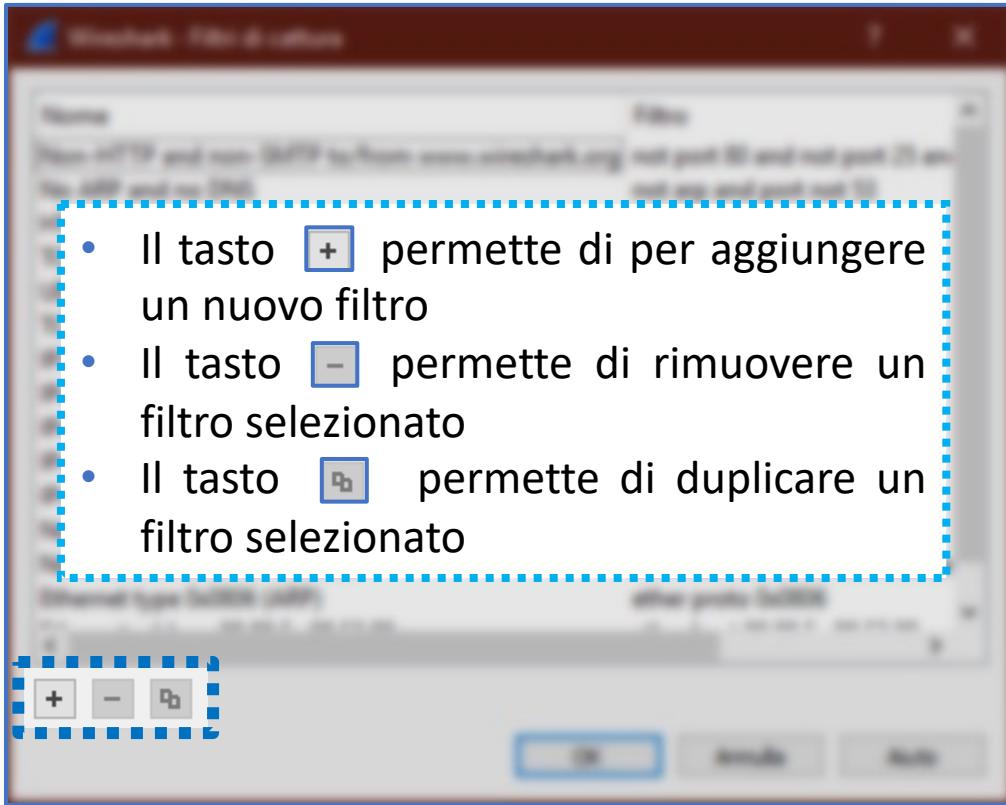
- *Filtri di Cattura* | 2/4



# Acquisizione Traffico di Rete con Wireshark

## Interfaccia Utente | 8/9

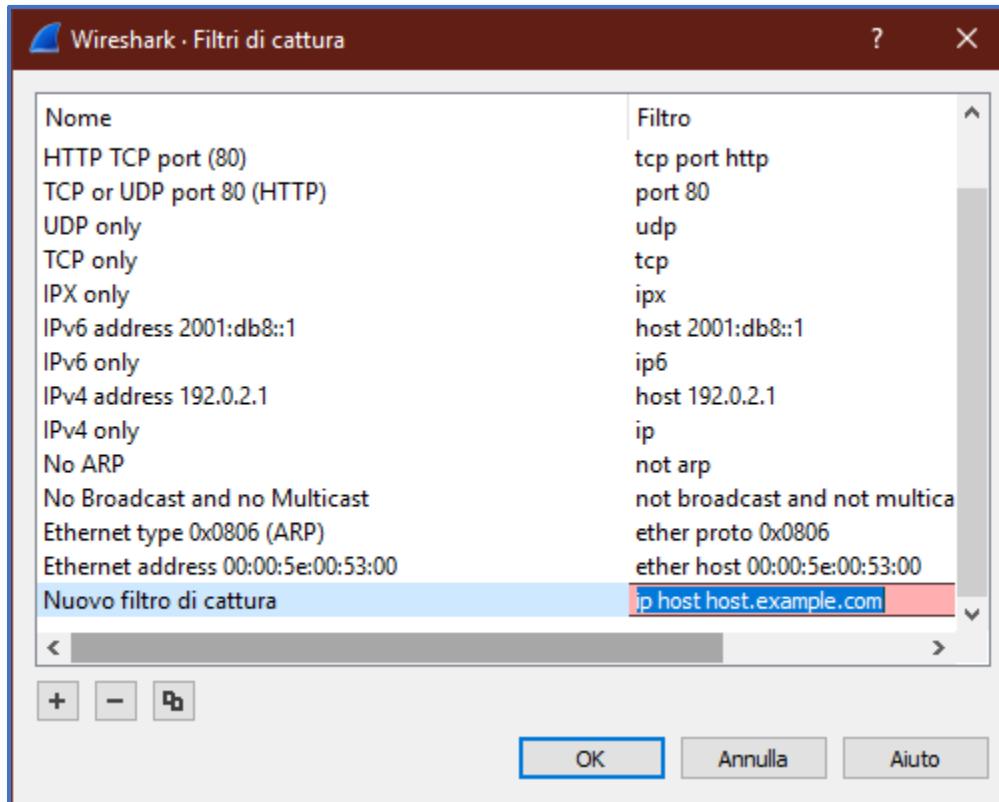
- *Filtri di Cattura* | 3/4



# Acquisizione Traffico di Rete con Wireshark

## Interfaccia Utente | 9/9

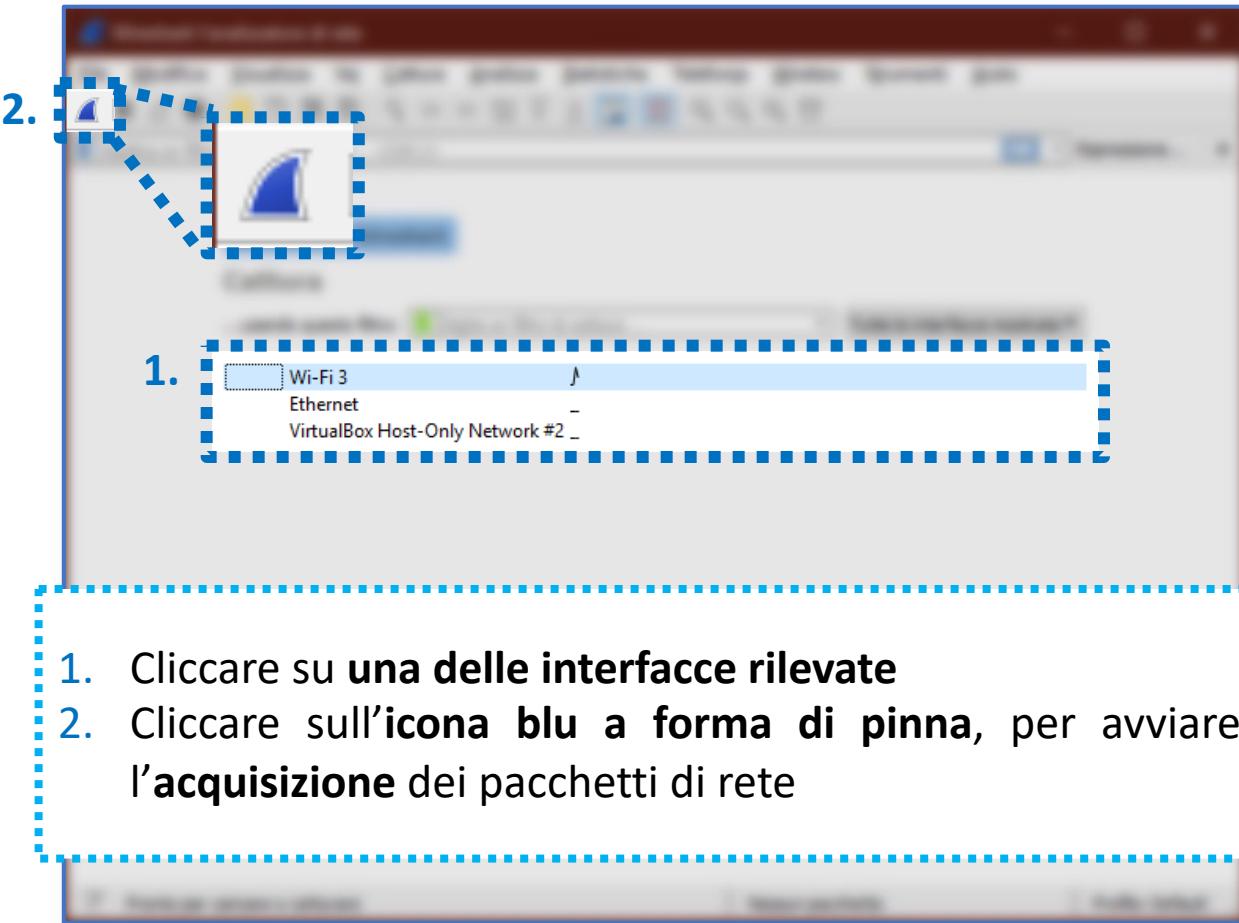
- *Filtri di Cattura | 4/4 | Aggiunta di un Nuovo Filtro*



# Acquisizione Traffico di Rete con Wireshark

## Esempio di Utilizzo | 1/12

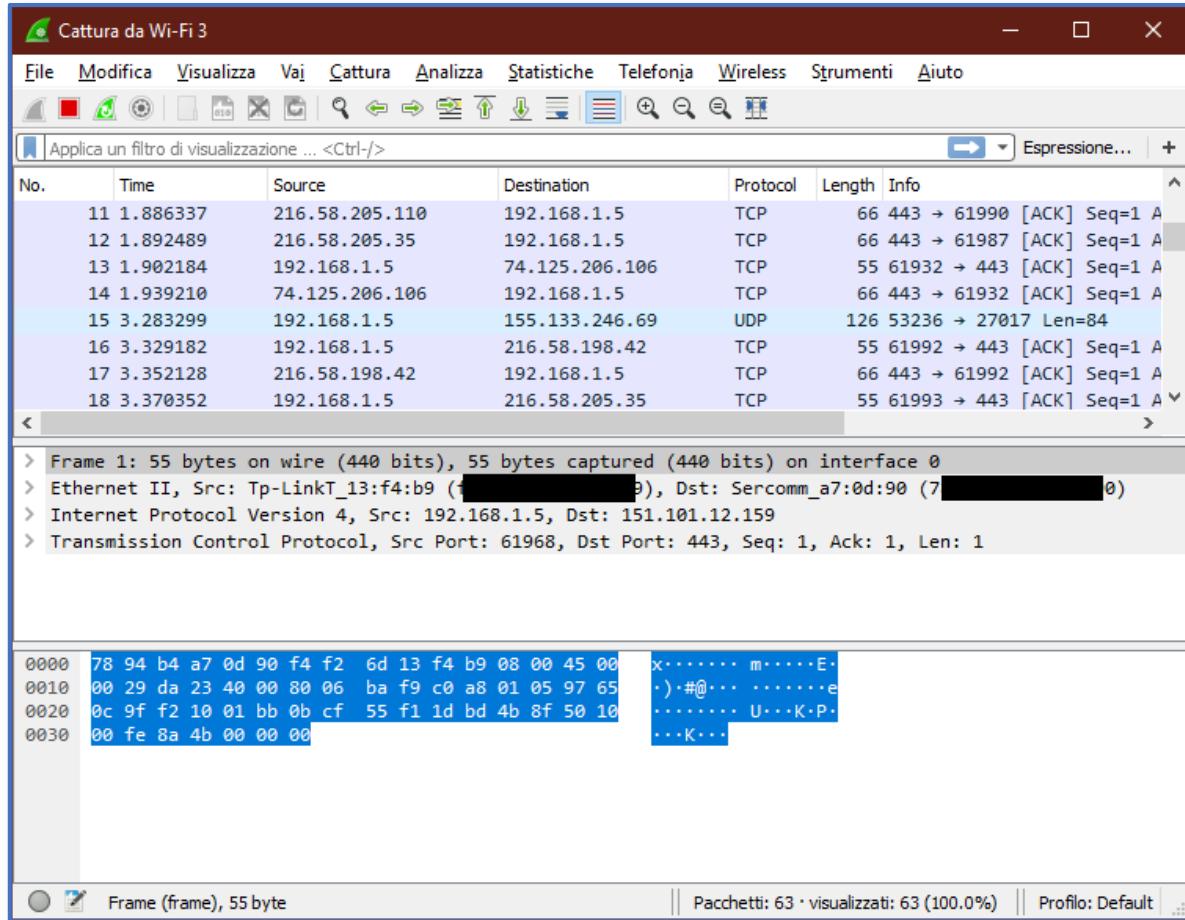
- *Avvio della Fase di Acquisizione*



# Acquisizione Traffico di Rete con Wireshark

## Esempio di Utilizzo | 2/12

- *Schermata Fase di Acquisizione*



# Acquisizione Traffico di Rete con Wireshark

## Esempio di Utilizzo | 2/12

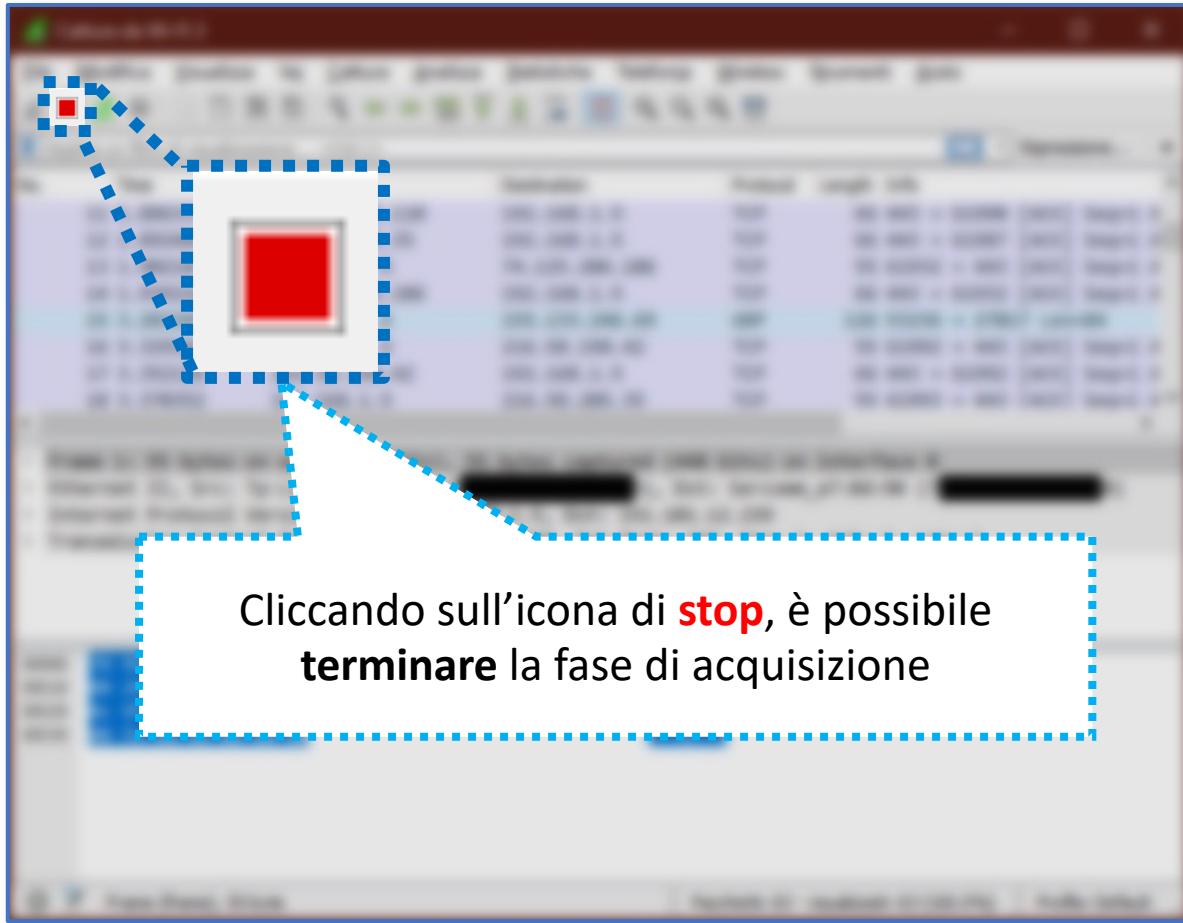
- *Schermata Fase di Acquisizione*



# Acquisizione Traffico di Rete con Wireshark

## Esempio di Utilizzo | 3/12

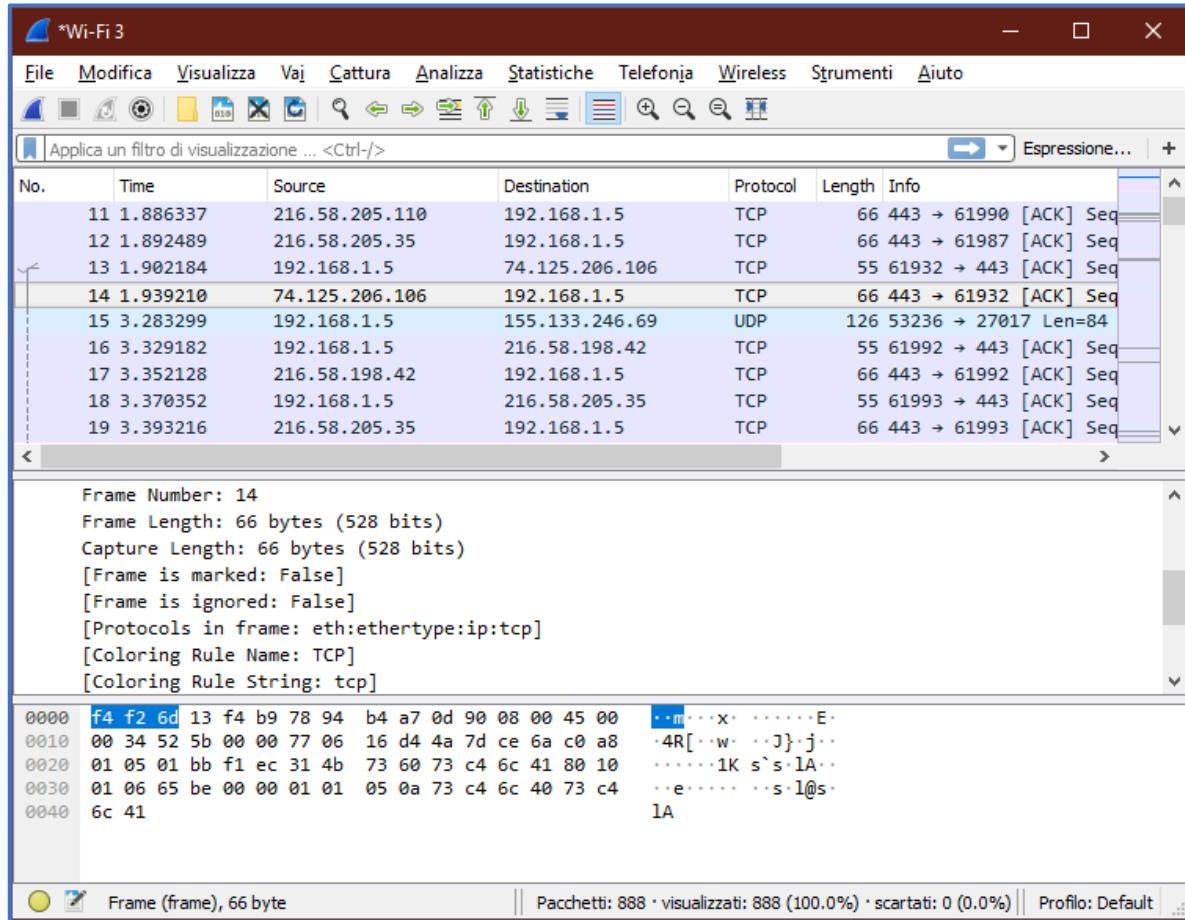
- *Schermata Fase di Acquisizione*



# Acquisizione Traffico di Rete con Wireshark

## Esempio di Utilizzo | 4/12

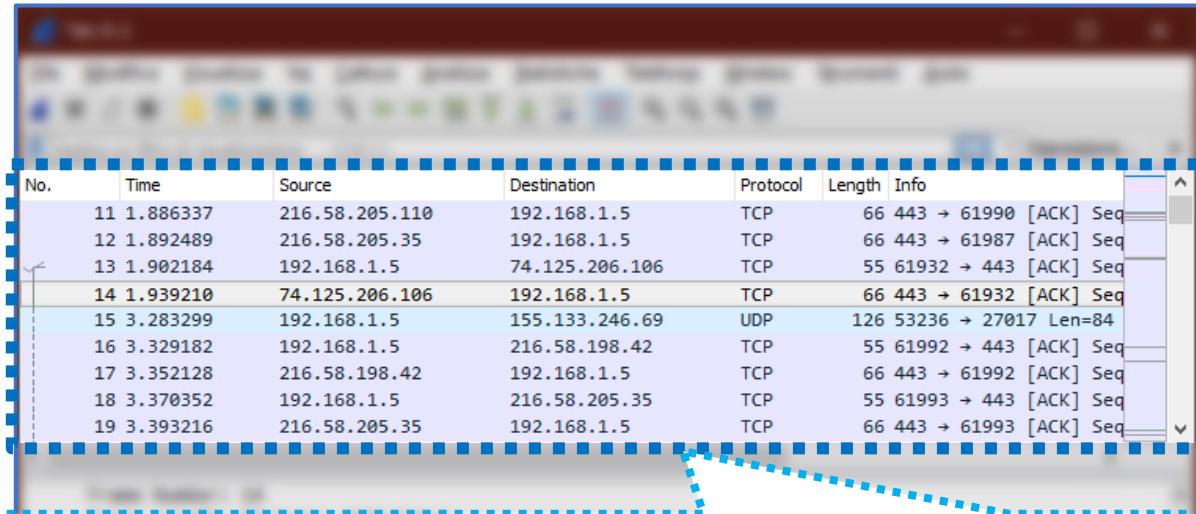
- *Schermata Fase di Acquisizione (Terminata)*



# Acquisizione Traffico di Rete con Wireshark

## Esempio di Utilizzo | 4/12

- *Schermata Fase di Acquisizione (Terminata)*



No.	Time	Source	Destination	Protocol	Length	Info
11	1.886337	216.58.205.110	192.168.1.5	TCP	66	443 → 61990 [ACK] Seq
12	1.892489	216.58.205.35	192.168.1.5	TCP	66	443 → 61987 [ACK] Seq
13	1.902184	192.168.1.5	74.125.206.106	TCP	55	61932 → 443 [ACK] Seq
14	1.939210	74.125.206.106	192.168.1.5	TCP	66	443 → 61932 [ACK] Seq
15	3.283299	192.168.1.5	155.133.246.69	UDP	126	53236 → 27017 Len=84
16	3.329182	192.168.1.5	216.58.198.42	TCP	55	61992 → 443 [ACK] Seq
17	3.352128	216.58.198.42	192.168.1.5	TCP	66	443 → 61992 [ACK] Seq
18	3.370352	192.168.1.5	216.58.205.35	TCP	55	61993 → 443 [ACK] Seq
19	3.393216	216.58.205.35	192.168.1.5	TCP	66	443 → 61993 [ACK] Seq

Elenco dei pacchetti acquisiti

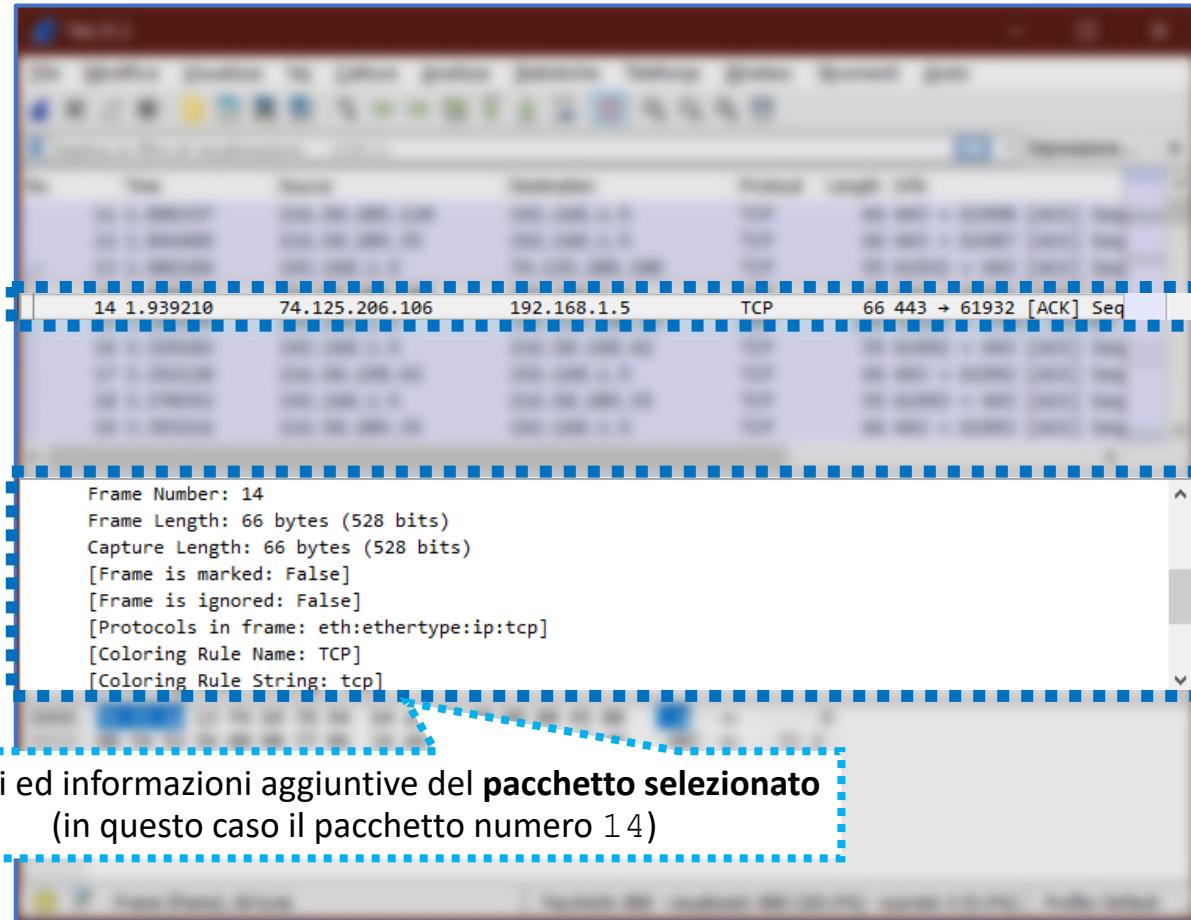
Per ciascun pacchetto (uno per ciascuna riga), vengono riportate diverse informazioni, tra cui:

- Numero e timestamp (*time*) del pacchetto
- Indirizzo IP **sorgente** e **destinazione**
- **Protocollo** (per facilitare la visualizzazione, le righe relative a pacchetti con diversi protocolli, vengono riportate di colore diverso)
- **Dimensioni** (in termini di byte)
- **Ulteriori informazioni**

# Acquisizione Traffico di Rete con Wireshark

## Esempio di Utilizzo | 4/12

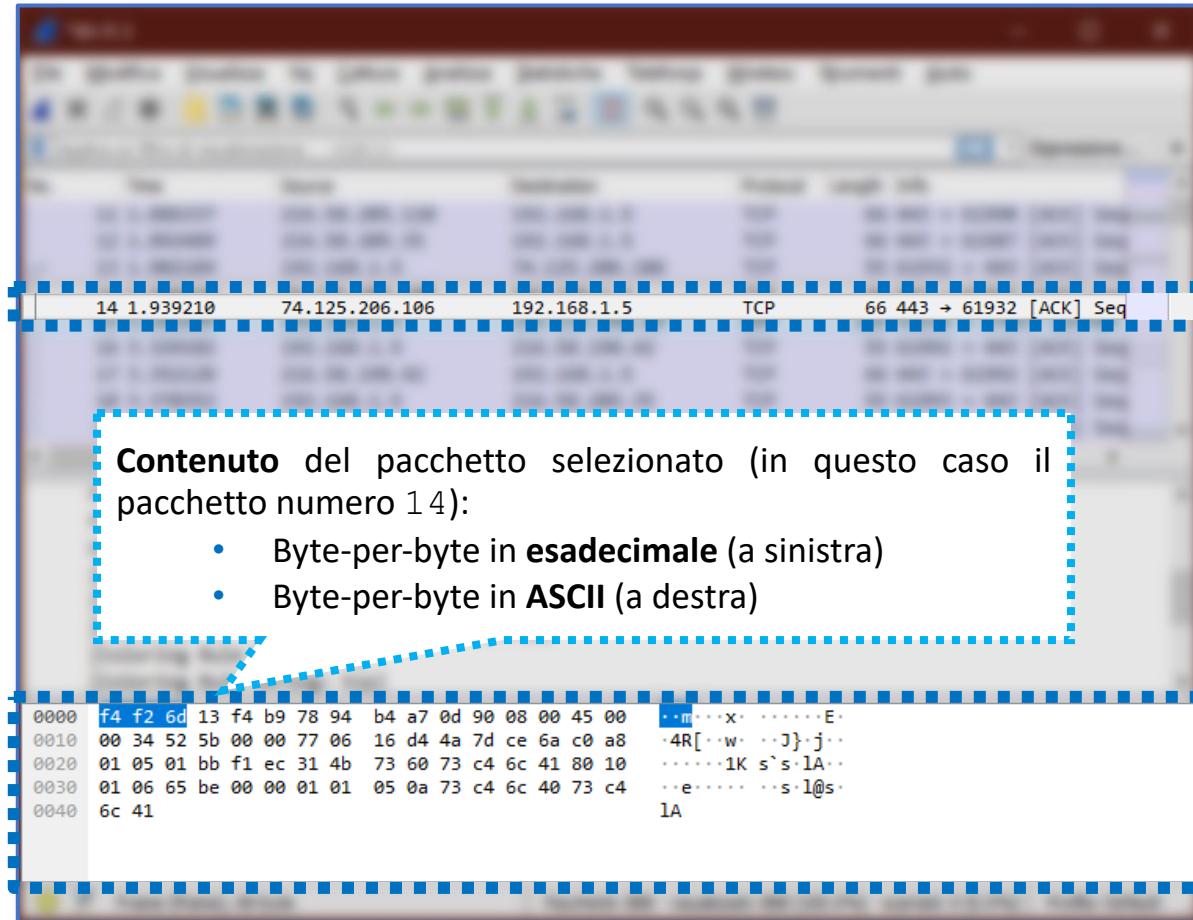
- *Schermata Fase di Acquisizione (Terminata)*



# Acquisizione Traffico di Rete con Wireshark

## Esempio di Utilizzo | 4/12

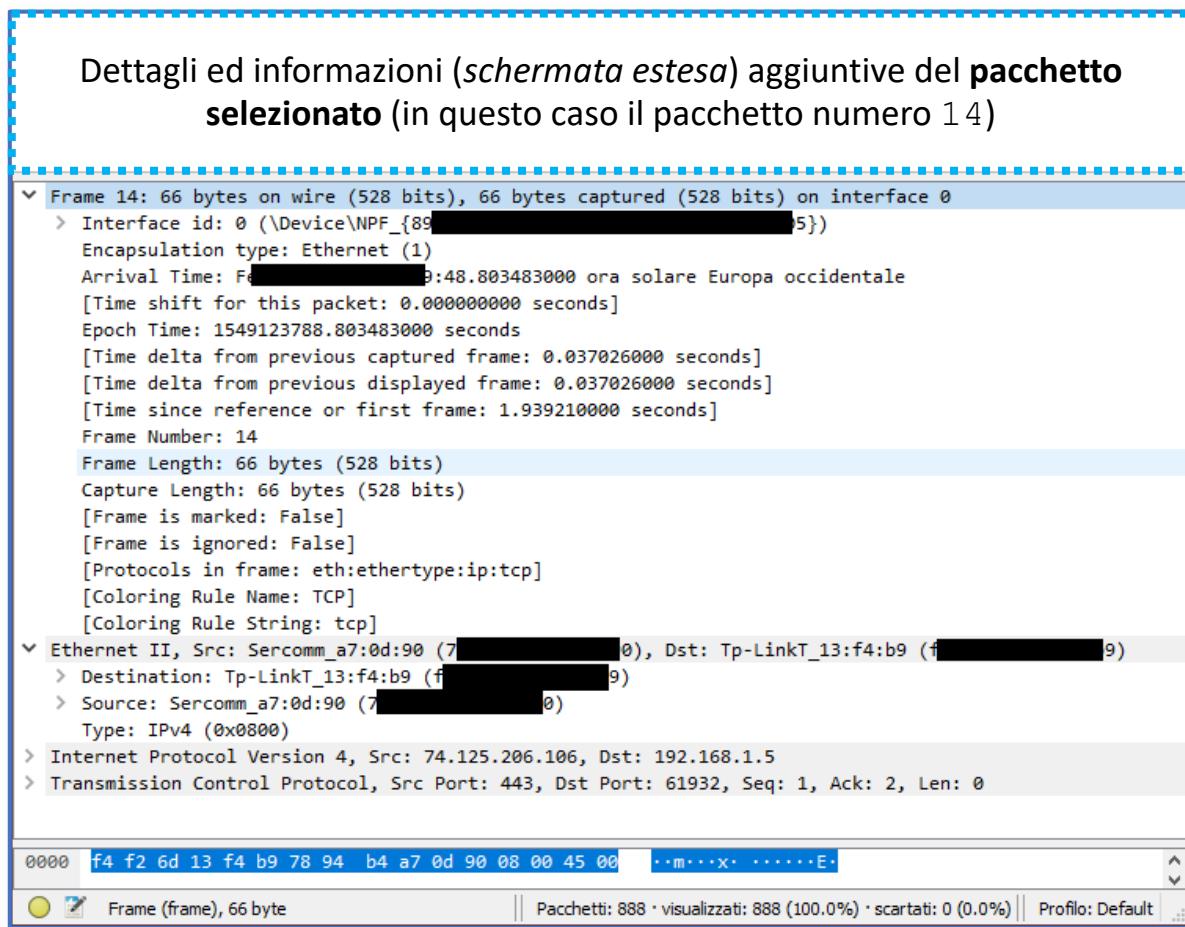
- *Schermata Fase di Acquisizione (Terminata)*



# Acquisizione Traffico di Rete con Wireshark

## Esempio di Utilizzo | 5/12

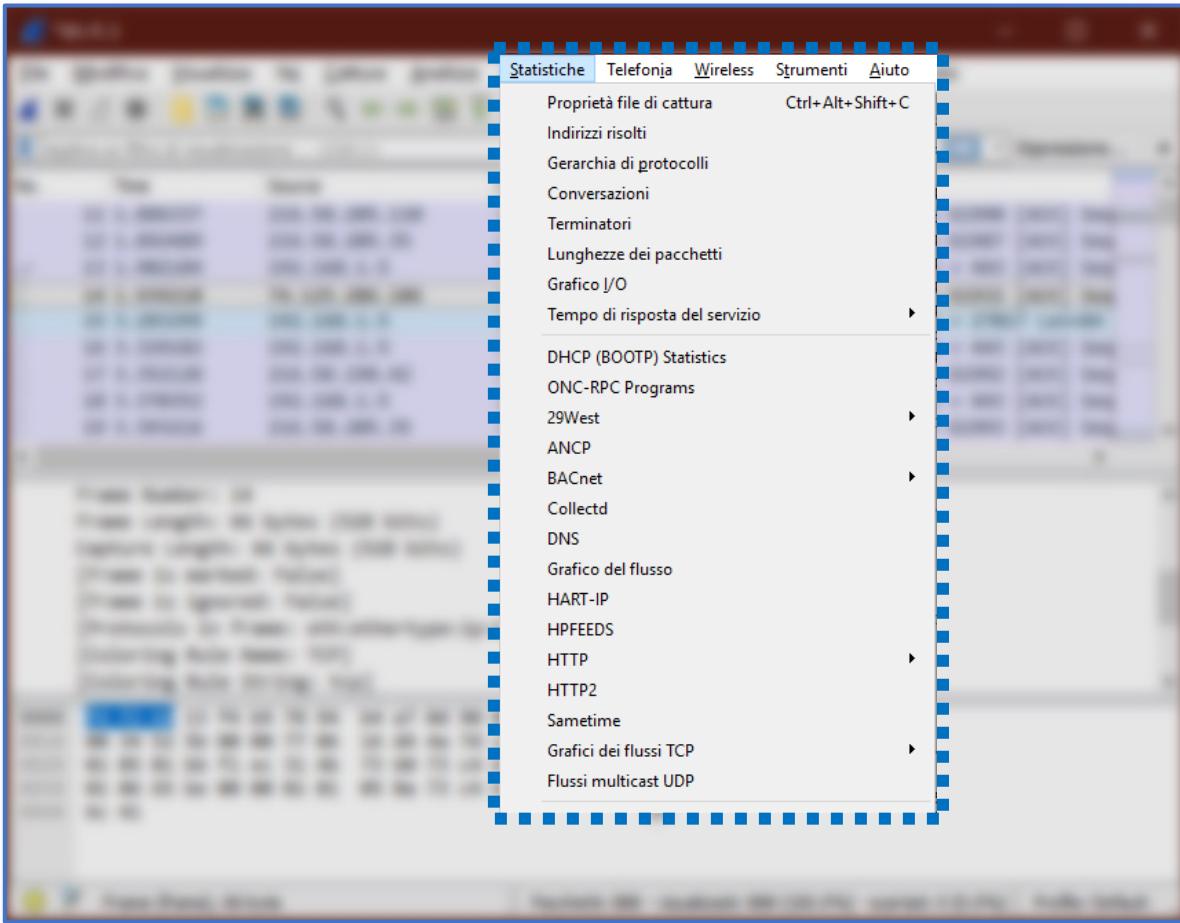
- *Schermata Fase di Acquisizione (Terminata)*



# Acquisizione Traffico di Rete con Wireshark

## Esempio di Utilizzo | 6/12

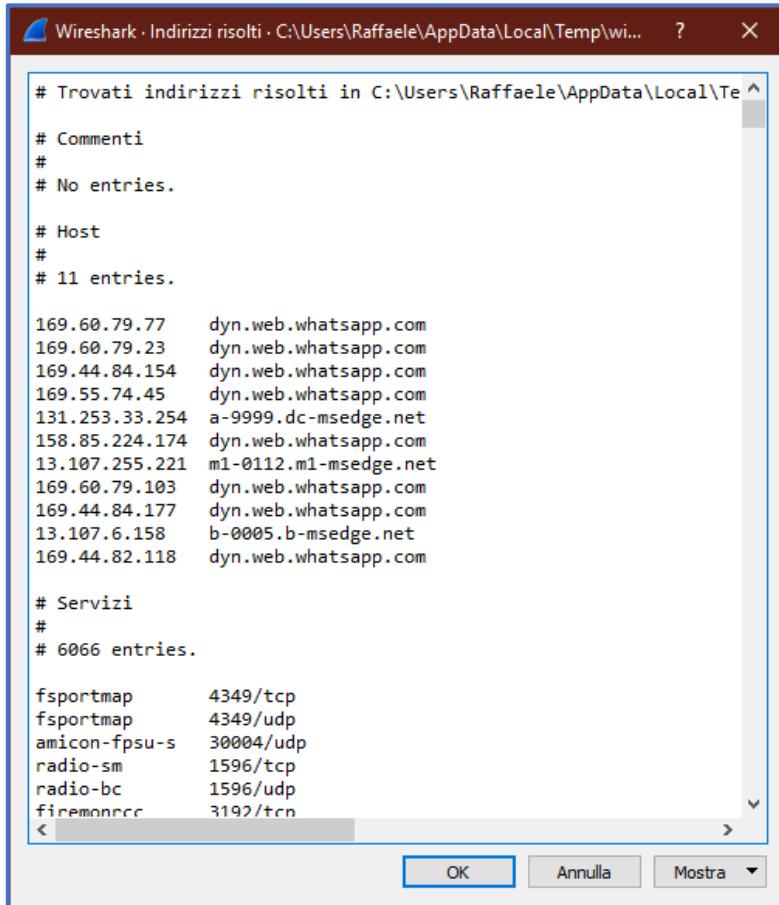
- *Menu Statistiche*



# Acquisizione Traffico di Rete con Wireshark

## Esempio di Utilizzo | 7/12

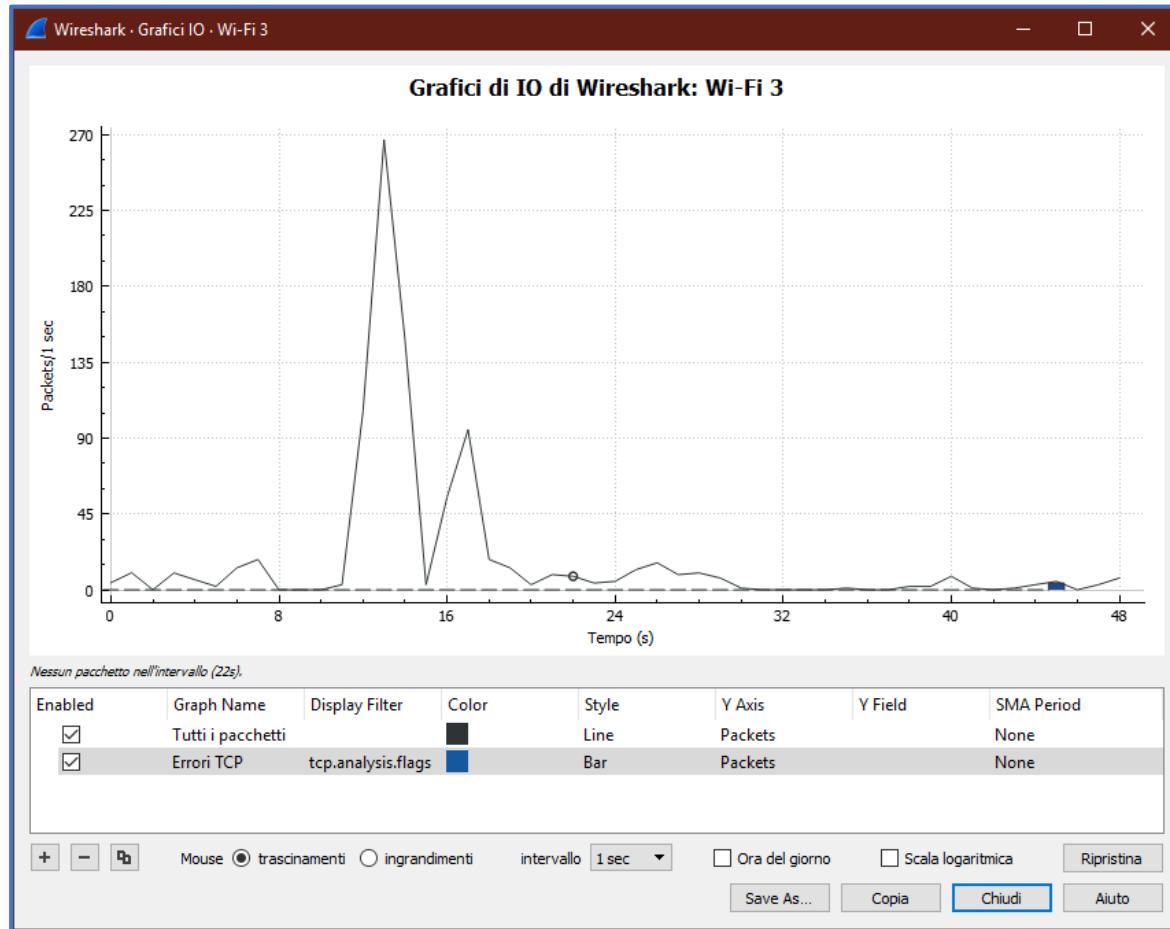
- *Menu Statistiche | Indirizzi risolti*



# Acquisizione Traffico di Rete con Wireshark

## Esempio di Utilizzo | 8/12

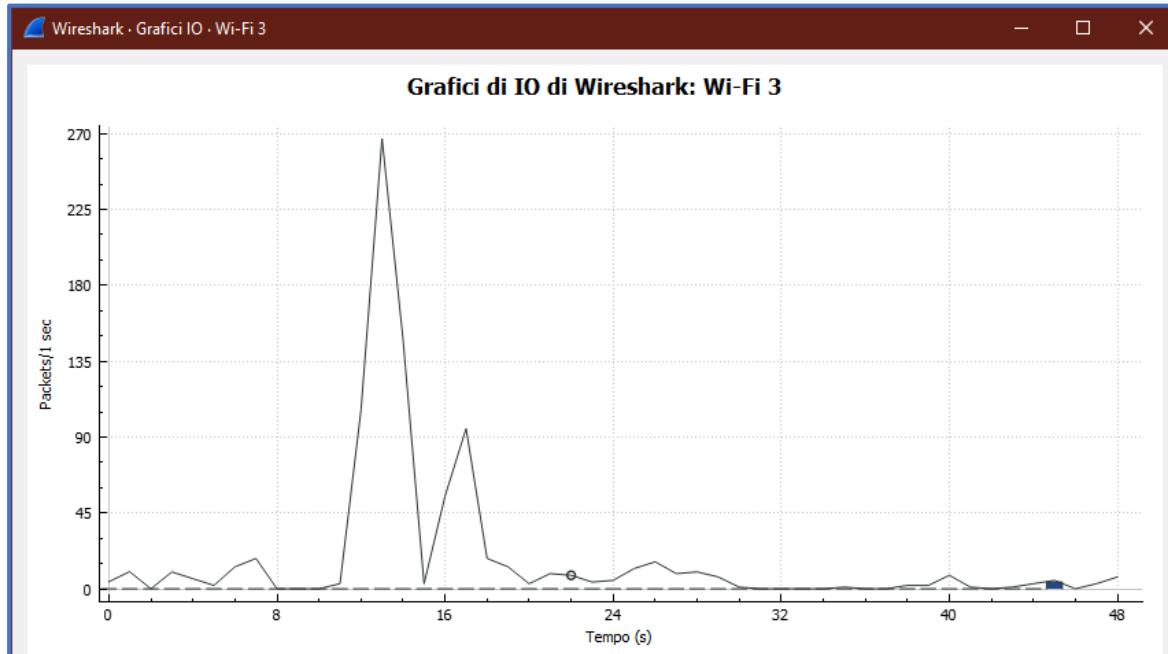
- *Menu Statistiche | Grafici IO*



# Acquisizione Traffico di Rete con Wireshark

## Esempio di Utilizzo | 8/12

- *Menu Statistiche | Grafici IO*



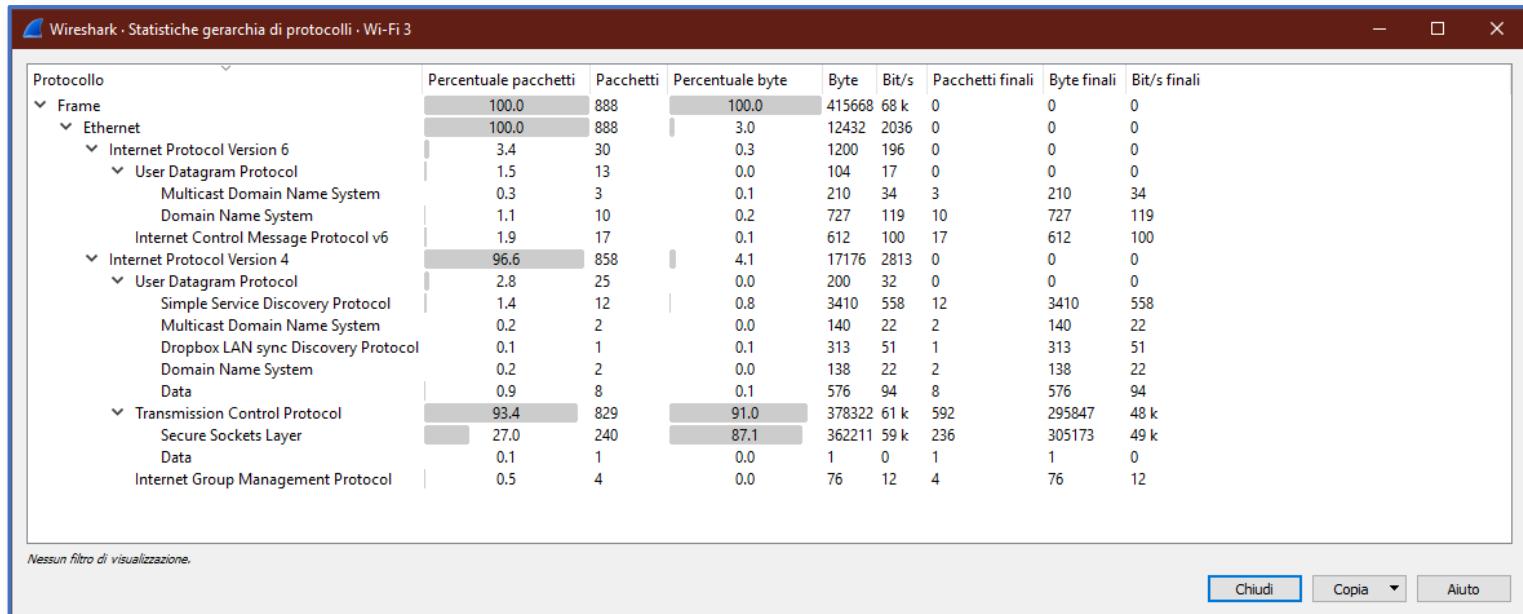
Per l'interfaccia di rete, selezionata precedentemente, nella schermata iniziale, viene riportato un **grafico** con la seguente **struttura**:

- **Asse Y:** Numero di pacchetti acquisiti al secondo
- **Asse X:** Tempo, espresso in secondi

# Acquisizione Traffico di Rete con Wireshark

## Esempio di Utilizzo | 9/12

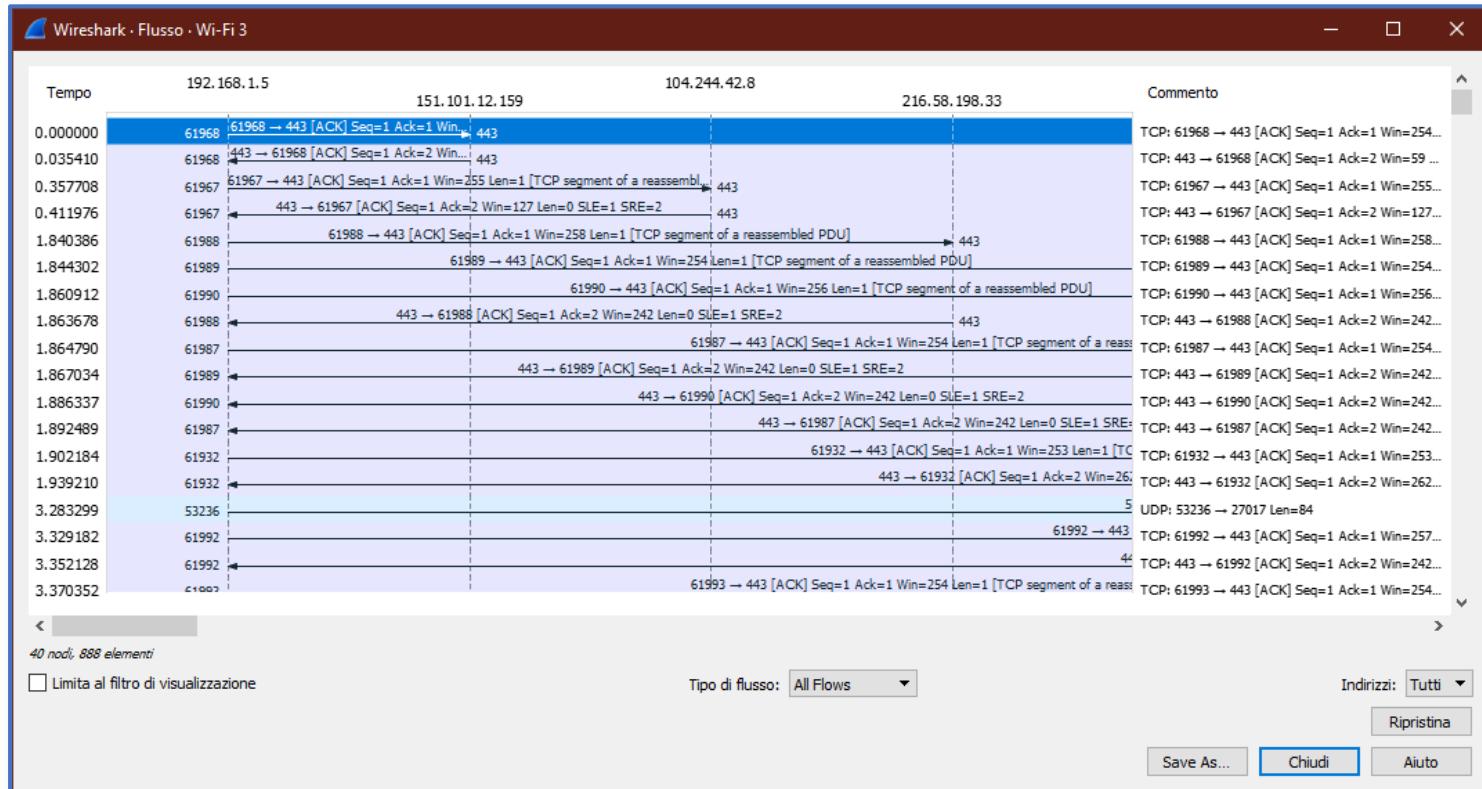
- *Menu Statistiche | Statistiche gerarchia di protocolli*



# Acquisizione Traffico di Rete con Wireshark

## Esempio di Utilizzo | 10/12

- *Menu Statistiche | Flusso*

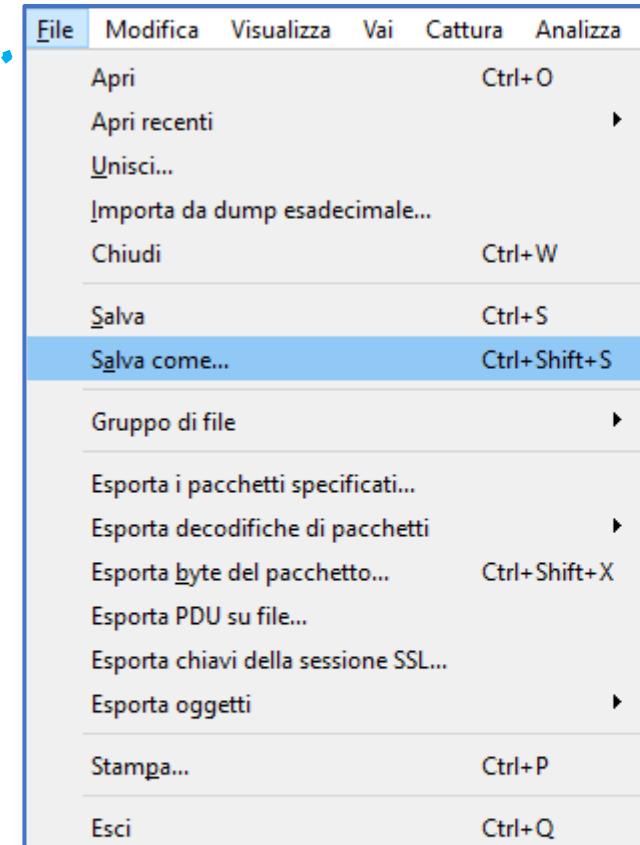


# Acquisizione Traffico di Rete con Wireshark

## Esempio di Utilizzo | 11/12

- *Salvataggio del traffico acquisito | 1/2*

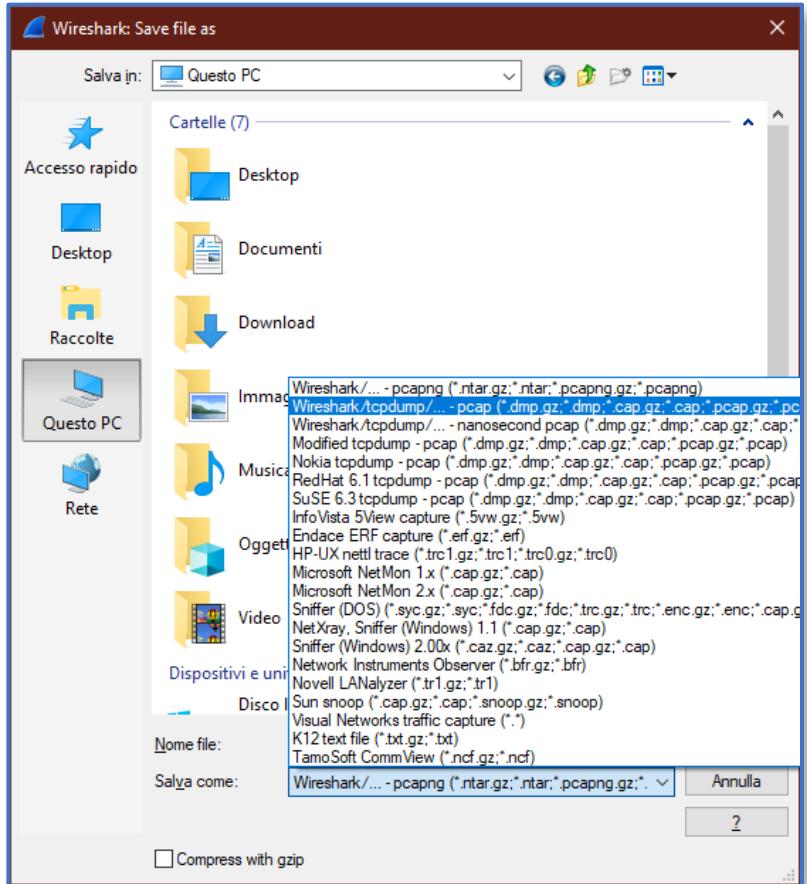
Per salvare il traffico acquisito,  
cliccare sul menu **File** e,  
successivamente su **Salva come...**



# Acquisizione Traffico di Rete con Wireshark

## Esempio di Utilizzo | 12/12

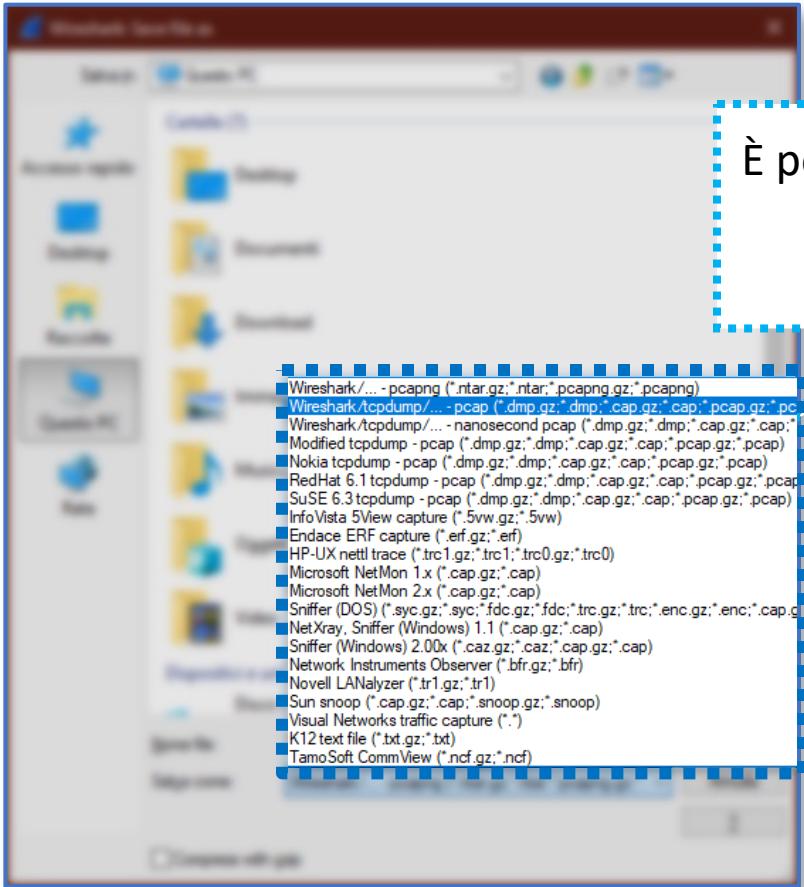
- *Salvataggio del traffico acquisito | 2/2*



# Acquisizione Traffico di Rete con Wireshark

## Esempio di Utilizzo | 12/12

- *Salvataggio del traffico acquisito | 2/2*



È possibile memorizzare il traffico acquisito, in diversi formati, fra cui il **formato PCAP** (utilizzabile dal tool Xplico)

# Riferimenti Bibliografici

- **Digital Forensics with Kali Linux, Shiva V.N. Parasram, Packt Publishing, 2017**
  - Capitolo 7
- **Xplico**
  - <https://www.xplico.org/>
- **Wireshark**
  - <https://www.wireshark.org>