POLITECNICO
MILANO 1863

# Fondamenti di Internet e Reti

Antonio Capone, Achille Pattavina,
Francesco Musumeci, Matteo Cesana

POLITECNICO
MILANO 1863

# Introduzione Wireshark

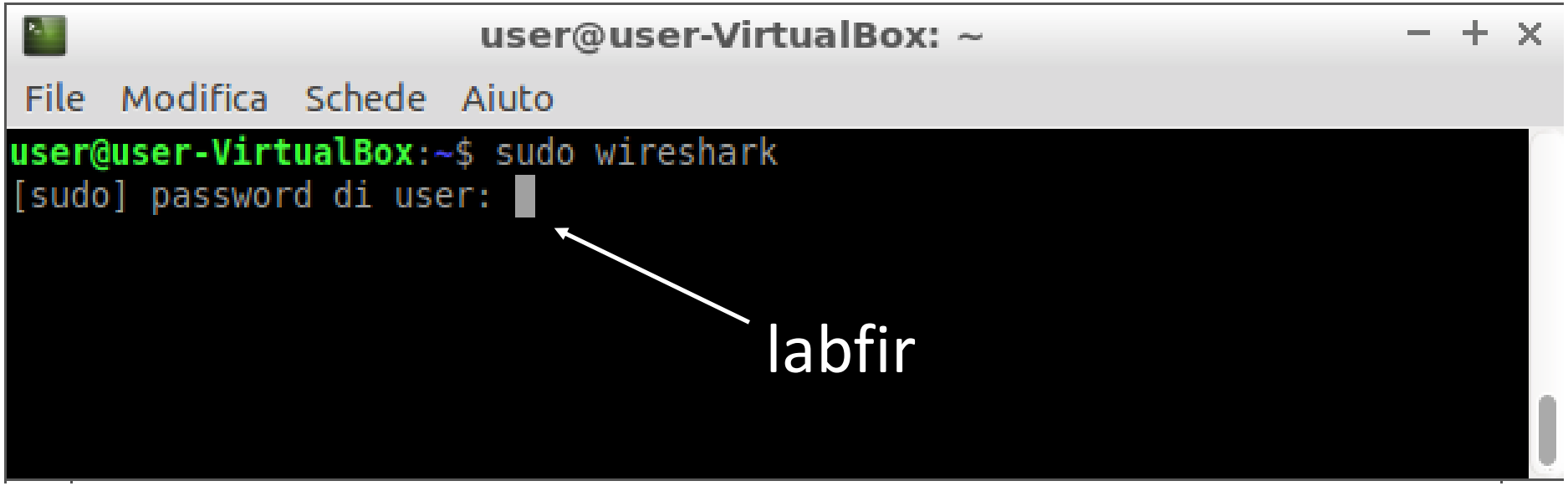
Antonio Capone, Achille Pattavina,
Francesco Musumeci, Matteo Cesana

Fondamenti di Internet e Reti

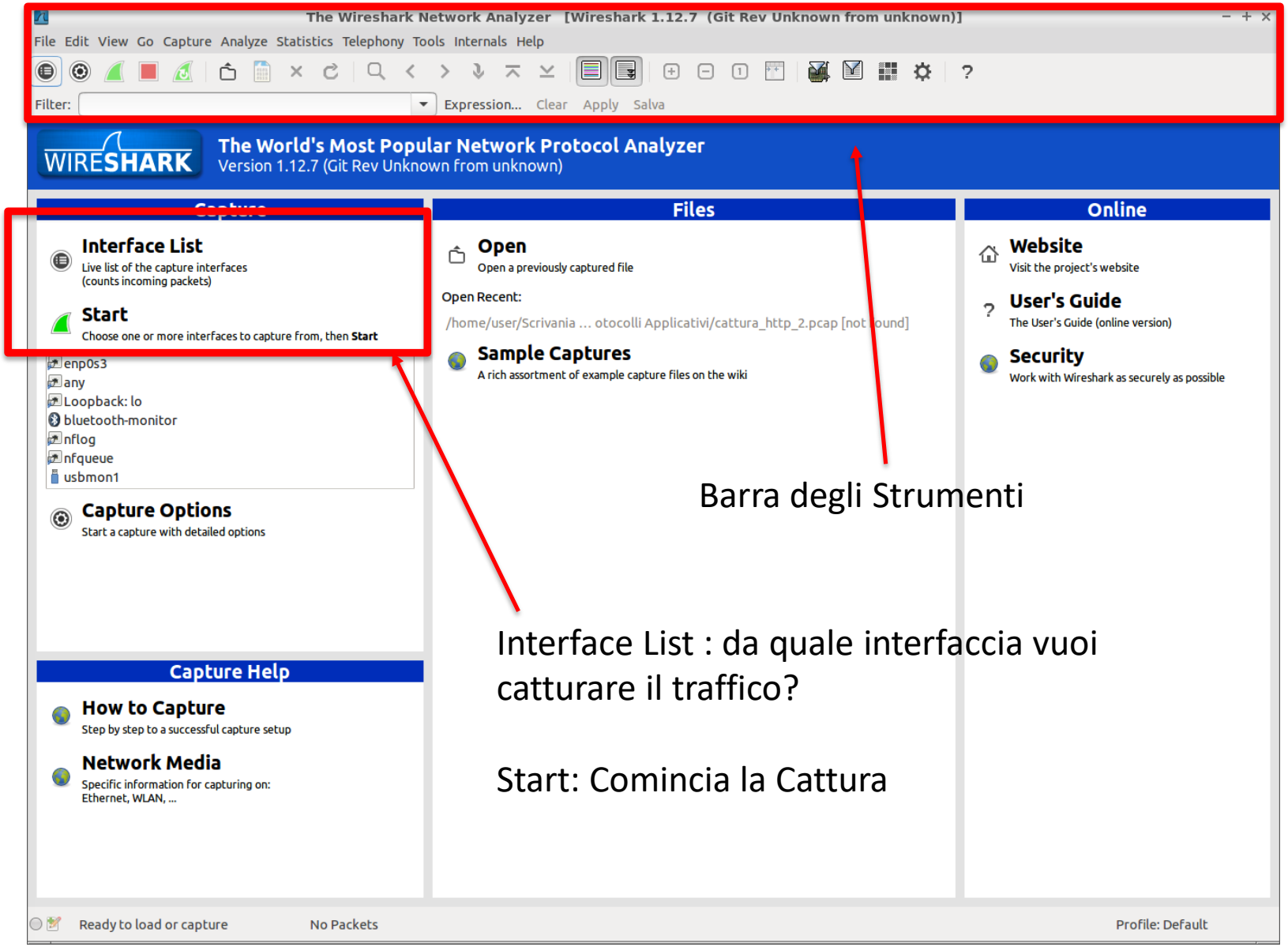
# Analisi dei Protocolli di Rete: HTTP, HTTPS and DNS

- WireShark permette di effettuare catture di traffico
- Consente l’analisi in dettaglio dei messaggi in ingresso e in uscita per ogni livello della pila dei protocolli

# Wireshark: Apertura del programma



# Wireshark: Pannello Iniziale

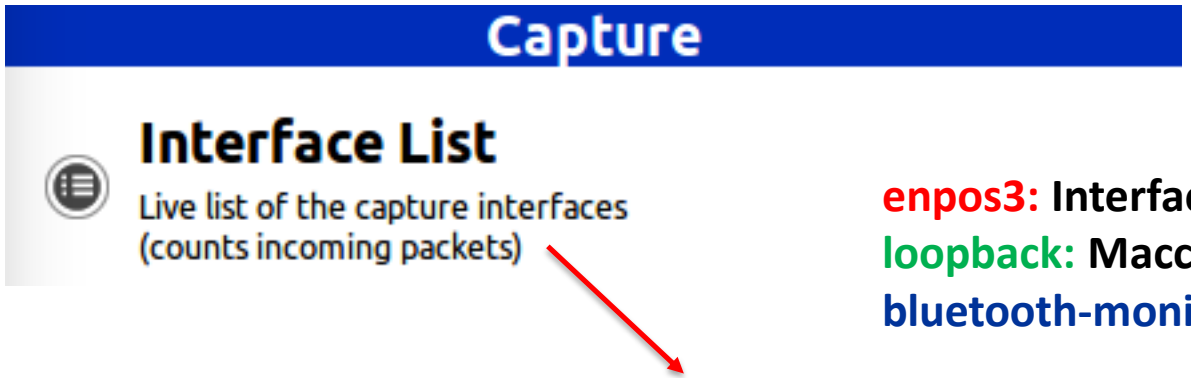



Barra degli Strumenti

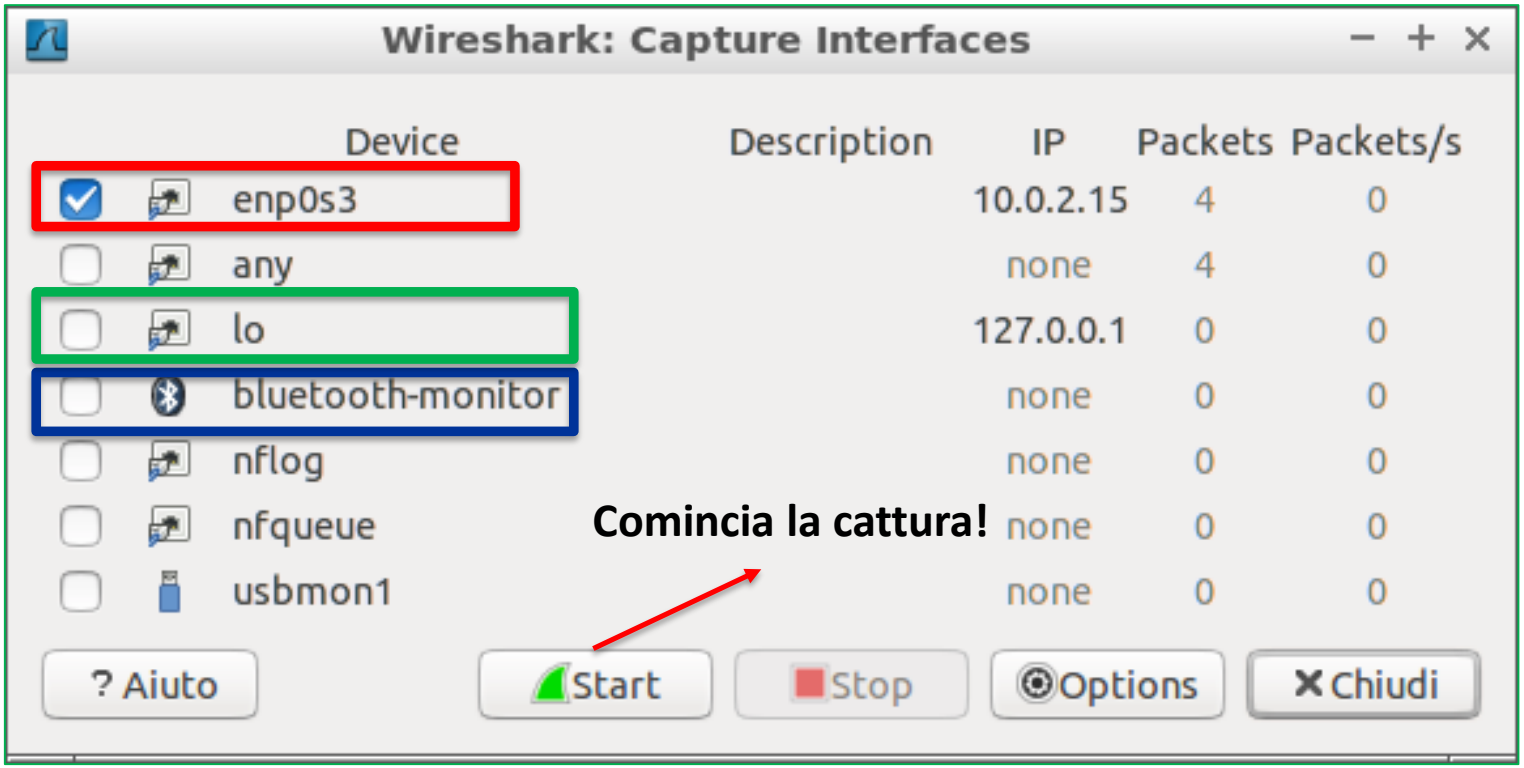
Interface List : da quale interfaccia vuoi catturare il traffico?

Start: Comincia la Cattura

# Wireshark: Scegliere l'Interfaccia di Cattura




**enpos3:** Interfaccia Ethernet
**loopback:** Macchina Locale
**bluetooth-monitor:** Interfaccia Bluetooth



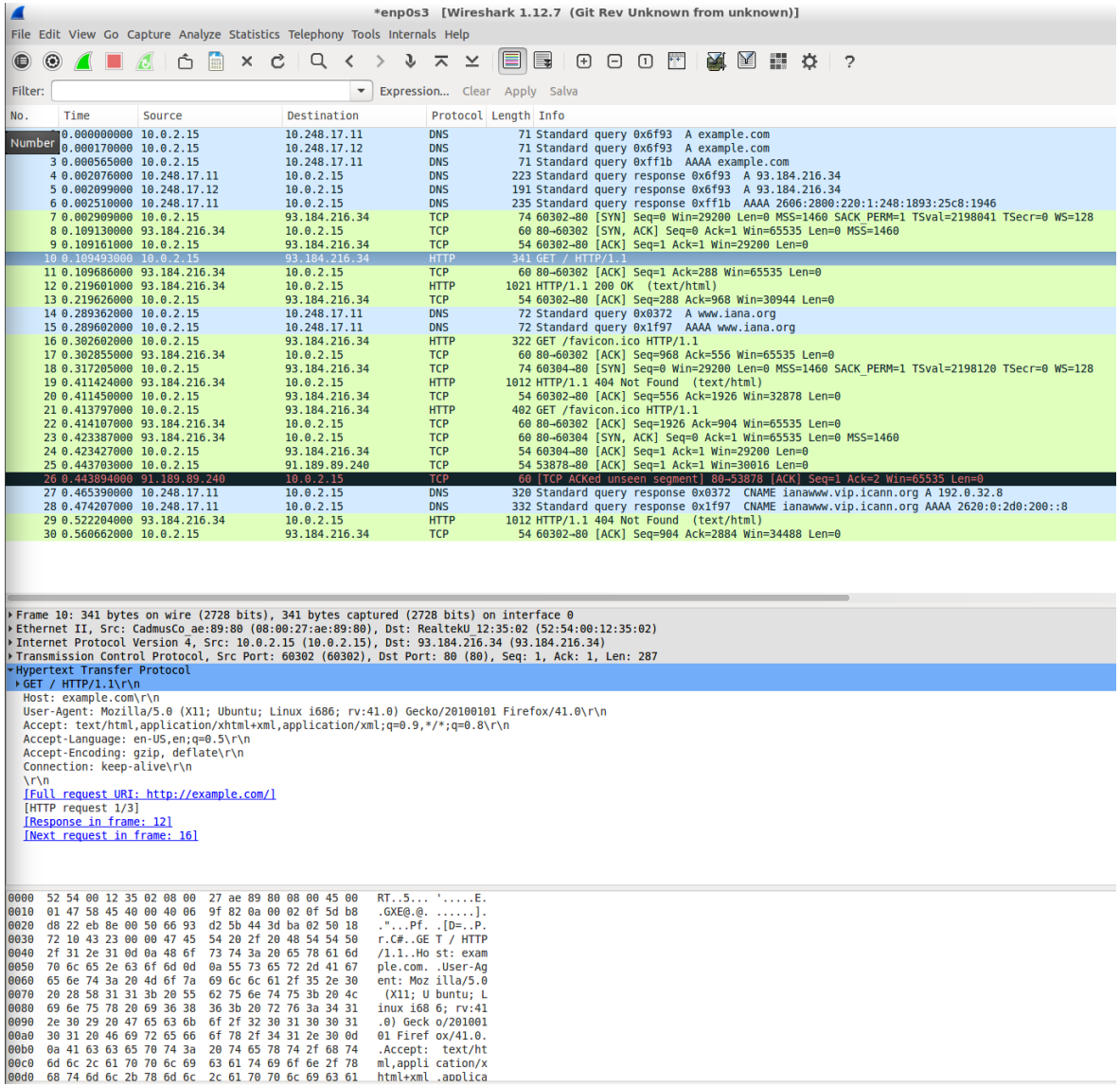

**Comincia la cattura!**

# Wireshark: Contattare un sito Web (HTTP)

Premere il pulsante **START** per far partire la cattura

Dal browser della macchina virtuale contattare il sito web: [www.example.com](http://www.example.com)

Interrompere la cattura tramite il quadrato rosso di **STOP**



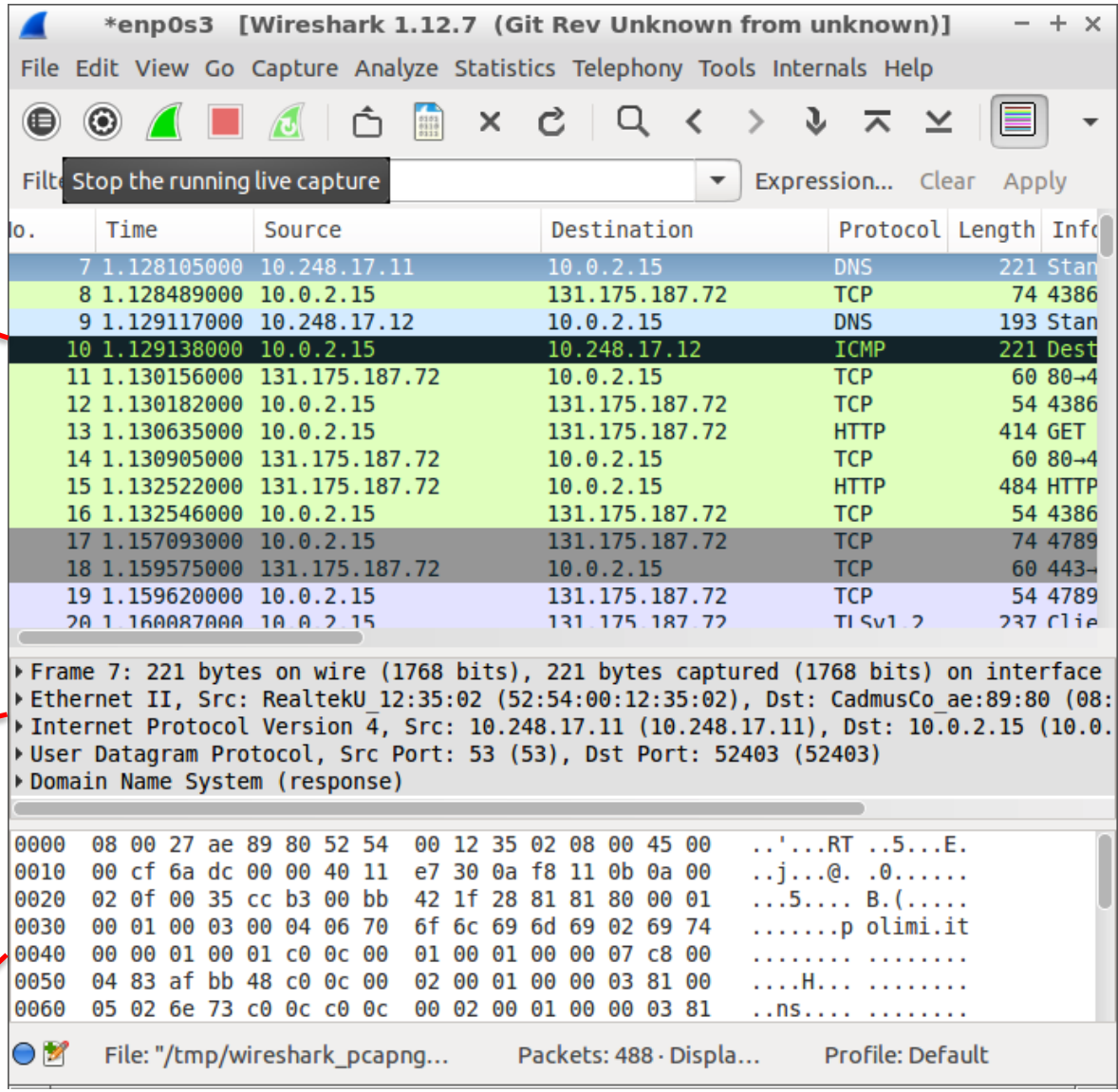
# Wireshark: Pannello di Cattura

Pacchetti Catturati con indicazione di:

- Istante di Cattura
- Sorgente (IP)
- Destinazione (IP)
- Protocollo
- etc.

Informazioni sul pacchetto selezionato

Valore dei campi in byte (esadecimale)



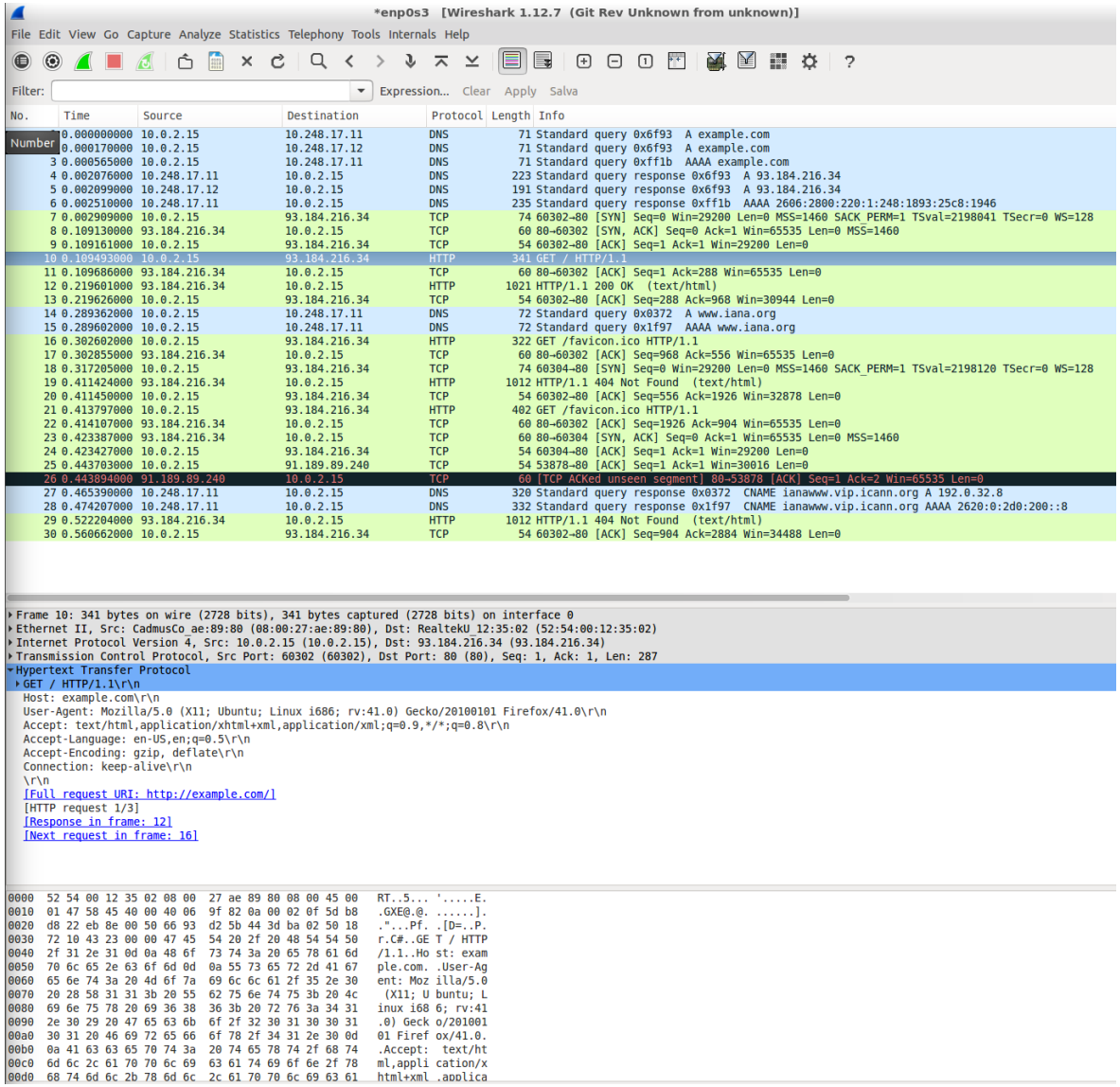
# Wireshark: Pannello di cattura

E' possibile salvare la traccia appena catturata:

- File → Save as..

Analogamente, è possibile caricare una traccia salvata per poterla analizzare offline:

- File → Open..



# Wireshark: Un esempio di Traccia HTTP

*enp0s3 [Wireshark 1.12.7 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http | Expression... Clear Apply Salva

**Filtra i pacchetti per protocollo**

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 13 | 0.114006000 | 10.0.2.15 | 93.184.216.34 | HTTP | 455 | GET / HTTP/1.1 |
| 15 | 0.227703000 | 93.184.216.34 | 10.0.2.15 | HTTP | 345 | HTTP/1.1 304 Not Modified |

```
▸ Frame 13: 455 bytes on wire (3640 bits), 455 bytes captured (3640 bits) on interface 0
▸ Ethernet II, Src: CadmusCo_ae:89:80 (08:00:27:ae:89:80), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 93.184.216.34 (93.184.216.34)
▸ Transmission Control Protocol, Src Port: 60182 (60182), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 401
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
  Host: www.example.com\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:41.0) Gecko/20100101 Firefox/41.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  If-Modified-Since: Fri, 09 Aug 2013 23:54:35 GMT\r\n
  If-None-Match: "1541025663+gzip"\r\n
  Cache-Control: max-age=0\r\n
  \r\n
  [Full request URI: http://www.example.com/]
  [HTTP request 1/1]
  [Response in frame: 15]
```

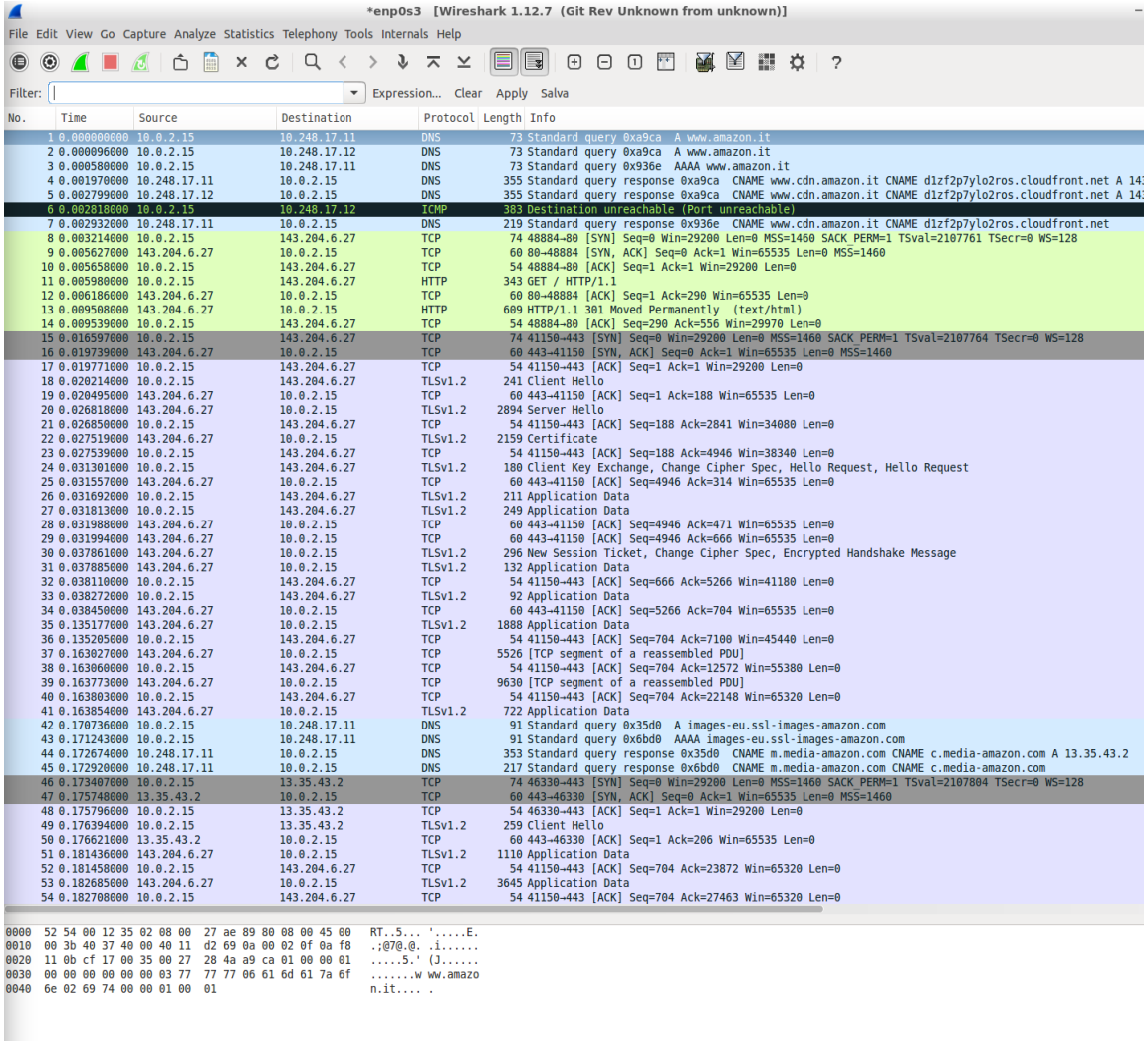
**Ispezione della richiesta HTTP GET: il campo “host” è in chiaro**

# Wireshark: Contattare un sito Web (HTTPS)

Premere nuovamente il pulsante **START** per far partire una nuova cattura

Contattare questa volta il sito: **www.amazon.it**

Interrompere nuovamente la cattura con il pulsante **STOP**



# Wireshark: Un esempio di Traccia HTTPS

*enp0s3 [Wireshark 1.12.7 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ssl | Expression... Clear Apply Salva

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 18 | 0.020214000 | 10.0.2.15 | 143.204.6.27 | TLSv1.2 | 241 | Client Hello |
| 20 | 0.026818000 | 143.204.6.27 | 10.0.2.15 | TLSv1.2 | 2894 | Server Hello |
| 22 | 0.027519000 | 143.204.6.27 | 10.0.2.15 | TLSv1.2 | 2159 | Certificate |
| 24 | 0.031301000 | 10.0.2.15 | 143.204.6.27 | TLSv1.2 | 180 | Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request |
| 26 | 0.031692000 | 10.0.2.15 | 143.204.6.27 | TLSv1.2 | 211 | Application Data |
| 27 | 0.031813000 | 10.0.2.15 | 143.204.6.27 | TLSv1.2 | 249 | Application Data |
| 30 | 0.037861000 | 143.204.6.27 | 10.0.2.15 | TLSv1.2 | 296 | New Session Ticket, Change Cipher Spec, Encrypted Handshake Message |
| 31 | 0.037885000 | 143.204.6.27 | 10.0.2.15 | TLSv1.2 | 132 | Application Data |
| 33 | 0.038272000 | 10.0.2.15 | 143.204.6.27 | TLSv1.2 | 92 | Application Data |
| 35 | 0.135177000 | 143.204.6.27 | 10.0.2.15 | TLSv1.2 | 1888 | Application Data |
| 41 | 0.163854000 | 143.204.6.27 | 10.0.2.15 | TLSv1.2 | 722 | Application Data |

```
▸ Frame 26: 211 bytes on wire (1688 bits), 211 bytes captured (1688 bits) on interface 0
▸ Ethernet II, Src: CadmusCo_ae:89:80 (08:00:27:ae:89:80), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 143.204.6.27 (143.204.6.27)
▸ Transmission Control Protocol, Src Port: 41150 (41150), Dst Port: 443 (443), Seq: 314, Ack: 4946, Len: 157
▾ Secure Sockets Layer
  ▾ TLSv1.2 Record Layer: Application Data Protocol: spdy
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 152
    Encrypted Application Data: 0000000000000000160388d8a0082e86f4ba0678658d25a18...
```

**Questa volta il campo dati è criptato: https implementa una transazione a livello applicativo “sicura”**

# Wireshark: Esercizio

Contattare il sito web: **www.polimi.it** :

- Indicare se si tratta di una richiesta http o https

- Individuare i messaggi **DNS** e ricavare l'indirizzo IP del server contattato
  - NB: L'utilizzo dei filtri è utile!

- Contattare lo stesso sito web dal browser ma utilizzando l'indirizzo IP trovato al punto precedente: si arriva alla stessa pagina web?