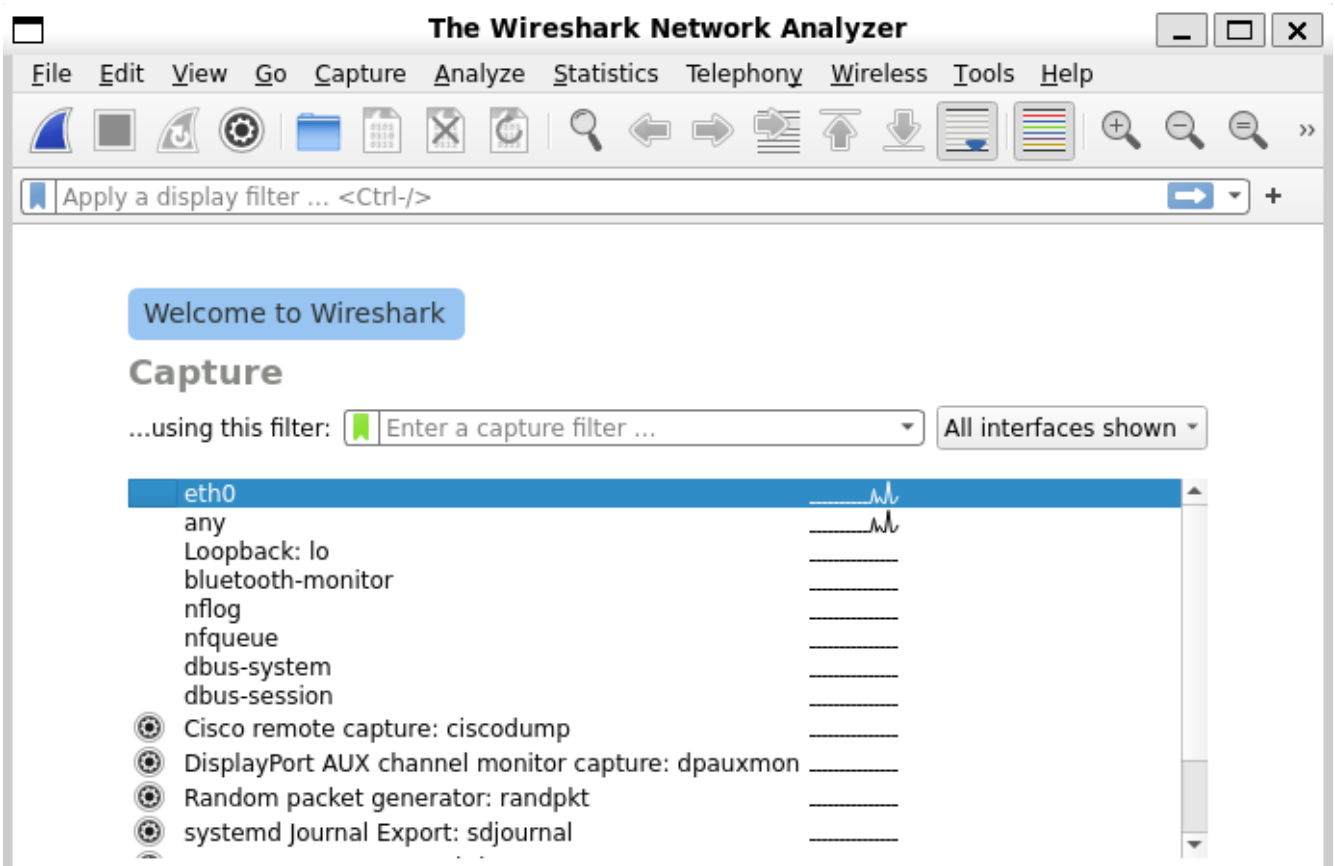
Avvertenze

Prestare attenzione alla sicurezza nella installazione di Wireshark. Il consiglio è di installarlo e utilizzarlo all'interno di un ambiente virtualizzato.

Referimenti:

- https://www.wireshark.org/docs/wsug_html_chunked/ChUseMainWindowSection.html
- https://www.wireshark.org/docs/wsdg_html_chunked/ChapterDissection.html#ChDissectWorks
- https://wiki.wireshark.org/DisplayFilters
- https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html

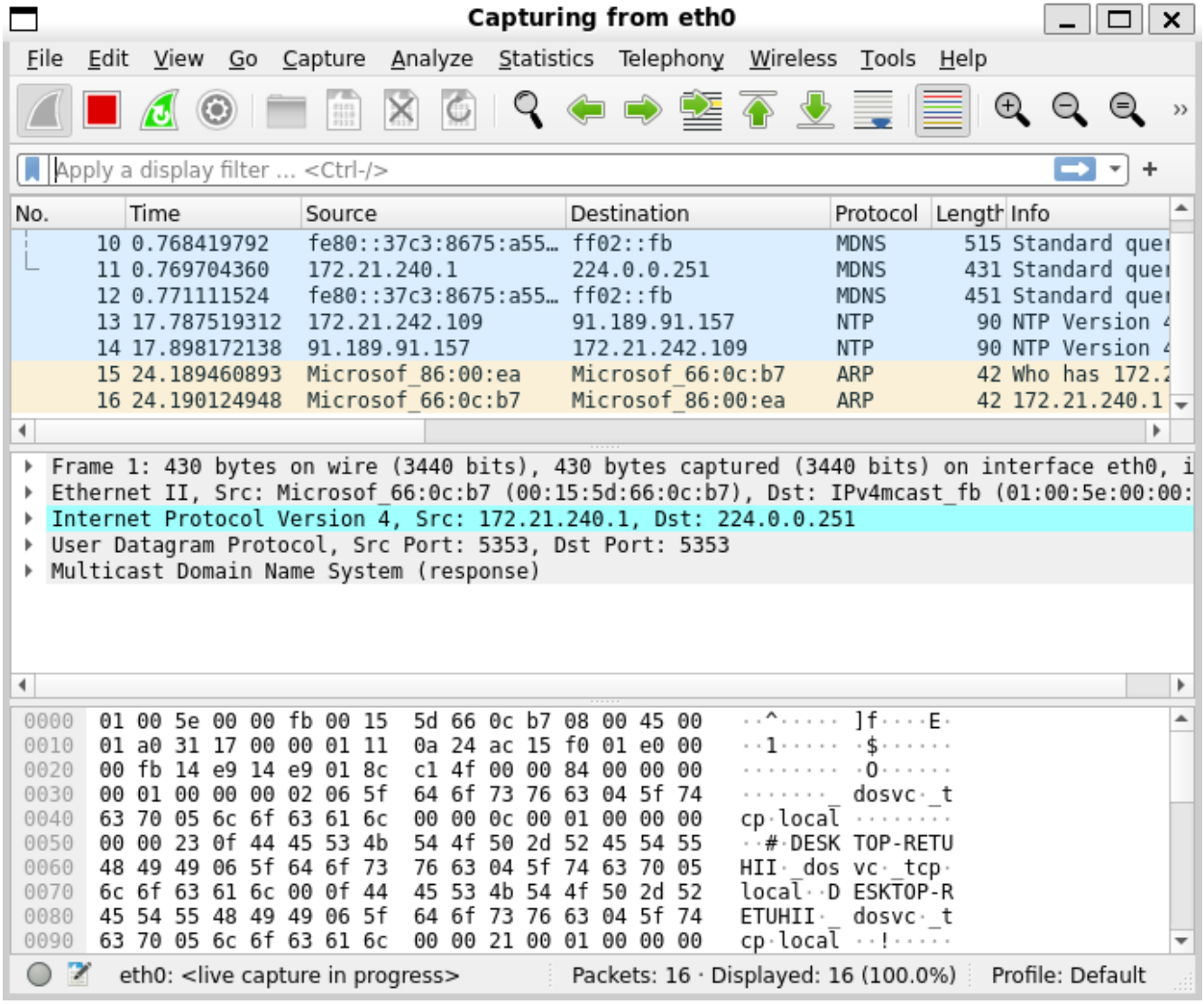
Quando si avvia Wireshark, la prima cosa mostrata è una finestra per la selezione dell'interfaccia su cui effettuare la cattura dei pacchetti.



Sotto WSL2, la scheda di rete (virtuale) principale è `eth0`.

`lo` è l'interfaccia di *loopback* utilizza per la comunicazione locale.

Facendo doppio click su una delle interfacce, viene avviata la cattura dei pacchetti e viene mostrata una nuova finestra simile alla seguente.



In alto a sinistra, troviamo i pulsanti per avviare, fermare o riavviare la cattura dei pacchetti (perdendo nell'ultimo caso tutti i pacchetti catturati).

Il campo di testo in cima permette di inserire delle espressioni, dette *filtri*, appunto per filtrare i pacchetti. Alcuni esempi:

- `nome-protocollo` (es. `http`): mostra i pacchetti contenti un certo protocollo
- `http.request.method == "POST"`: mostra i pacchetti contenenti richieste HTTP con il metodo POST

Il pannello immediatamente sottostante contiene la *lista dei pacchetti* dopo l'applicazione di eventuali filtri.

Il pacchetto selezionato all'interno della lista viene mostrato nel *pannello dei dettagli del pacchetto* (subito sotto) e nel *pannello dei byte del pacchetto*.

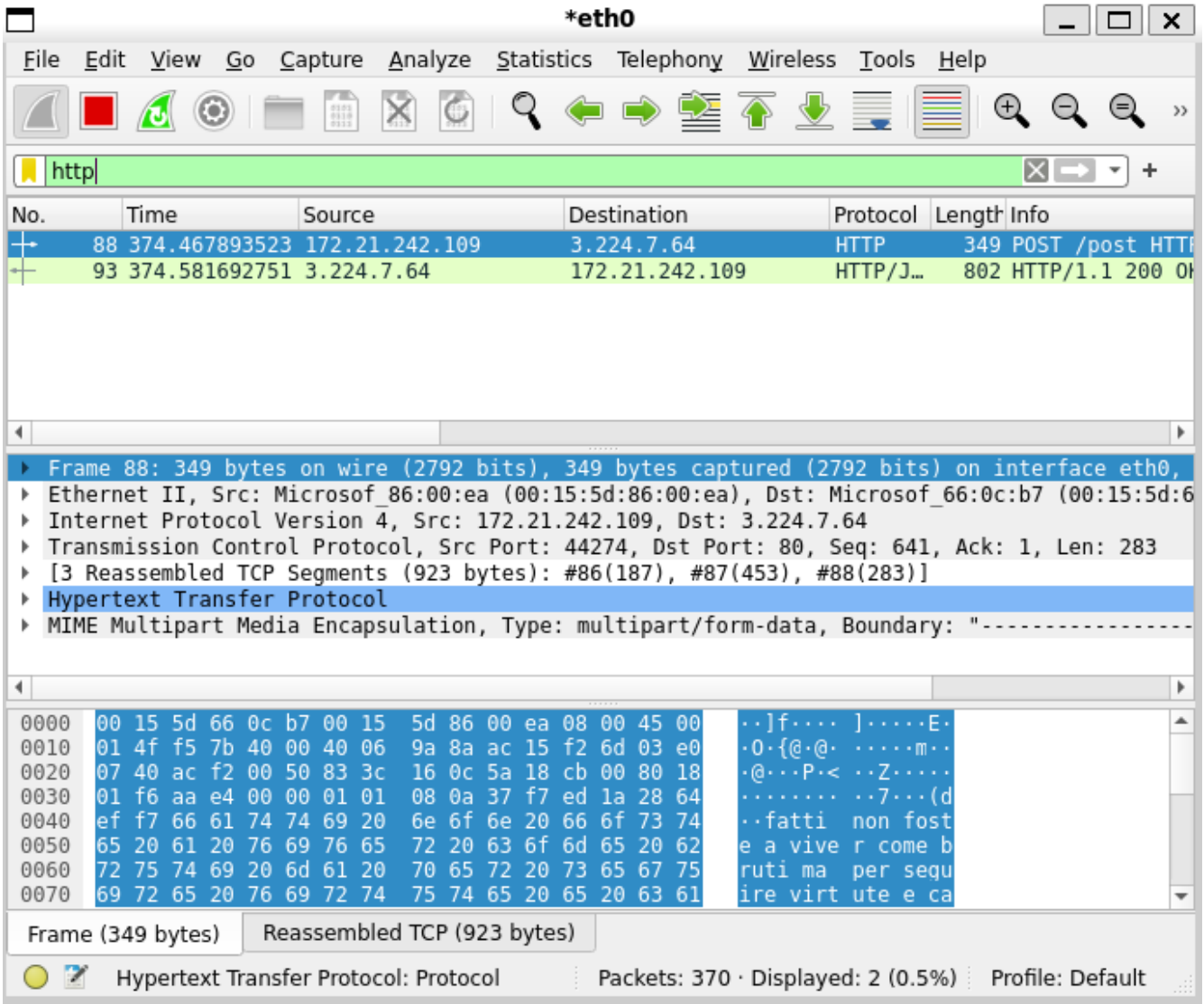
Il pannello dei dettagli del pacchetto è popolato per mezzo di vari *dissector*, ciascuno decodifica la parte di uno specifico protocollo, affidando la decodifica del protocollo incapsulato al relativo dissector.

Il pannello dei dettagli è in realtà un albero, in quando gli elementi possono essere espansi, per esempio per visualizzare i dettagli della intestazione di un certo livello. L'elemento selezionato viene inoltre selezionato nel pannello dei byte del pacchetto.

Nel seguito si assumerà di aver catturato i pacchetti relativi al seguente comando (mostrato durante la esercitazione HTTP):

```
curl --form "titolo=dante" --form "file1=@bruti.txt" --form
"file2=@bruti.txt;type=text/plain" --form "text=<bruti.txt"
http://httpbin.org/post
```

Usando il filtro `http`, si possono facilmente trovare la richiesta e la risposta.



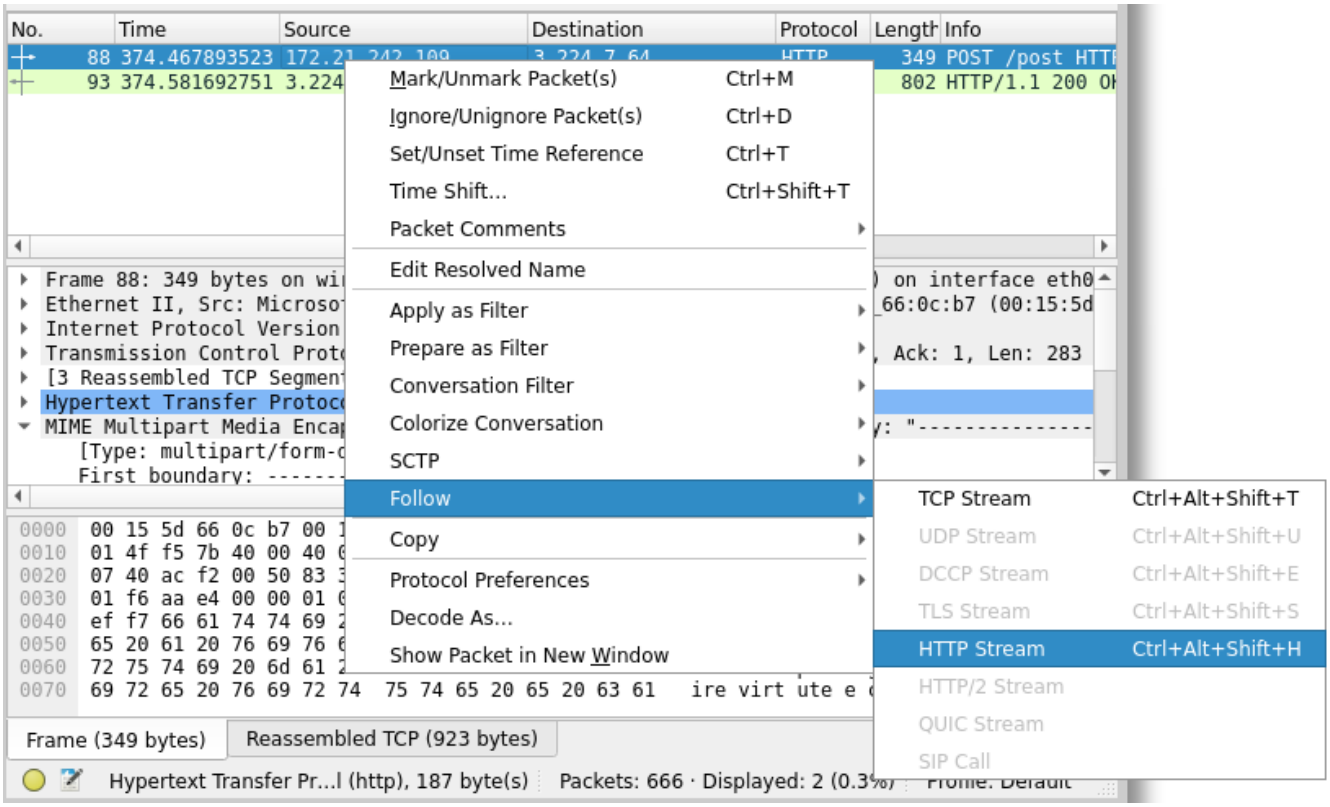
Nel pannello dei dettagli, osservare:

- il protocollo Ethernet (a livello di collegamento)
- il protocollo IP (a livello di rete), verificando che l'indirizzo sorgente e destinazione siano quello della macchina locale (trovare con `ip addr`) e quello di httpbin.org (trovare con `nslookup` oppure `dig`)
- il protocollo TCP (a livello di trasporto), verificano che la porta di destinazione è la 80
- la richiesta HTTP è stata ottenuta riassemblando più segmenti, nell'esempio 3, il cui payload complessivo è stato analizzato per ottenere la richiesta HTTP
- la richiesta HTTP è stata scomposta nella intestazione e nel corpo. Guardando la intestazione, osservare tutti i campi di intestazione, incluso quello che specifica il tipo del corpo della richiesta come `multipart/form-data` e definisce il delimitatore (boundary). Osservare anche fatto Wireshark ha generato l'URL completa ottenuta combinando path e host, nonché ci fornisce un link alla risposta.

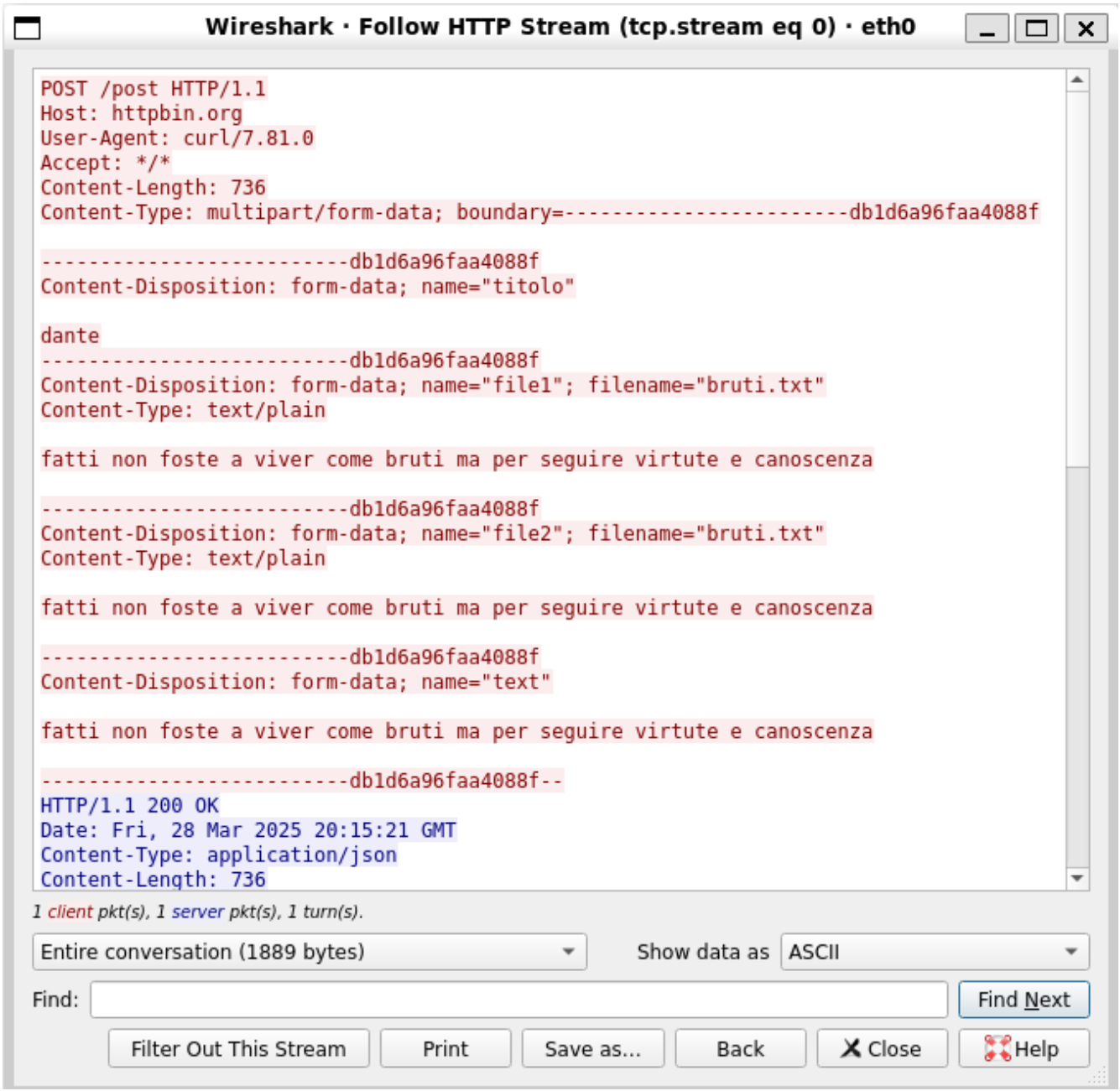
Notare che quando si opera a livello applicativo sono mostrati i byte prodotti dal riassemblamento dei segmenti TCP.

Per la risposta valgono considerazioni analoghe, ma attenzione che mittente e destinatario sono invertiti in molte intestazioni.

Premendo col tasto destro del mouse su un pacchetto a HTTP, selezione *follow/HTTP stream*.



In questo modo è possibile vedere agevolmente la richiesta http e la relativa risposta.



Quando viene chiusa la finestra, nella finestra principale si troverà un filtro tipo `tcp.stream eq N` dove *N* è il numero del flusso TCP (a partire da 0) che è stato utilizzato da quel flusso http.

Attenzione ai filtri: in presenza di un filtro eventuali collegamenti tra richiesta e risposta potrebbero non essere seguiti, se il pacchetto non è stato escluso dai filtri.