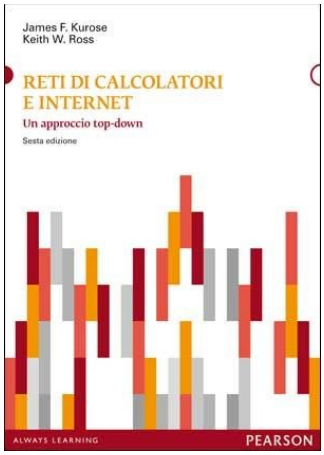
Laboratorio Wireshark: Introduzione



"Dimmi e io dimentico. Mostrami e io ricordo. Coinvolgimi e io comprendo."
Proverbio cinese

La comprensione personale dei protocolli di rete può essere approfondita vedendoli in azione e provandoli, osservando la sequenza di messaggi scambiati tra due entità di protocollo, approfondendo i dettagli delle operazioni e forzando i protocolli a effettuare determinate azioni per verificarne le conseguenze. Tutto questo può essere fatto o in scenari simulati o in un ambiente reale come Internet. Le applet Java del libro di testo scelgono il primo approccio. Nelle esercitazioni con Wireshark intraprenderemo invece il secondo approccio. Lancerete applicazioni di rete in diversi scenari e osserverete i protocolli di rete nel vostro calcolatore, interagendo e scambiando messaggi con l'entità di protocollo in esecuzione da qualche parte in Internet. Pertanto, voi e il vostro computer sarete parte integrante di queste esercitazioni dal vivo. Osserverete e imparerete, facendo.

Lo strumento di base per osservare i messaggi scambiati tra entità di protocollo in esecuzione è chiamato **packet sniffer**. Come suggerisce il nome, esso copia passivamente (ossia "sniffa, annusa") i messaggi che vengono inviati e ricevuti dal vostro computer; inoltre, mostra i contenuti dei vari campi di protocollo e dei messaggi catturati. Un packet sniffer è una entità passiva: osserva i messaggi inviati e ricevuti dalle applicazioni e dai protocolli in esecuzione sul vostro computer, ma non manda mai egli stesso dei pacchetti. Allo stesso modo, i pacchetti che riceve non sono mai stati inviati esplicitamente al packet sniffer. Al contrario, il packet sniffer riceve una *copia* dei pacchetti che sono spediti/ricevuti dalle applicazioni e dai protocolli in esecuzione.

La Figura 1 mostra la struttura di un packet sniffer. Sulla destra ci sono i protocolli (in questo caso, i protocolli di Internet) e le applicazioni (come i browser web o i client FTP) che normalmente girano su un computer. Il packet sniffer, mostrato all'interno del rettangolo tratteggiato, è una aggiunta al software usuale di un computer, e consiste di due parti. La **libreria di cattura dei pacchetti** riceve una copia di ogni frame a livello di collegamento che viene inviato o ricevuto dal vostro computer. Ricordate che, come discusso nella Sezione 1.5 del libro di testo (Figura 1.24[1]), i messaggi scambiati dai protocolli di livello superiore come HTTP, FTP, TCP, UDP, DNS o IP vengono tutti alla fine incapsulati in frame a livello di collegamento che sono trasmessi sul dispositivo fisico, quale ad esempio un cavo Ethernet. In Figura 1 si suppone che il dispositivo fisico sia proprio Ethernet, e così tutti i protocolli di livello superiore sono eventualmente incapsulati all'interno di un frame Ethernet. Catturare tutti i frame a livello di collegamento ci consente quindi di ottenere tutti i messaggi ricevuti o inviati da tutti i protocolli e le applicazioni in esecuzione sul computer.

La seconda componente di un packet sniffer è un **analizzatore di pacchetti**, che visualizza il contenuto di tutti i campi all'interno dei messaggi. A questo scopo, l'analizzatore di pacchetti deve "comprendere" la struttura di tutti i messaggi scambiati dai protocolli. Per esempio, supponete che siamo interessati a visualizzare i vari campi nei messaggi scambiati dal protocollo HTTP. L'analizzatore di pacchetti comprende il formato dei frame Ethernet, e così può identificare il datagramma IP presente all'interno del frame. Comprende anche il formato del datagramma IP, così

1 Il numero della figura si riferisce alla sesta edizione italiana del libro.

può estrarre il segmento TCP all'interno del datagramma IP. Inoltre, comprende la struttura del

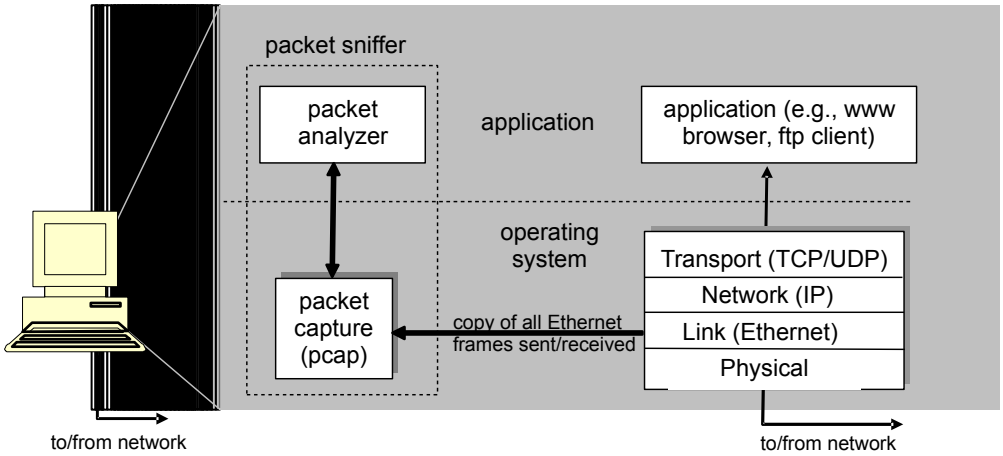


Figura 1: Struttura di un packet sniffer

segmento TCP, così può estrarre il messaggio HTTP contenuto nel segmento TCP. Infine, comprende il protocollo HTTP e così, per esempio, sa che i primi byte di un messaggio HTTP conterranno la stringa "GET", "POST" o "HEAD", come mostrato in Figure 2.8 nel libro di testo.

Useremo il packet sniffer Wireshark [http://www.wireshark.org], che ci consente di visualizzare i contenuti di tutti i messaggi inviati/ricevuti dai protocolli a differenti livelli della pila protocollare. (Dal punto di vista squisitamente tecnico, Wireshark è un analizzatore di pacchetti, che usa una libreria di cattura dei pacchetti presente già nel vostro computer). Wireshark è un software libero che gira su Windows, Linux/Unix e Mac OS. È un analizzatore di pacchetti ideale per il nostro laboratorio – è stabile, ha una vasta base di utenti e una buona documentazione in inglese (che include una guida per l'utente [http://www.wireshark.org/docs/wsug_html_chunked/], le pagine di manuale [http://www.wireshark.org/docs/man-pages/], e una FAQ dettagliata [http://www.wireshark.org/faq.htm]), varie funzionalità che includono la capacità di analizzare centinaia di protocolli, e una interfaccia utente ben congegnata. Opera su computer che utilizzano connessioni Ethernet, Token Ring, FDDI, seriali (PPP e SLIP), wireless basate su protocollo 802.11, e ATM (se il sistema operativo sul quale è in esecuzione lo consente).

Scaricare Wireshark

Per eseguire Wireshark avrete bisogno di accedere a un computer che supporti sia Wireshark sia le librerie di cattura dei pacchetti *libpcap* o *WinPCap*. La libreria *libpcap* verrà installata per voi assieme a Wireshark, se non è già presente.

Per quanto riguarda il sistema operativo Linux, Wireshark è incluso in pressoché qualunque distribuzione, per cui è sufficiente installarlo come si fa per tutto l'altro software. Per gli altri sistemi operativi, è possibile scaricare il codice eseguibile di Wireshark dalla pagina http://www.wireshark.org/download.html.

Si consiglia di scaricare anche la guida utente e di consultare le FAQ, che contengono un buon numero di consigli e informazioni varie, particolarmente utili se si hanno problemi nell'installazione o nell'esecuzione di Wireshark.

Eseguire Wireshark

Quando eseguite il programma Wireshark, ottenete una finestra di partenza come sotto:

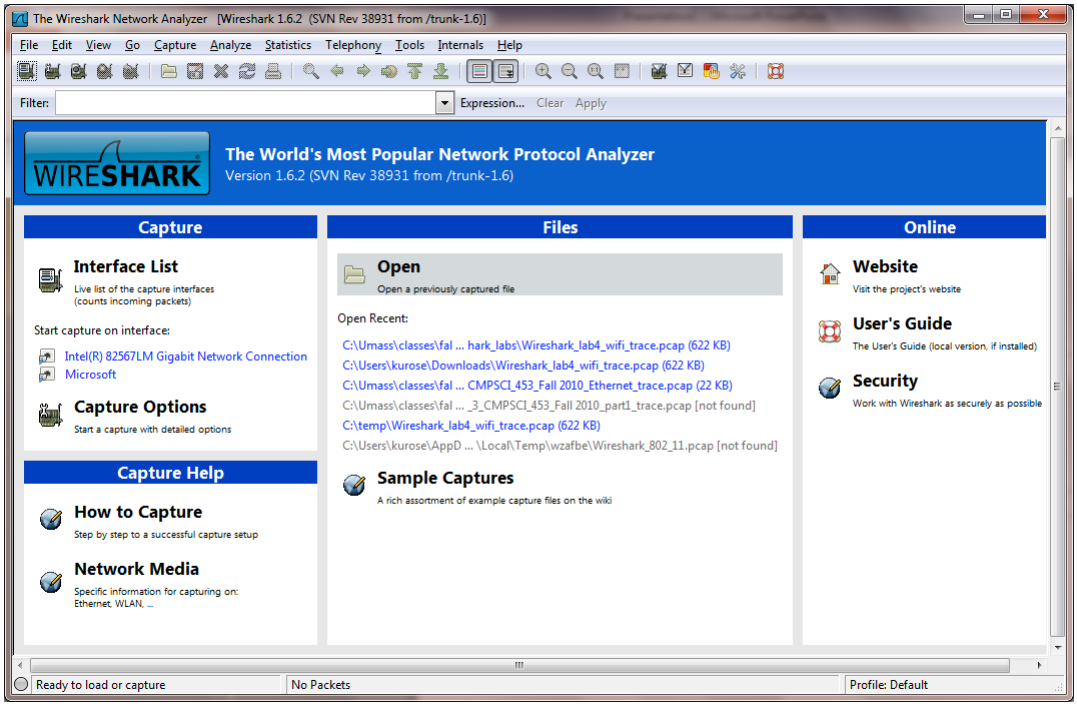


Figura 2: Schermo iniziale di Wireshark

Date uno sguardo al lato in alto a sinistra dello schermo, e trovere una “Interface list”. Questa è la lista delle interfacce di rete del vostro computer. Una volta selezionata una interfaccia, Wireshark catturerà tutti i pacchetti su di essa. Nell'esempio di sopra, c'è una interfaccia Ethernet (*Gigabit Network Connection*) e una interfaccia wireless (*Microsoft*). Su i sistemi Linux, le interfacce hanno tradizionalmente i nomi *eth0*, *eth1*, etc..., mentre *lo* (loopback) è una speciale interfaccia per comunicazioni all'interno dello stesso computer. Se cliccate su una di queste interfacce per far partire la cattura, apparirà una schermata come quella in Figura , che mostra informazioni sui pacchetti in corso di cattura. Potete interrompere la cattura using il menù *Capture* e selezionando *Stop*.

L'interfaccia di Wireshark ha cinque componenti principali:

- Il **menù dei comandi** è un tipico menù a discesa collocato in cima alla finestra. Di principale interesse per noi sono i menù File e Capture. Il menù File vi consente di salvare i dati catturati, aprire un file contenente dati precedentemente catturati e uscire da Wireshark. Il menù Capture vi consente di iniziare la cattura dei pacchetti.
- La **finestra di elenco dei pacchetti** mostra un riassunto di una linea per ogni pacchetto catturato, incluso il numero di pacchetto (che è un numero assegnato da Wireshark; *non* è contenuto nella intestazione di alcun protocollo), il tempo al quale il pacchetto è stato catturato, gli indirizzi sorgente e destinazione, il tipo di protocollo, e informazioni specifiche del protocollo contenuto nel pacchetto. L'elenco può essere ordinato sulla base di una di queste informazioni, semplicemente cliccando sul nome della colonna. Il campo con il tipo di protocollo mostra il protocollo di livello più alto contenuto nel pacchetto, ovvero il protocollo che è la sorgente o il destinatario finale per il pacchetto.
- La **finestra di dettaglio delle intestazioni** mostra dettagli sul pacchetto selezionato (evidenziato) nell'elenco dei pacchetti catturati. (Per selezionare un pacchetto, piazzare il cursore sopra la linea contenente le informazioni riassuntive sul pacchetto e fare click con il tasto sinistro del mouse). I dettagli includono informazioni sul frame Ethernet (supponendo che il pacchetto sia stato inviato/ricevuto su una interfaccia Ethernet) e il datagramma IP

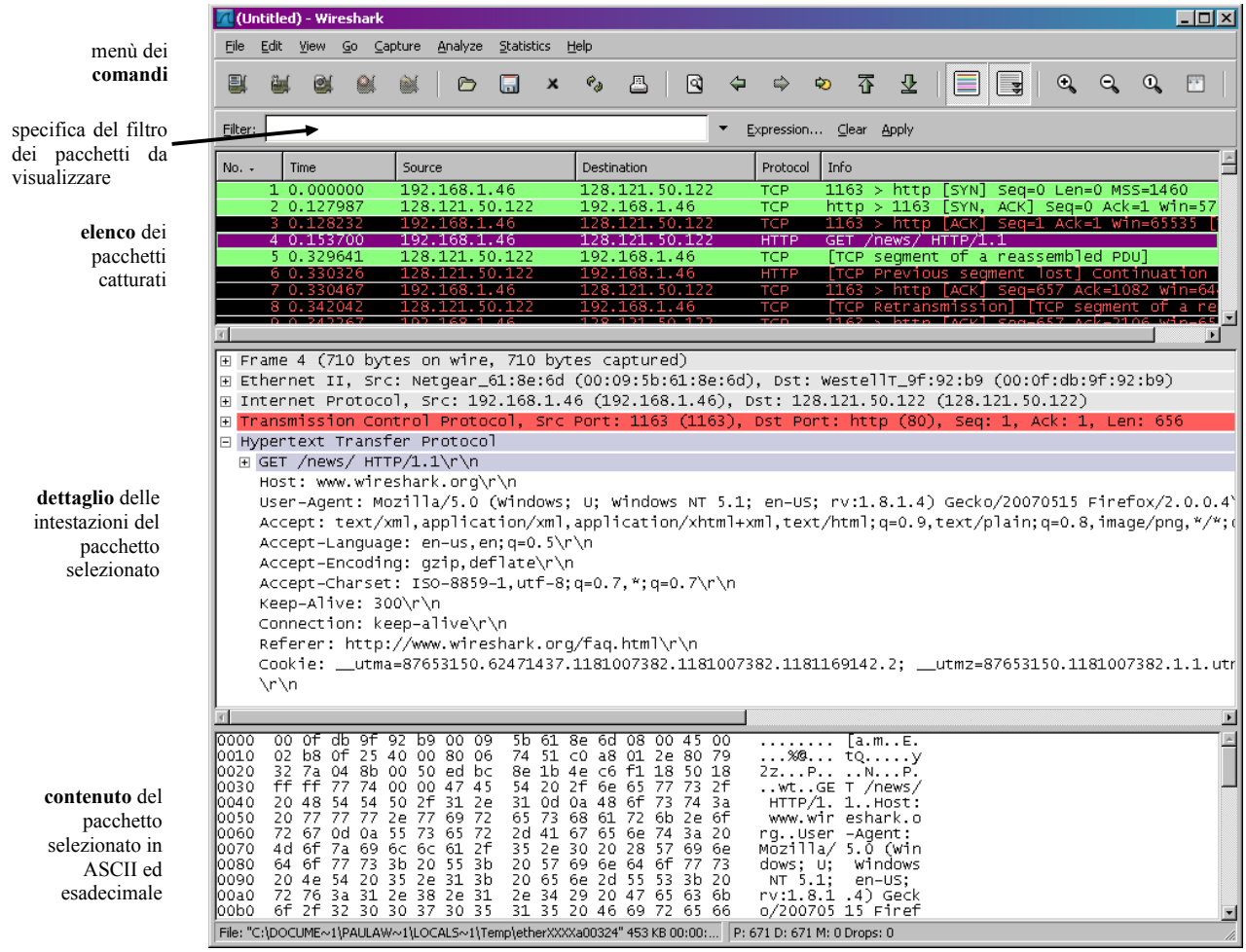


Figura 3: Interfaccia utente grafica di Wireshark, durante la cattura e analisi dei pacchetti

contenuti nel pacchetto. La quantità di informazioni visualizzate sui livelli Ethernet e IP può essere massimizzata o minimizzata cliccando sul riquadro più-o-meno alla sinistra della linea riservata al frame Ethernet o al datagramma IP nella finestra di dettaglio. Se il pacchetto è stato trasportato sopra TCP o UDP, verranno visualizzate anche informazioni sul segmento TCP o UDP, che possono essere espanse o minimizzate in maniera analoga. Infine, sono forniti anche i dettagli sul protocollo di livello superiore che ha inviato o ricevuto il pacchetto.

- La **finestra di contenuto del pacchetto** mostra l'intero contenuto del frame catturato, sia in forma esadecimale che ASCII.
- Verso la cima della finestra di Wireshark, è presente il campo per specificare un **filtro sui pacchetti da visualizzare**, all'interno del quale è possibile digitare un nome di protocollo o altre informazioni per *filtrare* i pacchetti da visualizzare nell'elenco dei pacchetti catturati (e quindi anche nelle finestre del dettaglio e dei contenuti). Nell'esempio che segue, utilizzeremo il filtro per istruire Wireshark a nascondere tutti i pacchetti, ad eccezione di quelli che corrispondono a messaggi HTTP.

Un giro di prova con Wireshark

La maniera migliore di imparare un nuovo software è quello di provarlo! Assumeremo che il vostro computer sia collegato a Internet attraverso una interfaccia Ethernet. Fate quanto segue:

1. Lanciate il vostro browser preferito, che visualizzerà la homepage da voi scelta.

2. Fate partire Wireshark. Vedrete inizialmente una finestra simile a quella in Figura 2. Wireshark non ha ancora iniziato a catturare i pacchetti.
3. Per iniziare la cattura dei pacchetti, selezionare *Capture* dal menù a discesa e quindi selezionare *Interfaces*. Questo causerà la visualizzazione della finestra "Wireshark: Capture Interfaces", come mostrato in Figura 4.

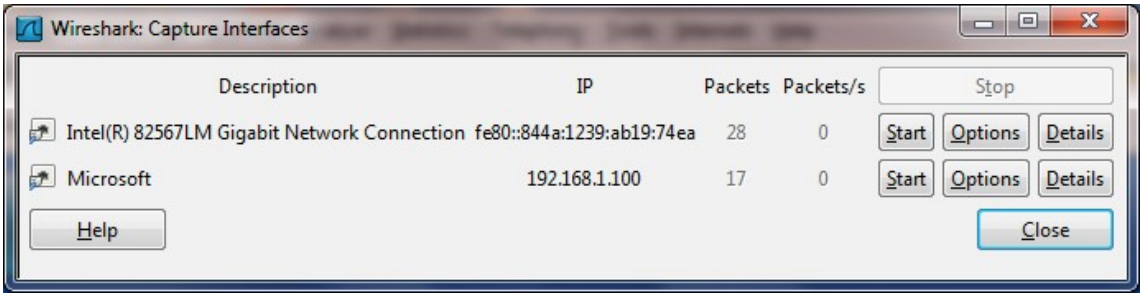


Figura 4: Finestra Wireshark: Capture Interface

4. Vedrete una lista di interfacce di rete presenti sul vostro computer, assieme ad un conteggio dei pacchetti che sono stati osservati su quella interfaccia fino ad ora. Cliccare Start per l'interfaccia sulla quale volete iniziare la cattura (nel caso in figura la Gigabit Ethernet Connection, su una macchina Linux probailmente eth0 o eth1). La cattura dei paccheti inizierà subito – Wireshark sta adesso catturando tutti i pacchetti inviati e ricevuti dal vostro computer!
5. Una volta iniziata la cattura dei pacchetti, apparirà una finestra riassuntiva sulla operazione di cattura, come quella mostrata in Figura 3. Dal menù *Capture*, selezionando *Stop* è possibile interrompere la cattura. Ma non fatelo per adesso, catturiamo prima qualche pacchetto interessante. Per far ciò, genereremo un po' di traffico di rete. Facciamolo usando un browser web, che utilizzerà il protocollo HTTP (lo vedremo in dettaglio durante il corso) per scaricare contenuti da un sito web.
6. Mentre Wireshark è in esecuzione, immettete la URL

   http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

   per visualizzare la corrispondente pagina nel vostro browser.

ATTENZIONE!!
Se state seguendo queste istruzioni dall'aula informatica, rimpiazzate tutte le occorrenze di "gaia.cs.umass.edu" con "goemon".

   Per poter visualizzare la pagina, il browser contatterà il server HTTP di nome gaia.cs.umass.edu e scambierà con esso dei messaggi HTTP allo scopo di scaricare la pagina, come discusso nella sezione 2.2 del libro di testo. I frame Ethernet contenenti i messaggi HTTP (assieme a tutti gli altri frame che eventualmente passino dall'interfaccia di rete) verranno catturati da Wireshark.
7. Dopo che il browser ha visualizzato la pagina INTRO-wire1.html (si tratta di una semplice riga di congratulazioni), interrompete la cattura dei pacchetti selezionando Stop nella finestra riassuntiva di cattura. Questo causerà la scomparsa della finestra di Figura 5 e la comparsa della finestra principale di Wireshark, simile a quella in Figura 3. Adesso avete dei pacchetti catturati dal vivo che contengono tutti i messaggi scambiati tra il vostro computer ed altre entità di rete! Lo scambio di messaggi HTTP col server web di gaia.cs.umass.edu dovrebbero apparire da qualche parte nell'elenco di pacchetti catturati. Ma ci saranno molti altri tipi di pacchetti visualizzati contemporaneamente (guardata, per esempio, i differenti

tipi di protocollo visualizzati nella colonna *Protocol* della Figura 3). Sebbene la sola azione effettuata sia stata quella di visualizzare una pagina web, ci sono evidentemente molti altri protocolli in esecuzione sul computer che sono invisibili all'utente. Impareremo qualcosa circa questi protocolli mano a mano che progrediremo attraverso il libro di testo! Per adesso, basta che siate cosciente del fatto che c'è molto più in esecuzione di quello che si vede.

8. Digitate "http" (senza le virgolette, e in minuscolo – tutti i nomi di protocollo sono in minuscolo in Wireshark) nel campo *Filter* in alto nella finestra principale di Wireshark. Quindi, selezionate *Apply* (alla destra di dove avete immesso "http"). A seguito di questa azione, la finesta con l'elenco dei pacchetti visualizzerà solo i messaggi relativi al protocollo HTTP.

9. Selezionate il primo pacchetto HTTP mostrato nell'elenco (dovrebbe essere un messaggio HTTP che contiene, nella colonna Info, la parola GET seguito dall'URL gaia.cs.umadd.edu che avete immesso nel browser). Quando selezionate il messaggio GET, verranno visualizzate nella finestra di dettaglio le informazioni sulla intestazione del frame Ethernet, datagramma IP, segmento TCP, e messaggio HTTP[2]. Con dei click sulle freccie alla sinistra della finestra dei dettagli, *minimizzate* la quantità di informazioni visualizzate su protocolli Ethernet, IP e TCP. *Massimizzate* invece la quantità di informazioni visualizzate sul protocollo HTTP. La vostra finestra Wireshark dovrebbe adesso somigliare a quella in Figura 5. (Notate, in particolare, le informazioni minimizzate per tutti i protocolli tranne HTTP, e le informazioni espanse per HTTP nella finestra dei dettagli).

10. Uscite da Wireshark.

Congratulazioni! Avete completato la prima esercitazione di laboratorio Wireshark.

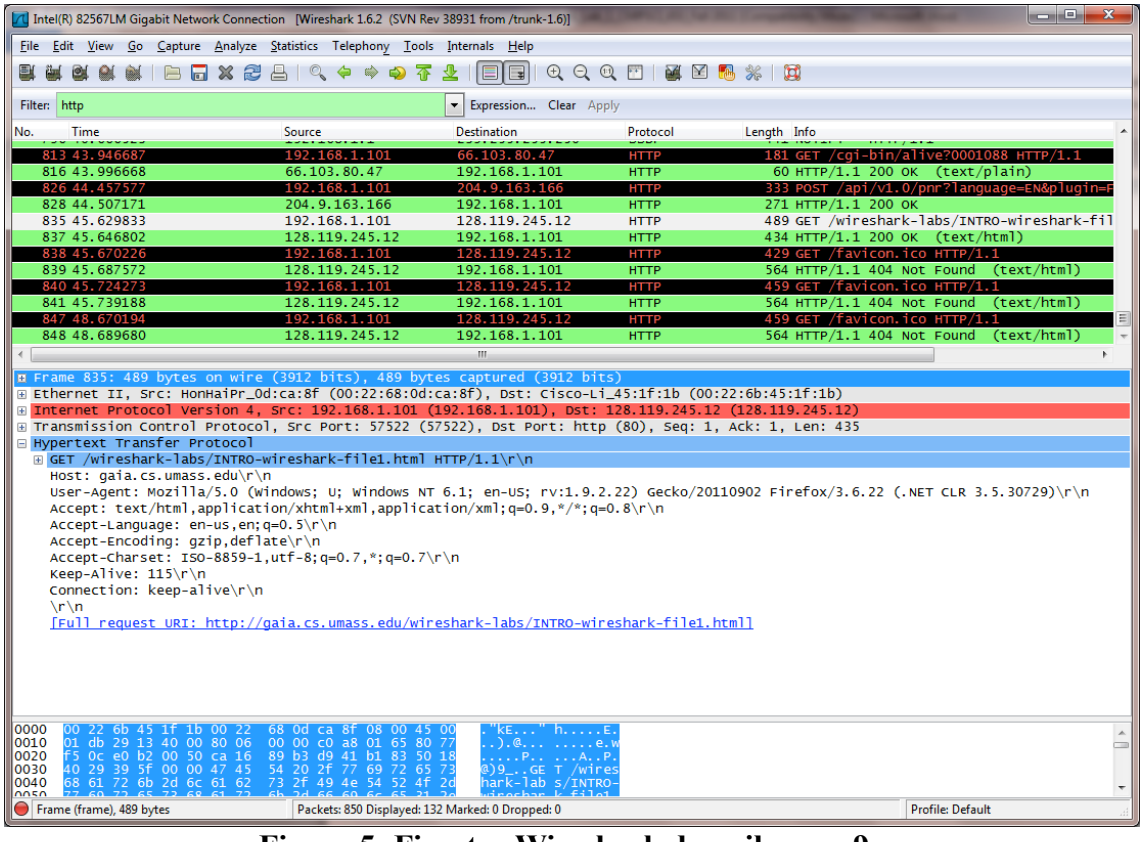


Figura 5: Finestra Wireshark dopo il passo 9

2 Ricordata che il messaggio HTTP GET inviato a gais.cs.umass.edu is contenuto all'interno di un segmento TCP, a sua volta contenuto (incapsulato) in un datagramma IP, che è incapsulato in un frame Ethernet. Se questo processo di incapsulamento non è chiaro, rivedere la sezione 1.5 nel libro di testo.

Cosa consegnare

L'obiettivo di questo primo laboratorio è stato principalmente quello di introdurvi all'uso di Wireshark. Le seguenti domande dimostreranno che siete stati in grado di avviare Wireshark, e che avete esplorato alcune delle sue caratteristiche. Rispondete alle seguenti domande, sulla base della vostra esperienza con Wireshark:

1. Indicate 5 differenti protocolli che appaiono nella colonna dei protocolli nell'elenco dei pacchetti catturati al passo 7 (prima della operazione di filtraggio).
2. Quando tempo è passato tra quando il messaggio HTTP GET è stato inviato a quando il messaggio HTTP OK di risposta è stato ricevuto completamente? (Per default, il valore della colonna Time nell'elenco dei pacchetti è l'ammontare di tempo, in secondi, da quando Wireshark ha iniziato la cattura. Per visualizzare nel campo Time l'ora del giorno, selezionare il menù a discesa *View*, quindi selezionare *Time Display Format* e infine *Time Of Day*).
3. Qual è l'indirizzo Internet di gaia.cs.umass.edu (anche noto come www-net.cs.umass.edu)? Qual è l'indirizzo Internet del vostro computer?
4. Stampa i due messaggi HTTP (GET e OK) di cui al passo 2. Per far questo, prima di tutto contrassegnare i pacchetti da stampare: selezionarli e premere “Ctrl+M” (o cliccare su “*Mark/Unmark Packet*” dal menù “*Edit*”). I pacchetti contrassegnati appaiono con lo sfondo nero. A questo punto selezionare *Print* dal menù a discesa *File*, e successivamente “Marked *Packets Only*”; infine, fare click su “*Print*”. Se non si ha a disposizione una stampante, si può attivare l'opzione “*Output to file*”: verrà generato un file contenente tutto ciò che normalmente viene inviato alla stampante. Il nome del file (che di default è `wireshark.out`) può essere scelto a piacere.