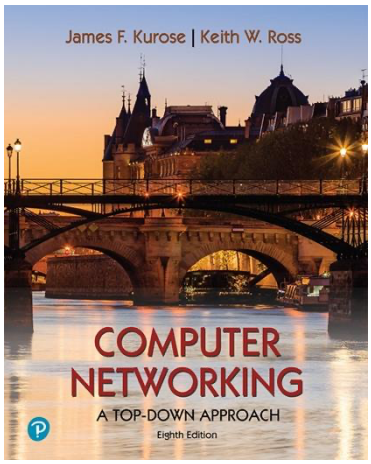
Laboratorio Wireshark: Primi passi versione 8.1



Supplemento 1 *Computer Networking: A Top-Down Approach, 8a ed .,* JF Kurose e KW Ross

"Dimmi e io dimentico. Mostramelo e io ricordo. Coinvolgimi e io capisco. proverbio cinese

© 2005-2021, JF Kurose e KW Ross, Tutti i diritti riservati

La propria comprensione dei protocolli di rete può spesso essere notevolmente approfondita "vedendo i protocolli in azione" e "giocando con i protocolli" - osservando la sequenza di messaggi scambiati tra due entità di protocollo, approfondendo i dettagli del funzionamento del protocollo e facendo in modo che i protocolli eseguire determinate azioni e quindi osservare queste azioni e le loro conseguenze. Questo può essere fatto in scenari simulati o in un ambiente di rete "reale" come Internet. Nei laboratori Wireshark che farai in questo corso, eseguirai varie applicazioni di rete in diversi scenari utilizzando il tuo computer. Osserverai i protocolli di rete nel tuo computer "in azione", interagendo e scambiando messaggi con entità di protocollo in esecuzione altrove in Internet. Pertanto, tu e il tuo computer sarete parte integrante di questi laboratori "dal vivo". Osserverai, e imparerai, facendo.

In questo primo laboratorio di Wireshark, imparerai a conoscere Wireshark e farai alcune semplici acquisizioni e osservazioni di pacchetti.

Lo strumento di base per osservare i messaggi scambiati tra le entità del protocollo in esecuzione è chiamato **packet sniffer** . Come suggerisce il nome, uno sniffer di pacchetti cattura ("annusa") i messaggi inviati/ricevuti da/dal tuo computer; tipicamente memorizzerà e/o visualizzerà anche il contenuto dei vari campi del protocollo in questi messaggi catturati. Uno sniffer di pacchetti stesso è passivo. Osserva i messaggi inviati e ricevuti dalle applicazioni e dai protocolli in esecuzione sul computer, ma non invia mai i pacchetti. Allo stesso modo, i pacchetti ricevuti non sono mai esplicitamente indirizzati allo sniffer di pacchetti. Invece, uno sniffer di pacchetti riceve una *copia* dei pacchetti che vengono inviati/ricevuti dall'applicazione e dai protocolli in esecuzione sulla tua macchina.

La Figura 1 mostra la struttura di uno sniffer di pacchetti. A destra della Figura 1 ci sono i protocolli (in questo caso, i protocolli Internet) e le applicazioni (come un browser Web o un client di posta elettronica) normalmente eseguiti sul computer. Lo sniffer di pacchetti, mostrato all'interno del rettangolo tratteggiato nella Figura 1, è un'aggiunta al normale software del computer ed è composto da due parti. La **libreria di acquisizione dei pacchetti** riceve una copia di ogni frame del livello di collegamento inviato o ricevuto dal

computer su una determinata interfaccia (livello di collegamento, come Ethernet o Wi-Fi). Ricordiamo dalla discussione dalla sezione 1.5 nel testo (Figura 1.24[1]) che i messaggi scambiati da protocolli di livello superiore come HTTP, FTP, TCP, UDP, DNS o IP vengono tutti alla fine incapsulati in frame a livello di collegamento che vengono trasmessi su supporti fisici come un cavo Ethernet o una radio WiFi 802.11. L'acquisizione di tutti i frame a livello di collegamento fornisce quindi tutti i messaggi inviati/ricevuti attraverso il collegamento monitorato da tutti i protocolli e le applicazioni in esecuzione nel computer.

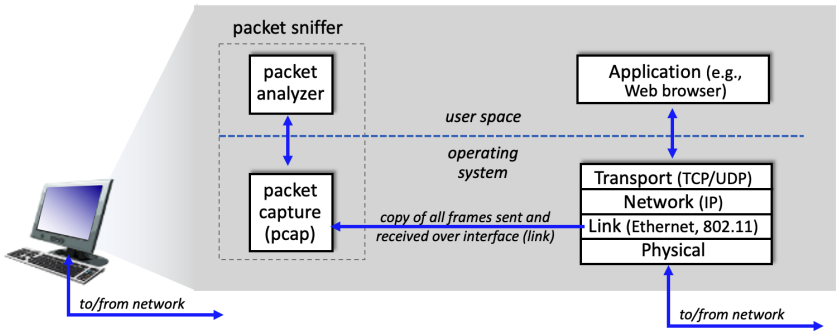


Figura 1: struttura dello sniffer di pacchetti

Il secondo componente di uno sniffer di pacchetti è l'**analizzatore di pacchetti**, che visualizza il contenuto di tutti i campi all'interno di un messaggio di protocollo. Per fare ciò, l'analizzatore di pacchetti deve "comprendere" la struttura di tutti i messaggi scambiati dai protocolli. Ad esempio, supponiamo di essere interessati a visualizzare i vari campi nei messaggi scambiati dal protocollo HTTP in Figura 1. L'analizzatore di pacchetti comprende il formato dei frame Ethernet e quindi può identificare il datagramma IP all'interno di un frame Ethernet. Comprende anche il formato del datagramma IP, in modo da poter estrarre il segmento TCP all'interno del datagramma IP. Infine, comprende la struttura del segmento TCP, quindi può estrarre il messaggio HTTP contenuto nel segmento TCP. Infine, comprende il protocollo HTTP e quindi, ad esempio, sa che i primi byte di un messaggio HTTP conterranno la stringa "GET", "POST" o "HEAD", come mostrato nella Figura 2.8 nel testo.
Useremo lo sniffer di pacchetti Wireshark [http://www.wireshark.org/] per questi laboratori, permettendoci di visualizzare il contenuto dei messaggi inviati/ricevuti dai protocolli a diversi livelli dello stack del protocollo. (Tecnicamente parlando, Wireshark è un analizzatore di pacchetti che utilizza una libreria di acquisizione di pacchetti nel computer. Inoltre, tecnicamente parlando, Wireshark acquisisce frame a livello di collegamento come mostrato nella Figura 1, ma utilizza il termine generico "pacchetto" per fare riferimento a livello di collegamento frame, datagrammi a livello di rete, segmenti a livello di trasporto e messaggi a livello di applicazione, quindi qui useremo il termine "pacchetto" meno preciso per seguire la convenzione di Wireshark). Wireshark è un

[1]I riferimenti a figure e sezioni si riferiscono all'ottava edizione del nostro testo, *Computer Networks, A Top-down Approach, 8 h ed., JF Kurose e KW Ross, Addison-Wesley/Pearson, 2020.* Il sito web dei nostri autori per questo libro è http://gaia.cs.umass.edu/kurose_ross Qui troverai molto materiale aperto interessante.

analizzatore di protocolli di rete gratuito che funziona su computer Windows, Mac e Linux/Unix. È un analizzatore di pacchetti ideale per i nostri laboratori: è stabile, ha un'ampia base di utenti e un supporto ben documentato che include una guida per l'utente (http://www.wireshark.org/docs/wsug_html_chunked/), pagine man (http://www.wireshark.org/docs/man-pages/), e una FAQ dettagliata (http://www.wireshark.org/faq.html), ricche funzionalità che includono la capacità di analizzare centinaia di protocolli e un'interfaccia utente ben progettata. Funziona su computer che utilizzano LAN wireless Ethernet, seriali (PPP), 802.11 (WiFi) e molte altre tecnologie a livello di collegamento.

Ottenere Wireshark

Per eseguire Wireshark, devi avere accesso a un computer che supporti sia Wireshark che la libreria di acquisizione dei pacchetti *libpcap* o *WinPCap* . Il software *libpcap* verrà installato per te, se non è installato nel tuo sistema operativo, quando installi Wireshark. Vedere http://www.wireshark.org/download.html per un elenco dei sistemi operativi supportati e dei siti di download.

Scarica e installa il software Wireshark:

- Vai su http://www.wireshark.org/download.html e scarica e installa il binario di Wireshark per il tuo computer.

Le FAQ di Wireshark contengono una serie di suggerimenti utili e informazioni interessanti, in particolare in caso di problemi con l'installazione o l'esecuzione di Wireshark.

Esecuzione di Wireshark

Quando esegui il programma Wireshark, otterrai una schermata di avvio simile alla schermata qui sotto. Diverse versioni di Wireshark avranno schermate di avvio diverse, quindi non farti prendere dal panico se la tua non è esattamente come la schermata qui sotto! La documentazione di Wireshark afferma “Poiché Wireshark funziona su molte piattaforme diverse con molti gestori di finestre diversi, stili diversi applicati e sono utilizzate diverse versioni del toolkit GUI sottostante, lo schermo potrebbe apparire diverso dagli screenshot forniti. Ma poiché non ci sono differenze reali nella funzionalità, questi screenshot dovrebbero essere comunque ben comprensibili.

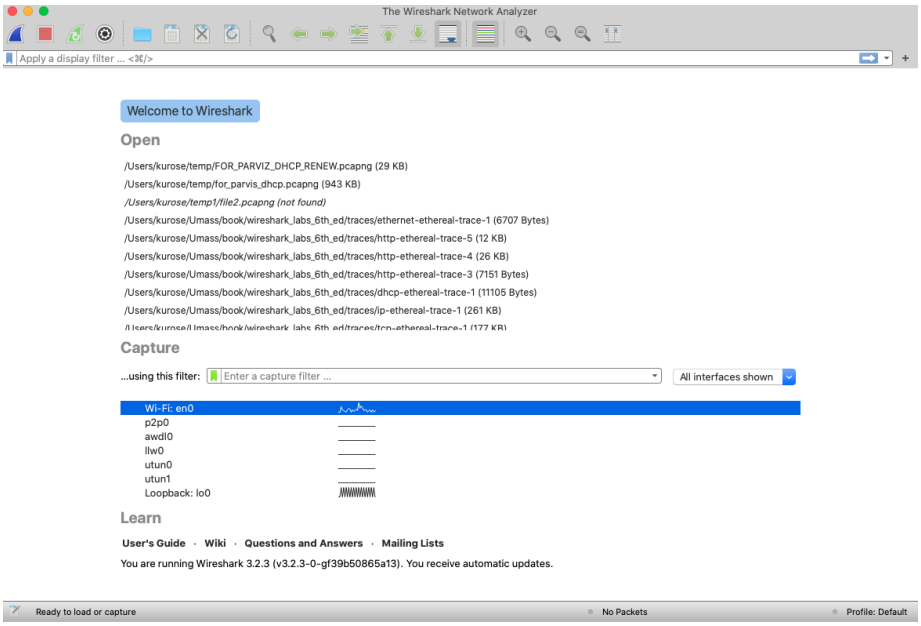


Figura 2: Schermata iniziale di Wireshark

Non c'è molto di interessante su questo schermo. Ma nota che sotto la sezione Capture, c'è un elenco delle cosiddette interfacce. Il computer Mac da cui prendiamo questi screenshot ha una sola interfaccia: "Wi-Fi en0" (ombreggiata in blu nella Figura 2), che è l'interfaccia per l'accesso Wi-Fi. Tutti i pacchetti da/verso questo computer passeranno attraverso l'interfaccia Wi-Fi, quindi è qui che vorremo acquisire i pacchetti. Su un Mac, fai doppio clic su questa interfaccia (o su un altro computer individua l'interfaccia nella pagina di avvio attraverso la quale ottieni la connettività Internet, ad esempio, molto probabilmente un'interfaccia WiFi o Ethernet, e seleziona quell'interfaccia).

Cominciamo a usare Wireshark! Se fai clic su una di queste interfacce per avviare l'acquisizione dei pacchetti (ad esempio, affinché Wireshark inizi a catturare tutti i pacchetti inviati a/da quell'interfaccia), verrà visualizzata una schermata come quella sottostante, che mostra le informazioni sui pacchetti catturati. Una volta avviata l'acquisizione dei pacchetti, è possibile interromperla utilizzando il menu a discesa Capture e selezionando Interrompi (o facendo clic sul pulsante quadrato rosso accanto alla pinna Wireshark nella Figura 2).[2]

[2] Se non sei in grado di eseguire Wireshark, puoi comunque usare il file traccia intro-wireshark-trace-1.pcap. Dopo aver scaricato un file di traccia, puoi caricarlo in Wireshark e visualizzare la traccia utilizzando il menu a discesa *File, scegliendo Apri* , quindi selezionando il file di traccia *intro-wireshark-trace* . La visualizzazione risultante dovrebbe essere simile alle figure 3 e 5. (L'interfaccia utente di Wireshark viene visualizzata in modo leggermente diverso su diversi sistemi operativi e in diverse versioni di Wireshark).

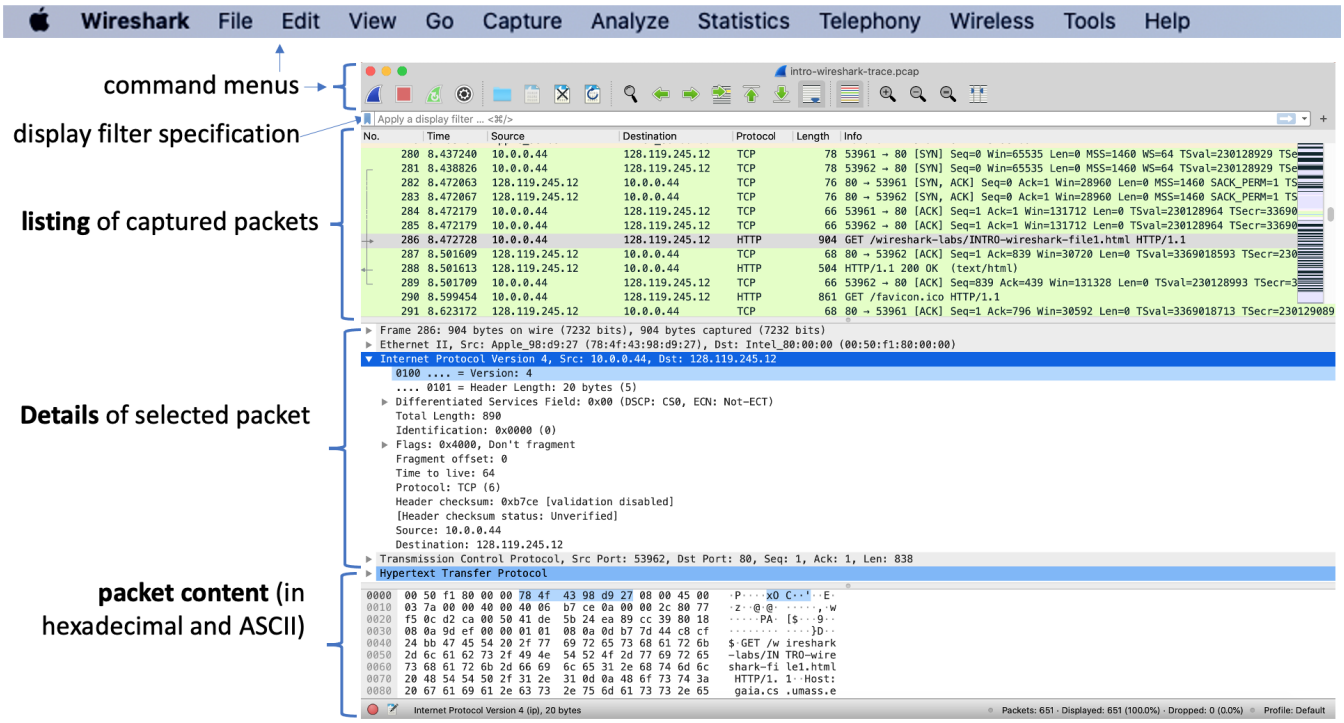


Figura 3: Finestra Wireshark, durante e dopo l'acquisizione

Questo sembra più interessante! L'interfaccia Wireshark ha cinque componenti principali:

- I **menu dei comandi** sono menu a discesa standard situati nella parte superiore della finestra di Wireshark (e su un Mac anche nella parte superiore dello schermo; lo screenshot nella Figura 3 è di un Mac). Di nostro interesse ora sono i menu File e Capture. Il menu File consente di salvare i dati del pacchetto acquisiti o aprire un file contenente i dati del pacchetto acquisiti in precedenza e uscire dall'applicazione Wireshark. Il menu Capture consente di iniziare la cattura dei pacchetti.
- La **finestra di elenco dei pacchetti** visualizza un riepilogo di una riga per ciascun pacchetto catturato, incluso il numero del pacchetto (assegnato da Wireshark; si noti che non si tratta di *un* numero di pacchetto contenuto nell'intestazione di alcun protocollo), l'ora in cui il pacchetto è stato catturato, il gli indirizzi di origine e di destinazione del pacchetto, il tipo di protocollo e le informazioni specifiche del protocollo contenute nel pacchetto. L'elenco dei pacchetti può essere ordinato in base a una qualsiasi di queste categorie facendo clic sul nome di una colonna. Il campo del tipo di protocollo elenca il protocollo di livello più alto che ha inviato o ricevuto questo pacchetto, ovvero il protocollo che è l'origine o il sink finale per questo pacchetto.
- La **finestra dei dettagli dell'intestazione del pacchetto** fornisce dettagli sul pacchetto selezionato (evidenziato) nella finestra dell'elenco dei pacchetti. (Per selezionare un pacchetto nella finestra di elenco dei pacchetti, posizionare il cursore sul riepilogo di una riga del pacchetto nella finestra di elenco dei pacchetti e fare clic con il pulsante sinistro del mouse.). Questi dettagli includono informazioni sul

frame Ethernet (supponendo che il pacchetto sia stato inviato/ricevuto tramite un'interfaccia Ethernet) e il datagramma IP che contiene questo pacchetto. La quantità di dettagli del livello Ethernet e IP visualizzati può essere ampliata o ridotta facendo clic sulle caselle più/meno o sui triangoli rivolti a destra/verso il basso a sinistra del frame Ethernet o della riga del datagramma IP nella finestra dei dettagli del pacchetto. Se il pacchetto è stato trasferito su TCP o UDP, verranno visualizzati anche i dettagli TCP o UDP, che possono essere analogamente espansi o ridotti a icona. Infine, vengono forniti anche i dettagli sul protocollo di livello più alto che ha inviato o ricevuto questo pacchetto.

- La **finestra del contenuto del pacchetto** visualizza l'intero contenuto del frame acquisito, sia in formato ASCII che esadecimale.
- Verso la parte superiore dell'interfaccia utente grafica di Wireshark, c'è il **campo del filtro di visualizzazione dei pacchetti,** in cui è possibile inserire un nome di protocollo o altre informazioni per filtrare le informazioni visualizzate nella finestra di elenco dei pacchetti. Nell'esempio seguente, utilizzeremo il campo del filtro di visualizzazione dei pacchetti per fare in modo che Wireshark nasconda (non visualizzi) i pacchetti ad eccezione di quelli che corrispondono ai messaggi HTTP.

Primi passi con Wireshark

Il modo migliore per conoscere qualsiasi nuovo software è provarlo! Supponiamo che il tuo computer sia connesso a Internet tramite un'interfaccia Ethernet cablata o un'interfaccia Wi-Fi 802.11 wireless. Eseguire le seguenti operazioni:

1. Avvia il tuo browser Web preferito, che visualizzerà la home page selezionata.

2. Avvia il software Wireshark. Inizialmente verrà visualizzata una finestra simile a quella mostrata nella Figura 2. Wireshark non ha ancora iniziato a catturare i pacchetti.

3. Per iniziare l'acquisizione dei pacchetti, selezionare il menu a discesa Acquisisci e selezionare *Interfacce.* Ciò causerà la visualizzazione della finestra "Wireshark: Capture Interfaces" (su un PC) oppure puoi scegliere Opzioni su un Mac. Dovresti vedere un elenco di interfacce, come mostrato nelle Figure 4a (Windows) e 4b (Mac).

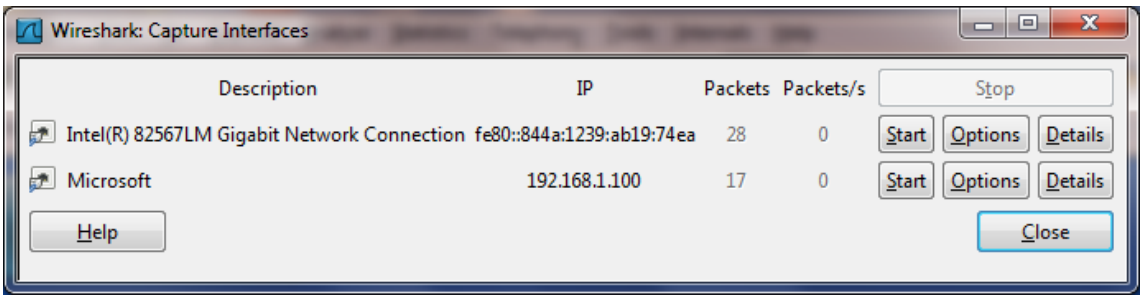


Figura 4a: Finestra dell'interfaccia di Wireshark Capture, su un computer Windows

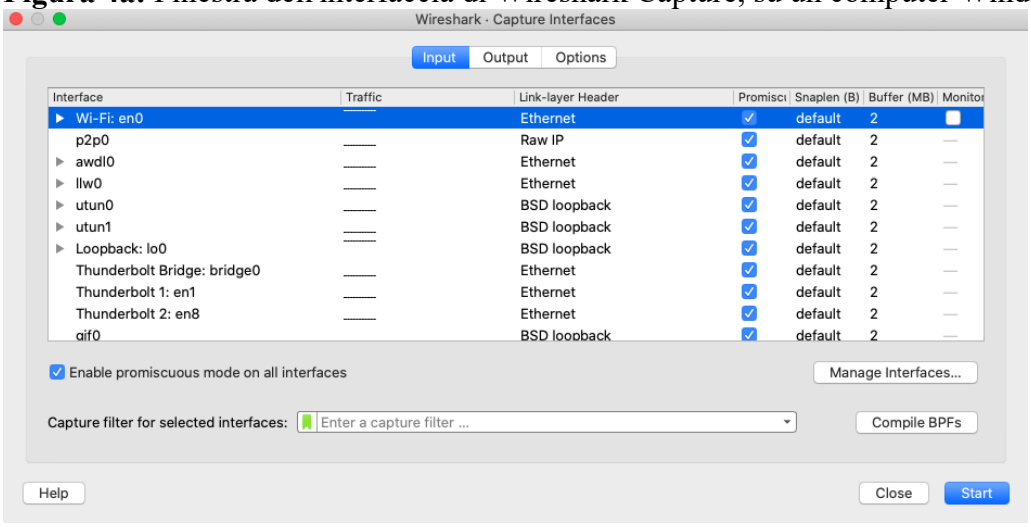


Figura 4b: Finestra dell'interfaccia di Wireshark Capture, su un computer Mac

4. Vedrai un elenco delle interfacce sul tuo computer e un conteggio dei pacchetti che sono stati osservati finora su quell'interfaccia. Su un computer Windows, fare clic su *Avvia* per l'interfaccia su cui si desidera iniziare l'acquisizione dei pacchetti (nel caso della Figura 4a, la connessione di rete Gigabit). Su un computer Windows, seleziona l'interfaccia e fai clic su Avvia nella parte inferiore della finestra). Ora inizierà l'acquisizione dei pacchetti: Wireshark sta ora catturando tutti i pacchetti inviati/ricevuti dal/dal tuo computer!

5. Una volta iniziata la cattura dei pacchetti, apparirà una finestra simile a quella mostrata nella Figura 3. Questa finestra mostra i pacchetti catturati. Selezionando il menu a discesa *Capture* e selezionando *Stop*, oppure facendo clic sul quadratino rosso Stop, è possibile interrompere la cattura dei pacchetti. Ma non interrompere ancora l'acquisizione dei pacchetti. Catturiamo prima alcuni pacchetti interessanti. Per fare ciò, avremo bisogno di generare del traffico di rete. Facciamolo utilizzando un browser web, che utilizzerà il protocollo HTTP che studieremo in dettaglio in classe per scaricare contenuti da un sito web.

6. Mentre Wireshark è in esecuzione, inserisci l'URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html e visualizza quella pagina nel tuo browser. Per visualizzare questa pagina, il tuo browser contatterà il server HTTP su gaia.cs.umass.edu e scambierà messaggi HTTP con il server per scaricare questa pagina, come discusso nella sezione 2.2 del testo. I frame Ethernet o WiFi contenenti questi messaggi HTTP (così come tutti gli altri frame che passano attraverso l'adattatore Ethernet o WiFi) verranno acquisiti da Wireshark.

7. Dopo che il tuo browser ha visualizzato la pagina INTRO-wireshark-file1.html (è una semplice riga di congratulazioni), interrompi l'acquisizione dei pacchetti Wireshark selezionando stop nella finestra di acquisizione Wireshark. La finestra

principale di Wireshark dovrebbe ora apparire simile alla Figura 3. Ora hai i dati dei pacchetti in tempo reale che contengono tutti i messaggi di protocollo scambiati tra il tuo computer e altre entità di rete! Gli scambi di messaggi HTTP con il server Web gaia.cs.umass.edu dovrebbero apparire da qualche parte nell'elenco dei pacchetti catturati. Ma verranno visualizzati anche molti altri tipi di pacchetti (vedere, ad esempio, i diversi tipi di protocollo mostrati nella colonna *Protocollo* in Figura 3). Anche se l'unica azione intrapresa è stata quella di scaricare una pagina web, evidentemente c'erano molti altri protocolli in esecuzione sul tuo computer che non sono stati visti dall'utente. Impareremo molto di più su questi protocolli man mano che avanziamo nel testo!

8. Digita "http" (senza virgolette e *in minuscolo*: tutti i nomi dei protocolli sono in minuscolo in Wireshark e assicurati di premere il tasto Invio/Invio) nella finestra delle specifiche del filtro di visualizzazione nella parte superiore della finestra principale di Wireshark. Quindi seleziona *Applica* (a destra di dove hai inserito "http") o semplicemente premi Invio. In questo modo nella finestra di elenco dei pacchetti verrà visualizzato solo il messaggio HTTP. La Figura 5 di seguito mostra uno screenshot dopo che il filtro http è stato applicato alla finestra di acquisizione dei pacchetti mostrata in precedenza nella Figura 3. Si noti inoltre che nella finestra dei dettagli del pacchetto selezionato, abbiamo scelto di mostrare il contenuto dettagliato per il messaggio dell'applicazione Hypertext Transfer Protocol che è stato trovato all'interno del segmento TCP, cioè all'interno del datagramma IPv4 che era all'interno del frame Ethernet II (WiFi). Concentrarsi sul contenuto a livello di messaggio, segmento, datagramma e frame specifico ci consente di concentrarci solo su ciò che vogliamo guardare (in questo caso i messaggi HTTP).

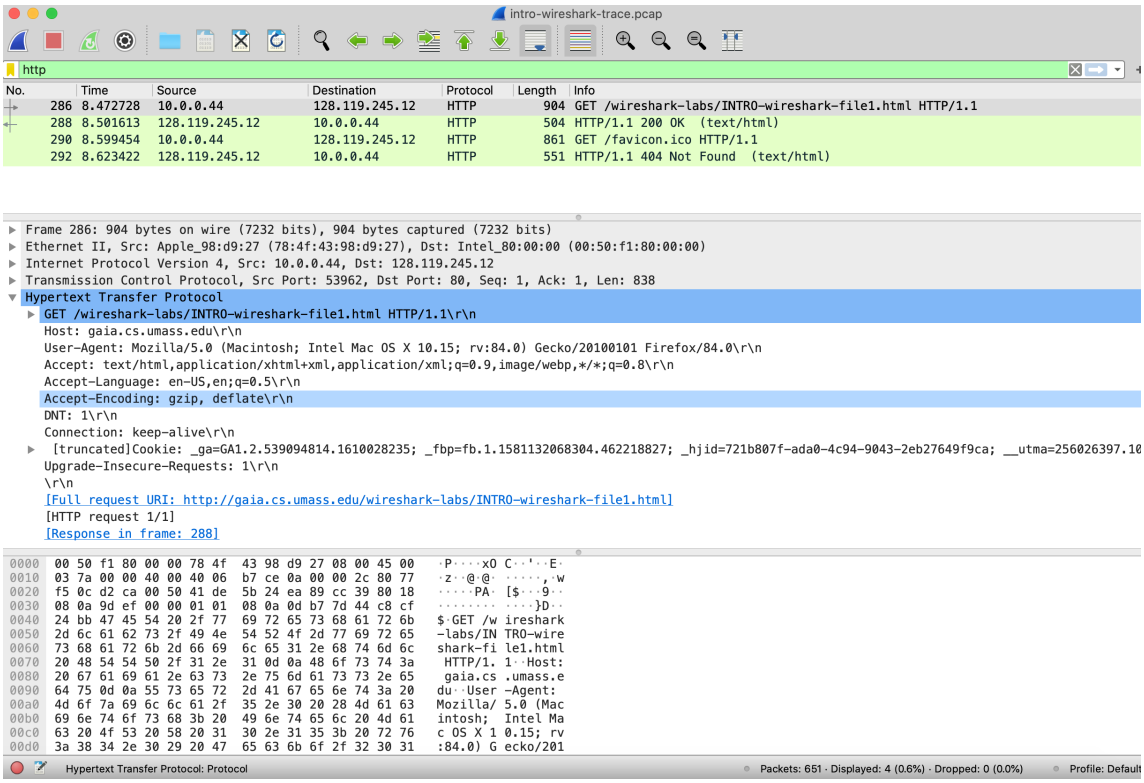


Figura 5: guardando i dettagli del messaggio HTTP che conteneva un GET di http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

9. Trova il messaggio HTTP GET che è stato inviato dal tuo computer al server HTTP gaia.cs.umass.edu. (Cerca un messaggio HTTP GET nella parte "elenco dei pacchetti acquisiti" della finestra Wireshark (vedi Figure 3 e 5) che mostra "GET" seguito dall'URL gaia.cs.umass.edu che hai inserito. Quando selezioni il messaggio HTTP GET, il frame Ethernet, il datagramma IP, il segmento TCP e le informazioni sull'intestazione del messaggio HTTP verranno visualizzati nella finestra dell'intestazione del pacchetto[3]. sul lato sinistro della finestra dei dettagli del pacchetto, *ridurre al minimo* la quantità di informazioni visualizzate relative a frame, Ethernet, protocollo Internet e protocollo di controllo della trasmissione. *Massimizzare* la quantità di informazioni visualizzate sul protocollo HTTP. Il display di Wireshark dovrebbe ora apparire all'incirca come mostrato nella Figura 5. (Notare, in particolare, la quantità minima di informazioni sul protocollo per tutti i protocolli tranne HTTP e la quantità massima di informazioni sul protocollo per HTTP nella finestra dell'intestazione del pacchetto).

10. Esci da Wireshark

[3]Ricordiamo che il messaggio HTTP GET che viene inviato al web server gaia.cs.umass.edu è contenuto all'interno di un segmento TCP, che è contenuto (incapsulato) in un datagramma IP, che è incapsulato in un frame Ethernet. Se questo processo di incapsulamento non è ancora del tutto chiaro, rivedere la sezione 1.5 nel testo

Congratulazioni! Ora hai completato il primo lab!
Ora rispondi alle domande seguenti. Se stai svolgendo questo laboratorio come parte della classe, il tuo insegnante fornirà dettagli su come consegnare i compiti, sia scritti che in un sistema di gestione dell'apprendimento (LMS). Se non sei in grado di eseguire Wireshark su una connessione di rete live o stai rispondendo alle domande tramite un LMS, puoi scaricare un file di traccia dei pacchetti che è stato acquisito durante la procedura descritta sopra.

1. Quali dei seguenti protocolli vengono mostrati come visualizzati (ovvero, sono elencati nella colonna "protocollo" di Wireshark) nel file di traccia: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2?
2. Quanto tempo è trascorso dall'invio del messaggio HTTP GET fino alla ricezione della risposta HTTP OK? (Per impostazione predefinita, il valore della colonna Time nella finestra di elenco dei pacchetti è la quantità di tempo, in secondi, dall'inizio del tracciamento di Wireshark. (Se si desidera visualizzare il campo Time nel formato dell'ora del giorno, selezionare il Wireshark *Visualizza* il menu a discesa, quindi seleziona *Formato di visualizzazione dell'ora*, quindi seleziona *Ora del giorno*.)
3. Qual è l'indirizzo Internet di gaia.cs.umass.edu (noto anche come www-net.cs.umass.edu)? Qual è l'indirizzo Internet del tuo computer o (se stai usando il file di traccia) il computer che ha inviato il messaggio HTTP GET?

Per rispondere alle due domande seguenti, dovrai selezionare il pacchetto TCP contenente la richiesta HTTP GET (suggerimento: questo è il pacchetto numero 286[4]). Lo scopo di queste due domande successive è di familiarizzare con l'utilizzo dei "Dettagli della finestra dei pacchetti selezionati" di Wireshark; vedere la Figura 3. Per fare ciò, fare clic su Packet 286 (lo schermo dovrebbe essere simile alla Figura 3). Per rispondere alla prima domanda di seguito, guarda nella finestra "Dettagli del pacchetto selezionato" attiva il triangolo per HTTP (lo schermo dovrebbe quindi apparire simile alla Figura 5); per la seconda domanda di seguito, dovrai espandere le informazioni sulla parte TCP (Transmission Control Protocol) di questo pacchetto.

4. Espandi le informazioni sul messaggio HTTP nella finestra "Dettagli del pacchetto selezionato" di Wireshark (vedi Figura 3 sopra) in modo da poter vedere i campi nel messaggio di richiesta HTTP GET. Quale tipo di browser Web ha emesso la richiesta HTTP? La risposta viene mostrata all'estremità destra delle informazioni dopo il campo "User-Agent:" nella visualizzazione espansa del messaggio HTTP. [Questo valore di campo nel messaggio HTTP è il modo in cui un server Web apprende quale tipo di browser stai utilizzando.]
    - Firefox, Safari, Microsoft Internet Edge, Altro
5. Espandere le informazioni sul protocollo di controllo della trasmissione per questo pacchetto nella finestra "Dettagli del pacchetto selezionato" di Wireshark (vedere la Figura 3 nel resoconto del laboratorio) in modo da poter vedere i campi nel segmento TCP che trasporta il messaggio HTTP. Qual è il numero della porta di

[4]Ricorda che questo "numero di pacchetto" viene assegnato da Wireshark solo a scopo di identificazione; NON è un numero di pacchetto contenuto in nessun header di pacchetto reale.

destinazione (il numero che segue "Dest Port:" per il segmento TCP contenente la richiesta HTTP) a cui viene inviata questa richiesta HTTP?