	POLO TECNOLOGICO IMPERIESE **LABORATORIO** **DI** **TELECOMUNICAZIONI**	Classe:5 D Data:20/11/2022

Cognome Nome:Moriano Matteo

ESERCITAZIONE: Utilizzo di Wireshark per la ricerca dei pacchetti: HTTP, DNS, ICMP, UDP.

BREVE INTRODUZIONE DELLE CONOSCENZE ACQUISITE NELLA FASE TEORICA DI PREPARAZIONE

MODELLO ISO-OSI:

Il modello ISO/OSI, Open Systems Interconnection è progettato dall'International Organization for Standardization (ISO). Viene utilizzato come modello di riferimento per consentire una comunicazione aperta tra diversi sistemi.
Il modello ISO/OSI è costituito da una pila (o stack) di protocolli attraverso i quali viene ridotta la complessità implementativa di un sistema di comunicazione per il networking.

HTTP:

Hypertext Transfert protocol, è un protocollo per la trasmissione di informazioni attraverso il WEB. Tutti i clients e servers Web devono essere capaci di gestire questo protocollo affinché possano scambiarsi i documenti ipermediali, per questa ragione i Web servers sono anche chiamati HTTP servers.

DNS:

Domain Name System è un protocollo che permette di assegnare un nome alle macchine in modo da individuare l'indirizzo corrispondente, converte i domini in indirizzi IP. Ogni macchina in Internet deve far riferimento a un suo server Dns.

ICMP:

Internet Control Message Protocol, è un protocollo che ha il compito di scambiare informazioni relative allo stato e messaggi di errore, ad esempio i router utilizzano questo protocollo per controllare il mittente del pacchetto.

UDP:

User Datagram Protocol è un protocollo che viene utilizzato in quei servizi che hanno delle esigenze di tempistica così stringenti da preferire una comunicazione con eventuali dati mancanti ad un ritardo nella comunicazione (come ad esempio i sistemi in tempo reale di trasmissione di dati audio-video).

* * * * * *

PROGRAMMA UTILIZZATO

Wireshark

Wireshark è un software che permetti di analizzare il traffico dati generato dal proprio computer e da tutte le periferiche di rete legate al proprio indirizzo IP.
E’ uno strumento di analisi della rete potente e allo stesso tempo versatile: consente di tenere sott’occhio tutto ciò che accade nella propria rete e prendere le adeguate contromisure.

* * * * * *

STRUMENTI, APPARECCHI E COMPONENTI, USATI PER LA PROVA

Per la prova non sono stati utilizzati strumenti o componenti, a parte un computer con il software Wireshark.

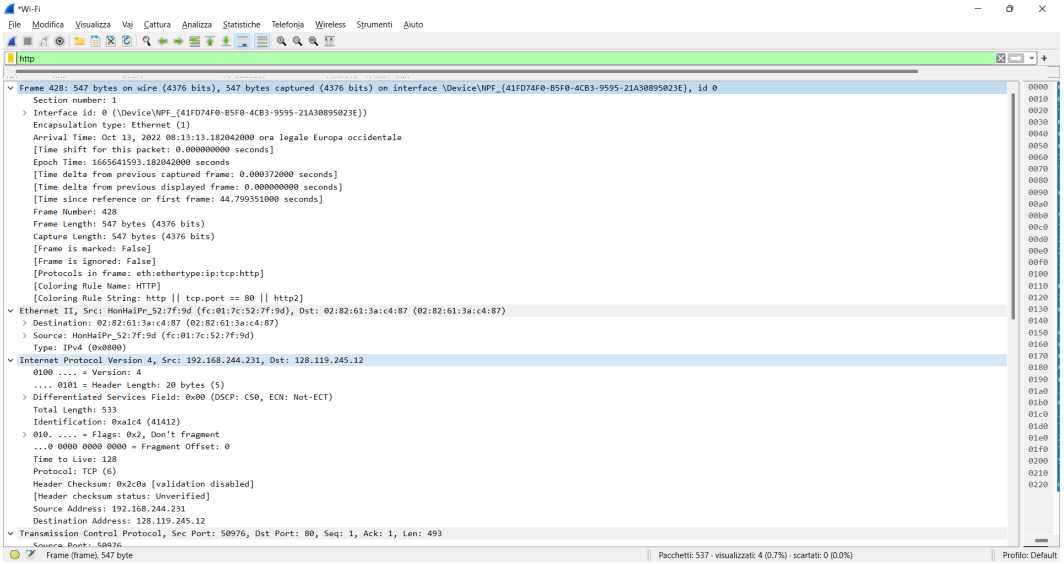
Quantità	Descrizione
1	Computer con software Wireshark

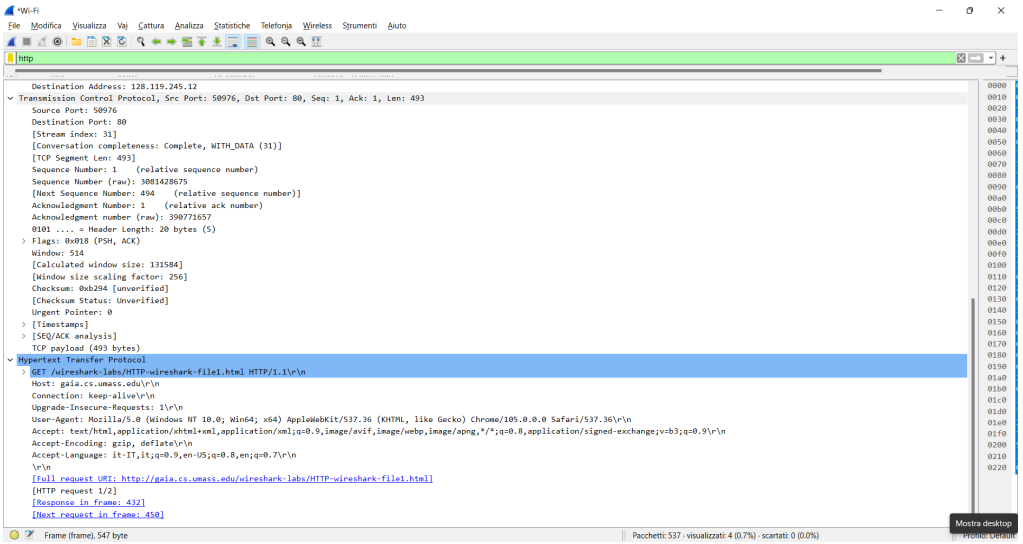
* * * * * *

- - - SVOLGIMENTO RELAZIONE - - -

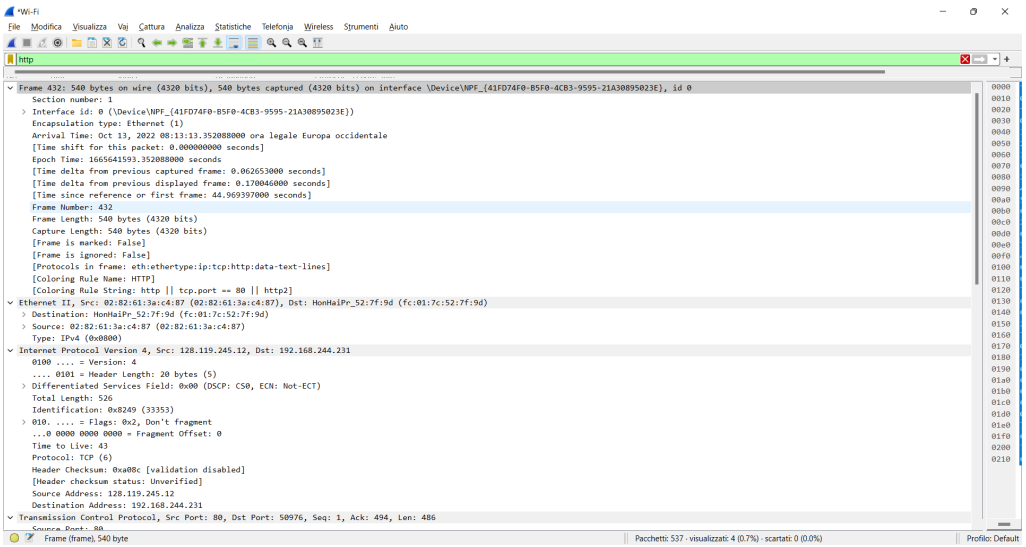
HTTP

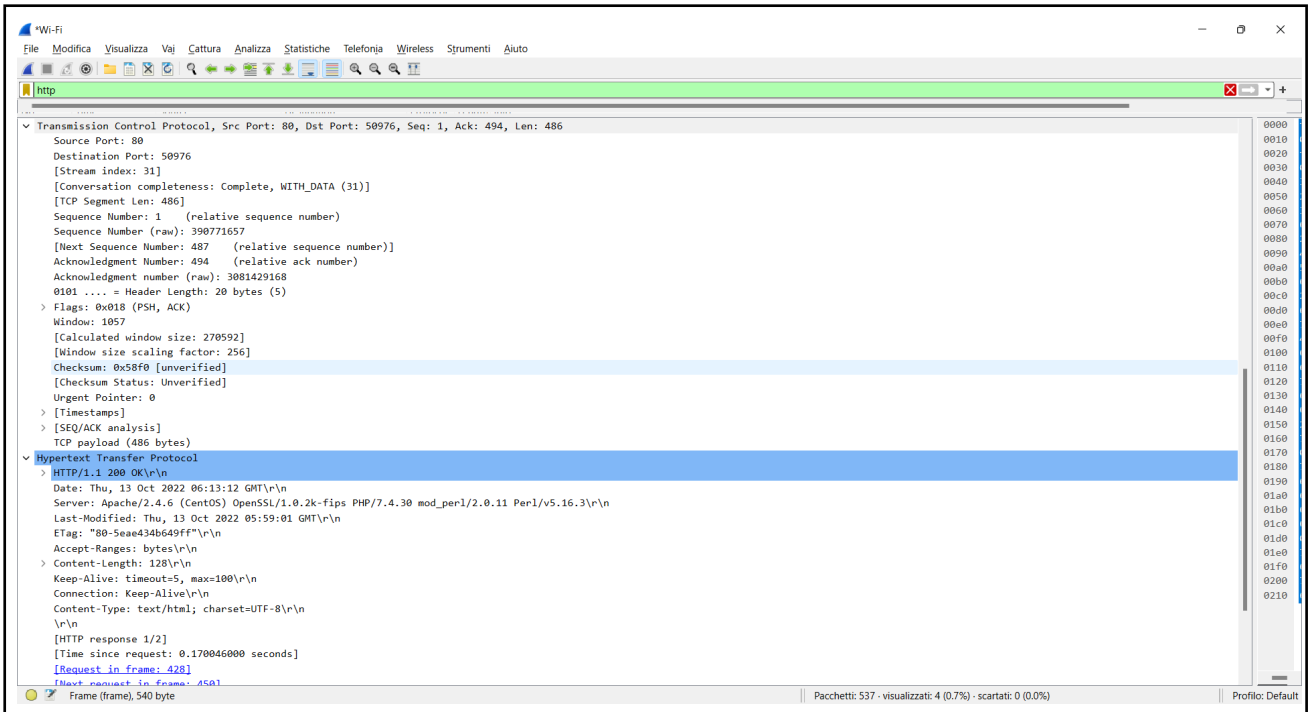
Pacchetto Get:

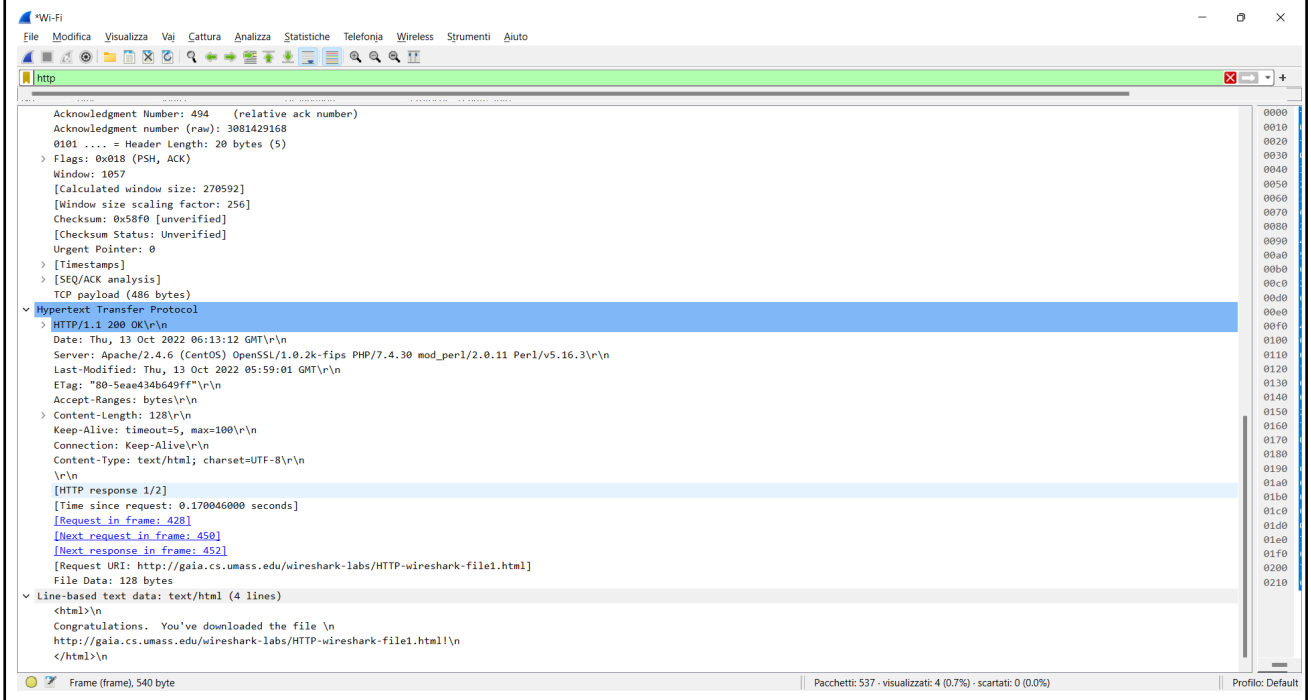




Pacchetto Http:







Esercitazione 1 http:

Per la prima esercitazione del protocollo http (interazione base: richiesta/risposta) si sono seguiti i seguenti punti:

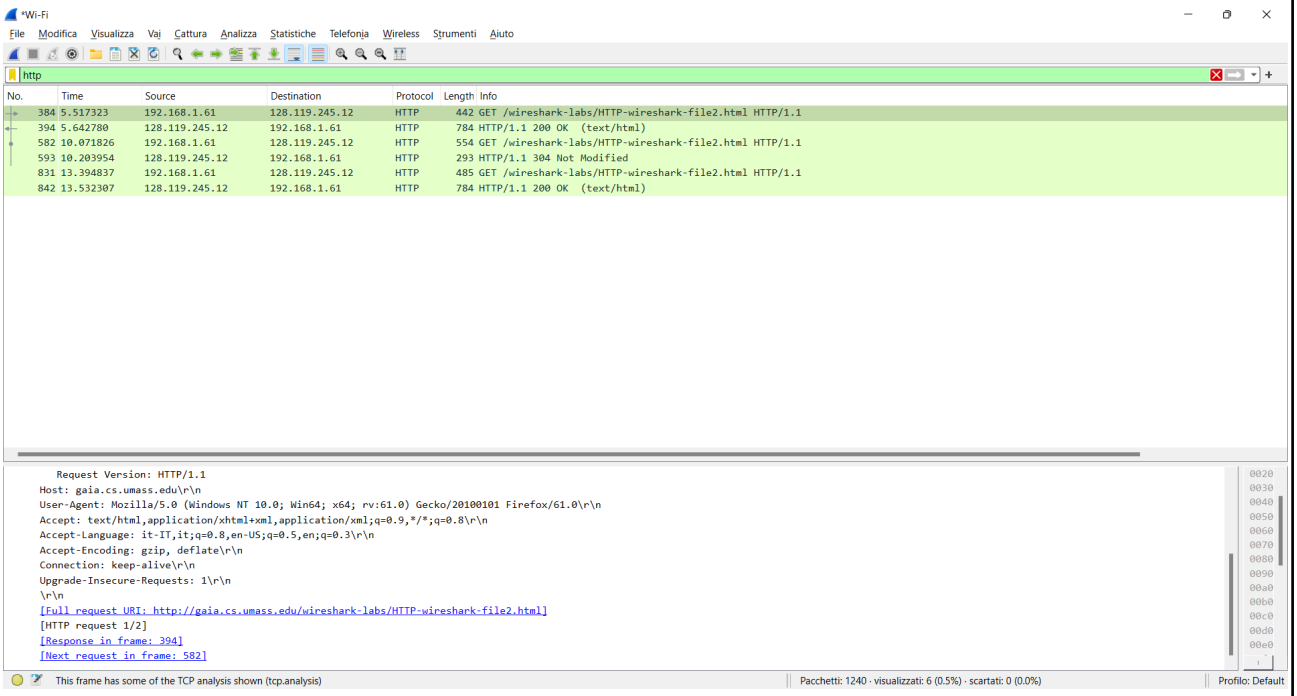
- Avviare il software Wireshark
- Avviare la cattura dei pacchetti
- Inserire nel browser il seguente link: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
- Attivare il filtro http e controllare i pacchetti ricevuti

I pacchetti ricevuti sono due: Get (che è il pacchetto inviato dal browser al server) e il messaggio di risposta dal server.

All'interno del pacchetto Get si è potuto ottenere le seguenti informazioni:

1. Sia il browser che il server usano una versione 1.1 di http
2. Le lingue accettate sono l'italiano e l'inglese
3. L'ip del computer è 192.168.244.231, mentre l'ip del server è 128.119.254.12
4. Il codice di stato restituito è 200, ovvero OK
5. Ultima modifica alla pagina è stata il 13 ottobre 2022 alle 12:13

6. Sono stati trasferiti 128 byte
7. No non ci sono state intestazioni che non sono state visualizzate nell'elenco dei pacchetti

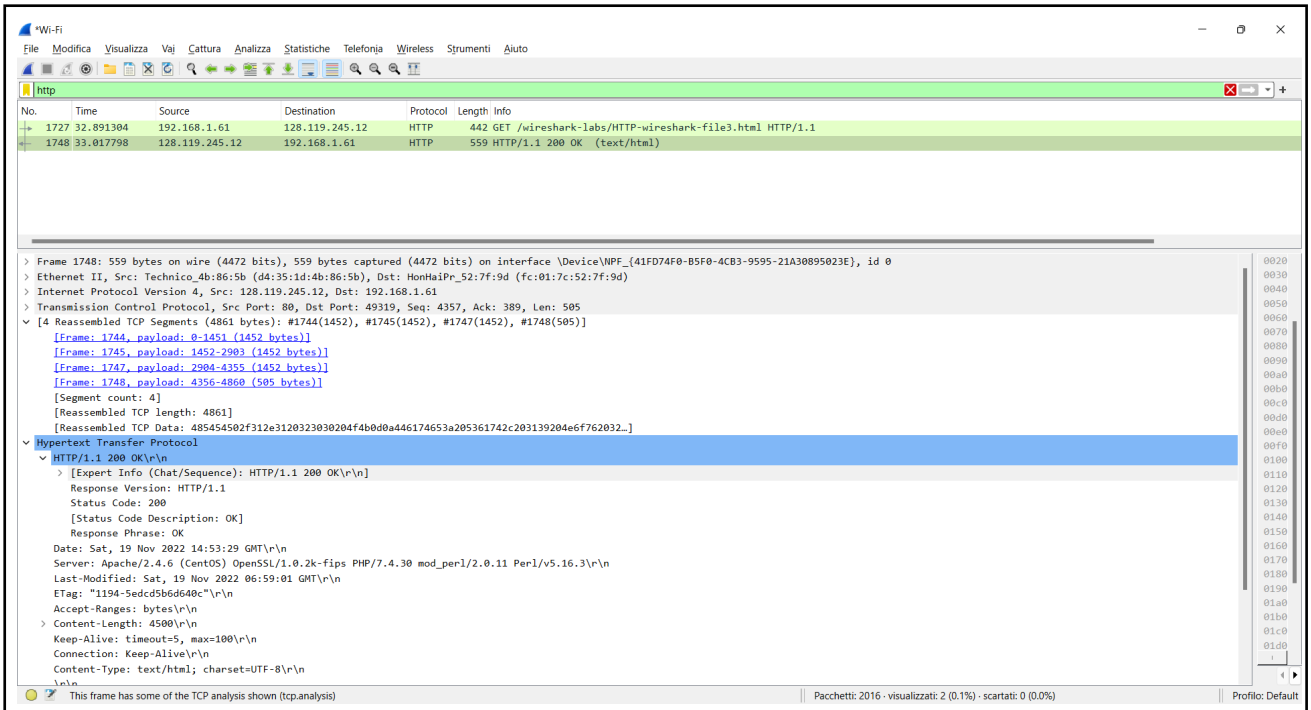


Per la seconda esercitazione (l'interazione GET condizionale/risposta) si è seguito i seguenti punti:

- Svuotare la cache del browser per evitare che esegua una Get condizionale
- Eseguire il Wireshark
- Inserire il link nel Browser: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html
- Refreshare la pagina
- Refreshare la pagina premendo il pulsante shift
- Interrompere la cattura e filtrare i pacchetti http

Dai pacchetti ricevuti si è potuto ottenere le seguenti informazioni:

8. Nella prima richiesta Get non è presente nessuna linea di intestazione "IF-MODIFIED-SINCE".
9. Il contenuto è stato effettivamente spedito, si può stabilire dalla linea di intestazione File data, nella quale si può ottenere la dimensione del pacchetto che è stato inviato: 371 bytes.
10. Nella seconda richiesta GET è presente una linea di intestazione "IF-MODIFIED-SINCE" con la data dell'ultima modifica
11. Il codice di stato restituito è 304 e la frase associata è "Not Modified", in questo caso il server non ha spedito il contenuto del file perchè non è stato modificato quindi non c'è alcun bisogno di essere rispedito.
12. Nella terza richiesta GET non è presente alcuna linea di intestazione"IF-MODIFIED-SINCE".
13. Il codice di stato in risposta al terzo GET è 200, il file è stato spedito in questo la ricarica è stata forzata con shift+reload, dunque il tutto è stato spedito nuovamente.

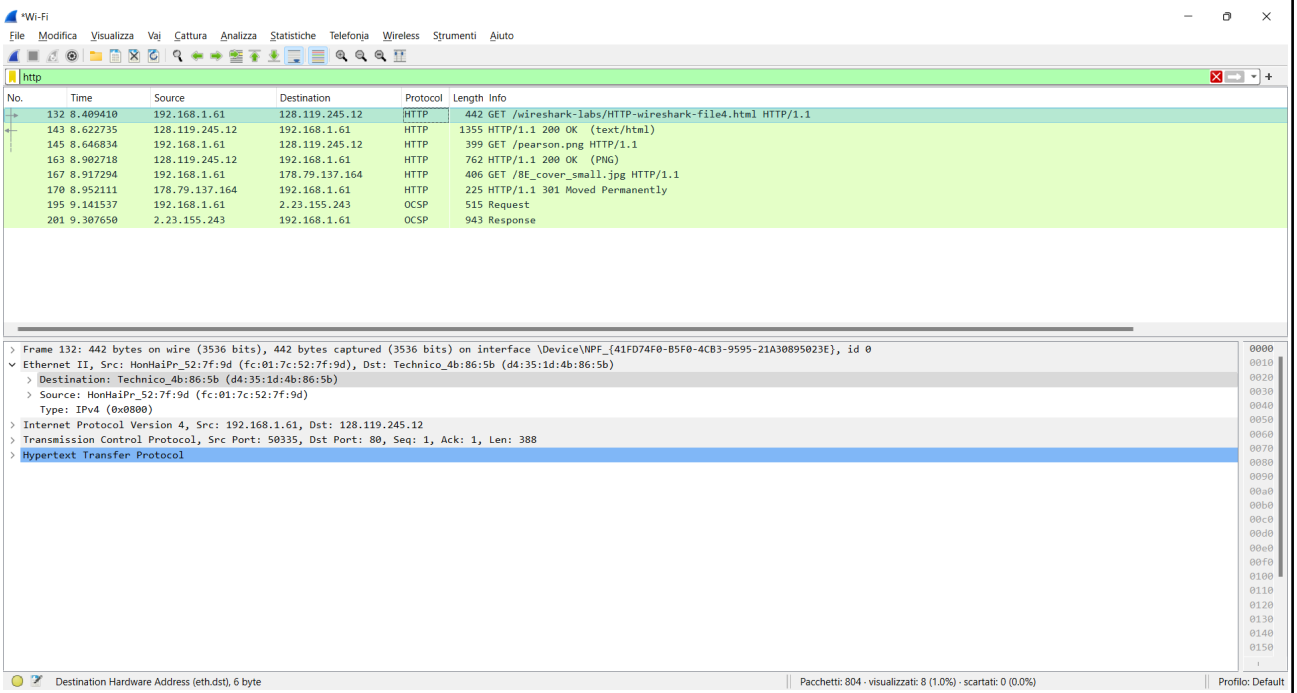


Per la terza esercitazione(recuperare documenti di grandi dimensioni) si sono seguiti i seguenti punti:

- Eseguire wireshark
- Avviare il browser con la cache vuota e inserire il link: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html
- Interrompere la raccolta di pacchetti e controllare i risultati con il filtro http

Dai pacchetti ricevuti si è potuto ottenere le seguenti informazioni:

14. E' stato inviato un solo messaggio GET, il quale contiene il numero di pacchetto 1727.
15. Il codice e la frase associate alla risposta sono 200 e OK.
16. E' necessario un solo segmento per contenere i dati per trasportare la risposta
17. Il numero del pacchetto contenente il codice di stato e la frase associata con la risposta alla richiesta è 1748
18. .



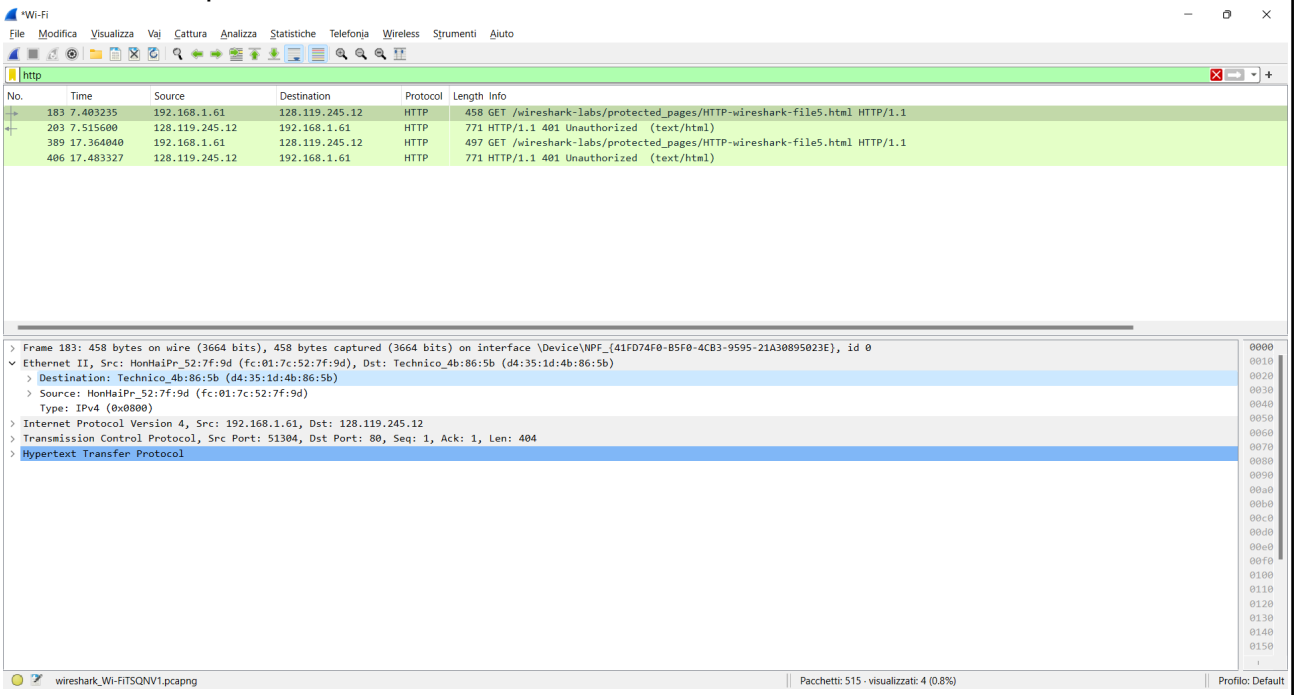
Per la quarta esercitazione (documenti HTML con oggetti integrati) si è seguito i seguenti punti:

- Eseguire Wireshark

- Inserire nel browser il link: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
- Interrompere Wireshark e controllare i pacchetti ricevuto con il filtro http

Dai pacchetti si possono ottenere le seguenti informazioni:

19. Sono state inviate 3 richieste Http Get: le prime due all'indirizzo ip 128.119.245.19 e l'ultimo all'indirizzo 178.79.137.164.
20. Sono state scaricate in modo sequenziale, dai tempi si può notare che viene effettuata la richiesta GET per la prima immagine, il pacchetto dopo è della risposta, successivamente viene effettuata la seconda richiesta, l'ultimo pacchetto è quello della risposta all'ultima richiesta.



Per la quinta esercitazione (autenticazione http) si sono svolti i seguenti punti:

- Eseguire Wireshark
- Inserire nel Browser il link: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html
- Refreshare la pagina premendo il pulsante shift
- Interrompere la cattura dei pacchetti e visualizzarli con il filtro http

Dai pacchetti si è potuto ottenere le seguenti informazioni:

21. Sono state inviate 3 richieste GET al server
22. La risposta alla prima è 401 Unauthorized
23. Nella seconda richiesta GET vengono aggiunte le credenziali nelle intestazioni
24. Si, il terzo messaggio contiene le credenziali immesse precedentemente

DNS

Per l'esercitazione sul Dns si è studiato in precedenza i comandi nslookup e ipconfig.

Nslookup: un comando del prompt dei comandi che serve per interrogare i server DNS.

Ipconfig: un comando del prompt dei comandi che serve per mostrare la configurazione TCP/IP corrente.

Si sono utilizzati i comandi per ricavare i seguenti dati:

1. Eseguite nslookup per ottenere l'indirizzo IP di un server web in Asia.
2. Eseguite nslookup per determinare i server DNS autoritativi di una università in Italia (diversa dalla Università di Chieti-Pescara).
3. Eseguite nslookup per determinare i server SMTP di Gmail.
4. Eseguite nslookup per determinare il nome di host canonico di fad.unich.it.

5. Solo se non siete in aula informatica, eseguite nslookup in modo tale che uno dei server ottenuti al punto 2 venga interrogato per ottenere i mail server di Gmail.

In seguito si è tracciato il protocollo DNS con wireshark seguendo i seguenti punti:

- Usare ipconfig per svuotare la cache del DNS e svuotare la cache del browser
- Avviare la cattura dei pacchetti con il filtro “DNS or Http”
- Usare nel browser il link:https://www.ietf.org/
- Interrompere la cattura di pacchetti

Dall’esercitazione si è potuto estrapolare le seguenti informazioni:

6. I messaggi di risposta del query Dns sono stati inviati tramite UDP
7. La porta di destinazione per le query DNS è 53 e la porta sorgente per i messaggi DNS di risposta è 54795.
8. La query Dns è stata inviata al nostro server DNS locale al l’indirizzo IP 192.168.0.5
9. La query Dns è un Type A e la query contiene delle risposte.
10. La risposta DNS contiene 3 record di risposta, ognuno di questi record contiene Name, Type, Class, Time to Live, Data Lenght e Address.
11. La query HTTP inviata corrisponde a uno degli indirizzi IP forniti nel messaggio di risposta DNS.
12. Prima di recuperare le immagine che contiene la pagina web sono state inviate altre query DNS

Nella seconda esercitazione Dns si sono seguiti i seguenti punti:

- Eseguire Wireshark
- Fare un nslookup su www.mit.edu
- Interrompere la cattura dei pacchetti

Dall’esercitazione si sono ottenute le seguenti informazioni:

13. .
14. La richiesta DNS è stata inviata a un DNS non locale all’indirizzo 0.0.0.0
15. Il messaggio di richiesta DNS nella finestra dei dettagli è un Type A di query e contiene dei record di risposta.
16. Il messaggio di risposta del server fornisce 3 record di risposta e ognuno contiene Name, Type, Class, Time to Live, Data Lenght, Address

ICMP

Per l’esercitazione del protocollo ICMP si sono seguiti i seguenti passaggi:

- Avviare Wireshark
- Inserire nella shell il comando: ping -c 10 gaia.ca.umass.edu
- Una volta terminato il ping interrompere la cattura dei pacchetti.

Dai pacchetti ricevuti si sono potute ottenere le seguenti informazioni:

1. L’indirizzo del nostro host è 192.168.1.132 mentre l’indirizzo dell’host di destinazione è 128.119.245.12
2. Un pacchetto ICMP non ha i numeri di porta e destinazione perchè perché lavora al livello 3 e si occupa solo di trasportare i dati da una sorgente a una destinazione e per compiere questa azione, il numero di porta non è rilevante.
3. In una richiesta GET il campo Type assume il valore “8”, il campo Code assume il valore “0”
4. Nella rispettiva risposta il campo Type assume il valore “0”, il campo Code assume il valore “0”

Dalla seconda esercitazione si è ottenuto le seguenti informazioni:

5. L’indirizzo del nostro host è 192.168.1.132 mentre l’indirizzo dell’host di destinazione è 128.119.245.12

6. Se ICMP avesse inviato pacchetti UDP, il numero di protocollo nel datagramma IP sarebbe sempre 01 per i pacchetti “sonda”.
7. Il pacchetto ICMP echo è diverso dal pacchetto inviato da Ping perchè sono presenti più field Time to Live.
8. I pacchetti di errori ICMP hanno più campi del pacchetto ICMP echo e in questi campi è incluso No response seen
9. Tra i pacchetti con errore e i pacchetti senza c’è una differenza nei campi Type e Code. Nei pacchetti con errore esce “Destination unreachable” e “Port unreachable” mentre nei pacchetti senza errore esce “Time to live exceeded” e “Time to live exceeded in transit”, con una aggiunta di un campo: “Lenght of original datagram”.

UDP

Nell’esercitazione UDP si sono analizzati i pacchetti di questo protocollo e si sono ottenute le seguenti informazioni:

1. In un pacchetto UDP sono presenti 4 campi in un’intestazione: Source Port, Destination Port, Lenght e Checksum
2. La lunghezza di ogni campo dell’intestazione UDP è 1037 byte
3. Il valore Lenght indica il numero di byte catturati in quel determinato frame
4. Il numero massimo di byte che può essere incluso nel carico di un pacchetto UDP è di 65527 byte.
5. Il valore più grande possibile per il numero di porta sorgente è 65535
6. Il numero del protocollo UDP in esadecimale e in decimale è 17 e 0x11.

RISPOSTE:

- NEL DETTAGLIO DEI PACCHETTI COME VENGONO NOMINATE LE LINEE?
.....PER ESEMPIO UN DETTAGLIO DI 5 LINEE. (attenzione l'ultima linea non è scontata che si tratta di quella applicativa, occhio ad ogni risultato!)

Nei pacchetti le linee vengono denominate: Frame, Ethernet, internet protocol, Protocol, Application.
La quinta linea non sempre è quella applicativa ma può essere Data.

- CHE COS'è WIRESHARK?

Wireshark è un programma che permette di analizzare i pacchetti all’interno di una rete, permettendo di filtrare e analizzare le caratteristiche.

- NEL DATAGRAMMA CHE COSA INDICA IL TOTAL LENGHT?

Il total lenght indica la grandezza in byte del payload+header

- COSA SI INTENDE PER PAYLOAD ED HEADER?

Con PayLoad si intende la parte informativa dei dati che vengono inviati.
Con Header si intende la parte iniziale del pacchetto che contiene informazioni rilevanti ai layer del modello ISO-OSI

- I TERMINI HTTP, DNS, ICMP ED UDP CHE COSA SIGNIFICANO?

Sono dei protocolli di rete e vogliono dire:
HTTP (Hypertext Transfer Protocol), DNS (Domain Name System), ICMP (Internet Control Message Protocol) e UDP (User Datagram Protocol).

- COSA INTENDE COME TERMINE SIP IN TELECOMUNICAZIONI?

Sip indica un protocollo di rete di controllo del livello applicativo usato per creare, modificare, e terminare sessioni tra uno o più partecipanti.

* * * CONCLUSIONI/ obiettivi raggiunti * * *

L'esperienza è stata svolta correttamente senza incontrare particolari problematiche.
Si fa notare come si sono riscontrate delle complicazioni nell'esperienza del DNS con problemi con i siti proposti dall'esercitazione. Il problema si è risolto dopo diversi tentativi, individuando la soluzione nel cambiare rete.