

# ESERCITAZIONE

## PARTE 1 (file capture.cap):

1. Che tipo di protocollo di livello Data-link è utilizzato? Come fa Wireshark a capirlo?

### RISPOSTA:

Il protocollo utilizzato è Ethernet. Lo possiamo vedere dal primo campo della sezione 'Frame' del (in generale dal livello inferiore a quello interessato è contenuto il campo che specifica il protocollo utilizzato dal livello superiore; in questo modo il campo header-length diventa inutile in quanto è standard dato un determinato protocollo);

2. Disegnare la PDU di livello Data-link indicando il valore dei vari campi.

### RISPOSTA:

```
-----+-----+-----+-----+-----+
| MAC Destinazione (6B) | MAC Sorgente (6B) | Type (2B) |
-----+-----+-----+-----+-----+
```

Destinazione: broadcast (ff:ff:ff:ff:ff:ff);

Mittente: 00:e0:81:24:dd:64;

Type: IPv4 //indica il protocollo del livello superiore;

**NB: quando apri un pacchetto visualizzi per righe i vari livelli TCP/IP del pacchetto partendo da quello fisico e andando in giù.**

3. Qual è il MAC sorgente? Di che tipo è: unicast o broadcast?

### RISPOSTA:

Lo ho già scritto prima, è di tipo unicast;

4. Qual è il MAC destinazione? Di che tipo è: unicast o broadcast?

### RISPOSTA:

Lo ho già scritto prima, è di tipo broadcast;

5. Che tipo di protocollo di livello Network è utilizzato? Come fa Wireshark a capirlo?

### RISPOSTA:

Il protocollo utilizzato è IPv4. Lo possiamo capire da uno dei campi indicati nel livello inferiore, in questo caso il campo Type del Data-Link;

6. Qual è la lunghezza dell'header IP?

**RISPOSTA:**

20 bytes;

7. Quali sono gli indirizzi IP sorgente e destinazione?

**RISPOSTA:**

L'indirizzo mittente è 157.27.252.223 mentre l'indirizzo destinatario è 157.27.252.255;

8. Che tipo di protocollo di livello trasporto è contenuto in IP? Come fa Wireshark a capirlo?

**RISPOSTA:**

Il protocollo del livello di trasporto è UDP, ed è capibile dal relativo campo nel livello di rete;

9. Quali sono le porte sorgente e destinazione a livello di trasporto?

**RISPOSTA:**

Porta 631 per entrambe le domande;

10. Creare un filtro per visualizzare solo i pacchetti che hanno ARP come protocollo (suggerimento: basta scrivere arp nella barra Filter sotto la toolbar; si ricordi di premere su Apply dopo aver scritto arp).

**RISPOSTA:**

Fatto;

11. Dopo aver applicato il filtro precedente qual è la percentuale di pacchetti che rimangono visualizzati rispetto al totale? (suggerimento: vedere entrambi i valori nella barra di stato in basso).

**RISPOSTA:**

Pacchetti totali 272, visualizzato dopo il filtro sul protocollo ARP 173 (63,6%);

12. Creare un filtro per visualizzare solo i pacchetti che hanno destinazione MAC 00:01:e6:57:4b:e0. (suggerimento: usare l'editor di espressioni; la categoria da selezionare è Ethernet; per 13 l'indirizzo MAC usare la notazione esadecimale con i due punti come separatori; si ricordi di premere su Apply dopo aver creato l'espressione).

**RISPOSTA:**

filtro: eth.dst == 00:01:e6:57:4b:e0

13. Dopo aver applicato il filtro precedente qual è la percentuale di pacchetti che rimangono visualizzati rispetto al totale? (suggerimento: vedere entrambi i valori nella barra di stato in basso).

**RISPOSTA:**

1 su 272, ossia il 0.4%;

14. Creare un filtro per visualizzare solo i pacchetti che hanno destinazione MAC broadcast. (suggerimento: nell'editor di espressioni la categoria da usare è Ethernet; per l'indirizzo MAC usare la notazione esadecimale con i due punti come separatori; si ricordi di premere su Apply dopo aver creato l'espressione).

**RISPOSTA:**

filtro: `eth.dst == ff:ff:ff:ff:ff:ff`

15. Dopo aver applicato il filtro precedente qual è la percentuale di pacchetti che rimangono visualizzati rispetto al totale? Sono molti? Perché?

**RISPOSTA:**

Sono 228 su 272, ossia il 83,8% del totale. Sono molti perché la maggior parte delle richieste sono volte a scoprire chi ha un determinato indirizzo IP (ARP request);

**PARTE 2 (file simpleHTTP.cap):**

1. Colorare di rosso tutti i pacchetti che contengono UDP e di verde tutti i pacchetti che contengono TCP. (suggerimento: nell'editor delle regole di colorazione è sufficiente portare in alto due regole già esistenti e modificarle per cambiarne i colori di sfondo).

**RISPOSTA:**

Su 'Visualizza' trovi la dicitura 'Regole di colorazione', selezioni il tipo di protocollo da colorare e poi in fondo premi su 'sfondo e scegli il colore, poi ok.

2. Cosa contengono i primi due pacchetti della sessione di cattura? IP sorgente, IP destinazione. Tipo di protocollo di trasporto. Tipo di protocollo di livello Applicazione. Come fa Wireshark a capirlo? Messaggio contenuto nel Payload di livello applicazione.

**RISPOSTA:**

- Pacchetto 1:
  1. Source Address: 157.27.252.202
  2. Destination Address: 157.27.10.10
  3. UDP;
  4. DNS;

- 5. c'è scritto;
- 6. [www.polito.it](http://www.polito.it);
- Pacchetto 2:
  - a. Source Address: 157.27.10.10
  - b. Destination Address: 157.27.252.202
  - c. UDP;
  - d. DNS;
  - e. c'è scritto;
  - f. 130.192.73.1

3. Prendere in considerazione il pacchetto n.3. per IP sorgente, IP destinazione. Tipo di protocollo di trasporto. IP sorgente e destinazione sono in qualche modo collegati con i messaggi scambiati a livello applicazione nei primi due pacchetti? È possibile fare delle ipotesi su cosa serve il protocollo di livello applicazione dei primi due pacchetti?

**RISPOSTA:**

Il protocollo del livello di trasporto è TCP, e non sono collegati con i pacchetti precedenti in quanto erano di una connessione con protocollo UDP. L'unico collegamento che si può fare è semantico e a livello di applicazione, in quanto i primi due pacchetti erano una richiesta DNS per l'IP del sito [www.polito.it](http://www.polito.it), mentre questo terzo pacchetto è una richiesta di connessione TCP proprio a quel sito (ossia indirizzo 130.192.73.1).

4. Creare un filtro per visualizzare solo i pacchetti TCP (compresi i pacchetti HTTP) e determinare il numero.

**RISPOSTA:**

Filtro: tcp && http ---> 134 su 823 (16,3%) con condizione AND, oppure Filtro: tcp || http con OR abbiamo 807 su 823 (98,1%);

5. Prendere in considerazione il pacchetto n. 6. IP sorgente, IP destinazione. Tipo di protocollo di trasporto. Tipo di protocollo di livello Applicazione. Perché prima della trasmissione del primo messaggio HTTP c'è lo scambio di tre pacchetti puramente TCP? Quali sono i flag settati nell'header TCP di questi tre pacchetti?

**RISPOSTA:**

TCP trasporto, HTTP applicazione. Lo scambio di pacchetti è il three-hands-shake per avviare la comunicazione affidabile. Le flag sono SYN, SYN-ACK e ACK.

5. Creare un filtro per visualizzare solo i pacchetti TCP (esclusi i pacchetti HTTP) e determinarne il numero. Qual è la percentuale sul totale dei pacchetti TCP trovata al punto 5? A cosa servono tali pacchetti? Se il protocollo DNS dei pacchetti 1 e 2 avesse usato il protocollo TCP, quanti pacchetti IP sarebbero stati generati? Sarebbe stato utile?

**RISPOSTA:**

Filtro: tcp && !http ---> 81,8% sul totale, sono tutti three-hands-shake. Se anche la richiesta DNS avesse usato TCP, i pacchetti totali sarebbero stati 5 (3 per l'apertura connessione e i 2 già presenti); no, non sarebbe servito a nulla in quanto la richiesta al DNS di un dominio non richiede l'utilizzo di un protocollo affidabile come TCP;

6. Selezionare il pacchetto 3 e seguire lo stream TCP col comando da menu Analyze/Follow TCP Stream. Cosa si può leggere? Qual è il messaggio contenuto nel payload della PDU di livello Applicazione?

**RISPOSTA:**

Analizza - Segui - TCP stream, permette di vedere le richieste HTTP (GET) più nel dettaglio. In particolare nel payload è possibile vedere tutto il codice HTML della pagina polito.it richiesta, compresa di immagini e quant'altro.

**PARTE 3 (file busyNetwork.cap):**

1. Elencare i protocolli di livello Applicazione che entrano in azione in questa cattura classificandoli in base al livello Trasporto utilizzato.

**RISPOSTA:**

HTTP (usa TCP), DNS (usa UDP), FTP, SSH;

2. Provare ad analizzare diversi stream TCP con sopra diversi protocolli di livello applicazione. Che differenza c'è tra il contenuto trasmesso in una connessione TCP per il protocollo FTP e quello trasmesso per il protocollo SSH?

**RISPOSTA:**

Per FTP (file transport) la porta usata è la 21 e la maggior parte dei dati trasmessi è facilmente visibile una volta catturato il traffico, mentre per SSH (secure shell) la porta è la 22, e i dati sono tutti crittografati, quindi illeggibili senza chiave di decrittazione.

**PARTE 4 (file pingCapture.cap):**

1. Individuare le richieste ping (pong) inviate e le relative risposte. Quante sono?

**RISPOSTA:**

basta mettere nel filtro 'icmp' e sono 22;

2. Quali sono IP sorgente e destinazione della richiesta ICMP? A quale ente o azienda sono intestati?

**RISPOSTA:**

univr;

3. Provare a invocare il comando ping dal proprio PC verso [www.google.com](http://www.google.com) e verso il proprio Default Gateway (come faccio a sapere il suo IP?) e osservare il RTT medio e la sua variazione. Chi mostra la media più grande? Perché? Chi mostra la variazione più grande? Perché?

**RISPOSTA:**

--- [www.google.com](http://www.google.com) ping statistics ---

10 packets transmitted, 10 received, 0% packet loss, time 9014ms

Per trovare invece il default Gateway immettiamo il comando 'ip route' e vediamo 'default via 192.168.1.1'. Eseguendo ping --->

--- 192.168.1.1 ping statistics ---

11 packets transmitted, 11 received, 0% packet loss, time 10019ms

## PARTE 5 ():

Entrare nel sistema Linux presente in cloud e digitare il comando `traceroute www.google.com`. Individuare le interfacce dei router attraversati. Individuare i nomi delle organizzazioni a cui sono intestati gli IP delle interfacce dei router attraversati.

**RISPOSTA:**

Dopo esserci connessi alla vpn dell'uni, ho avviato 'traceroute [www.google.com](http://www.google.com)', e come risultato ho ottenuto:

```
1  * * *
2  10.252.10.1 (10.252.10.1) 48.837 ms 48.778 ms 48.657 ms
3  198.51.100.129 (198.51.100.129) 48.730 ms 51.017 ms 48.602 ms
4  ru-univr-l1-rl1-vr00.vr00.garr.net (193.204.218.109) 48.478 ms 48.434 ms
   48.397 ms
5  * * *
6  rs1-mi01-re1-mi02.mi02.garr.net (185.191.180.158) 48.167 ms 48.282 ms
   48.174 ms
7  142.250.164.230 (142.250.164.230) 48.143 ms 48.071 ms
   142.250.174.46 (142.250.174.46) 48.041 ms
8  192.178.104.191 (192.178.104.191) 48.976 ms 192.178.104.103
   (192.178.104.103) 48.537 ms *
```

9 142.251.235.177 (142.251.235.177) 48.405 ms 192.178.82.62  
(192.178.82.62) 48.461 ms 142.251.235.177 (142.251.235.177) 48.308 ms  
10 142.251.235.177 (142.251.235.177) 48.263 ms mil04s51-in-f4.1e100.net  
(142.251.209.36) 48.184 ms 142.251.235.179 (142.251.235.179) 49.466 ms  
di cui le interfacce sono quelle esplicitate nelle parentesi dopo l'IP di  
riferimento del router attraversato. Per le aziende associate basta lanciare l'ip  
del gestore con whois;

### **PARTE 6():**

Cercare quali interfacce sono attualmente attive sul proprio PC. Qual è  
l'indirizzo IP dell'interfaccia che state utilizzando sul vostro host? E la netmask  
corrispondente? Qual è l'indirizzo IP di [www.univr.it](http://www.univr.it)?

### **RISPOSTA:**

Lancio nel terminale 'ifconfig' e vediamo subito le mie interfacce attive, ossia:

- wlo0 ---> connessione wifi;
- lo ---> loopback;
- enx527ac5ca44bc ---> non ne ho idea;
- eno1 ---> connessione ethernet;

Al momento sto utilizzando wlo0 e il mio indirizzo IP è 172.20.10.4, mentre la  
netmask corrispondente è 255.255.255.240. Infine con nslookup [www.univr.it](http://www.univr.it)  
è possibile risalire a 157.27.3.60, ossia l'indirizzo IP dell'uni.

**N.B:** in WSH vediamo sulla dicitura protocol il nome del protocollo di  
livello più alto che WSH stesso è riuscito a trovare e individuare. Quindi  
se vediamo per esempio TCP, significa che il pacchetto non ha (da solo  
magari unito ad altri sì) una parte di livello applicativo interpretabile allo  
stato attuale. Questa nota è particolarmente importante per esempio nel  
caso in cui leggessimo la flag FYN, comunemente associata al  
protocollo TCP, in un pacchetto interpretato come HTTP- Web Socket. In  
questo caso non è la flag FYN di chiusura connessione (ossia, lo è del  
Web Socket ma non della connessione intera TCP), ma potrebbe proprio  
significare completamente un'altra cosa in base al protocollo a cui fa  
riferimento.