

Ayudantía Tarea 3

Cristóbal Abarca caabarca1@uc.cl

Lukas Svicarovic lsvicarovic@uc.cl

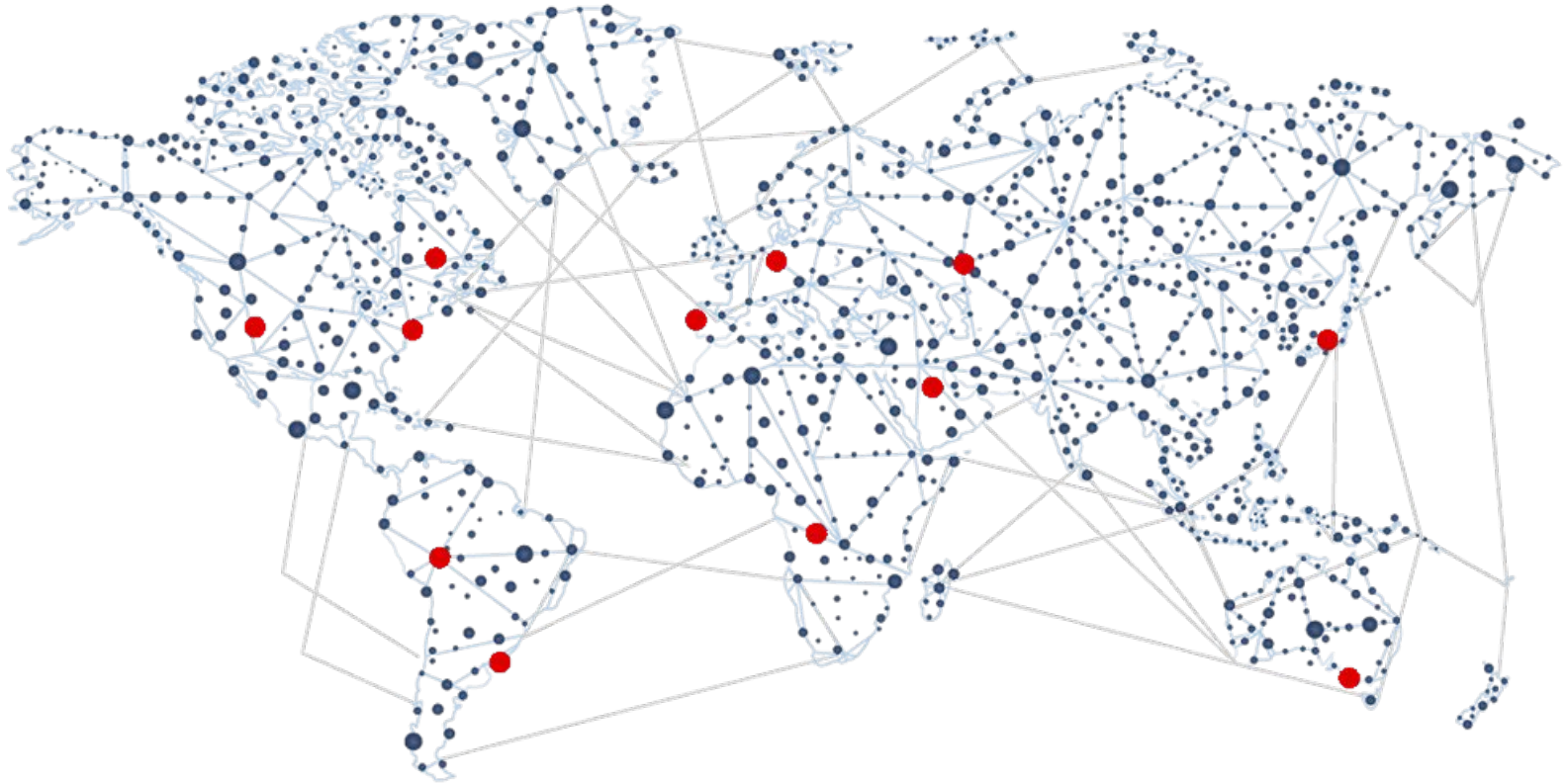
IP y Subredes

`http://www.google.com`  `64.233.186.100`

`http://www.facebook.com`  `179.60.193.35`

`http://www.ing.uc.cl`  `146.155.4.12`

IP y Subredes



IP y Subredes

- Direcciones de 32 bit = 4 byte (IPv4). Esto implica que existen 2^{32} direcciones distintas.
- Son del tipo:

$$\begin{array}{c} 146.155.13.45 \\ = \\ 10010010.10011011.00001101.00101101 \end{array}$$

- Son CASI únicas globalmente

Subredes y máscaras

- Sirven para identificar a un conjunto de nodos (computadores, smartphones, tablets) conectados a un router
- Primeros X bits definen la **subred**
- Por ejemplo: 10.200.73.252/24
 - Mascara /24 ó 255.255.255.0
 - IP & Máscara = Subred

Subredes y máscaras

- Últimos 32 - X bits definen el **host** dentro de la subred :
- Por ejemplo: 10.200.73.252/24
 - Mascara /24 ó 255.255.255.0
 - Subred: 10.200.73.0
 - Host: 10.200.73.252
 - HostMin: 10.200.73.1
 - HostMax: 254

Subredes y máscaras

- Últimos 32 - X bits definen el **host** dentro de la subred
- Por ejemplo: 10.200.73.252/24
 - Mascara /24 ó 255.255.255.0
 - Subred: 10.200.73.0
 - Broadcast 10.200.73.255
 - HostMin: 10.200.73.1
 - HostMax: 10.200.73.254
- Podemos notar que la máscara define el tamaño de la Subred
- ¿ Por qué solo podemos tener $2^{(32 - x)} - 2$ miembros en la subred?

ARP

- ARP: Address Resolution Protocol
- Se encarga de encontrar la MAC Address de una determinada dirección IP
- Se ocupa en 4 casos:
 - Cuando dos hosts están en la misma red y uno quiere enviar un paquete a otro
 - Cuando dos hosts están sobre redes diferentes y deben usar un gateway o router para alcanzar otro host
 - Cuando un router necesita enviar un paquete a un host a través de otro router
 - Cuando un router necesita enviar un paquete a un host de la misma red

Tablas ARP

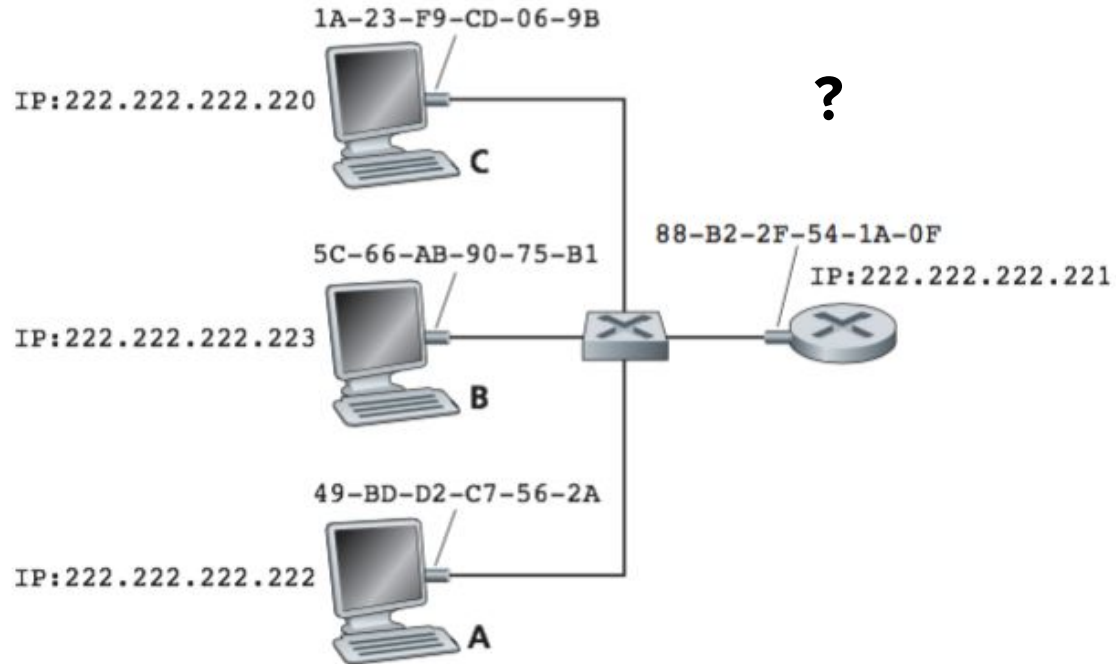
- Tablas que contienen asociaciones entre:

< IP, MAC ADDRESS, TTL >

- TTL: Time-To-Live: tiempo de vida de la asociación dentro de la tabla

Tablas ARP

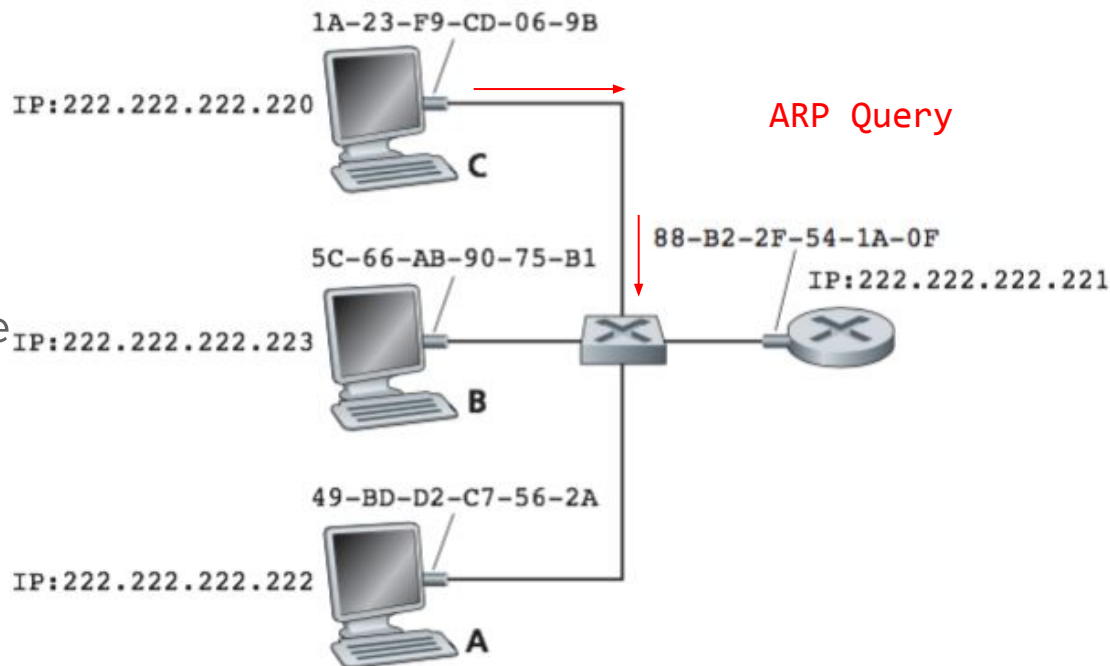
1. C quiere comunicarse con A, que no está en su tabla



IP Address	MAC Address	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

Tablas ARP

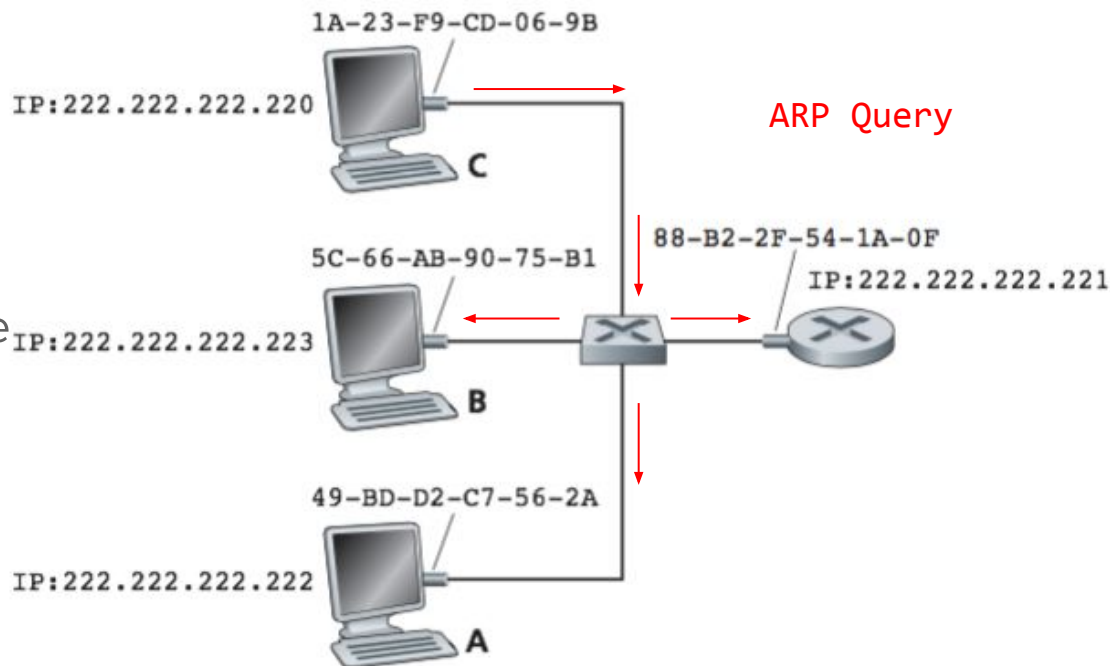
1. C quiere comunicarse con A, que no está en su tabla
2. C envía **ARP Query** con IP de A y MAC FF-FF-FF-FF-FF-FF



IP Address	MAC Address	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

Tablas ARP

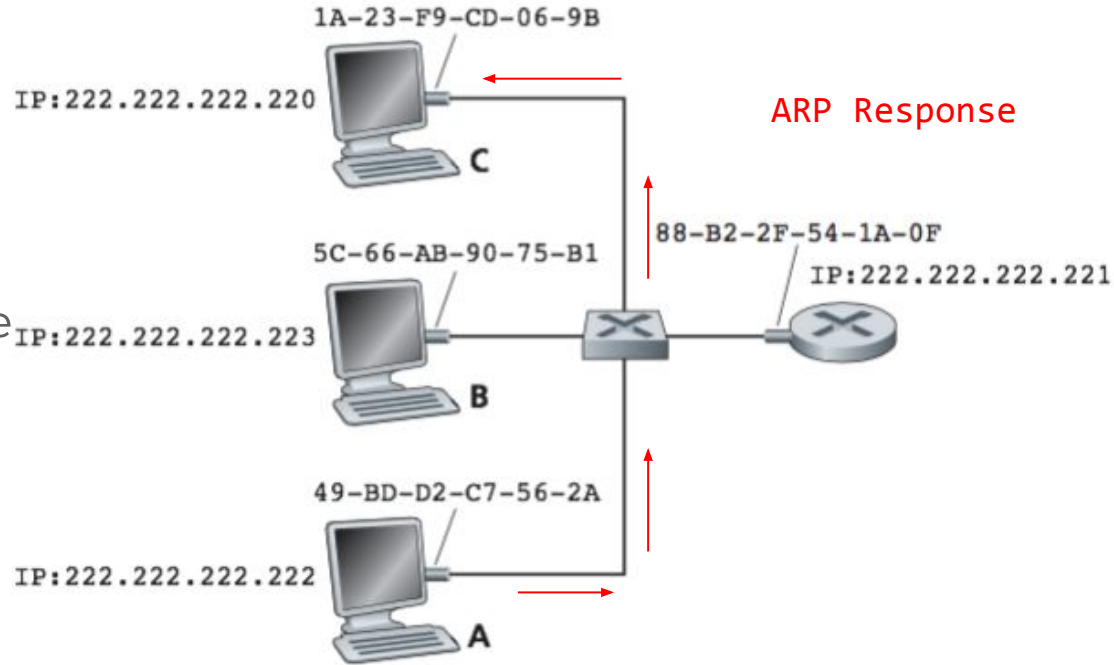
1. C quiere comunicarse con A, que no está en su tabla
2. C envía **ARP Query** con IP de A y MAC FF-FF-FF-FF-FF-FF
3. Todos reciben mensaje



IP Address	MAC Address	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

Tablas ARP

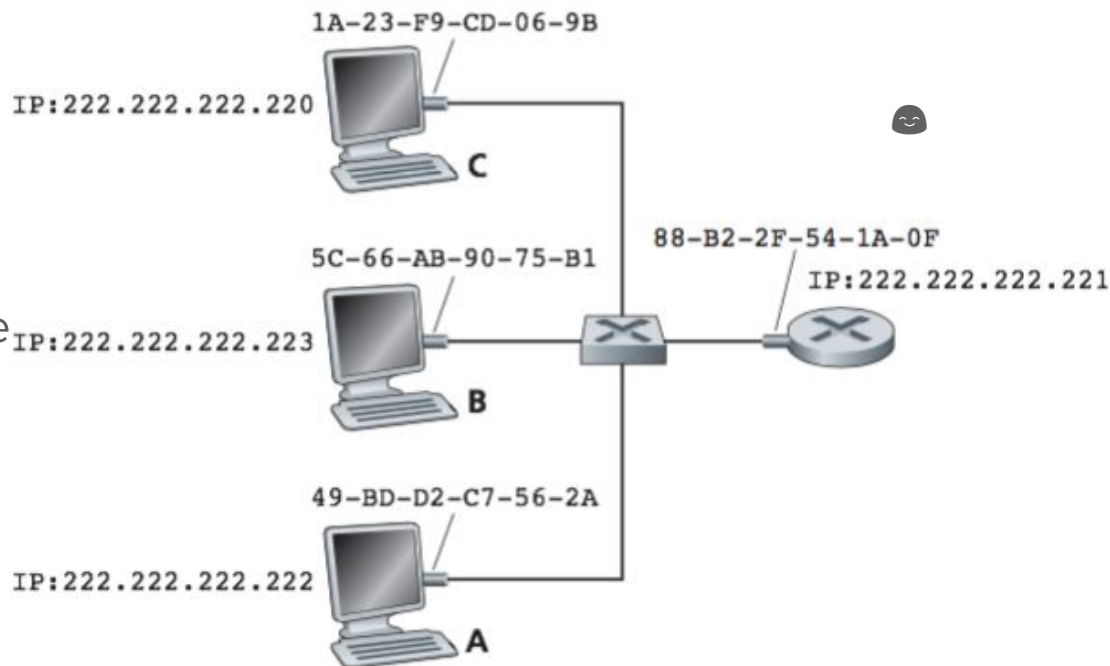
1. C quiere comunicarse con A, que no está en su tabla
2. C envía **ARP Query** con IP de A y MAC FF-FF-FF-FF-FF-FF
3. Todos reciben mensaje
4. A envía mensaje **ARP Response packet** con su MAC



IP Address	MAC Address	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

Tablas ARP

1. C quiere comunicarse con A, que no está en su tabla
2. C envía **ARP Query** con IP de A y MAC FF-FF-FF-FF-FF-FF
3. Todos reciben mensaje
4. A envía mensaje **ARP Response packet** con su MAC
5. C guarda en su tabla la asociación



IP Address	MAC Address	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00
222.222.222.222	49-BD-D2-C7-56-2A	15:00:00

Tablas ARP

¿Qué es el comando
arping?

Wireshark

En esta ayudantía veremos los siguientes responderemos las siguientes preguntas:

- ¿ Qué es?
- ¿ Cómo instalar Wireshark ?
- ¿ Cómo capturar paquetes ?
- ¿ Cómo filtrar los paquetes capturados ?
- DEMO

¿Qué es Wireshark?

- Herramienta para realizar análisis de redes (sniffing)
 - Permite ver todos los paquetes enviados/recibidos por la interfaz de red
 - Soporte para los protocolos comunes y muchos más.
 - Multiplataforma





Apply a display filter ... <Ctrl-/>

Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
391	4.922487977	190.160.0.15	192.168.0.16	DNS	121	Standard query response 0x1fe4 A getpocket.com A 18.234.20.180 A 18.234.20.181 A 18.234.20.184
392	5.017638671	ArrisGro_df:6c:30	Broadcast	ARP	56	who has 192.168.0.14? Tell 192.168.0.1
393	5.122707471	54.186.208.153	192.168.0.16	TLSPv1.2	117	Change Cipher Spec, Encrypted Handshake Message
394	5.151012191	192.168.0.16	172.217.162.78	TLSPv1.2	206	Application Data
395	5.165912828	192.168.0.16	54.186.208.153	TCP	66	54070 → 443 [ACK] Seq=644 Ack=3066 Win=35328 Len=0 TSval=2197297216 TSecr=264591550
396	5.174414923	172.217.162.78	192.168.0.16	TCP	66	443 → 42406 [ACK] Seq=182966 Ack=275 Win=1050 Len=0 TSval=3786205546 TSecr=2921883103
397	5.217687060	172.217.162.78	192.168.0.16	TLSPv1.2	167	Application Data
398	5.217721741	192.168.0.16	172.217.162.78	TCP	66	42406 → 443 [ACK] Seq=275 Ack=183067 Win=1219 Len=0 TSval=2921883169 TSecr=3786205588
399	5.218030506	172.217.162.78	192.168.0.16	TLSPv1.2	1484	Application Data
400	5.218043548	192.168.0.16	172.217.162.78	TCP	66	42406 → 443 [ACK] Seq=275 Ack=184485 Win=1219 Len=0 TSval=2921883170 TSecr=3786205588
401	5.219156173	172.217.162.78	192.168.0.16	TLSPv1.2	1484	Application Data
402	5.219177184	192.168.0.16	172.217.162.78	TCP	66	42406 → 443 [ACK] Seq=275 Ack=185003 Win=1219 Len=0 TSval=2921883171 TSecr=3786205588
403	5.220561824	172.217.162.78	192.168.0.16	TLSPv1.2	2128	Application Data
404	5.220581374	192.168.0.16	172.217.162.78	TCP	66	42406 → 443 [ACK] Seq=275 Ack=187965 Win=1219 Len=0 TSval=2921883172 TSecr=3786205588
405	5.220914708	172.217.162.78	192.168.0.16	Application Data		
406	5.220929968	192.168.0.16	172.217.162.78	TCP	66	42406 → 443 [ACK] Seq=275 Ack=188049 Win=1219 Len=0 TSval=2921883173 TSecr=3786205590
407	5.221058733	192.168.0.16	172.217.162.78	TLSPv1.2	112	Application Data
408	5.236759045	172.217.162.78	192.168.0.16	TCP	66	443 → 42406 [ACK] Seq=188049 Ack=321 Win=1050 Len=0 TSval=3786205607 TSecr=2921883173
409	5.532336757	172.217.162.78	192.168.0.16	TLSPv1.2	1484	Application Data
410	5.532424255	172.217.162.78	192.168.0.16	TLSPv1.2	1484	Application Data
411	5.532479618	192.168.0.16	172.217.162.78	TCP	66	42406 → 443 [ACK] Seq=321 Ack=190885 Win=1219 Len=0 TSval=2921883484 TSecr=3786205886
412	5.532540635	172.217.162.78	192.168.0.16	TLSPv1.2	1484	Application Data
413	5.532591837	172.217.162.78	192.168.0.16	Application Data		
414	5.532623704	192.168.0.16	172.217.162.78	TCP	66	42406 → 443 [ACK] Seq=321 Ack=195139 Win=1219 Len=0 TSval=2921883484 TSecr=3786205886
415	5.532650037	172.217.162.78	192.168.0.16	TLSPv1.2	1484	Application Data
416	5.532743057	172.217.162.78	192.168.0.16	TLSPv1.2	1484	Application Data
417	5.532773396	192.168.0.16	172.217.162.78	TCP	66	42406 → 443 [ACK] Seq=321 Ack=197975 Win=1219 Len=0 TSval=2921883484 TSecr=3786205887
418	5.532833848	172.217.162.78	192.168.0.16	TLSPv1.2	2902	Application Data
419	5.532862943	192.168.0.16	172.217.162.78	TCP	66	42406 → 443 [ACK] Seq=321 Ack=200811 Win=1219 Len=0 TSval=2921883485 TSecr=3786205889
420	5.532892185	172.217.162.78	192.168.0.16	TLSPv1.2	2902	Application Data
421	5.532914560	192.168.0.16	172.217.162.78	TCP	66	42406 → 443 [ACK] Seq=321 Ack=203647 Win=1219 Len=0 TSval=2921883485 TSecr=3786205892
422	5.532936216	172.217.162.78	192.168.0.16	TLSPv1.2	2902	Application Data
423	5.532958561	192.168.0.16	172.217.162.78	TCP	66	42406 → 443 [ACK] Seq=321 Ack=206483 Win=1219 Len=0 TSval=2921883485 TSecr=3786205894

- ▶ Frame 1: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
- ▶ Ethernet II, Src: ArrisGro_df:6c:30 (c0:05:c2:d6:6c:30), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- ▶ Address Resolution Protocol (request)

```

0000  ff ff ff ff ff ff c0 05  c2 df 6c 30 08 06 00 01  ....
0010  08 00 06 04 00 01 c0 05  c2 df 6c 30 c0 a8 00 01  ....
0020  00 00 00 00 00 00 c0 a8  00 00 00 00 00 00 00 00  ....
0030  00 00 00 00 00 00 00 00  ....

```

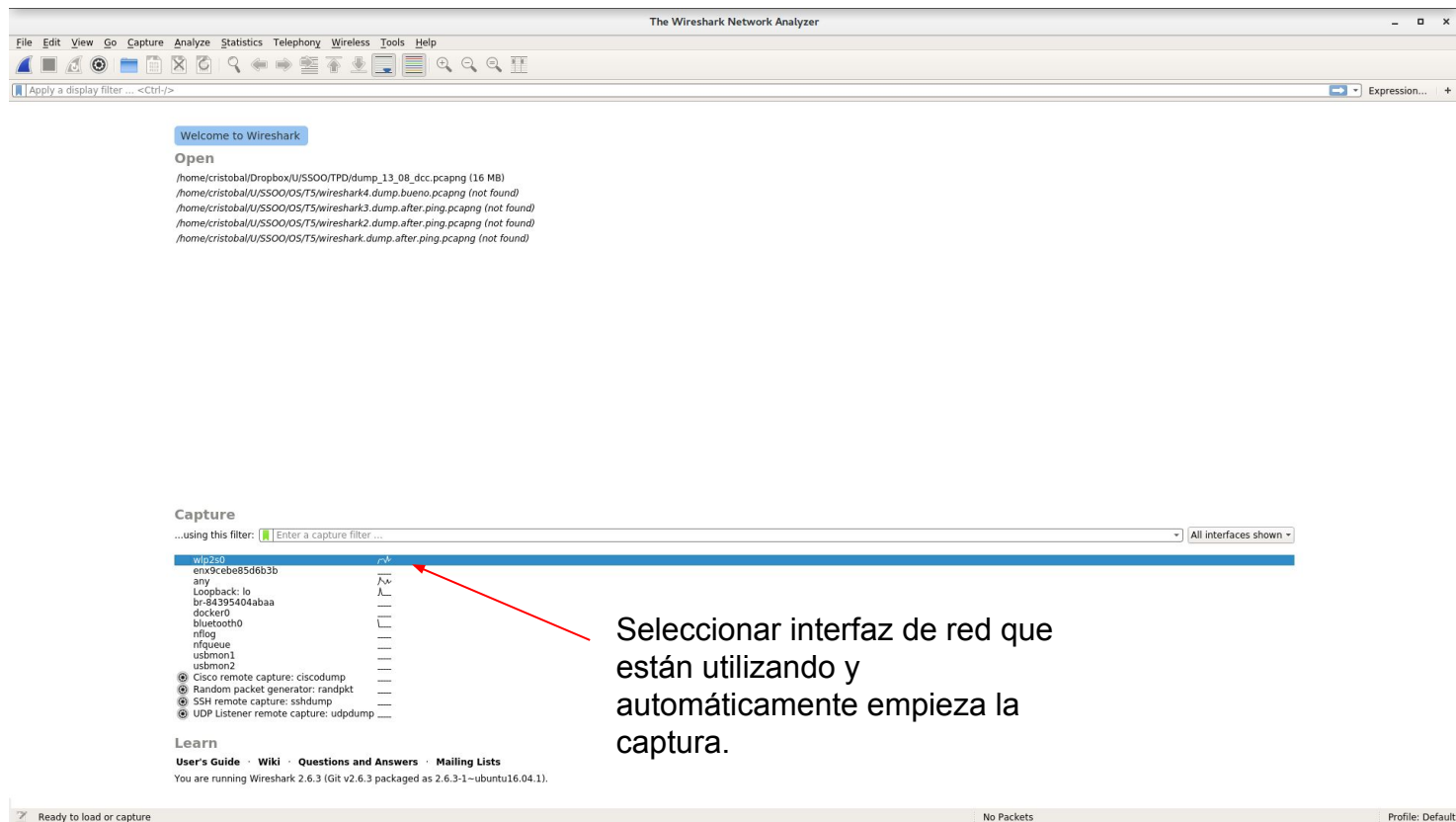
¿ Cómo instalar Wireshark?

- Simplemente ir al sitio oficial (<https://www.wireshark.org/#download>) y elegir su sistema operativo (MacOs / Windows)
- Para los que ocupan alguna versión de Ubuntu simplemente:

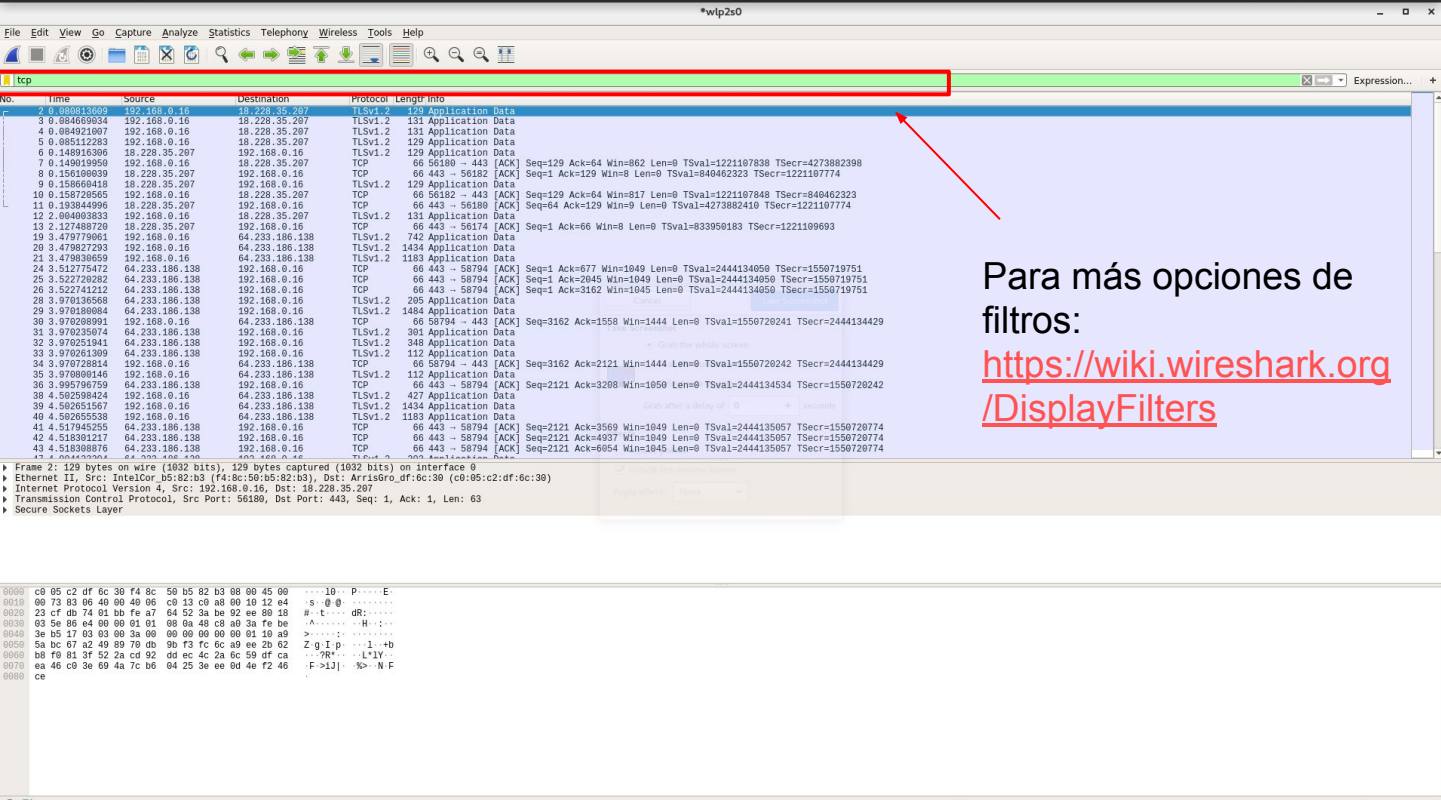
```
sudo add-apt-repository ppa:wireshark-dev/stable  
sudo apt-get update  
sudo apt-get install wireshark  
sudo wireshark Importante!
```

¿ Cómo capturar paquetes?

¿Cómo capturar paquetes?



¿Cómo filtrar los paquetes capturados?



Para más opciones de filtros:

<https://wiki.wireshark.org/DisplayFilters>

Transmission Control Protocol: Protocol

Packets: 61 · Displayed: 46 (75.4%) · Dropped: 0 (0.0%)

Profile: Default

DEMO

Ayudantía Tarea 3

Cristóbal Abarca caabarca1@uc.cl

Lukas Svicarovic lsvicarovic@uc.cl