DEPARTAMENTO DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Trabajo Práctico 1

Wiretapping

18 de abril de 2016 — Teoría de las comunicaciones

Integrante	LU	Correo electrónico
Interlandi, Daniel	—/–	danielinterlandi@gmail.com
Ladelfa, Hernán Nahuel	318/04	nahueladelfa@gmail.com

Instancia	Docente	Nota
Primera entrega		
Segunda entrega		

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2610 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (++54 +11) 4576-3300
http://www.exactas.uba.ar

Índice

1. Introducción

El objetivo de este trabajo es utilizar técnicas provistas por la teoría de la información para distinguir diversos aspectos de la red de manera analítica. Además, sugerimos el uso de dos herramientas modernas de manipulación y análisis de paquetes frecuentemente usadas en el dominio de las redes de computadoras: Wireshark [?] y Scapy [?].

2. Resultados

2.1. Segunda Consigna: Gráficos y Análisis

2.1.1. Red Doméstica

Para la primera captura, se eligió una red domestica de uno de los integrantes del grupo. La captura duro 30 minutos aproximados. Al ser una red pequeña podemos distinguir fácilmente los nodos destacados. La Figura 1. muestra 2 nodos destacados 192.168.0.1 que correspondes al router y el nodo 192.168.0.27 correspondiente al PC desde donde se tomaron las capturas.

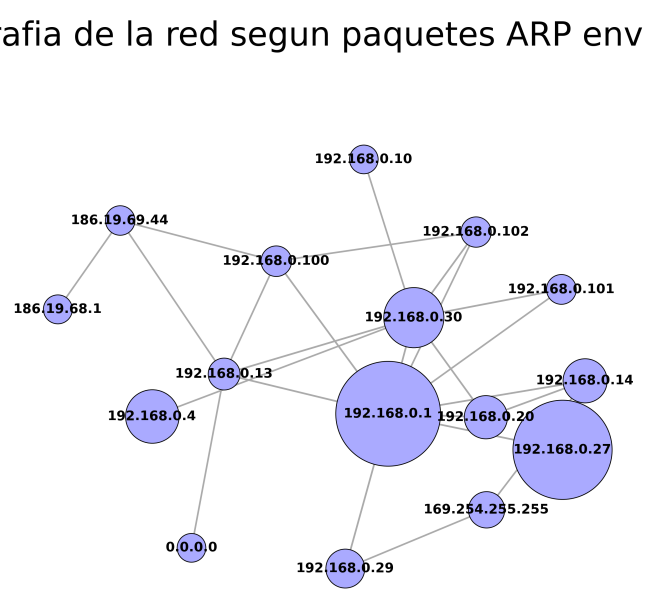

Figura 1: Mi Figura

2.1.2. Histogramas (de IPs y protocolos)

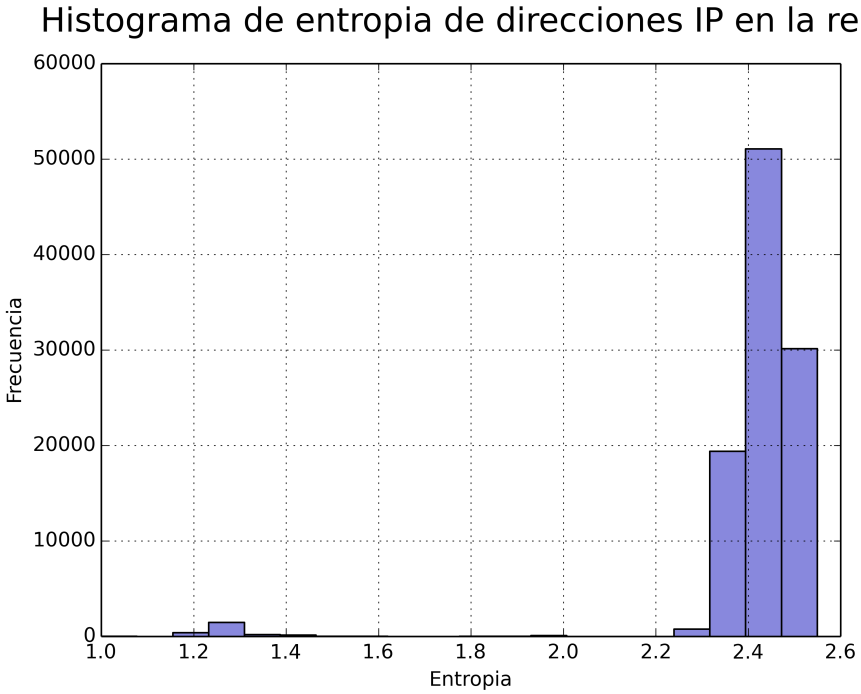

Figura 2: Mi Figura

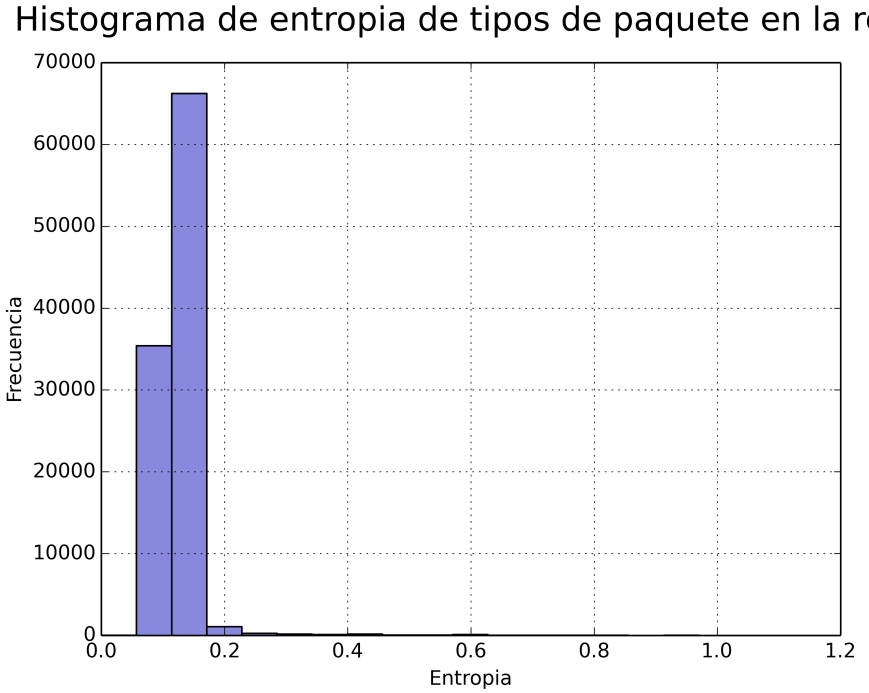

Figura 3: Mi Figura

2.1.3. Paquetes capturados e información

Los gráficos de torta, nos permiten ver la relación entre la cantidad de paquetes y la información que proveen cada nodo en la red. En los primeros 2 gráficos 4. 5. se toma como fuente las ips de la red. Podemos notar que los nodos mencionados anteriormente son los mas frecuentes y por lo tanto los que menos información tienen.

En los siguientes 2 gráficos 6. 7. la fuente es la indicada en la cátedra. Vemos que el protocolo que mas se repite es el IP con un porcentaje muy superior al resto y aportando información casi nula.

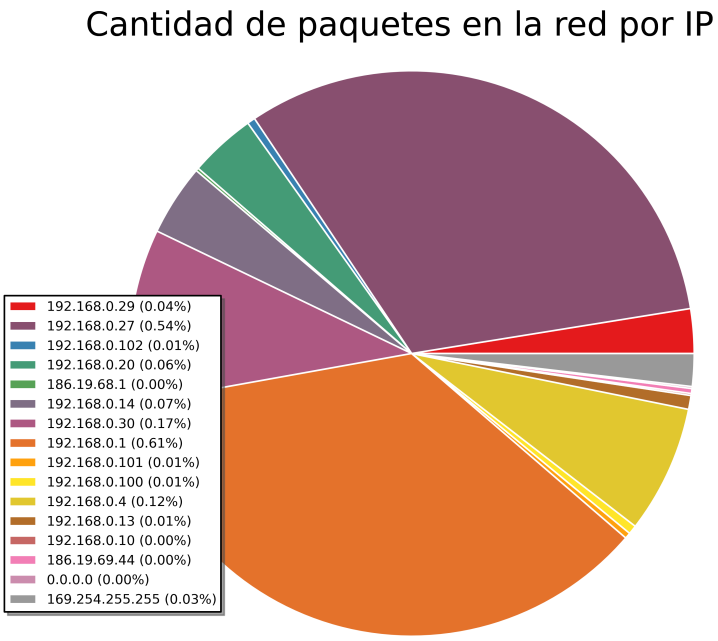

Figura 4: Mi Figura

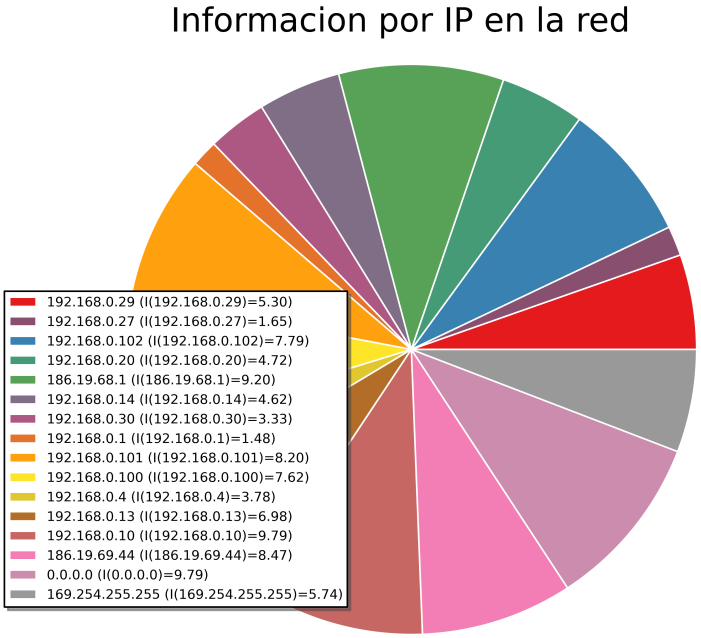

Figura 5: Mi Figura

Figura 6: Mi Figura

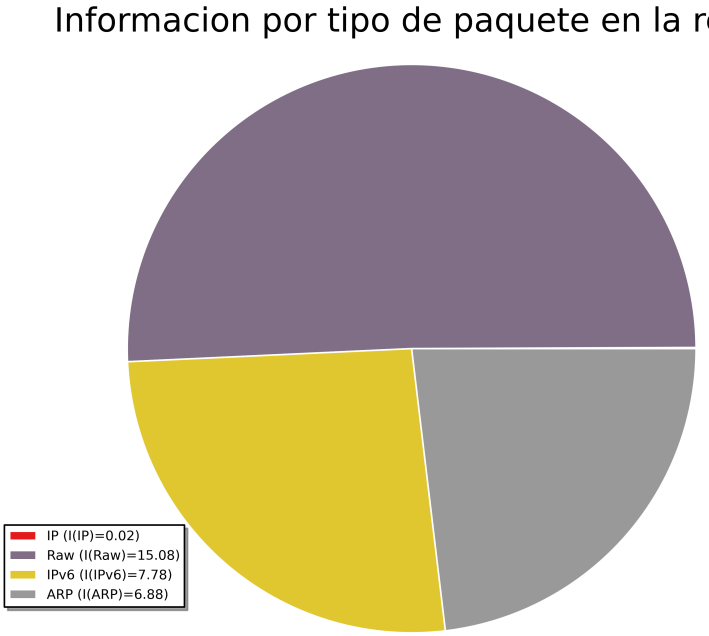

Figura 7: Mi Figura

3. Conclusiones

3.1. Instructivo

3.2. Ejecución

¿sudo ./sniffer.py ¡timeout¿
Filtrado por protocolo ARP:
¿sudo ./sniffer.py ¡timeout¿arp