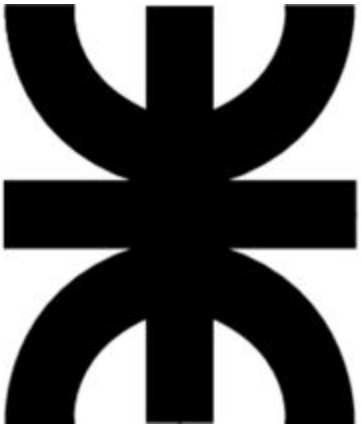
UNIVERSIDAD TECNOLÓGICA NACIONAL

Facultad Regional Resistencia

Ingeniería en Sistemas de Información



Redes de Información

Desafío Nº 1

Grupo: 7

Integrantes:

- Bravin, Juan Ignacio
- Cuzziol Boccioni, Facundo Ramiro
- Diez, Danilo Antonio
- Diaz Duarte, Nicolas
- Jaworski, Martín Ezequiel
- Nadal, Alejandro Fabian
- Rouvier, Selene Susana
- Schuster, Exequiel Andres
- Soto, Juan Cruz
- Teng, Jazmín Inés
- Thouzeau, Edgardo Hernán
- Troncoso, Mariano Adrian
- Zini, Nicolás Adrian

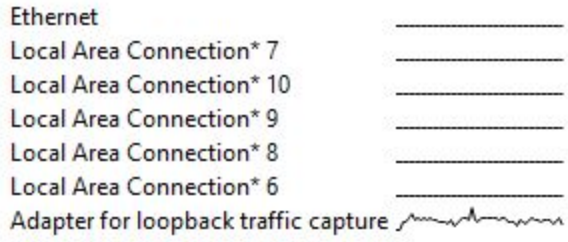
Profesores:

Scappini, Reinaldo J. R.

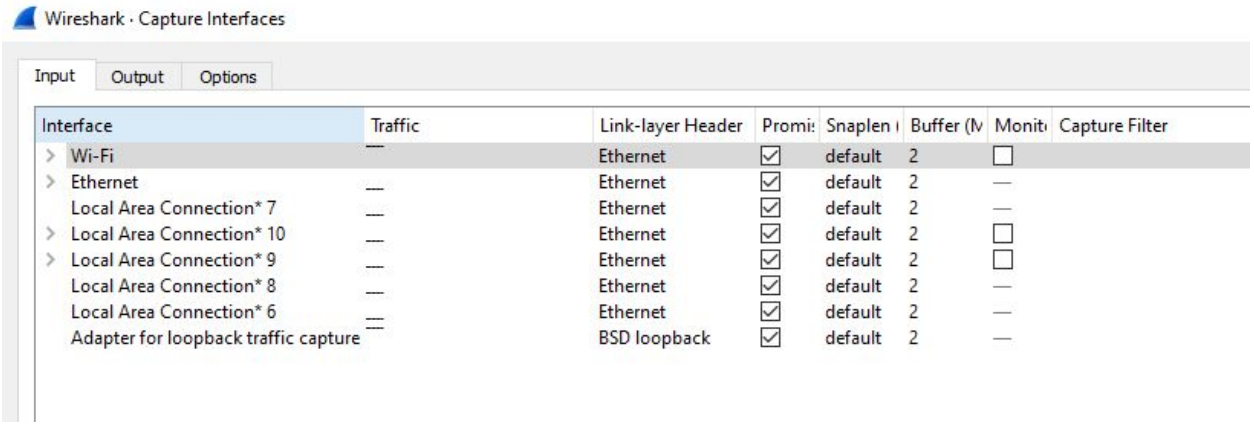
2020

1. ¿Cómo seleccionar interfaces? ¿Qué interfaces aparecen?

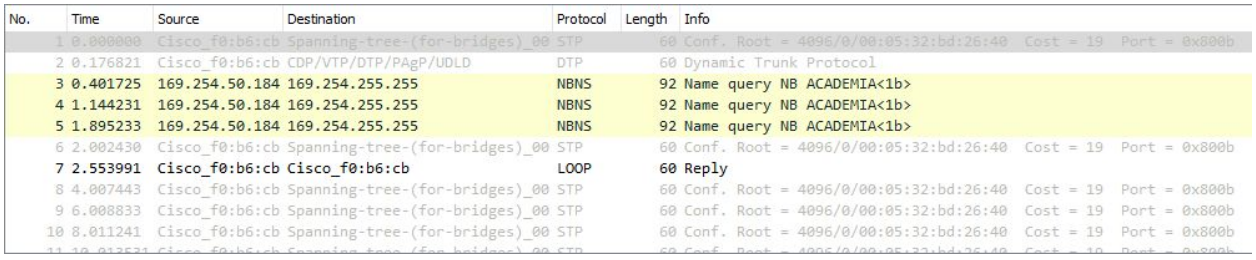
Al iniciar Wireshark se muestra un listado de las interfaces disponibles, pudiendo filtrarlas por nombre. Para seleccionar una basta con hacer doble click en ella.



A su vez, se puede acceder a la configuración de las interfaces mediante Ctrl + K o en Capture/Options.



2. Indique el significado de las columnas más importantes. ¿Qué columnas le parecen importantes para agregar?



Las columnas más importantes son:

- **No:** posición del paquete en la captura.

- **Time:** muestra el Timestamp del paquete. Su formato puede ser modificado desde el menú View Time Display Format.
- **Source:** dirección origen del paquete.
- **Destination:** dirección destino del paquete.
- **Protocol:** nombre del protocolo del paquete.
- **Length:** Longitud o tamaño en bytes del paquete.
- **Info:** información adicional del contenido del paquete.

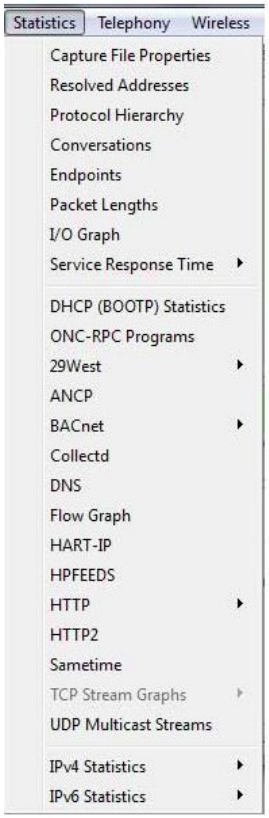
A su vez, también se podría agregar como columnas, el puerto de origen y el de destino.

3. ¿Cómo funcionan los filtros?

Los **filtros** se utilizan para mostrar únicamente los paquetes que cumplen con lo especificado en el filtro. En el caso de no establecer ninguno, Wireshark nos mostrará la totalidad del tráfico y nos lo presentará en la pantalla principal.

Cuándo estamos ante una toma de datos elevada, los filtros nos permiten mostrar únicamente aquellos paquetes que cumplen con los criterios dados.
Los filtros a su vez, pueden ser aplicados en dos lugares denominados como filtros de captura y filtros de muestra.

4. ¿Qué opciones de Estadística se pueden utilizar?



Existe una gran variedad de opciones estadísticas que se pueden utilizar desde el menú Statistics:

- **Capture file properties**: Muestra información relativa a la cantidad de paquetes, el tamaño de los mismos y el tiempo transcurrido sobre los datos capturados
- **Resolved addresses**: lista todas las direcciones IP y nombres DNS que se resolvieron en su captura de paquetes. De esta manera, puede tener una idea de todos los diferentes recursos a los que se accedió en la captura de paquete**s.**
- **Protocol Hierarchy**: Muestra un árbol jerárquico de las estadísticas de protocolo.
- **Conversations**: Muestra una lista de conversaciones (tráfico entre dos puntos finales).
- **Endpoints**: Muestra una lista de puntos finales (el tráfico hacia / desde una dirección). Un punto final de red es el punto final lógico de tráfico de protocolo separada de una capa de protocolo específico.
- **Packet Lengths**: Muestra la cantidad de paquetes agrupados por categorías según el tamaño de los mismos.
- **I/O Graphs**: Muestra gráficas específicas del usuario como por ejemplo, el número de paquetes a lo largo del tiempo.
- **Service Response Time**: Muestra el tiempo de respuesta de servicio, es decir, el tiempo transcurrido entre la solicitud y la respuesta correspondiente. Esta información está disponible para diversos protocolos: AFP, CAMEL, DCE-RPC, DIAMETER, FC, GTP, H.225 RAS, LDAP, MEGACO, MGCP, NCP, ONC-RPC, RADIUS, SCSI, SMB, SMB2.
- DHCP (BOOTP)
- ONC-RPC Programs
- 29West
- ANCP
- BACnet
- Collectd
- DNS
- Flow Graph
- HART-IO
- HPDEEDS
- HTTP
- HTTP2
- Sametime
- TCP Stream Graphs
- UDP Multicast Streams
- F5
- IPv4 Statistics
- IPv6 Statistics

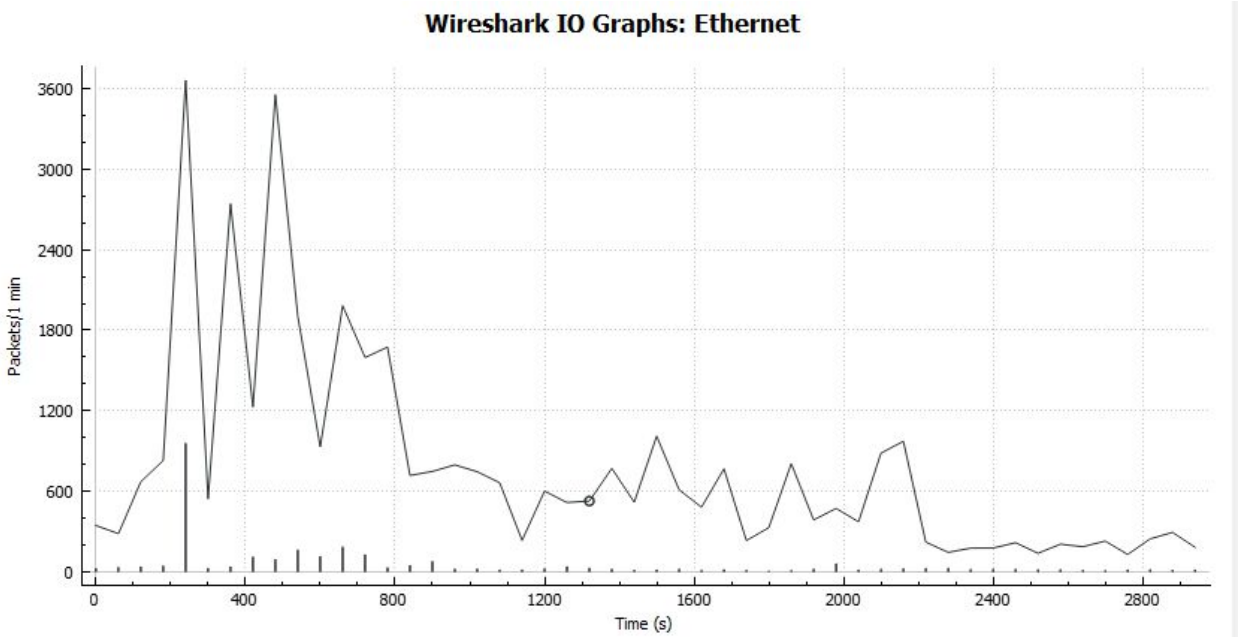
5. ¿Cuál es la utilidad de la opción Follow (Seguir)?

La opción Follow une el flujo de paquetes individuales de tal manera que podamos inspeccionarlo más cómodamente. Permite reensamblar una secuencia de paquetes en un formato fácil de entender. Las diferentes opciones son:

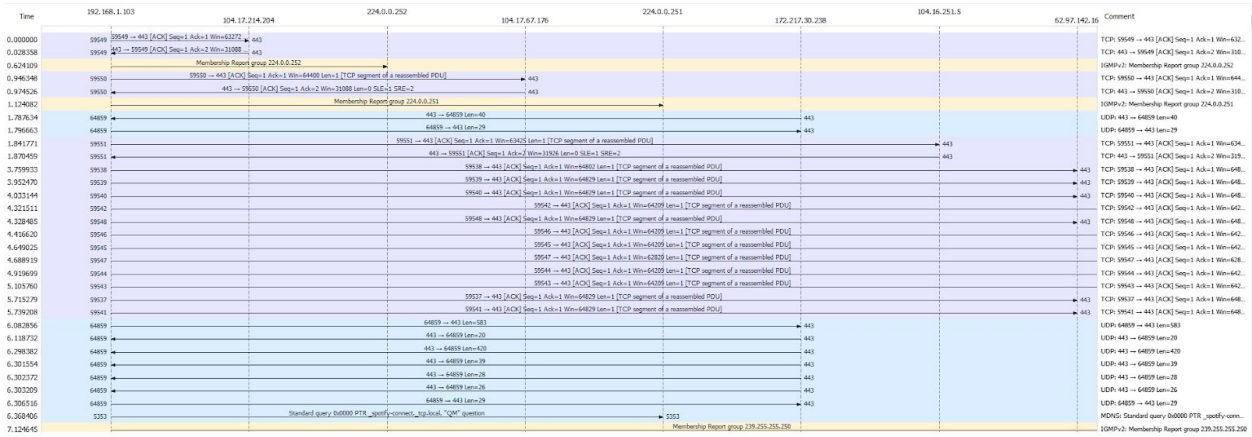
- Follow TCP Stream
- Follow UDP Stream
- Follow TLS Stream
- Follow HTTP Stream

6. ¿Qué opciones gráficas encontró? ¿Qué utilidad se imagina para las mismas?

I/O Graphs:
Gráfica personalizable y con diversas opciones que nos muestra el tráfico de entrada y salida de una captura.
Es sobre todo útil para solucionar problemas al ver picos y caídas en el tráfico.

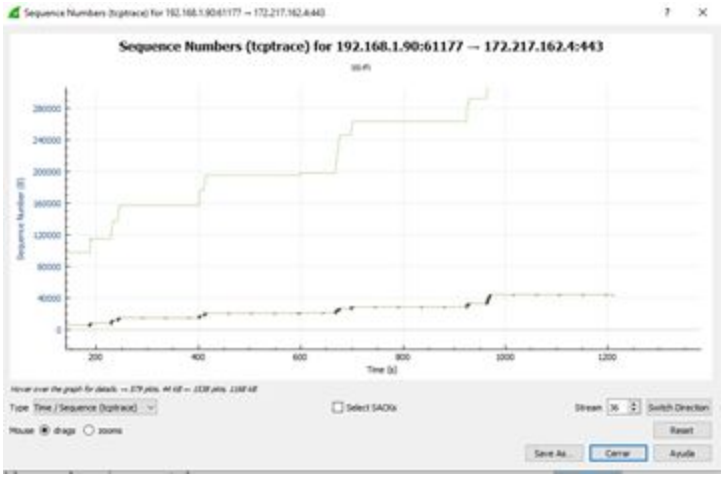


Flow Graph:
Permite la visualización gráfica del flujo de datos entre las diferentes conexiones realizadas entre hosts. Con este tipo de gráficos podemos estudiar, por ejemplo, los problemas que pudiesen surgir en un establecimiento de conexión.



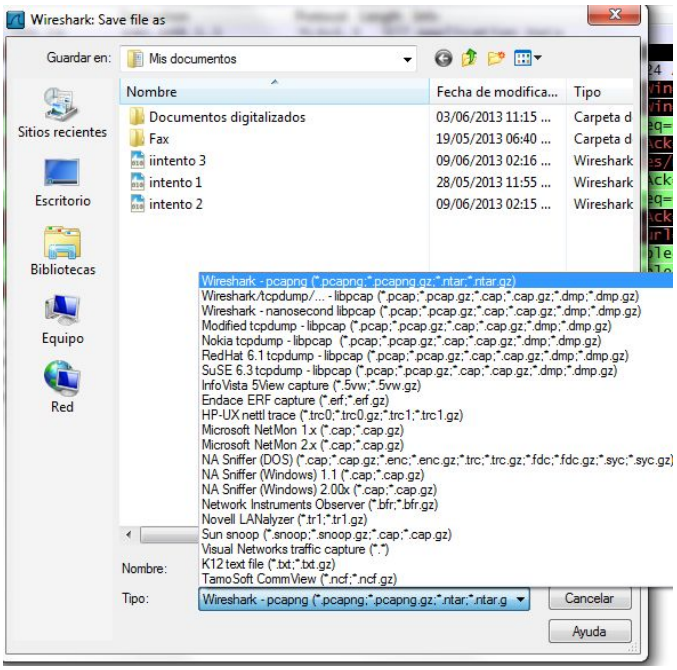
Gráficas tcptrace:
un tipo de gráficas basado en el número de secuencia respecto al tiempo.
¿Qué problemas podemos detectar con tcptrace?

- TCP ACK Retransmission
- ACKs Duplicados



7. ¿Cómo se guarda una captura? ¿Cómo se recupera? ¿Qué significan los distintos formatos?

Para guardar una captura se debe presionar Ctrl + S. Esta opción guarda la captura actual, si no ha configurado un nombre de archivo de captura por defecto. También la opción Guardar Como, que le permite guardar el archivo de captura actual a cualquier archivo que desee.
A continuación, aparece el archivo de captura cuadro de diálogo “Guardar Como”.



Los diferentes formatos disponibles son:

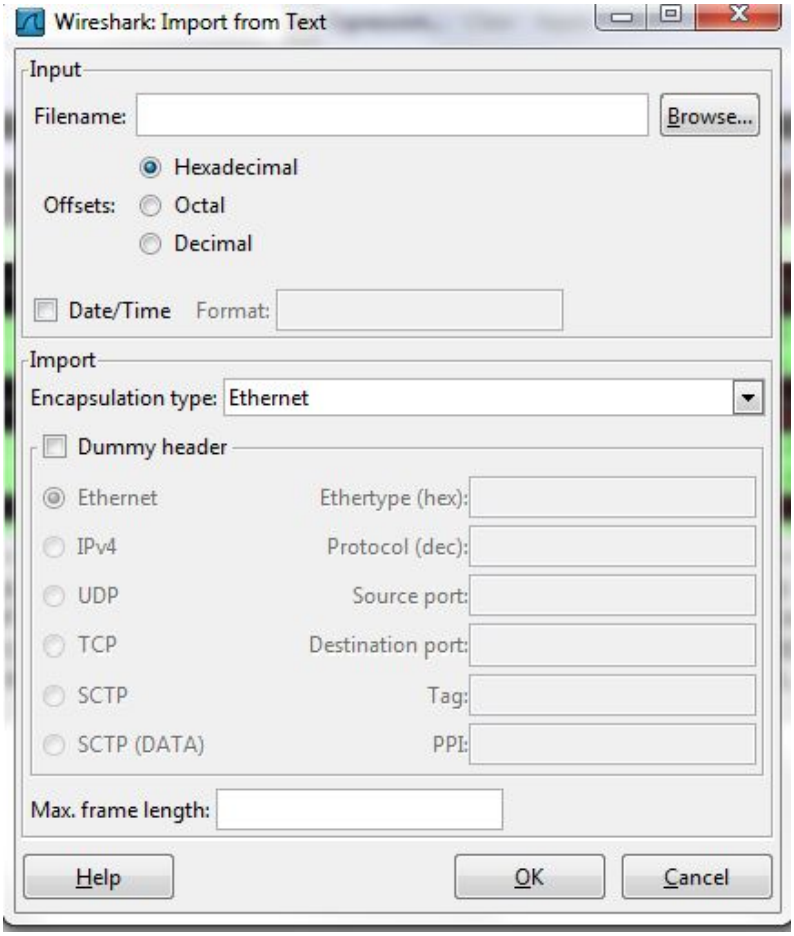
- pcapng (*.pcapng). Un formato flexible y ampliable para libpcap. Wireshark 1.8 y posteriores guardan los archivos por defecto como pcapng. Versiones anteriores 1 1.8 utilizan libpcap.
- libpcap, tcpdump y otras herramientas utilizan el formato de captura de cpdump (*.pcap,*.cap,*.dmp)
- Accellent 5Views (*.5vw)
- HP-UX's nettl (*.TRC0,*.TRC1)
- Microsoft Network Monitor - NetMon (*.cap)
- Network Associates Sniffer - DOS (*.cap,*.enc,*.trc,*fdc,*.syc)
- Network Associates Sniffer - Windows (*.cap)
- Network Instruments Observer version 9 (*.bfr)
- Novell LANalyzer (*.tr1)
- Oracle (previamente Sun) snoop (*.snoop,*.cap)
- Visual Networks Visual UpTime traffic (*.*)

Para importar capturas, el menú **file** contiene opciones para abrir y combinar archivos de captura, guardar / imprimir / exportar archivos de captura en su totalidad o en parte, y para salir de Wireshark.

Open: Este elemento de menú abre el cuadro de diálogo de abrir archivo que le permite cargar un archivo de captura para su visualización.

Open Recent: Este elemento de menú muestra un submenú que contiene los archivos de captura abiertos recientemente.

Importar capturas :Este elemento de menú abre el cuadro de diálogo de importación de archivos que le permite importar un archivo de texto en una nueva captura temporal.



Controles específicos de este diálogo de importación se dividen en dos secciones:

Importar - Import: Determinar cómo son los datos que desea importar.

Actividades específicas:

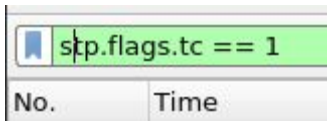
Actividad 1:

Con la captura llamada Captura 1, filtrar las tramas de forma que solo aparezcan aquellas que pertenezcan al protocolo Spanning Tree y que tengan el flag TC activado. Identifique el valor de los campos:

i. Message Age
ii. Max Age
iii. Hello Time
iv. Forward Delay

Desarrollo

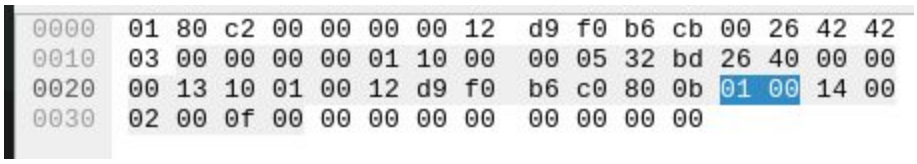
Para filtrar a la vez por tramas de Spanning Tree, y asegurarnos que tengan el campo TC (topology control) activado, colocamos el siguiente filtro en la barra de filtrado.



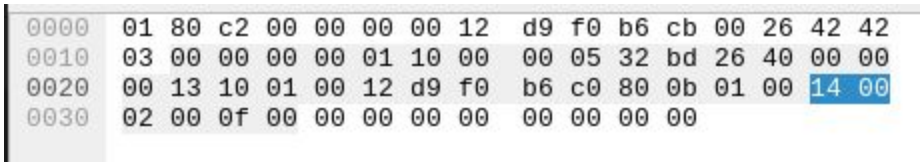
Aca podemos ver los cuatro segmentos de trama solicitados.

Los cuales, en hexa, son los siguientes:

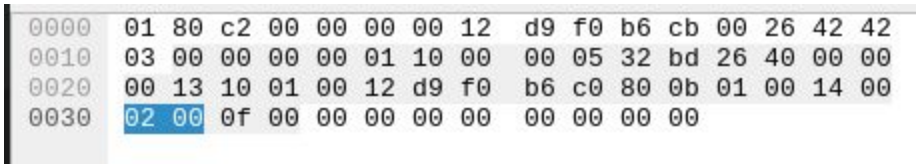
Message Age



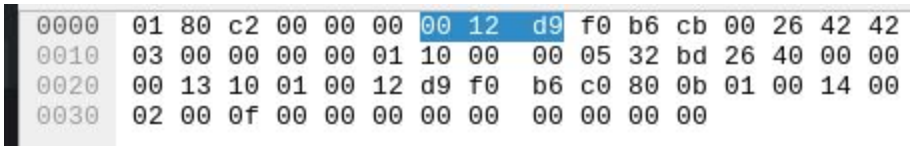
Max Age



Hello Time



Forward Delay



Actividad 2:

Con la captura llamada Captura 2, trate de identificar de qué se trata su contenido (que protocolos aparecen, si hay una secuencia que se pueda seguir etc.), ¿qué herramienta de las utilizadas le parece útil para lograr este objetivo?

Al importar la Captura 2, podemos ver que contiene los siguientes protocolos:

- **TCP:** Transmission Control Protocol
- **MSNMS:** MSN Messenger Service
- **TELNET:** Telecommunication Network

El uso del protocolo TELNET se utiliza en Internet o en una red de área local para dar una comunicación con otra computadora a través de una terminal, de forma muy insegura. Telnet no debe ser utilizado para esta tarea en la actualidad. Para esto, existe **ssh,** secure shell connection.

Además de este protocolo, también podemos ver que se utiliza el protocolo MSNMS (MSN Messenger Service), el cual podría usarse para servicio de mensajería de Microsoft en segundo plano.]

Vamos a filtrar por stream index, donde un stream index identifica una comunicación entre dos puertos TCP, de dos IP distintas fuente y destino.

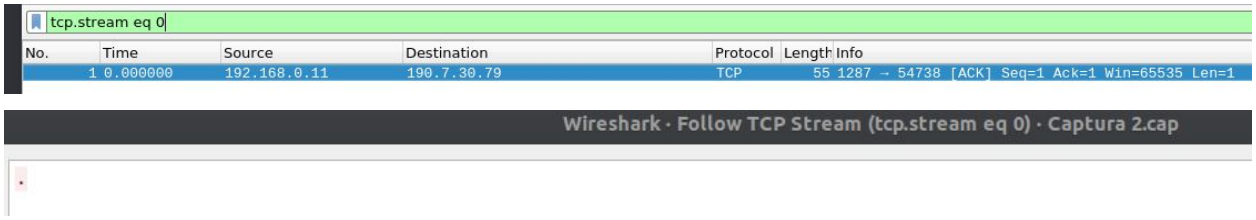
Utilizando este filtro identificamos las comunicaciones entre los siguientes pares de IP y de puertos:

- Stream 0: 102.168.0.11: 1287 - 190.7.30.79:54738
- Stream 1: 192.168.0.11:1260 - 207.46.106.42:1863
- Stream 2: 192.168.0.11 - 12.0.1.28:1295

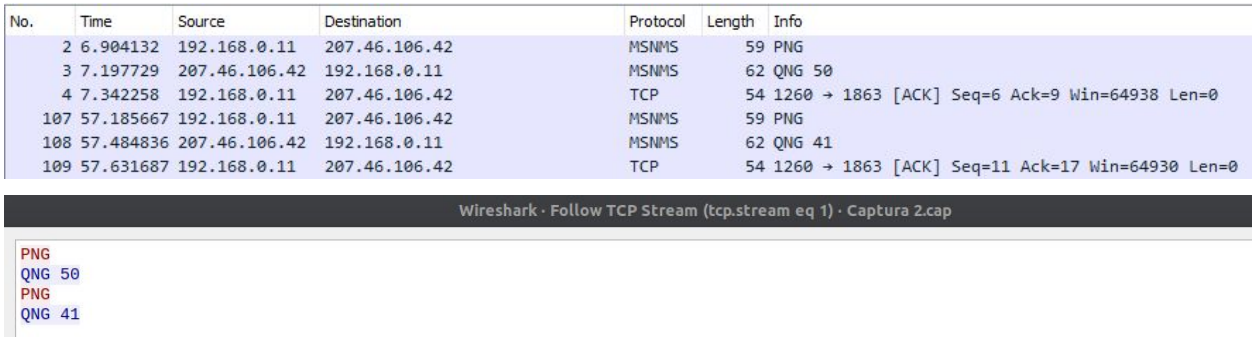
- Stream 3: 192.168.0.11:1292 - 65.54.170.28:443

Stream 0

Es posible que sea una conversación que no se concreta, puesto que consiste en un solo paquete ACK. La conversación puede haberse establecido pero nunca se compartió información.



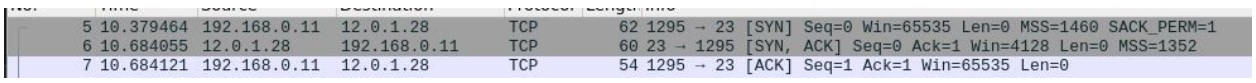
Stream 1



Aca podemos ver una conversación entre dos computadoras a través del protocolo MSNMS.

Stream 2

Acá tenemos una comunicación entre dos computadoras a través de TELNET. Podemos ver el establecimiento de la conexión mediante el handshake.
Spurious Retransmissions are one's that are considered unnecessary -- in Wireshark, a retransmission is marked as "spurious" when Wireshark has seen the ACK for the data already.



Luego, vemos que se mandan un conjunto de tramas, que contienen información de TELNET. Tras cada trama, el destino hace un mensaje de ACK, para reconocer la llegada.

```
23 22.875008  192.168.0.11  12.0.1.28      TELNET    55 Telnet Data ...
24 23.091005  12.0.1.28     192.168.0.11   TELNET    60 Telnet Data ...
25 23.091077  192.168.0.11  12.0.1.28      TELNET    55 Telnet Data ...
26 23.309762  12.0.1.28     192.168.0.11   TELNET    60 Telnet Data ...
27 23.343308  192.168.0.11  12.0.1.28      TELNET    55 Telnet Data ...
28 23.561542  12.0.1.28     192.168.0.11   TELNET    60 Telnet Data ...
29 23.736602  192.168.0.11  12.0.1.28      TCP       54 1295 → 23 [ACK] Seq=35 Ack=1737 Win=65484 Len=0
```

Hubo inconvenientes en la transmisión, entre ellos, paquetes fuera de orden y retransmisiones innecesarias

```
74 44.187053  12.0.1.28     192.168.0.11   TELNET    614 Telnet Data ...
75 44.187124  192.168.0.11  12.0.1.28      TCP        54 1295 → 23 [ACK] Seq=55 Ack=2890 Win=64331 Len=0
76 44.293431  12.0.1.28     192.168.0.11   TCP        60 [TCP Out-Of-Order] 23 → 1295 [PSH, ACK] Seq=1769 Ack=55 Win=4074 Len=1
```

```
87 47.070904  192.168.0.11  12.0.1.28      TCP        54 1295 → 23 [ACK] Seq=56 Ack=4051 Win=65497 Len=0
88 47.273688  12.0.1.28     192.168.0.11   TELNET     92 [TCP Spurious Retransmission] Telnet Data ...
```

Dejamos aquí el resultado de correr el seguimiento del stream con Follow TCP Transmission

```
..............CCCCCC
-------------- route-server.ip.att.net ---------------
---------  AT&T IP Services Route Monitor  -----------

The information available through route-server.ip.att.net is offered
by AT&T's Internet engineering organization to the Internet community.
This router has the global routing table view from each of the above
routers, providing a glimpse to the Internet routing table from the
AT&T network's perspective.

This router maintains eBGP peerings with customer-facing routers
throughout the AT&T IP Services Backbone:

 12.123.21.243 .............P....  Atlanta, GA            12.123.133.124
Austin, TX
 12.123.41.250   Cambridge, MA          12.123.5.240    Chicago,IL
 12.123.17.244   Dallas, TX             12.123.139.124  Detroit, MI
 12.123.37.250   Denver, CO             12.123.134.124  Houston, TX
 12.123.29.249   Los Angeles, CA        12.123.1.236    New York, NY
 12.123.33.249   Orlando,FL             12.123.137.124  Philadelphia, PA
 12.123.142.124  Phoenix, AZ            12.123.145.124  San Diego, CA
 12.123.13.241   San Francisco, CA      12.123.25.245   St. Louis, MO
 12.123.45.252   Seattle, WA            12.123.9.241    Washington, DC

*** Please Note:

Ping and traceroute delay figures measured with this box are unreliable,
due to the high CPU load this box experiences when complicated "show"
commands
are being executed.
```

```
For questions about this route-server, send email to: jayb@att.com

*** route-server.ip.att.net now uses AAA for logins.  Login with
    username "rviews".
*** 'terminal length 0' temporarily enforced for all logins -- sorry

-------------- route-server.ip.att.net ---------------


User Access Verification

Username: ..........ANSI..rrvviieewwss

route-server>sshh  iipp  pprroototcooclosl
s
*** IP Routing is NSF aware ***

Routing Protocol is "bgp 65000"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Route flap dampening configured and enabled
  Halflife time 15 minutes, reuse value 750
  Suppress value 2000, maximum suppress time 60
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Redistributing: static
  Neighbor(s):
    Address          FiltIn FiltOut DistIn DistOut Weight RouteMap
    12.123.1.236                                   1
    12.123.5.240                                   1
    12.123.9.241                                   1
    12.123.13.241                                  1
    12.123.17.244                                  1
    12.123.21.243                                  1
    12.123.25.245                                  1
    12.123.29.249                                  1
    12.123.33.249                                  1
    12.123.37.250                                  1
 --More--  .........        .........    Address          FiltIn FiltOut
DistIn DistOut Weight RouteMap
    12.123.41.250                                  1
```

```
    12.123.45.252                                 1
    12.123.133.124                                1
    12.123.134.124                                1
    12.123.137.124                                1
    12.123.139.124                                1
    12.123.142.124                                1
    12.123.145.124                                1
  Maximum path: 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    12.123.139.124         20      00:02:16
    12.123.137.124         20      00:01:26
    12.123.5.240           20      00:09:09
    12.123.142.124         20      00:11:42
    12.123.13.241          20      00:14:52
    12.123.134.124         20      00:13:48
    12.123.133.124         20      00:01:31
    12.123.9.241           20      00:05:53
    12.123.21.243          20      00:10:22
    12.123.17.244          20      00:02:45
    12.123.29.249          20      00:10:57
 --More--  .........        .........    Gateway         Distance      Last
Update
    12.123.145.124         20      00:06:37
    12.123.1.236           20      00:02:39
    12.123.25.245          20      00:03:27
    12.123.41.250          20      00:07:54
    12.123.45.252          20      00:01:52
    12.123.37.250          20      00:00:41
    12.123.33.249          20      00:09:26
  Distance: external 20 internal 200 local 200

route-server>eexxiitt
```

Las últimas tramas son las TCP destinadas a finalizar la comunicación.

103	51.936925	12.0.1.28	192.168.0.11	TCP	60 23 → 1295 [FIN, PSH, ACK] Seq=4501 Ack=62 Win=4067 Len=0
104	51.936996	192.168.0.11	12.0.1.28	TCP	54 1295 → 23 [ACK] Seq=62 Ack=4502 Win=65047 Len=0
105	51.937201	192.168.0.11	12.0.1.28	TCP	54 1295 → 23 [FIN, ACK] Seq=62 Ack=4502 Win=65047 Len=0
106	52.156713	12.0.1.28	192.168.0.11	TCP	60 23 → 1295 [ACK] Seq=4502 Ack=63 Win=4067 Len=0

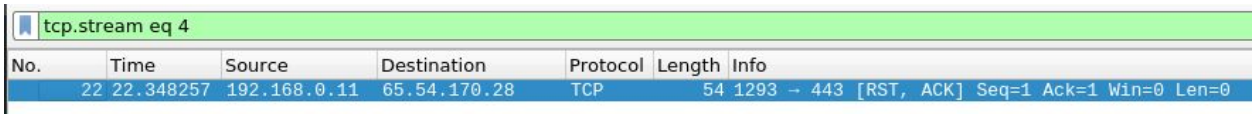
Stream 3

tcp.stream eq 3

No.	Time	Source	Destination	Protocol	Length	Info
21	17.348727	192.168.0.11	65.54.170.28	TCP	54	1292 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

En este stream y el siguiente, tenemos dos conexiones reseteadas, con los mismos orígenes y destinos.

Stream 4

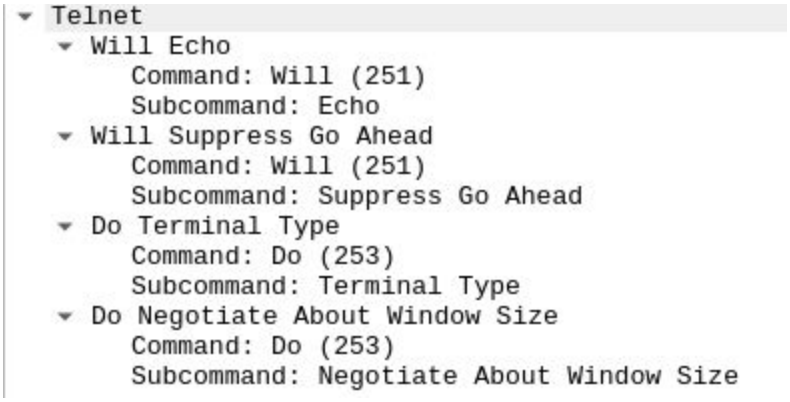


Stream 5

Son los mismos pares de IP que la Stream 3, pero se identifica con un id de stream distinto debido a que cambia el puerto origen de 1295 a 1296.

No.	Time	Source	Destination	Protocol	Length	Info
110	60.896203	192.168.0.11	12.0.1.28	TCP	62	1296 → 23 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
111	61.118246	12.0.1.28	192.168.0.11	TCP	60	23 → 1296 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1352
112	61.118315	192.168.0.11	12.0.1.28	TCP	54	1296 → 23 [ACK] Seq=1 Ack=1 Win=65535 Len=0
113	61.118699	192.168.0.11	12.0.1.28	TELNET	55	Telnet Data ...
114	61.341176	12.0.1.28	192.168.0.11	TELNET	66	Telnet Data ...
115	61.341252	192.168.0.11	12.0.1.28	TELNET	56	Telnet Data ...
116	61.344172	12.0.1.28	192.168.0.11	TELNET	614	Telnet Data ...
117	61.344228	192.168.0.11	12.0.1.28	TELNET	75	Telnet Data ...
118	61.346406	12.0.1.28	192.168.0.11	TELNET	614	Telnet Data ...
119	61.453683	192.168.0.11	12.0.1.28	TCP	54	1296 → 23 [ACK] Seq=25 Ack=1133 Win=64403 Len=0
120	61.540848	12.0.1.28	192.168.0.11	TCP	60	23 → 1296 [ACK] Seq=1133 Ack=2 Win=4127 Len=0
121	61.540917	192.168.0.11	12.0.1.28	TELNET	55	Telnet Data ...
122	61.677049	12.0.1.28	192.168.0.11	TELNET	607	Telnet Data ...
123	61.855995	192.168.0.11	12.0.1.28	TCP	54	1296 → 23 [ACK] Seq=26 Ack=1686 Win=65535 Len=0
124	61.960696	12.0.1.28	192.168.0.11	TCP	60	23 → 1296 [ACK] Seq=1686 Ack=26 Win=4103 Len=0
125	62.079019	12.0.1.28	192.168.0.11	TELNET	106	Telnet Data ...
126	62.079247	192.168.0.11	12.0.1.28	TELNET	64	Telnet Data ...
127	62.500377	12.0.1.28	192.168.0.11	TCP	60	23 → 1296 [ACK] Seq=1738 Ack=36 Win=4093 Len=0
128	63.700826	192.168.0.11	12.0.1.28	TELNET	55	Telnet Data ...
129	63.923583	12.0.1.28	192.168.0.11	TELNET	60	Telnet Data ...
130	64.068730	192.168.0.11	12.0.1.28	TCP	54	1296 → 23 [ACK] Seq=37 Ack=1741 Win=65480 Len=0
131	69.070839	192.168.0.11	12.0.1.28	TCP	54	1296 → 23 [FIN, ACK] Seq=37 Ack=1741 Win=65480 Len=0
132	69.292632	12.0.1.28	192.168.0.11	TCP	60	23 → 1296 [ACK] Seq=1741 Ack=38 Win=4092 Len=0
133	71.592198	12.0.1.28	192.168.0.11	TCP	60	23 → 1296 [FIN, PSH, ACK] Seq=1741 Ack=38 Win=4092 Len=0
134	71.592250	192.168.0.11	12.0.1.28	TCP	54	1296 → 23 [ACK] Seq=38 Ack=1742 Win=65480 Len=0

Se evidencia el inicio y fin de conversación con los handshakes correspondientes.
Hay paquetes telnet donde se establecen las características de la conexión entre terminales:



Paquete 114

Por ejemplo, will echo quiere decir que lo que se escriba en la terminal de origen, se escribirá en la de destino.

En rojo, se muestra la información enviada por la fuente, en el Follow TCP sobre el stream 5.

```
e............xiCCCCCC
-------------- route-server.ip.att.net ---------------
---------  AT&T IP Services Route Monitor  -----------

The information available through route-server.ip.att.net is offered
by AT&T's Internet engineering organization to the Internet community.
This router has the global routing table view from each of the above
routers, providing a glimpse to the Internet routing table from the
AT&T network's perspective.

This router maintains eBGP peerings with customer-facing routers
throughout the AT&T IP Services Backbone:

12.123.21.243 ................P....  Atlanta, GA            12.123.133.124
Austin, TX
12.123.41.250   Cambridge, MA          12.123.5.240    Chicago,IL
12.123.17.244   Dallas, TX             12.123.139.124  Detroit, MI
12.123.37.250   Denver, CO             12.123.134.124  Houston, TX
12.123.29.249   Los Angeles, CA        12.123.1.236    New York, NY
12.123.33.249   Orlando,FL             12.123.137.124  Philadelphia, PA
12.123.142.124  Phoenix, AZ            12.123.145.124  San Diego, CA
12.123.13.241   San Francisco, CA      12.123.25.245   St. Louis, MO
12.123t.45.252   Seattle, WA            12.123.9.241    Washington, DC

*** Please Note:
```

```
Ping and traceroute delay figures measured with this box are unreliable,
due to the high CPU load this box experiences when complicated "show"
commands
are being executed.

For questions about this route-server, send email to: jayb@att.com

*** route-server.ip.att.net now uses AAA for logins.  Login with
   username "rviews".
*** 'terminal length 0' temporarily enforced for all logins -- sorry

-------------- route-server.ip.att.net ---------------


User Access Verification

Username: exi......t....ANSI.... .
```

Nos pareció muy útil utilizar la herramienta de filtrado de streams, Coloring Rules y la de Follow el stream para identificar los contenidos que se transmitieron.