

Analizando capturas con Wireshark

Eva M. Castro

Universidad Rey Juan Carlos
eva.castro@urjc.es

Índice

- Escenario de capturas
- Tráfico capturado
- Wireshark
 - Perfiles
 - Conversaciones
 - Filtros
 - Columnas
 - Perfil personalizado para tráfico TCP
 - Gráfica de flujo
 - Gráfica de secuencia (tcptrace)
 - Gráfica e/s

Escenario de capturas

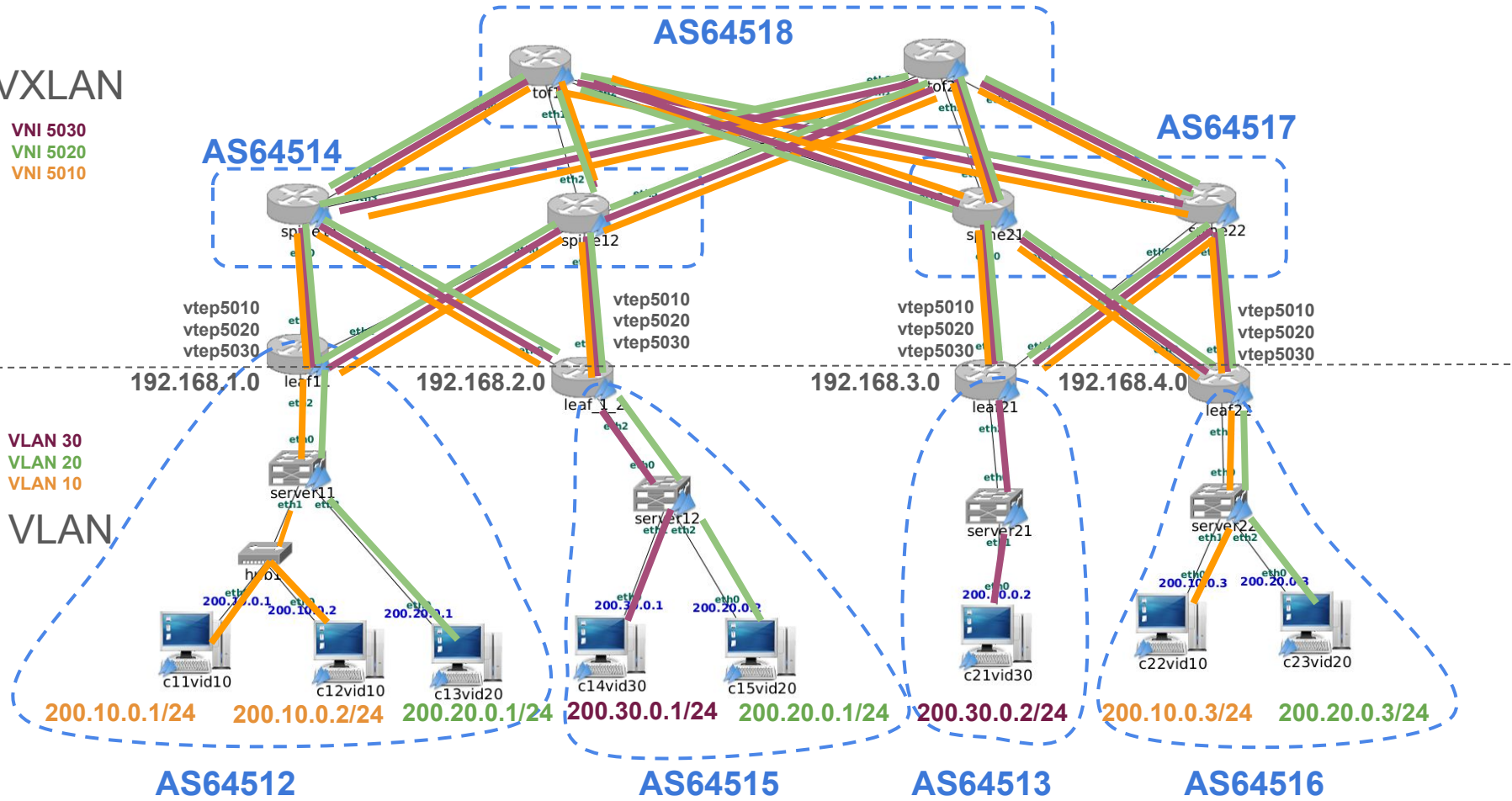
VXLAN

- VNI 5030
- VNI 5020
- VNI 5010

- VLAN 30
- VLAN 20
- VLAN 10

VLAN

- 200.10.0.1/24
- 200.10.0.2/24
- 200.20.0.1/24
- 200.30.0.1/24
- 200.20.0.1/24
- 200.30.0.2/24
- 200.10.0.3/24
- 200.20.0.3/24



AS64512

AS64515

AS64513

AS64516

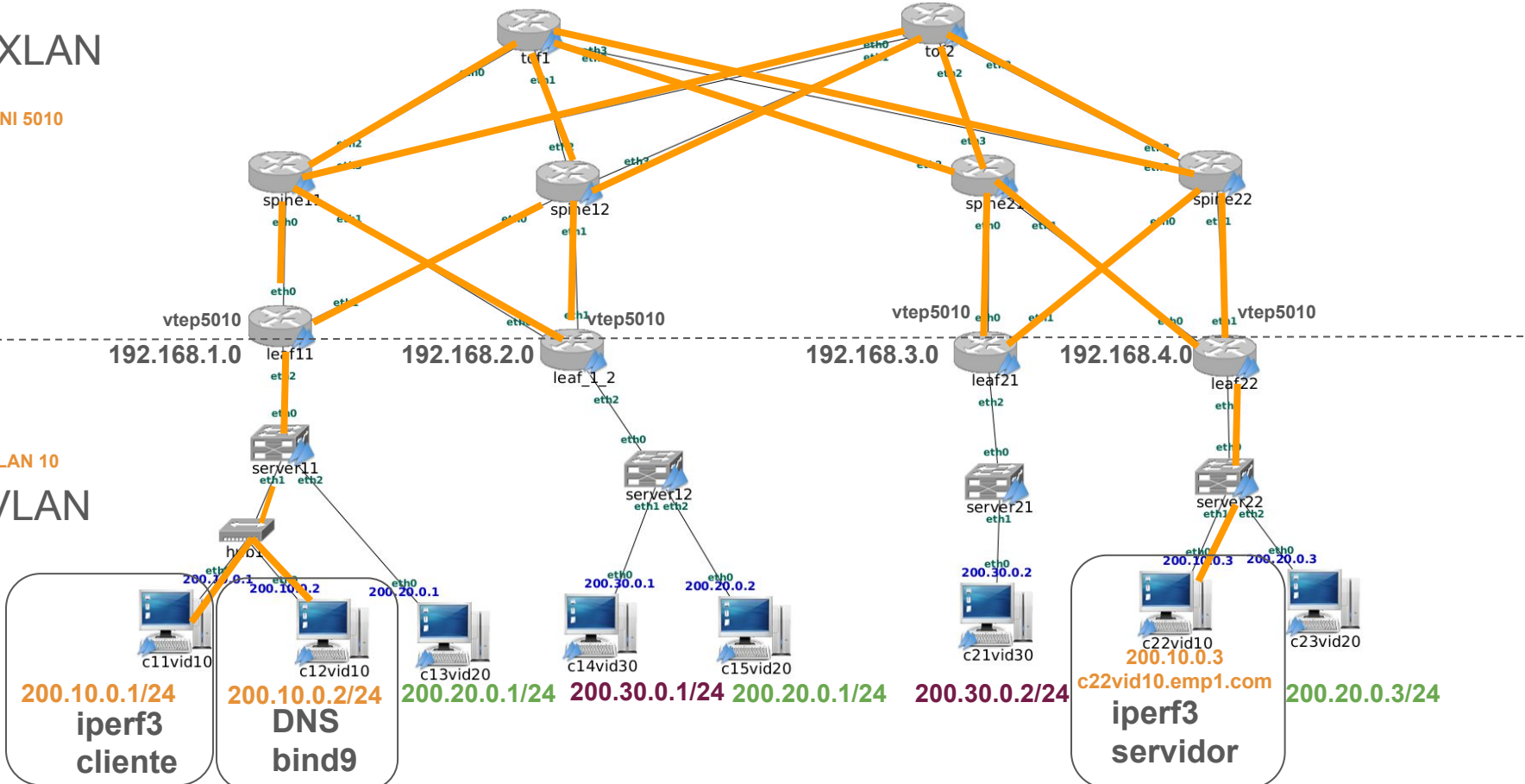
Escenario de capturas

VXLAN

VNI 5010

VLAN 10

VLAN



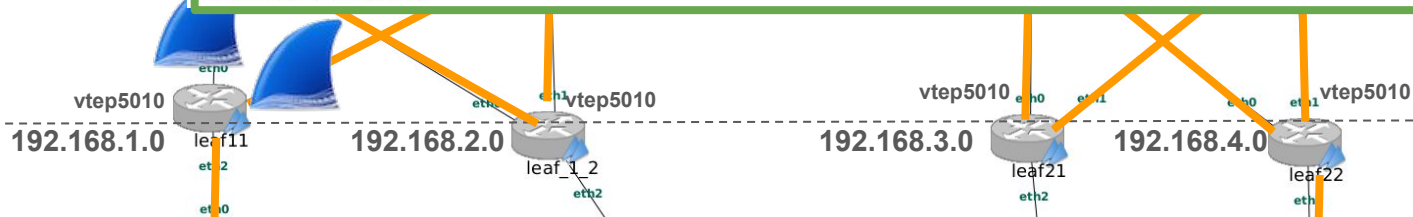
Interfaces donde se captura

VXLAN

VNI 5010

```
Frame 102: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on eth0  
Ethernet II, Src: 02:42:15:e1:01:00 (02:42:15:e1:01:00), Dst: 02:42:15:b1:11:00 (02:42:15:b1:11:00)  
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.4  
User Datagram Protocol, Src Port: 53612 (53612), Dst Port: vxlan (4789)  
Virtual extensible Local Area Network
```

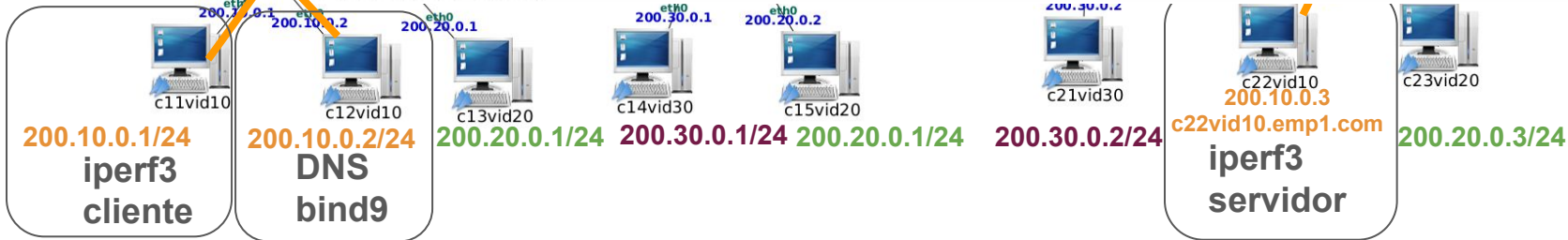
```
Frame 103: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on eth0  
Ethernet II, Src: 02:42:15:00:c1:11 (02:42:15:00:c1:11), Dst: 02:42:15:00:c2:21 (02:42:15:00:c2:21)  
Internet Protocol Version 4, Src: 200.10.0.1, Dst: 200.10.0.3  
Transmission Control Protocol, Src Port: 38944 (38944), Dst Port: targus-getdata1 (5201), Seq: 22906, Ack: 1, Len: 1398  
iPerf3 Speed Test  
Data (1398 bytes)
```



VLAN 10

VLAN

```
Frame 66: 1464 bytes on wire (11712 bits), 1464 bytes captured (11712 bits) on eth1  
Ethernet II, Src: 02:42:15:00:c1:11 (02:42:15:00:c1:11), Dst: 02:42:15:00:c2:21 (02:42:15:00:c2:21)  
Internet Protocol Version 4, Src: 200.10.0.1, Dst: 200.10.0.3  
Transmission Control Protocol, Src Port: 38944 (38944), Dst Port: targus-getdata1 (5201), Seq: 14518, Ack: 1, Len: 1398  
iPerf3 Speed Test  
Data (1398 bytes)
```

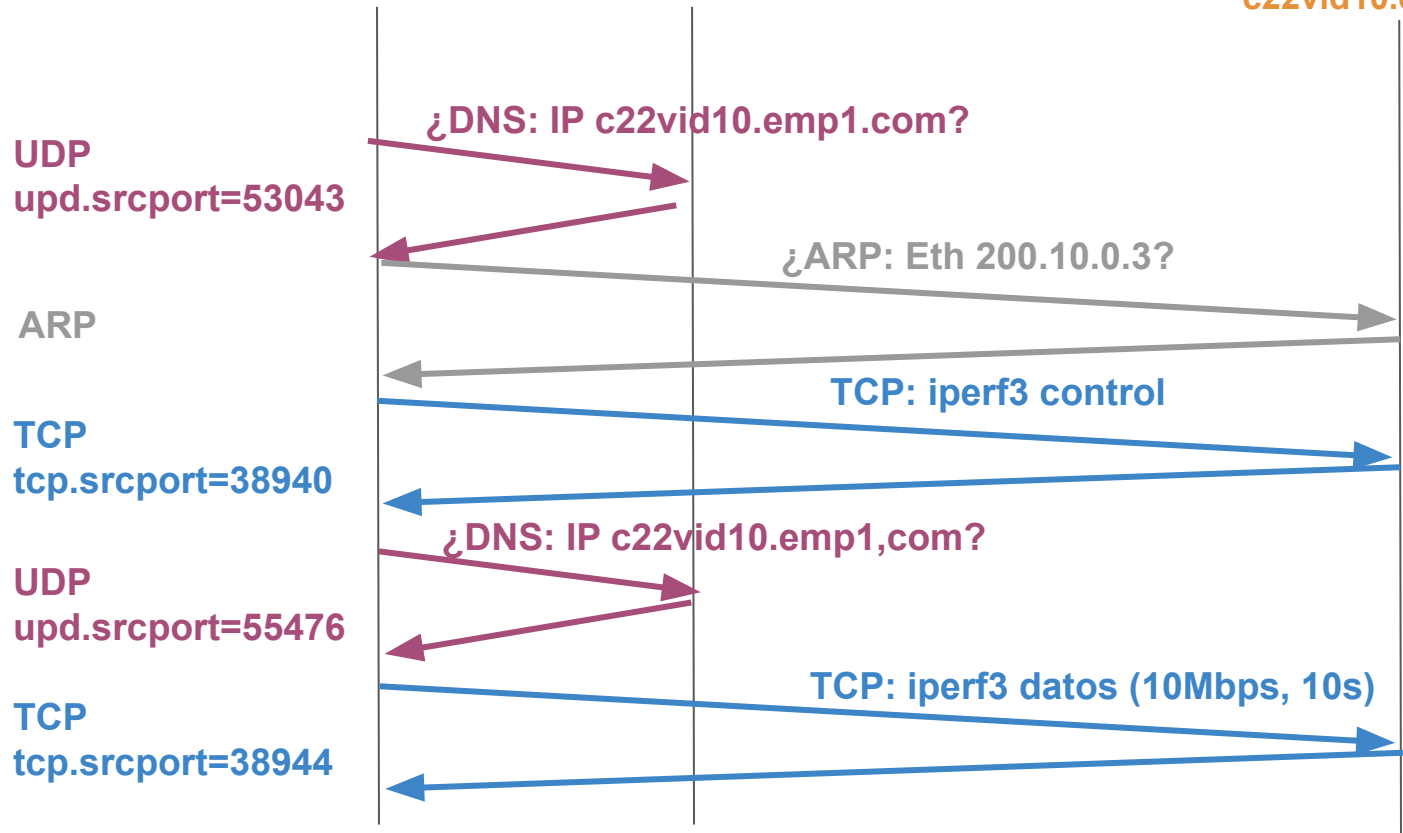


Tráfico

iperf3 cliente
200.10.0.1

DNS bind9
port=53
200.10.0.2

iperf3 servidor
port=5201
200.10.0.3
c22vid10.emp1.com



UDP
upd.srcport=53043

ARP

TCP
tcp.srcport=38940

UDP
upd.srcport=55476

TCP
tcp.srcport=38944

¿DNS: IP c22vid10.emp1.com?

¿ARP: Eth 200.10.0.3?

TCP: iperf3 control

¿DNS: IP c22vid10.emp1.com?

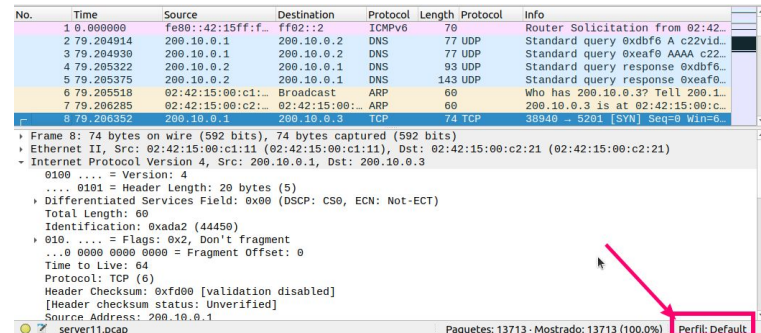
TCP: iperf3 datos (10Mbps, 10s)

Perfiles

- Wireshark permite la definición de perfiles para la visualización de paquetes cuyo objetivo es mostrar la información más adecuada en función de lo que queramos observar en una captura de tráfico. Se modifica la apariencia de la interfaz:
 - Distribución de los paneles
 - Reglas de coloreado de paquetes
 - Columnas del listado de paquete
 - Botones para el filtrado de paquetes
 - Filtros predefinidos
 - Analizadores de protocolos activado/desactivado (dissector)
 - ...

- Cada perfil en Linux se guarda como un conjunto de ficheros en una carpeta dentro de:

~/config/wireshark/profiles



No.	Time	Source	Destination	Protocol	Length	Protocol	Info
1	0.000000	fe80::42:15ff::	ff02::2	ICMPv6	78		Router Solicitation from 02:42:15:00:c2:11
2	79.204914	200.10.0.1	200.10.0.2	DNS	77	UDP	Standard query 0x6bf6 A c22vid
3	79.204930	200.10.0.1	200.10.0.2	DNS	77	UDP	Standard query 0xeafo AAAA c22vid
4	79.205322	200.10.0.2	200.10.0.1	DNS	93	UDP	Standard query response 0x6bf6
5	79.205375	200.10.0.2	200.10.0.1	DNS	143	UDP	Standard query response 0xeafo
6	79.205510	02:42:15:00:c2:11	Broadcast	ARP	60		Who has 200.10.0.3? Tell 200.10.0.1
7	79.206285	02:42:15:00:c2:11	02:42:15:00:c2:11	ARP	60		200.10.0.3 is at 02:42:15:00:c2:11
8	79.206352	200.10.0.1	200.10.0.3	TCP	74	TCP	38940 → 5201 [SYN] Seq=0 Win=0

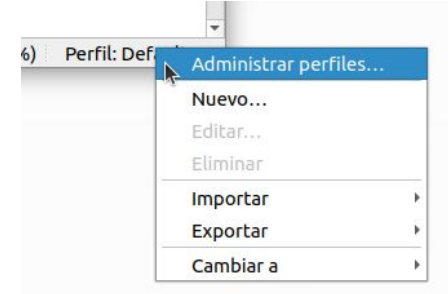
Frame 8: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: 02:42:15:00:c1:11 (02:42:15:00:c1:11), Dst: 02:42:15:00:c2:21 (02:42:15:00:c2:21)
Internet Protocol Version 4, Src: 200.10.0.1, Dst: 200.10.0.3

0100 = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0xada2 (44450)
010. = Flags: 0x2, Don't fragment
... 0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header checksum: 0xfd00 [validation disabled]
[Header checksum status: Unverified]
Source Address: 200.10.0.1

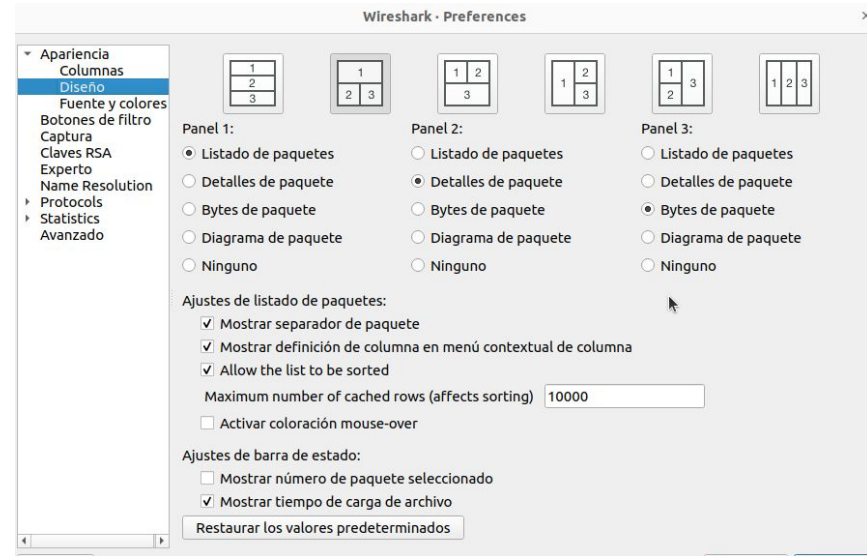
server11.pcap Paquetes: 13713 - Mostrado: 13713 (100.0%) Perfil: Default

Configuración de perfiles

- Menú: Edición-> Configuración de perfiles
- Hace una copia del actual con un nuevo nombre para partir de una configuración inicial



- Los cambios en las preferencias se almacenarán asociados al nuevo perfil.



Conversaciones

Menú: Estadísticas -> Conversaciones

Wireshark · Conversations · server11.pcap

Ethernet · 6		IPv4 · 2		IPv6 · 3		TCP · 2		UDP · 2	
Dirección A	Dirección B	Paquetes	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Inicio rel	
02:42:15:00:12:00	33:33:00:00:00:02	1	70 bytes	1	70 bytes	0	0 bytes	0.000000	
02:42:15:00:21:00	33:33:00:00:00:02	1	70 bytes	1	70 bytes	0	0 bytes	90.116218	
02:42:15:00:c1:11	02:42:15:00:c1:12	12	1 kB	6	428 bytes	6	592 bytes	79.204914	
02:42:15:00:c1:11	33:33:00:00:00:02	1	70 bytes	1	70 bytes	0	0 bytes	81.919272	
02:42:15:00:c1:11	ff:ff:ff:ff:ff:ff	1	60 bytes	1	60 bytes	0	0 bytes	79.205518	
02:42:15:00:c2:21	02:42:15:00:c1:11	13.697	14 MB	4.639	312 kB	9.058	13 MB	79.206285	

Crear filtro

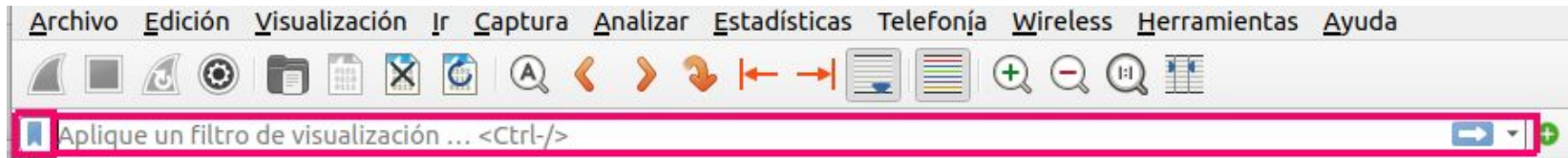
Ethernet · 6		IPv4 · 2		IPv6 · 3		TCP · 2		UDP · 2	
Dirección A	Dirección B	Paquetes	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Inicio rel	
200.10.0.1	Aplicar como filtro			Seleccionado		A ↔ B			
200.10.0.1	Preparar como filtro			No seleccionado		A → B			
	Buscar			...y seleccionado		B → A			
	Colorear			...O seleccionado		A ↔ Any			
	Copiar tabla Conversation			...Y no seleccionado		A → Any			
	Redimensionar todas las columnas al contenido			...O no seleccionado		Any → A			
						Any ↔ B			
						Any → B			
						B → Any			

Filtros

Permiten seleccionar los paquetes en los que estamos interesados. Dos tipos de filtros:

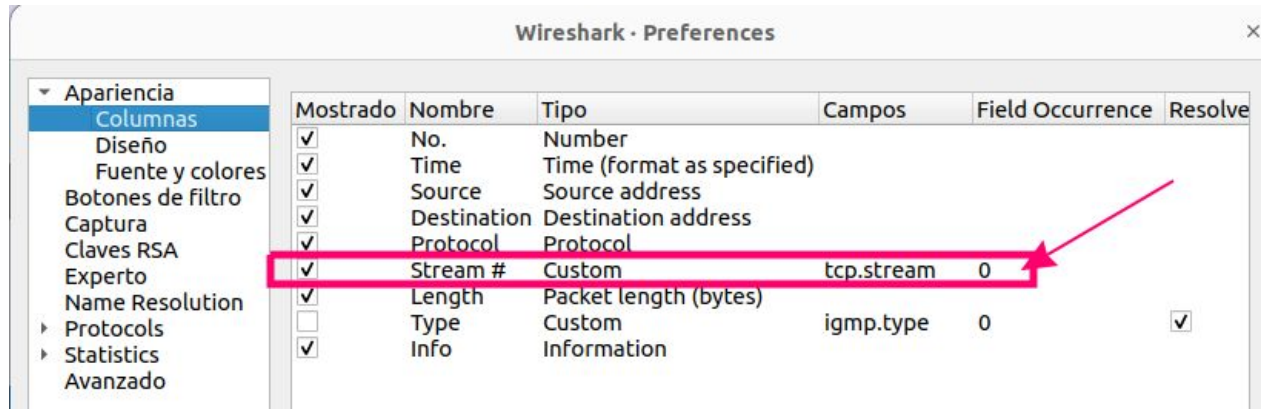
- Captura: sólo se capturan los paquetes especificados. Usan los filtros con la sintaxis BPF (Berkeley Packet Filter). También lo usan otras herramientas: TShark, Dumpcap, tcpdump.
- Visualización: sólo se visualizan los paquetes especificados.

Información: <https://www.wireshark.org/docs/dfref/>



Columnas

Menú: Edición -> Preferencias



The screenshot shows a portion of the Wireshark packet list table. The 'Stream #' column is highlighted with a red box, and a red arrow points to the value '1' in the row for packet 24.

No.	Time	Source	Destination	Protocol	Stream #	Length	Info
17	79.208452	200.10.0.3	200.10.0.1	TCP	0	66	5201 → 38940 [ACK] Seq=2 Ack=187 Win=65024 Len=0 T...
18	79.208526	200.10.0.3	200.10.0.1	iPerf3	0	67	5201 → 38940 CREATE_STREAMS(10)
23	79.208921	200.10.0.1	200.10.0.3	TCP	1	74	38944 → 5201 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 ...
24	79.209340	200.10.0.3	200.10.0.1	TCP	1	74	5201 → 38944 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=...
25	79.209414	200.10.0.1	200.10.0.3	TCP	1	66	38944 → 5201 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv...
26	79.209465	200.10.0.1	200.10.0.3	iPerf3	1	103	38944 → 5201 Cookie: "bd2gdri7jnvoya2t5gmoil3r4ywk...
27	79.209982	200.10.0.3	200.10.0.1	TCP	1	66	5201 → 38944 [ACK] Seq=1 Ack=38 Win=65152 Len=0 TS...

Menú: Analizar -> Seguir

Perfil personalizado para el tráfico TCP

- Organización de paneles
- Colores
- Filtros
- Botones
- Columnas
- ...

no.	ACK2F#	Time	ΔTCP	Source	Destination	SrcPort	DstPort	Protocol	Pkt Len	Rule	St#	TCP Len	iRTT	TCP Flags	WS Scale	BIF	SEQ
23	79.208921	0.000000000	200.10.0.1	200.10.0.3	38944	5201	TCP	74	N-TCP SYN	1	0	0.000493000S.....				
24	23	79.209340	0.000419000	200.10.0.3	200.10.0.1	5201	38944	TCP	74	N-TCP SYN	1	0	0.000493000A..S..			
25	24	79.209414	0.000074000	200.10.0.1	200.10.0.3	38944	5201	TCP	66	7-iperf3	1	0	0.000493000A....			
26	79.209465	0.000051000	200.10.0.1	200.10.0.3	38944	5201	iperf3	103	7-iperf3	1	37	0.000493000AP....	128		37	
27	26	79.209982	0.000517000	200.10.0.3	200.10.0.1	5201	38944	TCP	66	7-iperf3	1	0	0.000493000A....			
31	79.211001	0.001019000	200.10.0.1	200.10.0.3	38944	5201	TCP	1514	7-iperf3	1	1448	0.000493000A....	128	1448		
32	79.211190	0.000189000	200.10.0.3	200.10.0.1	38944	5201	ICMP	590	T-ICMP errors	1		A....	128		455477	
33	79.211443	0.000253000	200.10.0.1	200.10.0.3	38944	5201	TCP	1514	7-iperf3	1	1448	0.000493000A....	128		2896	
34	79.211454	0.000011000	200.10.0.1	200.10.0.3	38944	5201	TCP	1514	7-iperf3	1	1448	0.000493000A....	128		4344	
35	79.211458	0.000004000	200.10.0.1	200.10.0.3	38944	5201	TCP	1514	7-iperf3	1	1448	0.000493000A....	128		5792	
36	79.211462	0.000004000	200.10.0.1	200.10.0.3	38944	5201	TCP	1514	7-iperf3	1	1448	0.000493000AP....	128		7240	
37	79.211467	0.000005000	200.10.0.1	200.10.0.3	38944	5201	TCP	1514	7-iperf3	1	1448	0.000493000A....	128		8688	
38	79.211470	0.000003000	200.10.0.1	200.10.0.3	38944	5201	TCP	1514	7-iperf3	1	1448	0.000493000A....	128		10136	
39	79.211474	0.000004000	200.10.0.1	200.10.0.3	38944	5201	TCP	1514	7-iperf3	1	1448	0.000493000A....	128		11584	
40	79.211491	0.000017000	200.10.0.1	200.10.0.3	38944	5201	TCP	1514	7-iperf3	1	1448	0.000493000A....	128		13032	
41	79.211607	0.000116000	200.10.0.1	200.10.0.3	38944	5201	TCP	1514	7-iperf3	1	1448	0.000493000AP....	128	14480	13032	
42	79.211646	0.000039000	200.10.0.3	200.10.0.1	38944	5201	ICMP	590	T-ICMP errors	1		A....	128		455480	
43	79.211672	0.000026000	200.10.0.1	200.10.0.3	38944	5201	TCP	1464	T-Retrans	1	1398	0.000493000A....	128		14480	
44	79.211783	0.000111000	200.10.0.1	200.10.0.3	38944	5201	TCP	1464	T-TCP Error	1	1398	0.000493000A....	128		14480	
45	79.211819	0.000036000	200.10.0.3	200.10.0.1	38944	5201	ICMP	590	T-ICMP errors	1		A....	128		455504	

Análisis de TCP

BIF	RTT ACK	Size	Conv.Complete
Transmission Control Protocol			
Bytes in flight (tcp.analysis.bytes_in_flight)			
27662		64256	Complete, WITH_DATA
29060		64256	Complete, WITH_DATA
	0.003526000	75776	Complete, WITH_DATA
29060		64256	Complete, WITH_DATA

- ▼ [SEQ/ACK analysis]
 - [iRTT: 0.000493000 seconds]
 - [Bytes in flight: 14480]
 - [Bytes sent since last PSH flag: 5592]
- ▼ [TCP Analysis Flags]
 - ▼ [Expert Info (Note/Sequence): This frame is a (suspected) retransmission]
 - [This frame is a (suspected) retransmission]
 - [Severity level: Note]
 - [Group: Sequence]
 - [The RTT for this segment was: 0.000901000 seconds]
 - [RTT based on delta from frame: 40]

Reglas de coloreado de paquetes

Menú: Visualización -> Reglas de coloreado

Nombre	Filtro
<input checked="" type="checkbox"/> W-SYN with Zero Window	tcp.flags.syn eq 1 and tcp.flags.ack eq 0 and tcp.window_size_value eq 0
<input checked="" type="checkbox"/> W-SYN with no options	tcp.flags.syn eq 1 and tcp.hdr_len eq 20
<input checked="" type="checkbox"/> T-TCP ZeroWindow	tcp.analysis.zero_window
<input checked="" type="checkbox"/> T-TCP SmallWinSize	!icmp and tcp.window_size lt 1260 and tcp.window_size gt 0 and tcp.flags.fin eq 0 and tcp.flags.reset eq 0 and
<input checked="" type="checkbox"/> T-TCP Slow	tcp.time_delta gt 0.5 and tcp.flags.reset eq 0 and tcp.flags.fin eq 0 and not tcp.analysis.keep_alive
<input checked="" type="checkbox"/> T-TCP-Out-Of-Order	tcp.analysis.out_of_order
<input checked="" type="checkbox"/> T-TCP-Retrans	tcp.analysis.retransmission
<input checked="" type="checkbox"/> T-TCP-FastRetrans	tcp.analysis.fast_retransmission
<input checked="" type="checkbox"/> T-TCP Error	tcp.analysis.flags and !(tcp.analysis.window_update or tcp.analysis.window_full or tcp.analysis.duplicate_ack
<input checked="" type="checkbox"/> T-TCP RST	tcp.flags.reset eq 1
<input checked="" type="checkbox"/> T-TCP WinFull	tcp.analysis.window_full
<input checked="" type="checkbox"/> T-ICMP errors	icmp.type in {3..5, 11} or icmpv6.type in {1..4}
<input checked="" type="checkbox"/> N-TCP Ack Unseen	tcp.analysis.ack_lost_segment
<input checked="" type="checkbox"/> N-TCP Dup Ack	tcp.analysis.duplicate_ack
<input checked="" type="checkbox"/> N-TCP Keep-Alive	tcp.analysis.keep_alive or tcp.analysis.keep_alive_ack
<input checked="" type="checkbox"/> N-TCP WindowUpdate	tcp.analysis.window_update
<input checked="" type="checkbox"/> N-No WinScale or SACK	!(tcp.option_kind eq 3 or tcp.option_kind eq 4) and tcp.flags.syn eq 1
<input checked="" type="checkbox"/> N-TCP SYN	tcp.flags.syn eq 1
<input checked="" type="checkbox"/> N-TCP FIN	tcp.flags.fin eq 1
<input checked="" type="checkbox"/> 7-iperf3	tcp.port==5201 or udp.port==5201
<input checked="" type="checkbox"/> 7-DNS	dns
<input checked="" type="checkbox"/> 7-HTTP	tcp.port in {80,8080} or http or http2 or http3
<input checked="" type="checkbox"/> 4-TCP	tcp
<input checked="" type="checkbox"/> 4-QUIC	quic
<input checked="" type="checkbox"/> 4-UDP	udp
<input checked="" type="checkbox"/> 3-ICMP	icmp icmpv6
<input checked="" type="checkbox"/> 3-TTL low or unexpected	(!ip.dst eq 224.0.0.0/4 and ip.ttl lt 5 and !pim and !ospf) (ip.dst eq 224.0.0.0/24 and ip.dst != 224.0.0.251 and
<input checked="" type="checkbox"/> 3-Routing	hsrp eigrp ospf bgp cdp vrrp carp gvrp igmp ismp
<input checked="" type="checkbox"/> 2-STP	stp
<input checked="" type="checkbox"/> 2-ARP	arp

Conexión TCP completa (tcp.completeness)

Para un flujo de paquetes pertenecientes a una conexión TCP se busca si hay paquetes con los siguientes flags activados según el siguiente patrón bitmap:

RST	FIN	DATA	ACK	SYN+ACK	SYN
2^5	2^4	2^3	2^2	2^1	2^0

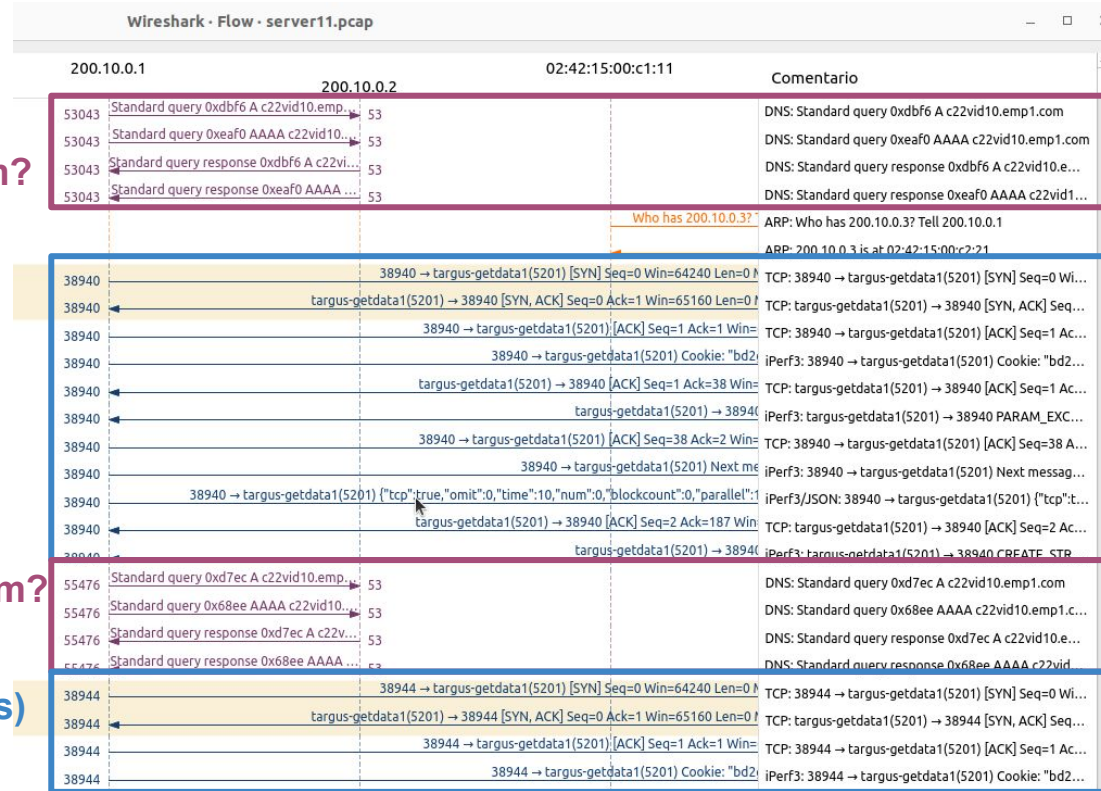
Una conexión que haya finalizado e intercambiado datos deberá tener segmentos TCP con los siguientes flags, resultando el valor 31 en decimal:

RST	FIN	DATA	ACK	SYN+ACK	SYN
0	1	1	1	1	1

Gráfica de flujo

Menú: Estadísticas -> Gráfica de flujo

¿IP c22vid10.emp1.com?



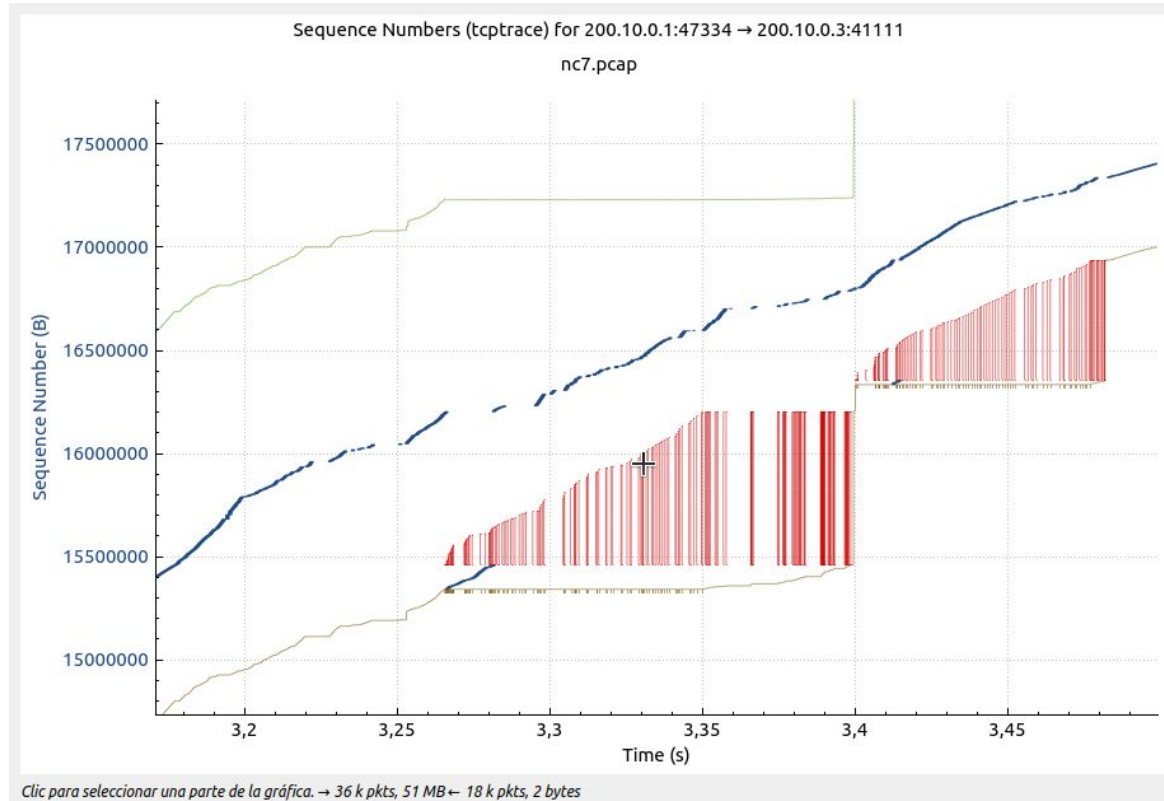
iPerf3 control

¿IP c22vid10.emp1.com?

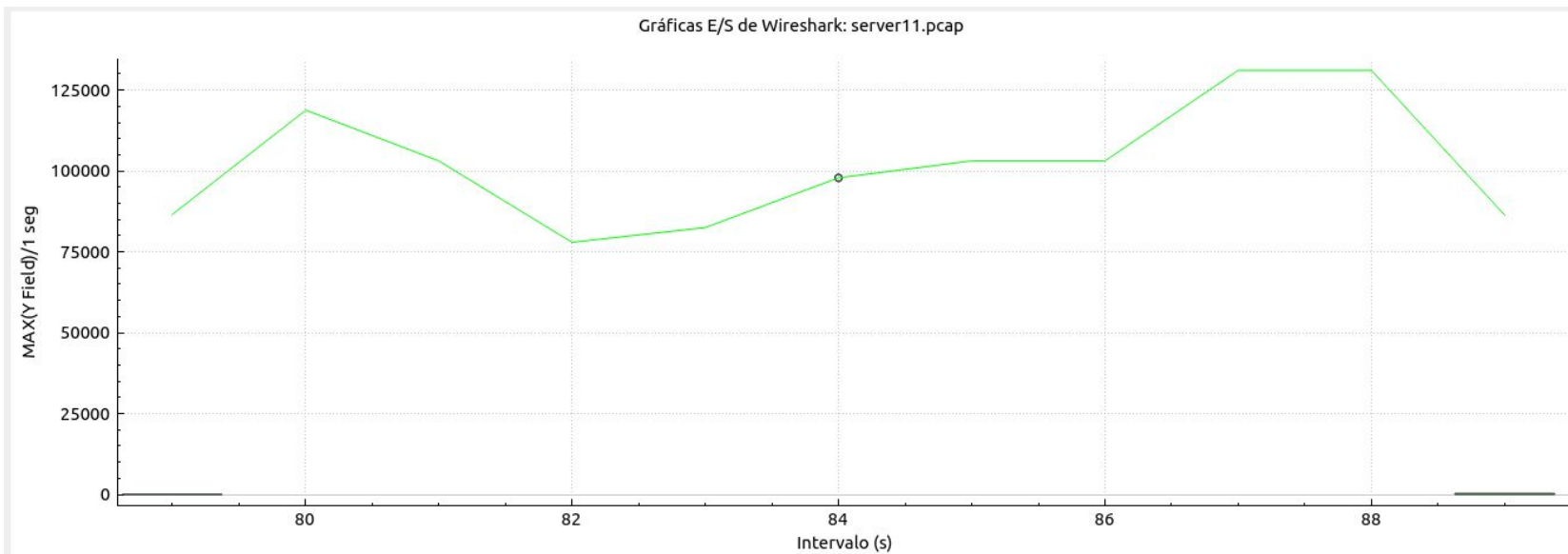
iPerf3 datos (10Mbps, 10s)

Gráfica de secuencia TCP

Menú: Estadísticas -> Gráficas de secuencia TCP -> Duración de secuencia (tcptrace)



Gráfica e/s



Clic para seleccionar paquete 8013 (84s = 9.786e+04).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
<input type="checkbox"/>	TCP Errors	tcp.analysis.flags	■	Bar	Packets		None
<input checked="" type="checkbox"/>	BytesInFlightMaxX	(tcp.srcport < tcp.dstport)	■	Bar	MAX(Y Field)	tcp.analysis.bytes_in_flight	None
<input type="checkbox"/>	CalcWinSizeMaxX	(tcp.srcport >= tcp.dstport)	■	Line	MAX(Y Field)	tcp.window_size	None
<input type="checkbox"/>	TcpWinFullX	(tcp.srcport < tcp.dstport)	■	Line	COUNT FRAMES(Y Field)	tcp.analysis.window_full	None
<input type="checkbox"/>	TcpZeroWinX	(tcp.srcport >= tcp.dstport)	■	Line	COUNT FRAMES(Y Field)	tcp.analysis.zero_window	None
<input type="checkbox"/>	Blank		■	Line	Packets		None
<input checked="" type="checkbox"/>	BytesInFlightMaxY	(tcp.srcport >= tcp.dstport)	■	Line	MAX(Y Field)	tcp.analysis.bytes_in_flight	None

Referencias

- Wireshark: <https://www.wireshark.org>
- Kathará: <https://www.kathara.org/>