



Universidad Simón Bolívar  
Departamento de Computación y tecnología de la información  
Redes de Computadoras I (CI-4835)  
Trimestre Septiembre Diciembre 2017

## **Informe Taller de Trabajo en Casa II**

### **Integrantes**

Carlos Martínez – 11-10584  
Carlos Ferreira – 11-10323

## Parte I. Introducción

Uno de los desafíos que se enfrenta al momento de diseñar una red de computadoras es instalarla de manera que la información viaje entre todos los nodos interconectados eficientemente disminuyendo el congestionamiento u otros problemas que pudiesen afectar el rápido acceso a la información.

Para lograr esto, es necesario que el administrador de redes tenga a su disposición herramientas que permitan monitorear el flujo de paquetes que viajan por los diferentes puntos de una red, filtrar esta información, obtener estadísticas y demás datos que ayuden a detectar problemas y así poder solucionarlos.

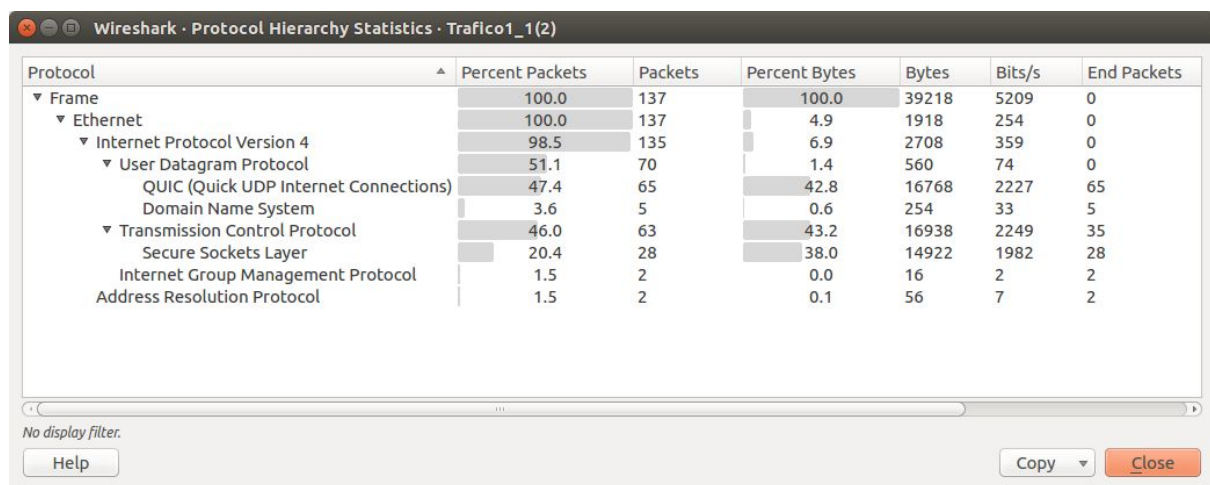
Una de las más importantes herramientas para lograr este objetivo se trata de **Wireshark**, un poderoso analizador de protocolos de software libre con una gran cantidad de funcionalidades para el monitoreo de redes, captura de paquetes y organización y filtrado de información.

En el siguiente informe se explicarán varias actividades realizadas haciendo uso de la herramienta **Wireshark**, como parte de la actividad número dos del Laboratorio de Redes de Computadoras I.

## Parte II. Desarrollo

### Parte 1:

Para la captura de datos de esta actividad se tuvo un browser abierto (Google Chrome) con la página de Gmail, Youtube y Whatsapp web en las primeros 2 monitoreos y en la tercera se agrego la página de Facebook a ver si se notaba algún cambio, todos los datos fueron capturados en una hora cercana a las 9 por una cantidad cercana de 60 segundos, se monitoreo con Wireshark y se tomaron los datos, a siguiente se muestra la jerarquía estadística de los datos tomados.



En la primera captura de datos se nota un alto uso de UDP en comparación a otros monitoreos de redes en casa, esto se debe al protocolo QUIC, protocolo creado por Google para Google Chrome y sus aplicaciones como Gmail o Youtube, UDP es mayor que TCP pero por muy poco.

Wireshark · Protocol Hierarchy Statistics · Trafico1\_2(2)

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets
▼ Frame	100.0	275	100.0	43653	5222	0
▼ Ethernet	100.0	275	8.8	3850	460	0
▼ Internet Protocol Version 4	99.3	273	12.5	5460	653	0
▼ User Datagram Protocol	40.0	110	2.0	880	105	0
Simple Service Discovery Protocol	1.5	4	1.6	684	81	4
QUIC (Quick UDP Internet Connections)	34.9	96	57.6	25126	3005	96
Domain Name System	3.6	10	1.0	445	53	10
▼ Transmission Control Protocol	59.3	163	16.4	7152	855	126
Secure Sockets Layer	13.5	37	5.0	2200	263	37
Address Resolution Protocol	0.7	2	0.1	56	6	2

No display filter.

Help Copy Close

En el segundo monitoreo dió una cantidad mayor de datos pero al ser un período de tiempo tan poco no es un dato interesante analizar, vemos que la cantidad de TCP aumentó un poco, pero no de manera tan considerable, y el protocolo UDP tiene una buena presencia debido a que se está usando Google Chrome con aplicaciones de Google.

Wireshark · Protocol Hierarchy Statistics · Trafico1\_3(2)

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets
▼ Frame	100.0	176	100.0	28688	3579	0
▼ Ethernet	100.0	176	8.6	2464	307	0
▼ Internet Protocol Version 4	99.4	175	12.2	3508	437	0
▼ User Datagram Protocol	23.3	41	1.1	328	40	0
Simple Service Discovery Protocol	2.3	4	2.4	684	85	4
QUIC (Quick UDP Internet Connections)	18.2	32	15.9	4554	568	32
Domain Name System	2.8	5	1.3	367	45	5
▼ Transmission Control Protocol	75.0	132	58.3	16739	2088	83
Secure Sockets Layer	27.8	49	48.3	13863	1729	49
Internet Group Management Protocol	1.1	2	0.1	16	1	2
Address Resolution Protocol	0.6	1	0.1	28	3	1

No display filter.

Help Copy Close

El tercer monitoreo tenemos una variable extra que es tener la página de Facebook agregada a el resto de páginas webs, aquí se ve como la cantidad de paquetes TCP aumentó de manera considerable debido a esta página extra, y de nuevo se nota la presencia del protocolo UDP por el protocolo QUIC.

También se realizó un monitoreo por 30 segundos los 3 días con un vídeo de Youtube abierto, la única diferencia encontrada fue la gran cantidad del protocolo QUIC debido al streaming donde se envían paquetes constantemente para cargar el vídeo.

## Parte 2:

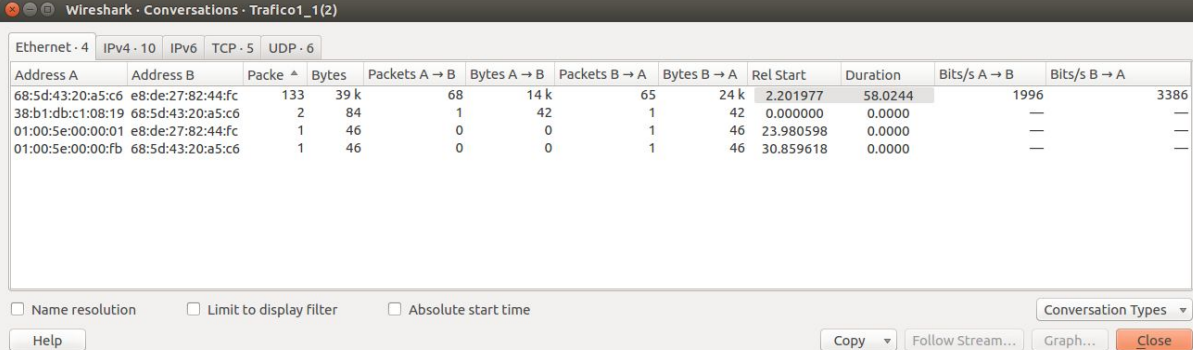
Se capturaron 3 datos de descargas en diferentes momentos, todas descargando desde Dropbox, la primera se descargaba un solo archivo, la segunda y la tercera descargando 3 archivos al mismo tiempo. La descarga de paquetes de los diferentes archivos no mostró mucha diferencias entre sí, se notó que la tasa de descarga de paquetes era constante por la duración del monitoreo, sin importar la cantidad de archivos que se estuvieran descargando, esto se debe a que la cantidad de banda ancha para la descarga se distribuye para los archivos que se estén descargando y no se genera un cuello de botella, se le da un poco de prioridad al primer archivo que se empezó a descargar pero al notar el retraso de la descarga en cada paquete no hubo una diferencia notable.

## Parte 3: Conversaciones

En esta parte fueron exploradas las estadísticas de conversaciones entre distintas entidades lógicas durante las capturas de datos.

En términos generales se aprecia que la mayor cantidad de paquetes intercambiados entre los distintos puntos fue mediante el protocolo de internet versión cuatro (IPv4) mayoritariamente entre la computadora de prueba y los servidores de Google.

## Estadísticas de conversaciones para la captura 1



The image shows the 'Conversations' window in Wireshark for capture 'Trafico1\_1(2)'. It displays a table of network conversations. The top tabs show 'Ethernet · 4', 'IPv4 · 10', 'IPv6', 'TCP · 5', and 'UDP · 6'. The table has columns for Address A, Address B, Packets A → B, Bytes A → B, Packets B → A, Bytes B → A, Rel Start, Duration, Bits/s A → B, and Bits/s B → A. The first row shows a conversation between 68:5d:43:20:a5:c6 and e8:de:27:82:44:fc with 133 packets and 39 kbytes in each direction. The second row shows a conversation between 38:b1:db:c1:08:19 and 68:5d:43:20:a5:c6 with 2 packets and 84 bytes in each direction. The third row shows a conversation between 01:00:5e:00:00:01 and e8:de:27:82:44:fc with 1 packet and 46 bytes in each direction. The fourth row shows a conversation between 01:00:5e:00:00:fb and 68:5d:43:20:a5:c6 with 1 packet and 46 bytes in each direction. At the bottom, there are checkboxes for 'Name resolution', 'Limit to display filter', and 'Absolute start time', along with a 'Help' button and a 'Conversation Types' dropdown menu.

Address A	Address B	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
68:5d:43:20:a5:c6	e8:de:27:82:44:fc	133	39 k	68	14 k	2.201977	58.0244	1996	3386
38:b1:db:c1:08:19	68:5d:43:20:a5:c6	2	84	1	42	0.000000	0.0000	—	—
01:00:5e:00:00:01	e8:de:27:82:44:fc	1	46	0	0	23.980598	0.0000	—	—
01:00:5e:00:00:fb	68:5d:43:20:a5:c6	1	46	0	0	30.859618	0.0000	—	—

## Captura 1 ethernet

Wireshark · Conversations · Trafico1\_1(2)

Ethernet · 4		IPv4 · 10		IPv6		TCP · 5		UDP · 6					
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A		
4.4.4.4	192.168.0.107	1	79	0	0	1	79	48.668264	0.0000	—	—		
8.8.8.8	192.168.0.107	4	385	2	231	2	154	48.668289	11.0897	166	111		
74.125.141.189	192.168.0.107	10	740	5	383	5	357	4.511735	55.7147	54	51		
108.177.12.188	192.168.0.107	2	132	1	66	1	66	19.635562	0.0951	5552	5552		
162.125.18.133	192.168.0.107	7	539	4	341	3	198	15.801711	0.1405	19 k	11 k		
169.55.74.56	192.168.0.107	16	1870	7	1066	9	804	2.201977	54.1432	157	118		
172.217.2.197	192.168.0.107	38	16 k	18	14 k	20	1668	13.451638	34.8160	3417	383		
172.217.2.206	192.168.0.107	55	18 k	28	7602	27	11 k	5.229337	54.6332	1113	1633		
192.168.0.1	224.0.0.1	1	46	1	46	0	0	23.980598	0.0000	—	—		
192.168.0.107	224.0.0.251	1	46	1	46	0	0	30.859618	0.0000	—	—		

☐ Name resolution
 ☐ Limit to display filter
 ☐ Absolute start time

Help
 Copy
 Follow Stream...
 Graph...
 Close

## Captura 1 IPv4



Conversación con mayor intercambio en la captura 1: Entre máquina local y un servidor de Google con 18 Kilobytes intercambiados.

Endpoints:

- 192.168.0.107:51983
- 172.217.2.206:443

## Estadísticas de conversaciones para la captura 2

Wireshark · Conversations · Trafico1\_2(2)

Ethernet · 2		IPv4 · 25		IPv6		TCP · 20		UDP · 9					
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A		
68:5d:43:20:a5:c6	e8:de:27:82:44:fc	271	42 k	134	22 k	137	20 k	0.000000	66.8705	2708	0		
01:00:5e:7f:ff:fa	68:5d:43:20:a5:c6	4	852	0	0	4	852	57.899555	3.0024	0	0		

☐ Name resolution
 ☐ Limit to display filter
 ☐ Absolute start time

Help
 Copy
 Follow Stream...
 Graph...
 Close

## Captura 2 ethernet

Wireshark - Conversations - Trafico1\_2(2)

Ethernet - 2   IPv4 - 25   IPv6   TCP - 20   UDP - 9

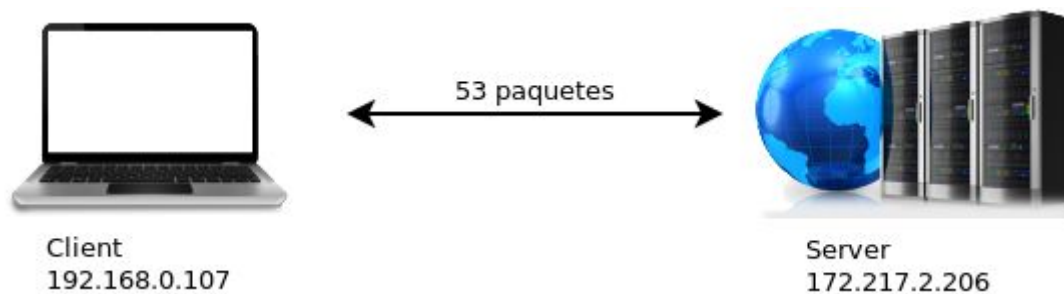
Address A	Address B	Packet	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
172.217.2.206	192.168.0.107	53	12 k	29	5567	24	7359	6.499692	58.1122	766	1013
157.240.14.35	192.168.0.107	19	1336	9	748	10	588	8.337478	34.8250	171	135
31.13.67.35	192.168.0.107	18	1270	8	682	10	588	7.340014	0.6263	8711	7510
172.217.2.195	192.168.0.107	17	8754	10	4932	7	3822	48.868996	0.2546	154 k	120 k
192.168.0.107	216.58.192.35	16	6714	8	4669	8	2045	7.210617	15.1940	2458	1076
192.168.0.107	216.58.192.51	14	1570	7	947	7	623	38.399962	5.6670	1336	879
158.85.224.178	192.168.0.107	12	1386	5	714	7	672	11.879946	54.9906	103	97
157.240.14.15	192.168.0.107	11	767	5	407	6	360	24.064026	19.9155	163	144
157.240.14.16	192.168.0.107	11	767	5	407	6	360	21.215956	20.0507	162	143
157.240.14.36	192.168.0.107	11	767	5	407	6	360	0.000000	19.7240	165	146
74.125.141.189	192.168.0.107	10	764	5	394	5	370	7.494690	49.6687	63	59
157.240.14.19	192.168.0.107	9	659	4	341	5	318	4.351942	19.7146	138	129
23.14.84.194	192.168.0.107	8	559	4	295	4	264	22.015949	13.9557	169	151
8.8.8.8	192.168.0.107	8	705	4	395	4	310	7.135497	41.7291	75	59
23.4.241.42	192.168.0.107	7	493	4	295	3	198	4.607942	14.9121	158	106
23.14.84.16	192.168.0.107	7	493	4	295	3	198	19.967989	14.3255	164	110
23.14.85.27	192.168.0.107	7	493	4	295	3	198	24.063988	14.0347	168	112
77.234.42.43	192.168.0.107	6	427	3	229	3	198	28.159967	19.0080	96	83
104.237.191.1	192.168.0.107	6	459	4	327	2	132	32.255987	10.3760	252	101
172.217.8.142	192.168.0.107	6	459	3	261	3	198	3.215562	0.0723	28 k	21 k
172.217.8.66	192.168.0.107	5	393	3	261	2	132	0.443731	0.0761	27 k	13 k
173.194.211.188	192.168.0.107	4	264	2	132	2	132	11.776010	45.1914	23	23
192.168.0.107	239.255.255....	4	852	4	852	0	0	57.899555	3.0024	2270	0
172.217.2.197	192.168.0.107	2	132	1	66	1	66	34.303969	0.0706	7482	7482
4.4.4.4	192.168.0.107	2	160	0	0	2	160	7.135470	36.2873	0	35

☐ Name resolution   ☐ Limit to display filter   ☐ Absolute start time

Help   Copy   Follow Stream...   Graph...   Close

Conversation Types

## Captura 2 IPv4



Conversación con mayor intercambio en la captura 2: Entre máquina local y un servidor de Google con 12 Kilobytes intercambiados.

Endpoints:

- 192.168.0.107:52199
- 172.217.2.206:443



## Estadísticas de conversaciones para la captura 3

Wireshark · Conversations - Traffic\_1\_3(2)

Ethernet · 5IPv4 · 24IPv6TCP · 15UDP · 9

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
00:13:02:ad:94:21	ff:ff:ff:ff:ff:ff	1	42	1	42	0	0	25.537993	0.0000	—	—
01:00:5e:00:00:01	e8:de:27:82:44:fc	1	46	0	0	1	46	17.141291	0.0000	—	—
01:00:5e:00:00:fb	68:5d:43:20:a5:c6	1	46	0	0	1	46	20.291135	0.0000	—	—
01:00:5e:7f:ff:fa	68:5d:43:20:a5:c6	4	852	0	0	4	852	41.288483	3.0011	0	2271
68:5d:43:20:a5:c6	e8:de:27:82:44:fc	169	27 k	90	14 k	79	13 k	0.000000	64.1113	1755	1701

☐ Name resolution☐ Limit to display filter☐ Absolute start time

Conversation Types ▾

HelpCopy ▾Follow Stream...Graph...Close

## Captura 3 ethernet

Wireshark · Conversations · Traffic1\_3(2)

Ethernet · 5IPv4 · 24IPv6TCP · 15UDP · 9

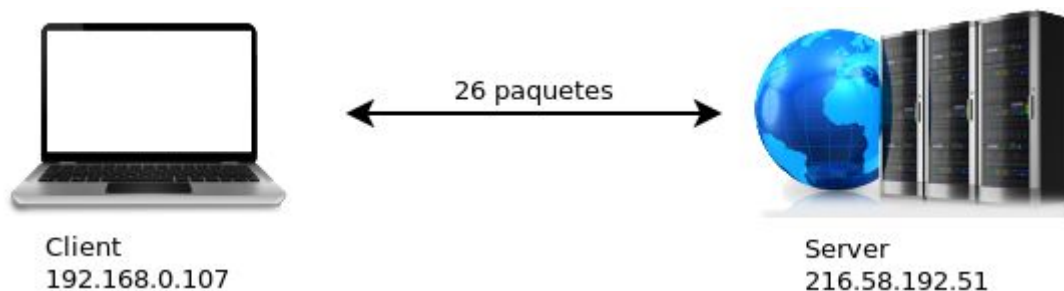
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.0.107	216.58.192.51	26	3020	13	1840	13	1180	13.027172	10.8680	1354	868
23.14.84.251	192.168.0.107	21	4096	10	2294	11	1802	23.761706	40.3496	454	357
157.240.14.35	192.168.0.107	21	6309	9	2307	12	4002	13.011182	10.6305	1736	3011
157.240.14.15	192.168.0.107	16	4175	7	2977	9	1198	18.179150	5.1200	4651	1871
172.217.8.78	192.168.0.107	14	4536	7	1988	7	2548	13.240607	15.1885	1047	1342
169.55.74.45	192.168.0.107	11	1089	4	513	7	576	0.000000	48.8870	83	94
74.125.141.189	192.168.0.107	10	762	5	392	5	370	0.832120	58.2370	53	50
157.240.14.19	192.168.0.107	9	659	4	341	5	318	22.851159	18.5606	146	137
77.234.42.217	192.168.0.107	6	427	3	229	3	198	37.187159	19.2000	95	82
192.168.0.107	239.255.255.250	4	852	4	852	0	0	41.288483	3.0011	2271	0
74.125.141.188	192.168.0.107	4	264	2	132	2	132	2.411181	45.1911	23	23
172.217.2.68	192.168.0.107	4	264	2	132	2	132	18.803174	45.1417	23	23
172.217.8.110	192.168.0.107	4	264	2	132	2	132	12.611189	45.1416	23	23
8.8.8.8	192.168.0.107	4	496	2	345	2	151	13.167984	10.5931	260	114
172.217.2.69	192.168.0.107	4	264	2	132	2	132	37.215150	8.2343	128	128
172.217.2.78	192.168.0.107	4	280	2	150	2	130	6.213271	3.2874	365	316
172.217.2.67	192.168.0.107	2	137	1	72	1	65	8.821774	0.0960	6001	5418
192.168.0.107	216.58.219.174	2	132	1	66	1	66	37.187194	0.0699	7550	7550
172.217.2.206	192.168.0.107	2	132	1	66	1	66	26.995182	0.0695	7595	7595
192.168.0.107	216.58.219.78	2	132	1	66	1	66	24.919151	0.0695	7601	7601
192.168.0.107	200.90.6.14	2	183	1	65	1	118	3.045355	0.0622	8359	15 k
4.4.4.4	192.168.0.107	1	81	0	0	1	81	23.660736	0.0000	—	—
192.168.0.1	224.0.0.1	1	46	1	46	0	0	17.141291	0.0000	—	—
192.168.0.107	224.0.0.251	1	46	1	46	0	0	20.291135	0.0000	—	—

☐ Name resolution☐ Limit to display filter☐ Absolute start time

Conversation Types ▾

HelpCopy ▾Follow Stream...Graph...Close

## Captura 3 IPv4



Conversación con mayor intercambio en la captura 3: Entre máquina local y un servidor de Google con 3020 bytes intercambiados.

Endpoints:

- 192.168.0.107:36192
- 256.58.192.51:443



Es interesante notar cómo en la mayoría de las capturas la cantidad de conexiones a ethernet siempre fue relativamente baja, en cuanto a las direcciones de IPv4 se puede notar que la mayoría de las direcciones que estaban transmitiendo más frecuentemente se encontraban en el dominio de Google, ya que al introducir la IP te direcciona directo a la página de Google.

#### **Parte 4:**

Procesador: Intel® Core™ i5-3210M CPU @ 2.50GHz × 4

Tarjeta Grafica: Intel® Ivybridge Mobile

Sistema Operativo: ubuntu 16.04 LTS 64-bit

Wireshark Version 2.4.2

## **Conclusiones**

Haciendo uso de Wireshark fue posible capturar todo el tráfico de paquetes de los distintos protocolos que pasaron por la red monitoreada y descubrir qué usos del internet ocasionan un mayor tráfico, comparar el flujo de la red en distintas ocasiones y obtener estadísticas sobre los nodos de la red que intercambiaron las mayores cantidades de paquetes en el momento de la captura.

Si bien todo fue parte de pruebas con fines de aprendizaje, en un contexto verdadero toda esta información habría sido de mucha ayuda al momento de detectar inconvenientes para poder actuar al respecto y mantener la red en cuestión en el mejor estado posible.

## Bibliografía

- <https://es.wikipedia.org/wiki/QUIC>
- [https://www.wireshark.org/docs/wsug\\_html\\_chunked/](https://www.wireshark.org/docs/wsug_html_chunked/)