

INSTITUTO TECNOLÓGICO DE CANCUN



Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

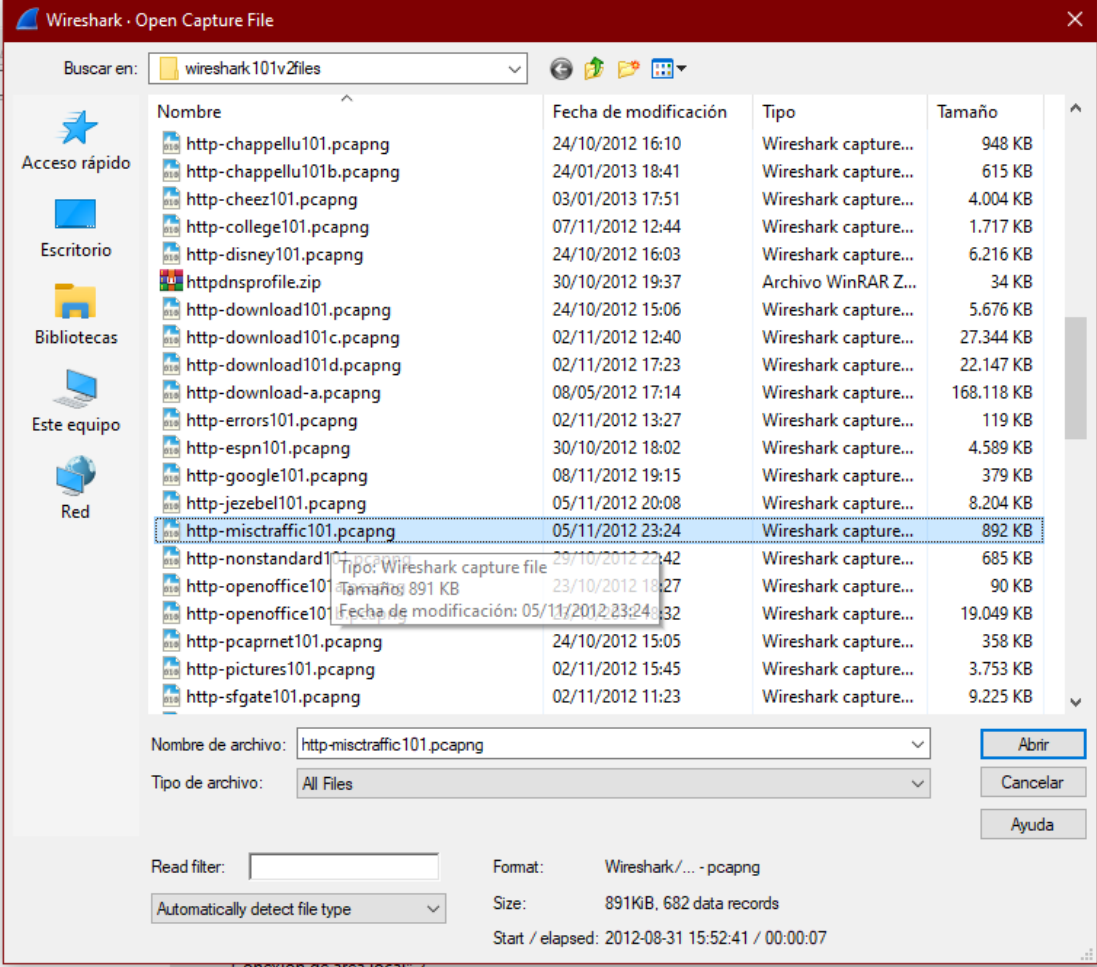
N.º De Actividad: Laboratorio 31

Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

Lab31- Filter on the Most Active TCP Conversation

Paso 1:



The Wireshark Network Analyzer

Wireshark - Open Capture File

Buscar en: wireshark101v2files

Nombre	Fecha de modificación	Tipo	Tamaño
http-chappellu101.pcapng	24/10/2012 16:10	Wireshark capture...	948 KB
http-chappellu101b.pcapng	24/01/2013 18:41	Wireshark capture...	615 KB
http-cheez101.pcapng	03/01/2013 17:51	Wireshark capture...	4.004 KB
http-college101.pcapng	07/11/2012 12:44	Wireshark capture...	1.717 KB
http-disney101.pcapng	24/10/2012 16:03	Wireshark capture...	6.216 KB
httpdnsprofile.zip	30/10/2012 19:37	Archivo WinRAR Z...	34 KB
http-download101.pcapng	24/10/2012 15:06	Wireshark capture...	5.676 KB
http-download101c.pcapng	02/11/2012 12:40	Wireshark capture...	27.344 KB
http-download101d.pcapng	02/11/2012 17:23	Wireshark capture...	22.147 KB
http-download-a.pcapng	08/05/2012 17:14	Wireshark capture...	168.118 KB
http-errors101.pcapng	02/11/2012 13:27	Wireshark capture...	119 KB
http-espn101.pcapng	30/10/2012 18:02	Wireshark capture...	4.589 KB
http-google101.pcapng	08/11/2012 19:15	Wireshark capture...	379 KB
http-jezebel101.pcapng	05/11/2012 20:08	Wireshark capture...	8.204 KB
http-misctraffic101.pcapng	05/11/2012 23:24	Wireshark capture...	892 KB
http-nonstandard101.pcapng	29/10/2012 22:42	Wireshark capture...	685 KB
http-openoffice101.pcapng	23/10/2012 18:27	Wireshark capture...	90 KB
http-openoffice101b.pcapng	05/11/2012 23:24	Wireshark capture...	19.049 KB
http-pcaprnet101.pcapng	24/10/2012 15:05	Wireshark capture...	358 KB
http-pictures101.pcapng	02/11/2012 15:45	Wireshark capture...	3.753 KB
http-sfgate101.pcapng	02/11/2012 11:23	Wireshark capture...	9.225 KB

Nombre de archivo: http-misctraffic101.pcapng

Tipo de archivo: All Files

Read filter: Automatically detect file type

Format: Wireshark / ... - pcapng

Size: 891KB, 682 data records

Start / elapsed: 2012-08-31 15:52:41 / 00:00:07

Abrir

Cancelar

Ayuda

Conexión de área local* 2

Conexión de área local* 1

Wi-Fi

Radmin VPN

Conexión de área local* 8

Conexión de área local* 10

Ethernet

Conexión de área local* 9

VirtualBox Host-Only Network

Adapter for loopback traffic capture

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

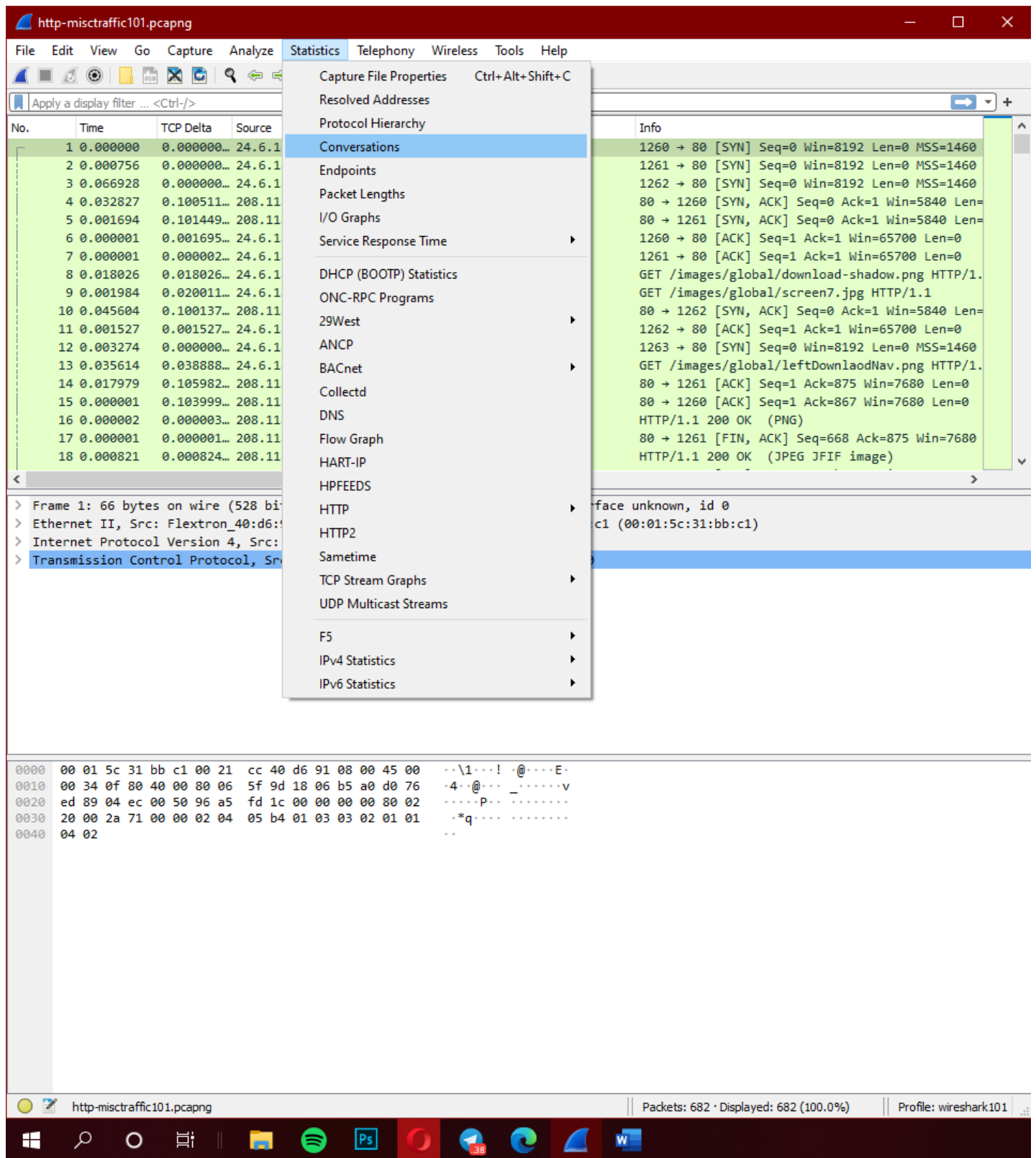
You are running Wireshark 3.4.0 (v3.4.0-0-g9733f173ea5e). You receive automatic updates.

Ready to load or capture

No Packets

Profile: wireshark101

Paso 2:



The image shows the Wireshark network protocol analyzer interface. The main window displays a packet capture file named "http-misctrffic101.pcapng". The Statistics pane is open, showing the Conversations tab. The packet list shows 18 packets, and the packet details pane shows the structure of the first packet (Frame 1: 66 bytes on wire).

Statistics Pane - Conversations Tab:

No.	Time	TCP Delta	Source
1	0.000000	0.000000...	24.6.1
2	0.000756	0.000000...	24.6.1
3	0.066928	0.000000...	24.6.1
4	0.032827	0.100511...	208.11
5	0.001694	0.101449...	208.11
6	0.000001	0.001695...	24.6.1
7	0.000001	0.000002...	24.6.1
8	0.018026	0.018026...	24.6.1
9	0.001984	0.020011...	24.6.1
10	0.045604	0.100137...	208.11
11	0.001527	0.001527...	24.6.1
12	0.003274	0.000000...	24.6.1
13	0.035614	0.038888...	24.6.1
14	0.017979	0.105982...	208.11
15	0.000001	0.103999...	208.11
16	0.000002	0.000003...	208.11
17	0.000001	0.000001...	208.11
18	0.000821	0.000824...	208.11

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	24.6.1	208.11	TCP	60	1260 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
2	0.000756	24.6.1	208.11	TCP	60	1261 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
3	0.066928	24.6.1	208.11	TCP	60	1262 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
4	0.032827	208.11	24.6.1	TCP	60	80 → 1260 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
5	0.001694	208.11	24.6.1	TCP	60	80 → 1261 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
6	0.000001	24.6.1	208.11	TCP	60	1260 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
7	0.000001	24.6.1	208.11	TCP	60	1261 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
8	0.018026	24.6.1	208.11	HTTP	100	GET /images/global/download-shadow.png HTTP/1.1
9	0.001984	24.6.1	208.11	HTTP	100	GET /images/global/screen7.jpg HTTP/1.1
10	0.045604	208.11	24.6.1	TCP	60	80 → 1262 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
11	0.001527	24.6.1	208.11	TCP	60	1262 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
12	0.003274	24.6.1	208.11	TCP	60	1263 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
13	0.035614	24.6.1	208.11	HTTP	100	GET /images/global/leftDownloadNav.png HTTP/1.1
14	0.017979	208.11	24.6.1	TCP	60	80 → 1261 [ACK] Seq=1 Ack=875 Win=7680 Len=0
15	0.000001	208.11	24.6.1	TCP	60	80 → 1260 [ACK] Seq=1 Ack=867 Win=7680 Len=0
16	0.000002	208.11	24.6.1	HTTP	100	HTTP/1.1 200 OK (PNG)
17	0.000001	208.11	24.6.1	HTTP	100	80 → 1261 [FIN, ACK] Seq=668 Ack=875 Win=7680
18	0.000821	208.11	24.6.1	HTTP	100	HTTP/1.1 200 OK (JPEG JFIF image)

Packet Details - Frame 1:

- Frame 1: 66 bytes on wire (528 bits)
- Ethernet II, Src: Flextron_40:d6:00:00:00:00, Dst: 08:00:00:00:00:00
- Internet Protocol Version 4, Src: 24.6.1, Dst: 208.11.0.0
- Transmission Control Protocol, Src Port: 1260, Dst Port: 80
- Hypertext Transfer Protocol

Packet Bytes:

```
0000 00 01 5c 31 bb c1 00 21 cc 40 d6 91 08 00 45 00 ..\1...! .@....E.
0010 00 34 0f 80 40 00 80 06 5f 9d 18 06 b5 a0 d0 76 -4..@... _.....v
0020 ed 89 04 ec 00 50 96 a5 fd 1c 00 00 00 00 80 02 .....P.....
0030 20 00 2a 71 00 00 02 04 05 b4 01 03 03 02 01 01 ..*q.....
0040 04 02
```

Paso 3:

The image shows the Wireshark network protocol analyzer interface. The main window displays a packet capture file named 'http-misctrffic101.pcapng'. The packet list shows three TCP SYN packets from 24.6.181.160 to 208.118.237.137. Below the packet list, the 'Conversations' pane is open, showing a table of traffic statistics between two IP addresses: 24.6.181.160 and 208.118.237.137. The table includes columns for Address A, Address B, Packets, Bytes, and various flow statistics. The bottom status bar indicates that 682 packets are displayed (100.0% of the capture).

Wireshark - Conversations - http-misctrffic101.pcapng

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
24.6.181.160	107.6.133.250	475	533k	126	8261	349	525k	5.720527	1.9523	33k	2153k
24.6.181.160	208.118.237.137	207	177k	71	9483	136	168k	0.000000	1.3153	57k	1024k

Conversation Types

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

http-misctrffic101.pcapng | Packets: 682 · Displayed: 682 (100.0%) | Profile: wireshark101

Paso 4:

http-misctrffic101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	TCP Delta	Source	Destination	Protocol	Info
1	0.000000	0.000000...	24.6.181.160	208.118.237.137	TCP	1260 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
2	0.000756	0.000000...	24.6.181.160	208.118.237.137	TCP	1261 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
3	0.066928	0.000000...	24.6.181.160	208.118.237.137	TCP	1262 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460

Wireshark · Conversations · http-misctrffic101.pcapng

Ethernet · 1		IPv4 · 2		IPv6		TCP · 7		UDP									
Address A	Port A	Address B	Port 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				
24.6.181.160	1266	107.6.133.250	80	475	533k	126	8261	349	525k	5.720527	1.9523	33k	2153k				
24.6.181.160	1260	208.118.237.137	80	127	133k	37	3086	90	130k	0.000000	1.3153	18k	795k				
24.6.181.160	1264	208.118.237.137	80	40	36k	14	1705	26	34k	0.294237	0.7301	18k	376k				
24.6.181.160	1261	208.118.237.137	80	10	2141	5	1174	5	967	0.000756	0.3405	27k	22k				
24.6.181.160	1263	208.118.237.137	80	10	2012	5	1175	5	837	0.172622	0.3237	29k	20k				
24.6.181.160	1262	208.118.237.137	80	10	2011	5	1174	5	837	0.067684	0.3449	27k	19k				
24.6.181.160	1265	208.118.237.137	80	10	1821	5	1169	5	652	0.348607	0.3110	30k	16k				

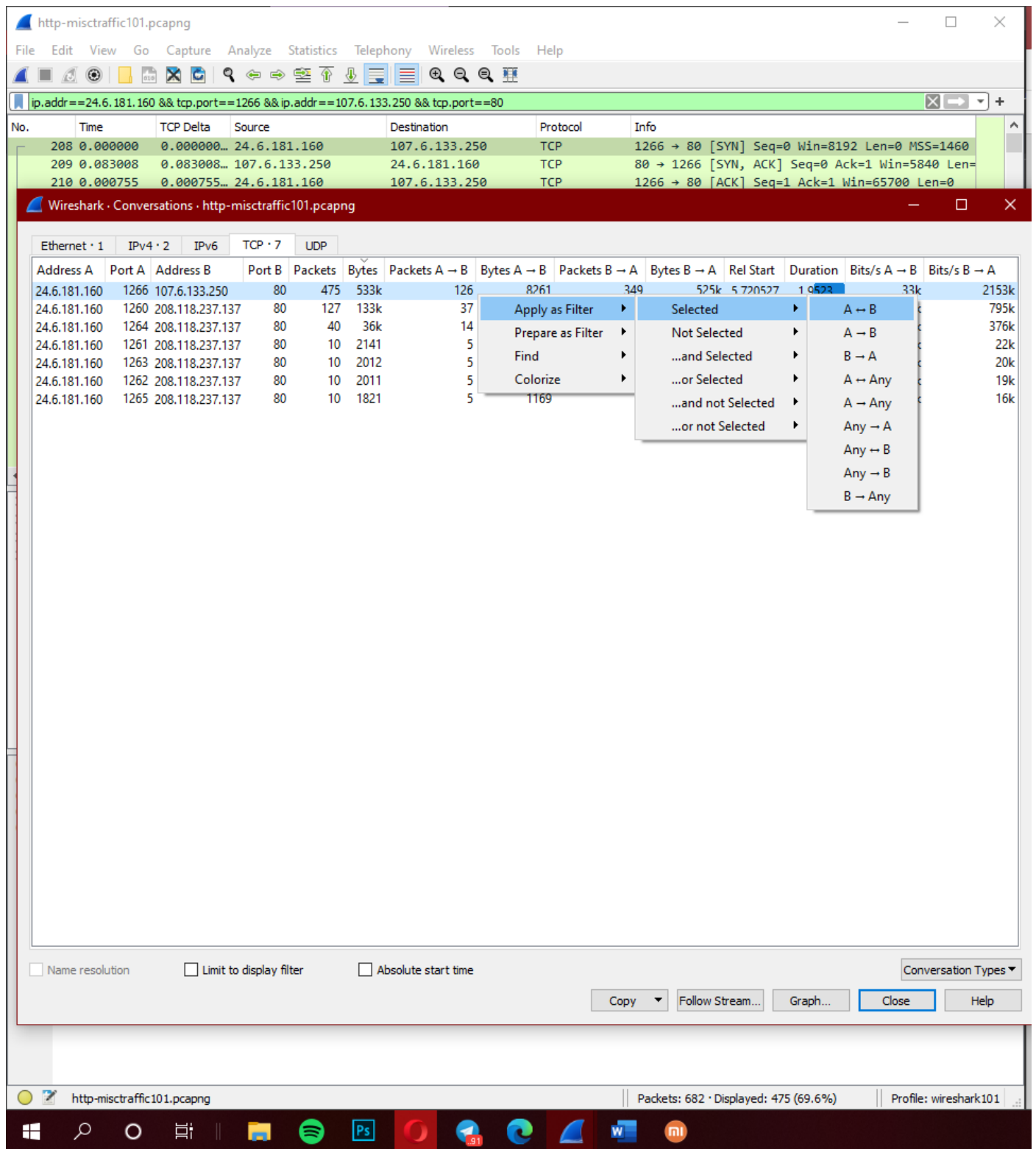
☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

Conversation Types ▾

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

http-misctrffic101.pcapng | Packets: 682 · Displayed: 682 (100.0%) | Profile: wireshark101

Paso 5:



http-misctraffic101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==24.6.181.160 && tcp.port==1266 && ip.addr==107.6.133.250 && tcp.port==80

No.	Time	TCP Delta	Source	Destination	Protocol	Info
208	0.000000	0.000000...	24.6.181.160	107.6.133.250	TCP	1266 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
209	0.083008	0.083008...	107.6.133.250	24.6.181.160	TCP	80 → 1266 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
210	0.000755	0.000755...	24.6.181.160	107.6.133.250	TCP	1266 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0

Wireshark · Conversations · http-misctraffic101.pcapng

Ethernet · 1		IPv4 · 2		IPv6		TCP · 7		UDP					
Address A	Port A	Address B	Port 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
24.6.181.160	1266	107.6.133.250	80	475	533k	126	8261	349	525k	5.720527	1.0593	33k	2153k
24.6.181.160	1260	208.118.237.137	80	127	133k	37							795k
24.6.181.160	1264	208.118.237.137	80	40	36k	14							376k
24.6.181.160	1261	208.118.237.137	80	10	2141	5							22k
24.6.181.160	1263	208.118.237.137	80	10	2012	5							20k
24.6.181.160	1262	208.118.237.137	80	10	2011	5							19k
24.6.181.160	1265	208.118.237.137	80	10	1821	5	1169						16k

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

Conversation Types ▾

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

http-misctraffic101.pcapng | Packets: 682 · Displayed: 475 (69.6%) | Profile: wireshark101

Paso 6:

http-misctraffic101.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==24.6.181.160 && tcp.port==1266 && ip.addr==107.6.133.250 && tcp.port==80

No.	Time	TCP Delta	Source	Destination	Protocol	Info
208	0.000000	0.000000...	24.6.181.160	107.6.133.250	TCP	1266 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
209	0.083008	0.083008...	107.6.133.250	24.6.181.160	TCP	80 → 1266 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=
210	0.000755	0.000755...	24.6.181.160	107.6.133.250	TCP	1266 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
211	0.014505	0.014505...	24.6.181.160	107.6.133.250	HTTP	GET /data/releases/metasploit-latest-windows-i
212	0.084223	0.084223...	107.6.133.250	24.6.181.160	TCP	80 → 1266 [ACK] Seq=1 Ack=702 Win=7296 Len=0
213	0.001248	0.001248...	107.6.133.250	24.6.181.160	HTTP	HTTP/1.1 200 OK (application/x-msdos-program)
214	0.000799	0.000799...	107.6.133.250	24.6.181.160	HTTP	Continuation
215	0.001509	0.001509...	107.6.133.250	24.6.181.160	HTTP	Continuation
216	0.000004	0.000004...	24.6.181.160	107.6.133.250	TCP	1266 → 80 [ACK] Seq=702 Ack=4381 Win=65700 Len=
217	0.081719	0.081719...	107.6.133.250	24.6.181.160	HTTP	Continuation
218	0.000003	0.000003...	107.6.133.250	24.6.181.160	HTTP	Continuation
219	0.000003	0.000003...	107.6.133.250	24.6.181.160	HTTP	Continuation
220	0.000780	0.000780...	107.6.133.250	24.6.181.160	HTTP	Continuation
221	0.004718	0.004718...	24.6.181.160	107.6.133.250	TCP	1266 → 80 [ACK] Seq=702 Ack=10221 Win=65700 Le
222	0.082874	0.082874...	107.6.133.250	24.6.181.160	HTTP	Continuation
223	0.000775	0.000775...	107.6.133.250	24.6.181.160	HTTP	Continuation
224	0.000003	0.000003...	107.6.133.250	24.6.181.160	HTTP	Continuation
225	0.000792	0.000792...	107.6.133.250	24.6.181.160	HTTP	Continuation

> Frame 208: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface unknown, id 0
 > Ethernet II, Src: Flextron_40:d6:91 (00:21:cc:40:d6:91), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
 > Internet Protocol Version 4, Src: 24.6.181.160, Dst: 107.6.133.250
 > Transmission Control Protocol, Src Port: 1266, Dst Port: 80, Seq: 0, Len: 0

```

0000  00 01 5c 31 bb c1 00 21 cc 40 d6 91 08 00 45 00  ..\1...! .@....E.
0010  00 34 0f f2 40 00 80 06 2c 2b 18 06 b5 a0 6b 06  .4..@... ,+...k.
0020  85 fa 04 f2 00 50 97 7c eb 89 00 00 00 00 80 02  ....P| .....
0030  20 00 08 27 00 00 02 04 05 b4 01 03 03 02 01 01  ...'....
0040  04 02
  
```

http-misctraffic101.pcapng | Packets: 682 · Displayed: 475 (69.6%) | Profile: wireshark101