

# INSTITUTO TECNOLÓGICO DE CANCUN



Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio 19

Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

# Lab19- Detect Background File Transfers on Startup

## Paso 1:

The screenshot shows the Wireshark 'Open Capture File' dialog box. The 'Buscar en:' field is set to 'wireshark101v2files'. The file list contains various capture files, with 'gen-startupchatty101.pcapng' selected. The 'Nombre de archivo:' field also shows 'gen-startupchatty101.pcapng'. The 'Tipo de archivo:' is set to 'All Files'. The 'Read filter:' is empty, and the 'Format:' is 'Wireshark/... - pcapng'. The 'Size:' is '3239 KiB, 3290 data records'. The 'Start / elapsed:' is '2012-11-02 15:18:45 / 00:02:15'. The 'Abrir' button is highlighted.

Nombre	Fecha de modificación	Tipo	Tamaño
challenge101-8.pcapng	12/11/2012 16:38	Wireshark capture...	1.276 KB
dfilters_sample.txt	24/01/2013 18:38	Documento de te...	1 KB
dhcp-serverdiscovery101.pcapng	03/11/2012 19:30	Wireshark capture...	6 KB
dns-nmap101.pcapng	30/10/2012 15:10	Wireshark capture...	8 KB
filterexpressions101.txt	19/11/2012 21:22	Documento de te...	1 KB
ftp-bounce.pcapng	09/05/2012 14:39	Wireshark capture...	51 KB
ftp-clientside101.pcapng	03/11/2012 18:55	Wireshark capture...	5.999 KB
ftp-crack101.pcapng	03/11/2012 19:35	Wireshark capture...	1.906 KB
ftp-download101.pcapng	21/10/2012 12:14	Wireshark capture...	24.344 KB
ftp-passwords101.pcapng	14/07/2016 22:17	Wireshark capture...	1.200 KB
general101.pcapng	25/10/2012 23:55	Wireshark capture...	92 KB
general101b.pcapng	02/11/2012 15:13	Wireshark capture...	182 KB
general101c.pcapng	06/11/2012 13:38	Wireshark capture...	449 KB
general101d.pcapng	06/11/2012 15:47	Wireshark capture...	34.807 KB
gen-startupchatty101.pcapng	02/11/2012 14:28	Wireshark capture...	3.240 KB
http-au101b.pcapng	23/10/2012 17:09	Wireshark capture...	747 KB
http-browse101a.pcapng	02/11/2012 17:50	Wireshark capture...	1.719 KB
http-browse101b.pcapng	02/11/2012 14:55	Wireshark capture...	119 KB
http-browse101c.pcapng	04/11/2012 20:31	Wireshark capture...	838 KB
http-browse101d.pcapng	04/11/2012 20:31	Wireshark capture...	838 KB
http-chappellu101.pcapng	24/10/2012 16:10	Wireshark capture...	948 KB

Read filter:  Format: Wireshark/... - pcapng  
Automatically detect file type Size: 3239 KiB, 3290 data records  
Start / elapsed: 2012-11-02 15:18:45 / 00:02:15

Abrir Cancelar Ayuda

0060 6c 64 2d 73 65 72 76 65 72 73 03 6e 65 74 00 05 ld-serve rs.net..  
0070 6e 73 74 6c 64 0c 76 65 72 69 73 69 67 6e 2d 67 nstld-ve risign-g  
0080 72 73 c0 1c 50 94 1d b8 00 00 07 08 00 00 03 84 rs..P... ..  
0090 00 09 3a 80 00 01 51 80 ..:..Q.

http-errors101.pcapng Packets: 28 · Displayed: 28 (100.0%) Profile: Default

## The screenshot displays the Wireshark application window titled "gen-startupchatty101.pcapng". The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. A filter bar at the top right shows "Apply a display filter ... &lt;Ctrl-/&gt;". The main packet list pane shows a single entry (No. 1) at Time 0.000000, identified as DHCP Request - Transaction ID 0x5f64a1. Below this, the "Conversations" pane highlights the selected packet. The central packet details pane shows the hierarchy: Ethernet II (13), IPv4 (15), TCP (6), and UDP (52). The bottom pane displays the raw packet data in hexadecimal and ASCII. At the very bottom, a status bar indicates "Packets: 3290 · Displayed: 3290 (100.0%)" and "Profile: wireshark101".

### Paso 3:

The image shows the Wireshark network protocol analyzer interface. The main window displays a list of captured packets. The first packet is a DHCP Request (Transaction ID 0x5f64a1). A context menu is open over the first packet, showing options like 'Apply as Filter', 'Prepare a Filter', 'Find', and 'Colorize'. The 'Apply as Filter' option is selected, and a sub-menu is open showing various filter expressions like 'Selected', 'Not Selected', 'A → B', etc.

**Wireshark - Conversations - gen-startupchatty101.pcapng**

Ethernet · 13	IPv4 · 15	IPv6 · 12	TCP · 6	UDP · 52		
No.	Time	TCP Delta	Source	Destination	Protocol	Info
1	0.000000		0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x5f64a1

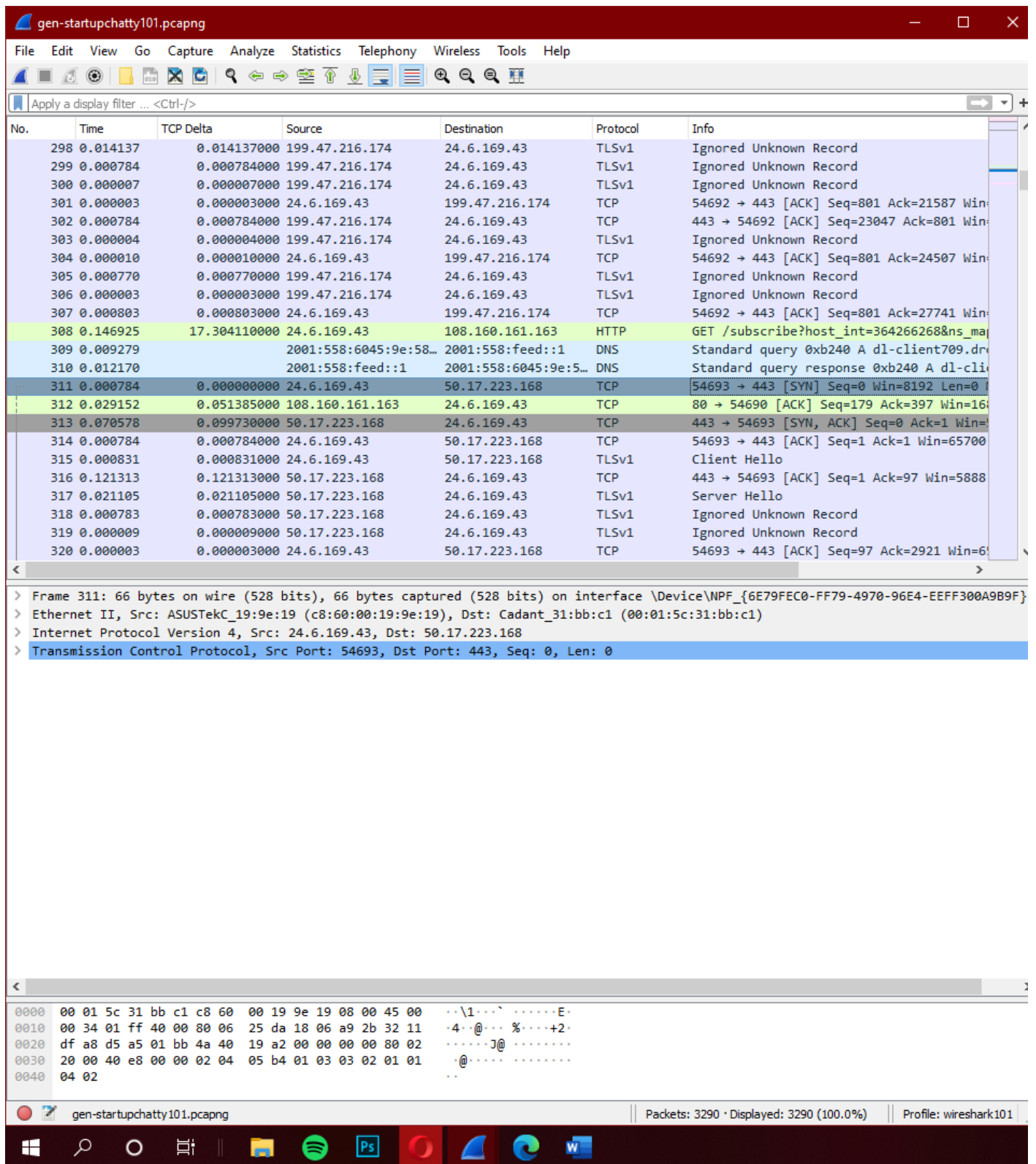
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
24.6.169.43	54693	50.17.223.168	443	2,886	297,116	0	0	1	1,021	2012.1	117.4765	3968	198 k
24.6.169.43	54692	199.47.216.174	443	45	3	1	50	0	0	24.0885	24.0885	120	1887
24.6.169.43	54689	199.47.217.177	443	26	1	1	7,241	0	0	7.2411	7.2411	1663	6373
24.6.169.43	54694	24.6.173.220	17500	27	4	1	11,485	0	0	11.4851	11.4851	167	187
24.6.169.43	54690	108.160.161.163	80	17	2	1	35,126	0	0	35.1267	35.1267	74	62
24.6.169.43	54675	65.54.87.217	80	3	0	0	0	1	28,001	28.0016	28.0016	0	11

☐ Name resolution    ☐ Limit to display filter    ☐ Absolute start time    Conversation Types ▾

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

0000 ff ff ff ff ff ff c8 60 00 19 9e 19 08 00 45 00 .....E  
0010 01 4c 01 71 00 00 80 11 38 31 00 00 00 00 ff ff ..L.q....81....  
0020 ff ff 00 44 00 43 01 38 5c 78 01 01 06 00 5f 64 ...D.C.8 \x....d  
0030 a1 65 00 00 00 00 00 00 00 00 00 00 00 00 00 ..e.....  
0040 00 00 00 00 00 00 c8 60 00 19 9e 19 00 00 00 00 .....  
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
gen-startupchatty101.pcapng    Packets: 3290 · Displayed: 3290 (100.0%)    Profile: wireshark101

## Paso 4:



The image shows a Wireshark packet capture analysis of a file named `gen-startupchatty101.pcapng`. The main display area shows a list of network packets with columns for No., Time, TCP Delta, Source, Destination, Protocol, and Info. The selected packet is number 311, which is an HTTP GET request to `/subscribe?host_int=364266268&ns_ma` from source `24.6.169.43` to destination `50.17.223.168`. The packet details pane below the list shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (Seq: 0, Len: 0).

No.	Time	TCP Delta	Source	Destination	Protocol	Info
298	0.014137	0.014137000	199.47.216.174	24.6.169.43	TLSv1	Ignored Unknown Record
299	0.000784	0.000784000	199.47.216.174	24.6.169.43	TLSv1	Ignored Unknown Record
300	0.000007	0.000007000	199.47.216.174	24.6.169.43	TLSv1	Ignored Unknown Record
301	0.000003	0.000003000	24.6.169.43	199.47.216.174	TCP	54692 → 443 [ACK] Seq=801 Ack=21587 Win=
302	0.000784	0.000784000	199.47.216.174	24.6.169.43	TCP	443 → 54692 [ACK] Seq=23047 Ack=801 Win=
303	0.000004	0.000004000	199.47.216.174	24.6.169.43	TLSv1	Ignored Unknown Record
304	0.000010	0.000010000	24.6.169.43	199.47.216.174	TCP	54692 → 443 [ACK] Seq=801 Ack=24507 Win=
305	0.000770	0.000770000	199.47.216.174	24.6.169.43	TLSv1	Ignored Unknown Record
306	0.000003	0.000003000	199.47.216.174	24.6.169.43	TLSv1	Ignored Unknown Record
307	0.000803	0.000803000	24.6.169.43	199.47.216.174	TCP	54692 → 443 [ACK] Seq=801 Ack=27741 Win=
308	0.146925	17.304110000	24.6.169.43	108.160.161.163	HTTP	GET /subscribe?host_int=364266268&ns_ma
309	0.009279		2001:558:6045:9e:58...	2001:558:feed::1	DNS	Standard query 0xb240 A dl-client709.dr
310	0.012170		2001:558:feed::1	2001:558:6045:9e:5...	DNS	Standard query response 0xb240 A dl-cli
311	0.000784	0.000000000	24.6.169.43	50.17.223.168	TCP	54693 → 443 [SYN] Seq=0 Win=8192 Len=0
312	0.029152	0.051385000	108.160.161.163	24.6.169.43	TCP	80 → 54690 [ACK] Seq=179 Ack=397 Win=16
313	0.070578	0.099730000	50.17.223.168	24.6.169.43	TCP	443 → 54693 [SYN, ACK] Seq=0 Ack=1 Win=
314	0.000784	0.000784000	24.6.169.43	50.17.223.168	TCP	54693 → 443 [ACK] Seq=1 Ack=1 Win=65700
315	0.000831	0.000831000	24.6.169.43	50.17.223.168	TLSv1	Client Hello
316	0.121313	0.121313000	50.17.223.168	24.6.169.43	TCP	443 → 54693 [ACK] Seq=1 Ack=97 Win=5888
317	0.021105	0.021105000	50.17.223.168	24.6.169.43	TLSv1	Server Hello
318	0.000783	0.000783000	50.17.223.168	24.6.169.43	TLSv1	Ignored Unknown Record
319	0.000009	0.000009000	50.17.223.168	24.6.169.43	TLSv1	Ignored Unknown Record
320	0.000003	0.000003000	24.6.169.43	50.17.223.168	TCP	54693 → 443 [ACK] Seq=97 Ack=2921 Win=6

Frame 311: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}

Ethernet II, Src: ASUSTekC\_19:9e:19 (c8:60:00:19:9e:19), Dst: Cadant\_31:bb:c1 (00:01:5c:31:bb:c1)

Internet Protocol Version 4, Src: 24.6.169.43, Dst: 50.17.223.168

Transmission Control Protocol, Src Port: 54693, Dst Port: 443, Seq: 0, Len: 0

0000 00 01 5c 31 bb c1 c8 60 00 19 9e 19 08 00 45 00 ..\1... ..E.  
0010 00 34 01 ff 40 00 80 06 25 da 18 06 a9 2b 32 11 .4..@... %...+2.  
0020 df a8 d5 a5 01 bb 4a 40 19 a2 00 00 00 80 02 .....J@ .....  
0030 20 00 40 e8 00 00 02 04 05 b4 01 03 03 02 01 01 .@..... ..  
0040 04 02 ..

gen-startupchatty101.pcapng | Packets: 3290 · Displayed: 3290 (100.0%) | Profile: wireshark101