INSTITUTO TECNOLOGICO DE CANCUN

Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

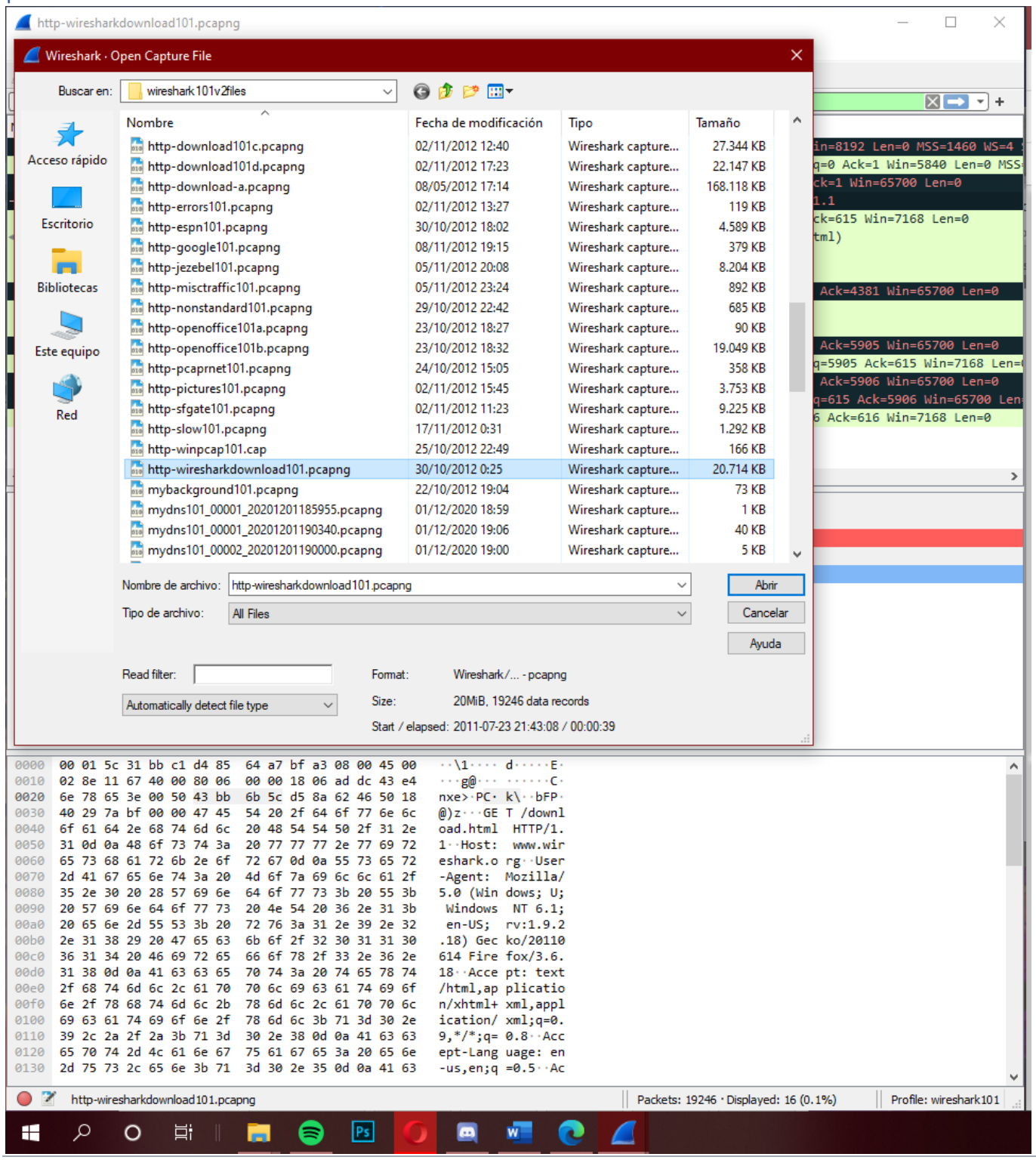
N.º De Actividad: Laboratorio 37

Nombre Del Alumno: Vazquez Canto Andres Omar

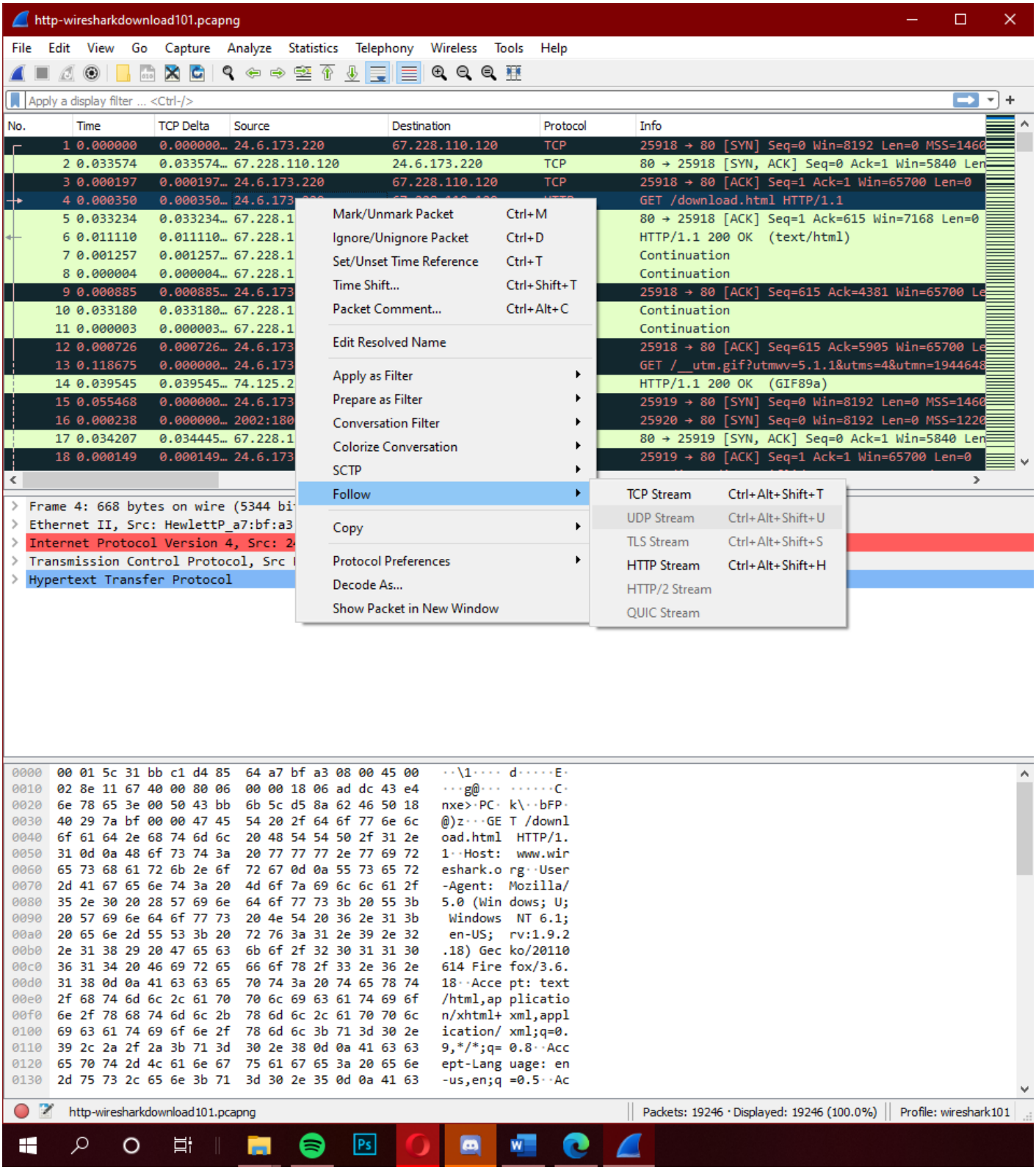
N.º De Control: 17530439

Lab37- Use Reassembly to Find a Web Site's Hidden HTTP Message

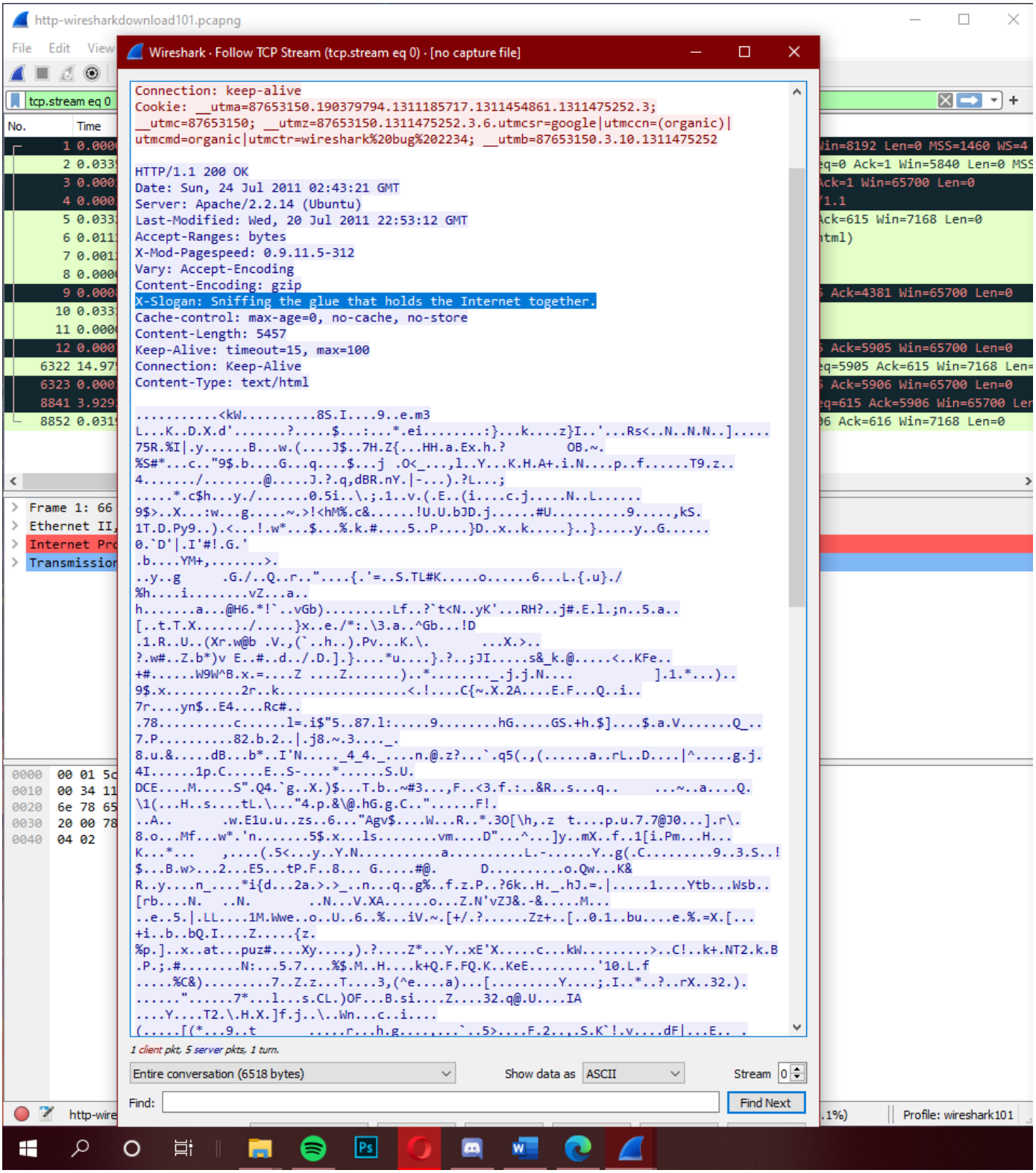
paso 1:



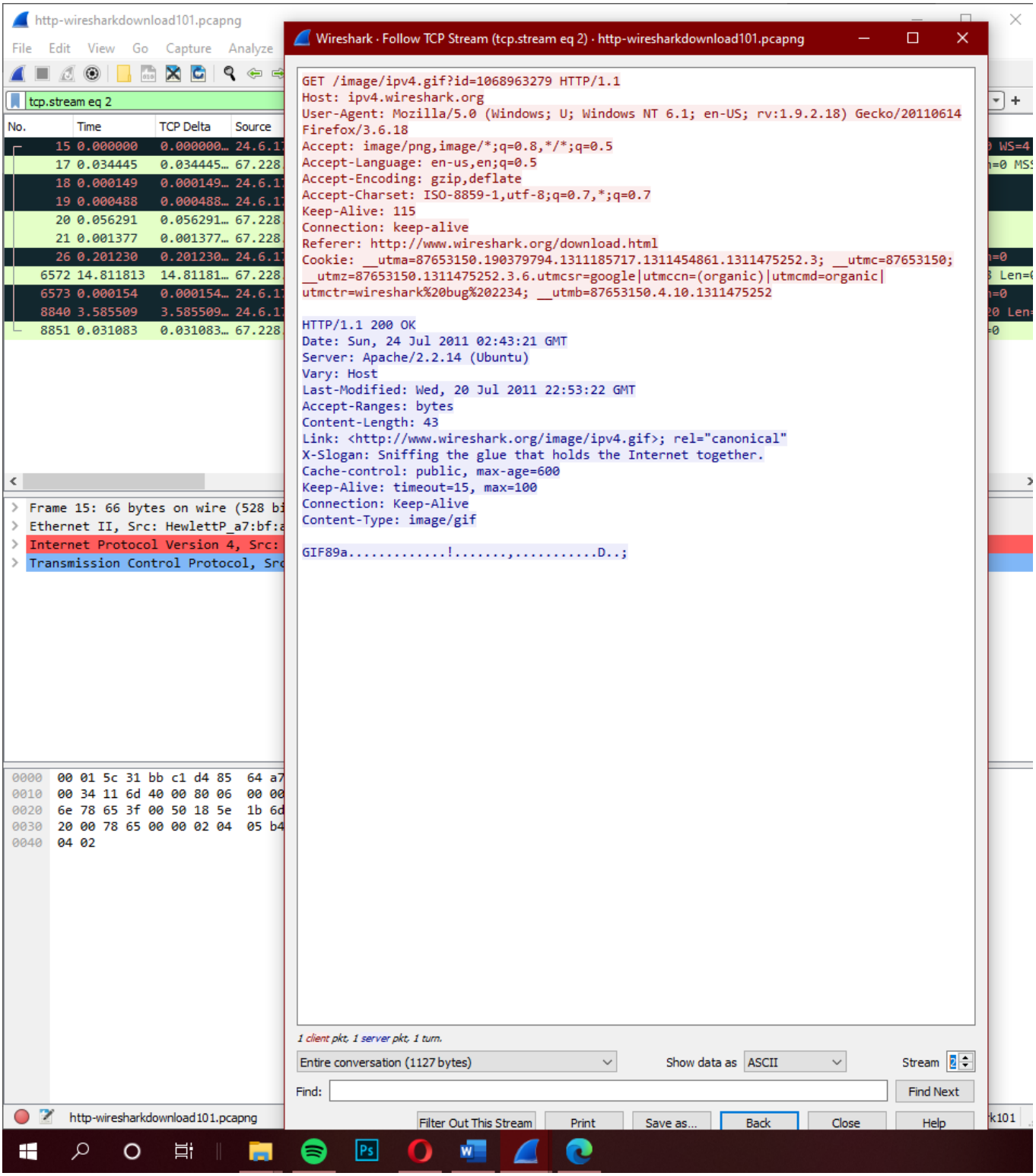
paso 2:


http-wiresharkdownload101.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… 24.6.173.220 67.228.110.120 TCP 25918 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
2 0.033574 0.033574… 67.228.110.120 24.6.173.220 TCP 80 → 25918 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len
3 0.000197 0.000197… 24.6.173.220 67.228.110.120 TCP 25918 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
4 0.000350 0.000350… 24.6.173 GET /download.html HTTP/1.1
5 0.033234 0.033234… 67.228.1 80 → 25918 [ACK] Seq=1 Ack=615 Win=7168 Len=0
6 0.011110 0.011110… 67.228.1 HTTP/1.1 200 OK (text/html)
7 0.001257 0.001257… 67.228.1 Continuation
8 0.000004 0.000004… 67.228.1 Continuation
9 0.000885 0.000885… 24.6.173 25918 → 80 [ACK] Seq=615 Ack=4381 Win=65700 Le
10 0.033180 0.033180… 67.228.1 Continuation
11 0.000003 0.000003… 67.228.1 Continuation
12 0.000726 0.000726… 24.6.173 25918 → 80 [ACK] Seq=615 Ack=5905 Win=65700 Le
13 0.118675 0.000000… 24.6.173 GET /__utm.gif?utmwv=5.1.1&utms=4&utmn=1944648
14 0.039545 0.039545… 74.125.2 HTTP/1.1 200 OK (GIF89a)
15 0.055468 0.000000… 24.6.173 25919 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
16 0.000238 0.000000… 2002:180 25920 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1220
17 0.034207 0.034445… 67.228.1 80 → 25919 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len
18 0.000149 0.000149… 24.6.173 25919 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
Frame 4: 668 bytes on wire (5344 bi
Ethernet II, Src: HewlettP_a7:bf:a3
Internet Protocol Version 4, Src: 2
Transmission Control Protocol, Src
Hypertext Transfer Protocol
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ··\1···· d·····E·
0010 02 8e 11 67 40 00 80 06 00 00 18 06 ad dc 43 e4 ···g@··· ·····C·
0020 6e 78 65 3e 00 50 43 bb 6b 5c d5 8a 62 46 50 18 nxe>·PC· k\··bFP·
0030 40 29 7a bf 00 00 47 45 54 20 2f 64 6f 77 6e 6c @)z···GE T /downl
0040 6f 61 64 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e oad.html HTTP/1.
0050 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 77 69 72 1··Host: www.wir
0060 65 73 68 61 72 6b 2e 6f 72 67 0d 0a 55 73 65 72 eshark.o rg··User
0070 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
0080 35 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 5.0 (Win dows; U;
0090 20 57 69 6e 64 6f 77 73 20 4e 54 20 36 2e 31 3b Windows NT 6.1;
00a0 20 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 39 2e 32 en-US; rv:1.9.2
00b0 2e 31 38 29 20 47 65 63 6b 6f 2f 32 30 31 31 30 .18) Gec ko/20110
00c0 36 31 34 20 46 69 72 65 66 6f 78 2f 33 2e 36 2e 614 Fire fox/3.6.
00d0 31 38 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 18··Acce pt: text
00e0 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f /html,ap plicatio
00f0 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c n/xhtml+ xml,appl
0100 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e ication/ xml;q=0.
0110 39 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 9,*/*;q= 0.8··Acc
0120 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e ept-Lang uage: en
0130 2d 75 73 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 -us,en;q =0.5··Ac
http-wiresharkdownload101.pcapng
Packets: 19246 · Displayed: 19246 (100.0%)
Profile: wireshark101

Paso 3:


http-wiresharkdownload101.pcapng
File Edit View
Wireshark · Follow TCP Stream (tcp.stream eq 0) · [no capture file]
tcp.stream eq 0
No. Time
Connection: keep-alive
Cookie: __utma=87653150.190379794.1311185717.1311454861.1311475252.3;
__utmc=87653150; __utmz=87653150.1311475252.3.6.utmcsr=google|utmccn=(organic)|
utmcmd=organic|utmctr=wireshark%20bug%202234; __utmb=87653150.3.10.1311475252
HTTP/1.1 200 OK
Date: Sun, 24 Jul 2011 02:43:21 GMT
Server: Apache/2.2.14 (Ubuntu)
Last-Modified: Wed, 20 Jul 2011 22:53:12 GMT
Accept-Ranges: bytes
X-Mod-Pagespeed: 0.9.11.5-312
Vary: Accept-Encoding
Content-Encoding: gzip
X-Slogan: Sniffing the glue that holds the Internet together.
Cache-control: max-age=0, no-cache, no-store
Content-Length: 5457
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
1 client pkt, 5 server pkts, 1 turn.
Entire conversation (6518 bytes)
Show data as ASCII
Stream 0
Find:
Find Next
Frame 1: 66
Ethernet II,
Internet Pro
Transmissior
Profile: wireshark101

Paso 4 y 5:


http-wiresharkdownload101.pcapng
File Edit View Go Capture Analyze
tcp.stream eq 2
No. Time TCP Delta Source
15 0.000000 0.000000… 24.6.1
17 0.034445 0.034445… 67.228
18 0.000149 0.000149… 24.6.1
19 0.000488 0.000488… 24.6.1
20 0.056291 0.056291… 67.228
21 0.001377 0.001377… 67.228
26 0.201230 0.201230… 24.6.1
6572 14.811813 14.81181… 67.228
6573 0.000154 0.000154… 24.6.1
8840 3.585509 3.585509… 24.6.1
8851 0.031083 0.031083… 67.228
Frame 15: 66 bytes on wire (528 bi
Ethernet II, Src: HewlettP_a7:bf:a
Internet Protocol Version 4, Src:
Transmission Control Protocol, Src
0000 00 01 5c 31 bb c1 d4 85 64 a7
0010 00 34 11 6d 40 00 80 06 00 00
0020 6e 78 65 3f 00 50 18 5e 1b 6d
0030 20 00 78 65 00 00 02 04 05 b4
0040 04 02
http-wiresharkdownload101.pcapng
Wireshark · Follow TCP Stream (tcp.stream eq 2) · http-wiresharkdownload101.pcapng
GET /image/ipv4.gif?id=1068963279 HTTP/1.1
Host: ipv4.wireshark.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.18) Gecko/20110614 Firefox/3.6.18
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.wireshark.org/download.html
Cookie: __utma=87653150.190379794.1311185717.1311454861.1311475252.3; __utmc=87653150; __utmz=87653150.1311475252.3.6.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=wireshark%20bug%202234; __utmb=87653150.4.10.1311475252
HTTP/1.1 200 OK
Date: Sun, 24 Jul 2011 02:43:21 GMT
Server: Apache/2.2.14 (Ubuntu)
Vary: Host
Last-Modified: Wed, 20 Jul 2011 22:53:22 GMT
Accept-Ranges: bytes
Content-Length: 43
Link: <http://www.wireshark.org/image/ipv4.gif>; rel="canonical"
X-Slogan: Sniffing the glue that holds the Internet together.
Cache-control: public, max-age=600
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: image/gif
GIF89a.....!.....,.....D..;
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (1127 bytes)
Show data as ASCII
Stream 2
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help