INSTITUTO TECNOLOGICO DE CANCUN

Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

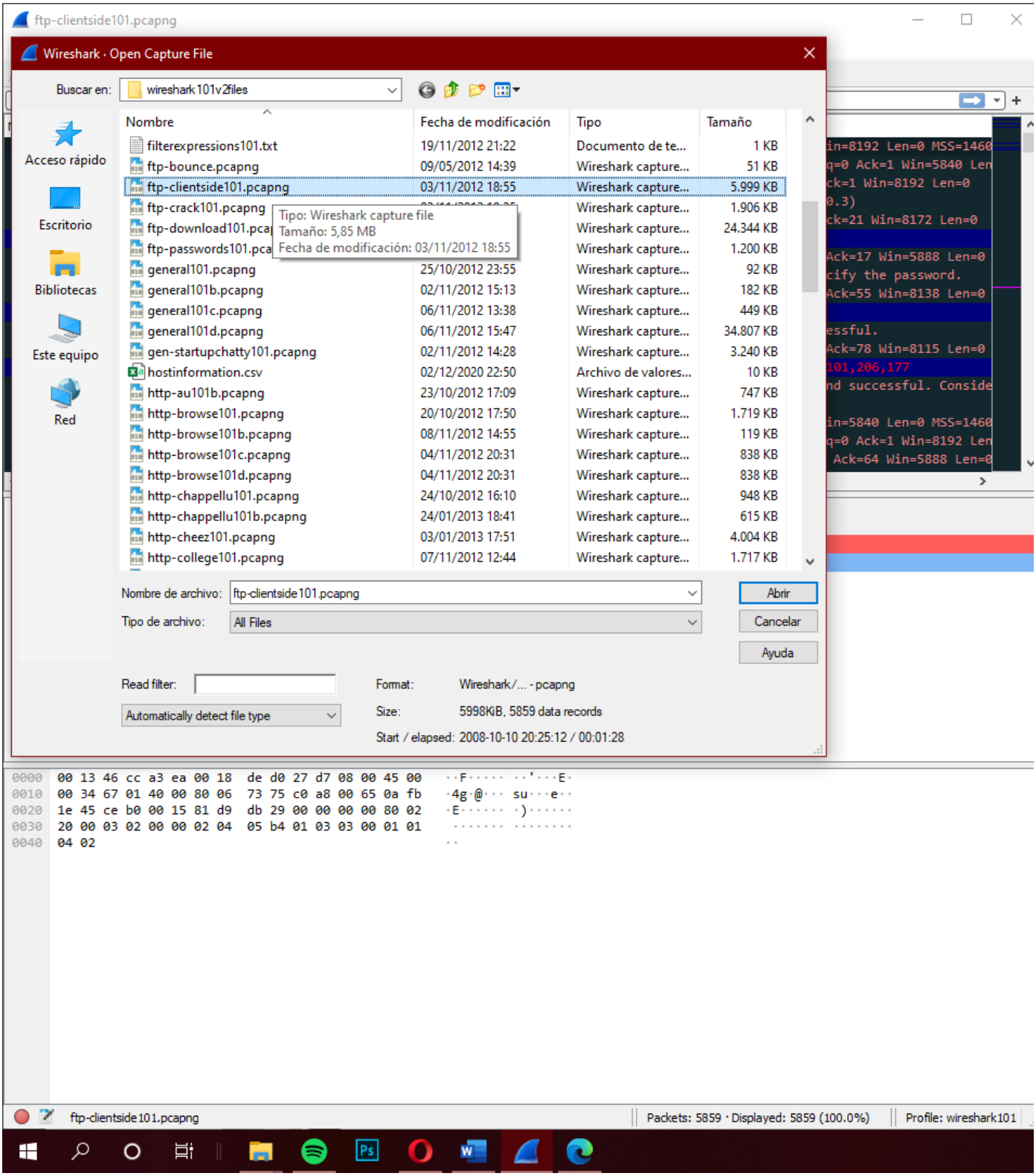
N.º De Actividad: Laboratorio 38

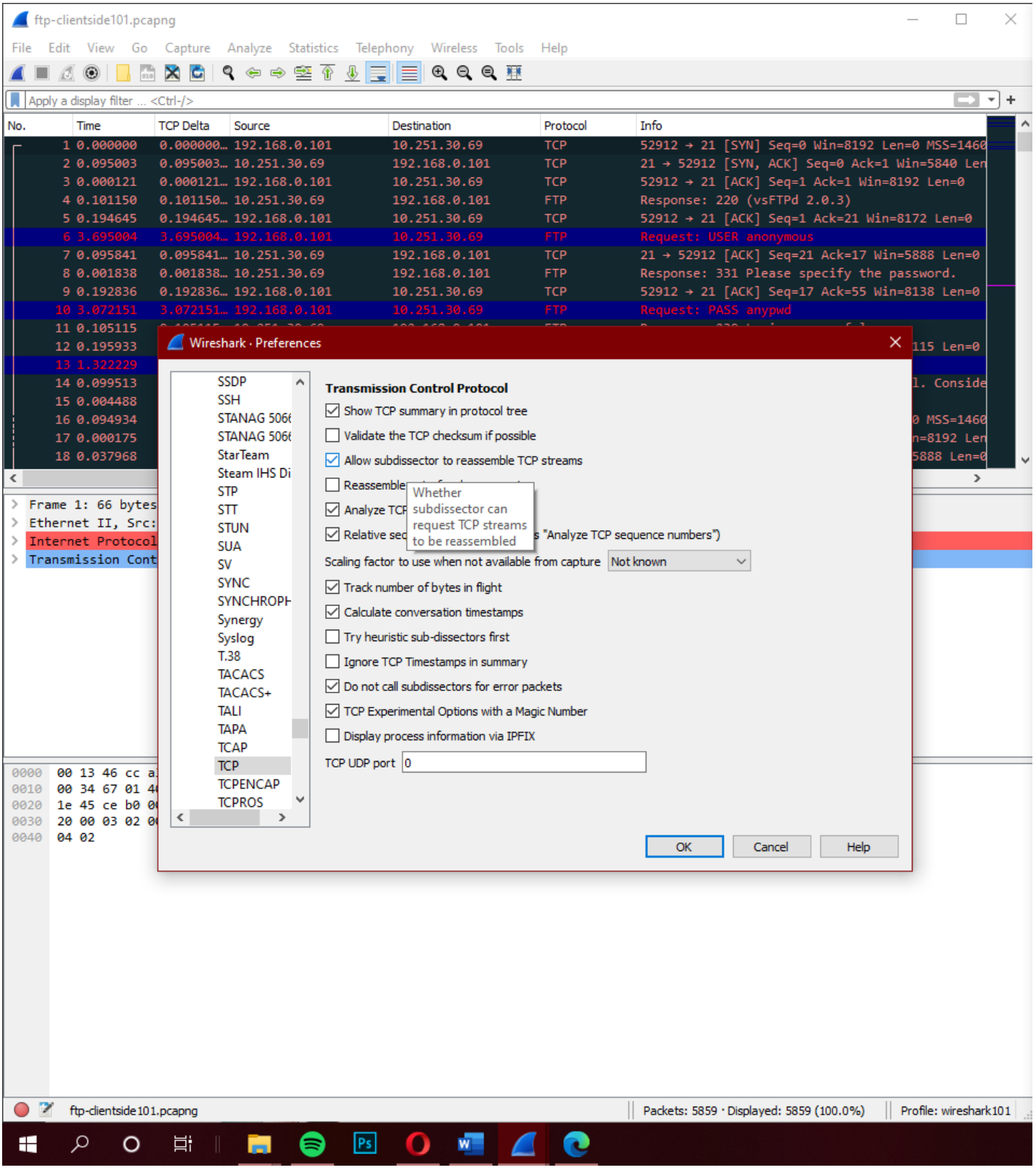
Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

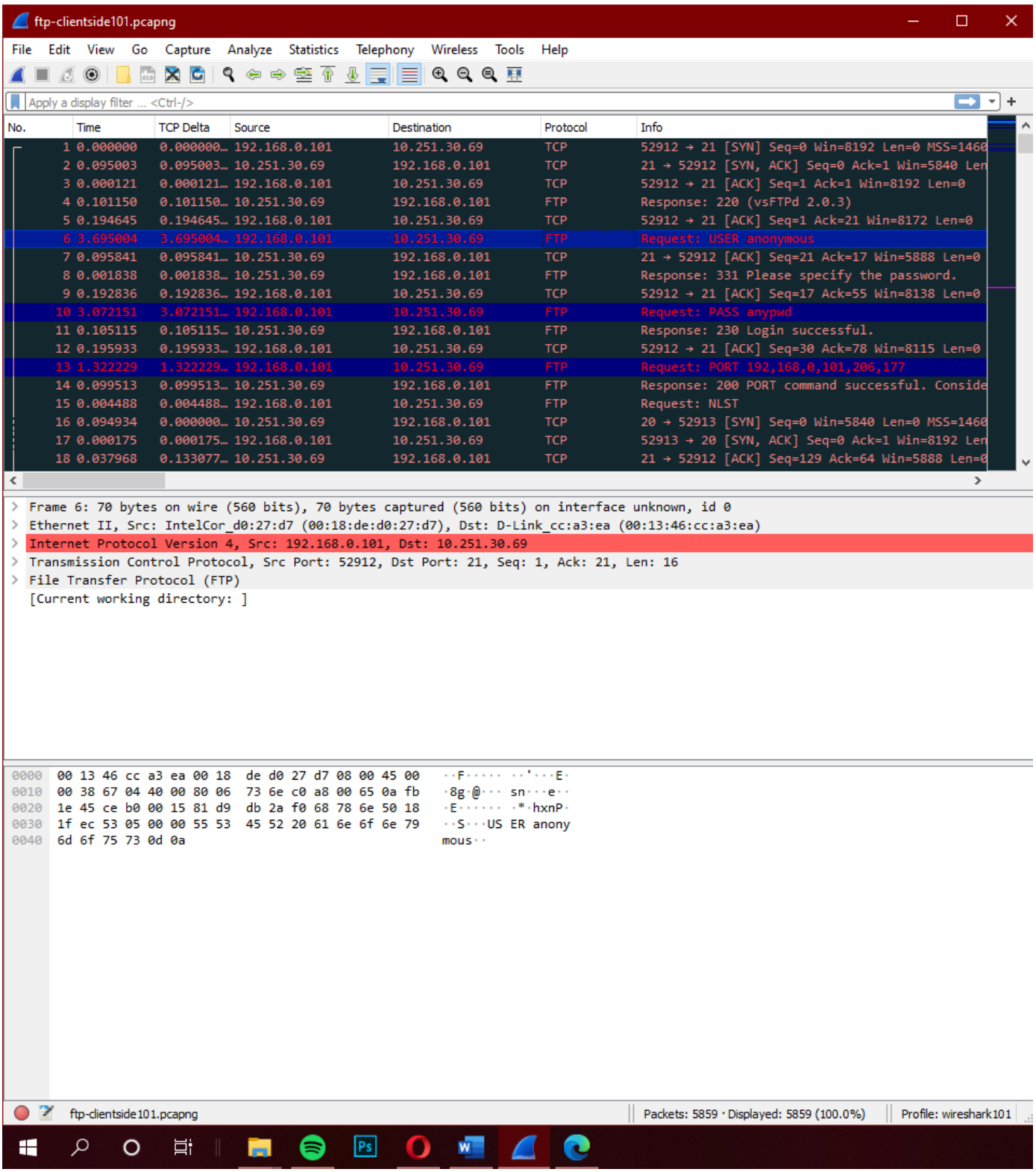
Lab38- Extract a File from an HTTP File Transfer

Paso 1:

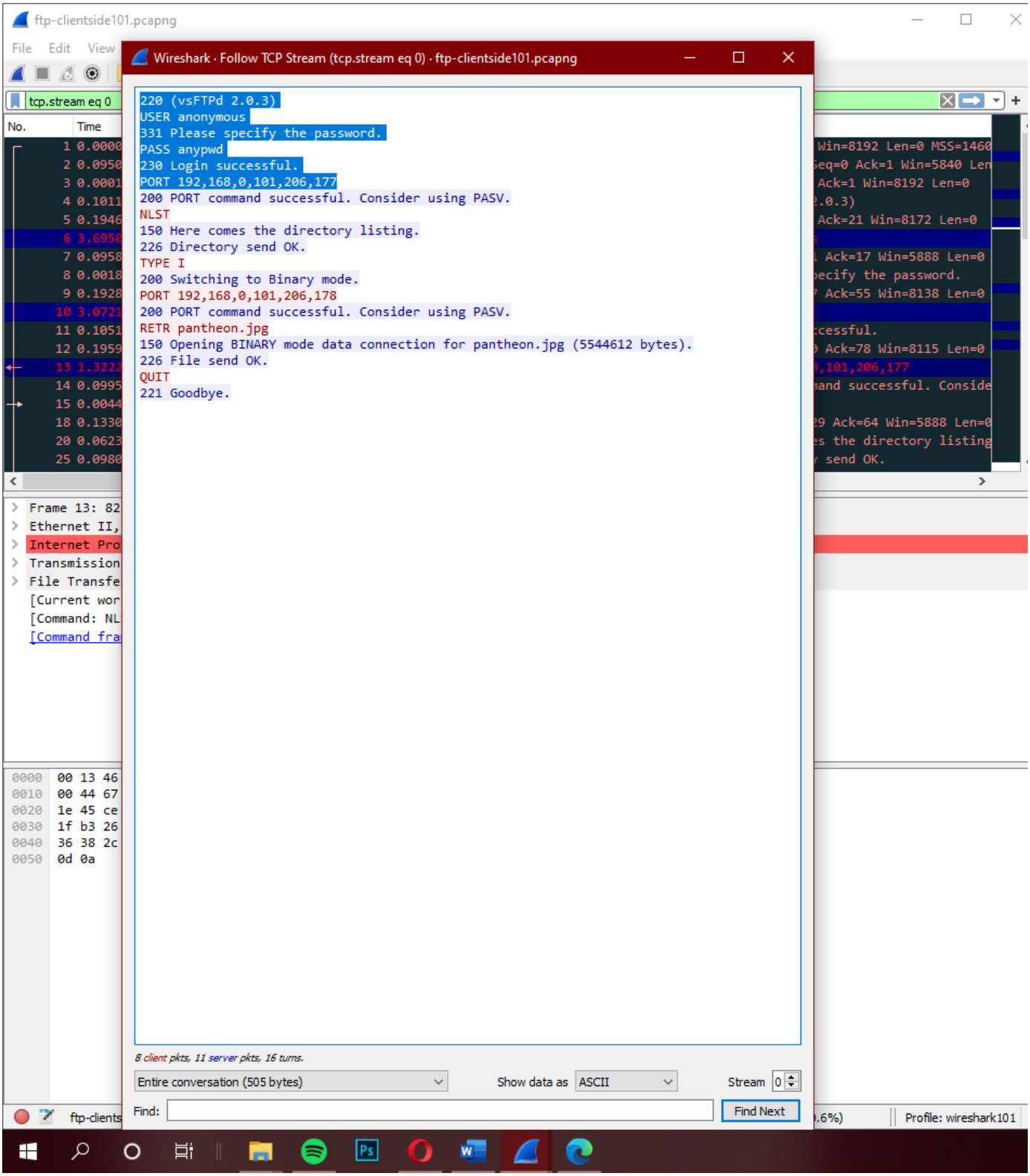



ftp-clientside101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time TCP Delta Source Destination Protocol Info
1 0.000000 0.000000… 192.168.0.101 10.251.30.69 TCP 52912 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
2 0.095003 0.095003… 10.251.30.69 192.168.0.101 TCP 21 → 52912 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len
3 0.000121 0.000121… 192.168.0.101 10.251.30.69 TCP 52912 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
4 0.101150 0.101150… 10.251.30.69 192.168.0.101 FTP Response: 220 (vsFTPd 2.0.3)
5 0.194645 0.194645… 192.168.0.101 10.251.30.69 TCP 52912 → 21 [ACK] Seq=1 Ack=21 Win=8172 Len=0
6 3.695004 3.695004… 192.168.0.101 10.251.30.69 FTP Request: USER anonymous
7 0.095841 0.095841… 10.251.30.69 192.168.0.101 TCP 21 → 52912 [ACK] Seq=21 Ack=17 Win=5888 Len=0
8 0.001838 0.001838… 10.251.30.69 192.168.0.101 FTP Response: 331 Please specify the password.
9 0.192836 0.192836… 192.168.0.101 10.251.30.69 TCP 52912 → 21 [ACK] Seq=17 Ack=55 Win=8138 Len=0
10 3.072151 3.072151… 192.168.0.101 10.251.30.69 FTP Request: PASS anypwd
11 0.105115
12 0.195933
13 1.322229
14 0.099513
15 0.004488
16 0.094934
17 0.000175
18 0.037968
Frame 1: 66 bytes
Ethernet II, Src:
Internet Protocol
Transmission Cont
0000 00 13 46 cc a
0010 00 34 67 01 4
0020 1e 45 ce b0 0
0030 20 00 03 02 0
0040 04 02
Wireshark · Preferences
SSDP
SSH
STANAG 5066
STANAG 5066
StarTeam
Steam IHS Di
STP
STT
STUN
SUA
SV
SYNC
SYNCHROPH
Synergy
Syslog
T.38
TACACS
TACACS+
TALI
TAPA
TCAP
TCP
TCPENCAP
TCPROS
Transmission Control Protocol
Show TCP summary in protocol tree
Validate the TCP checksum if possible
Allow subdissector to reassemble TCP streams
Reassemble
Analyze TCP
Relative sec
Whether subdissector can request TCP streams to be reassembled
"Analyze TCP sequence numbers")
Scaling factor to use when not available from capture
Not known
Track number of bytes in flight
Calculate conversation timestamps
Try heuristic sub-dissectors first
Ignore TCP Timestamps in summary
Do not call subdissectors for error packets
TCP Experimental Options with a Magic Number
Display process information via IPFIX
TCP UDP port
0
OK
Cancel
Help
ftp-clientside101.pcapng
Packets: 5859 · Displayed: 5859 (100.0%)
Profile: wireshark101

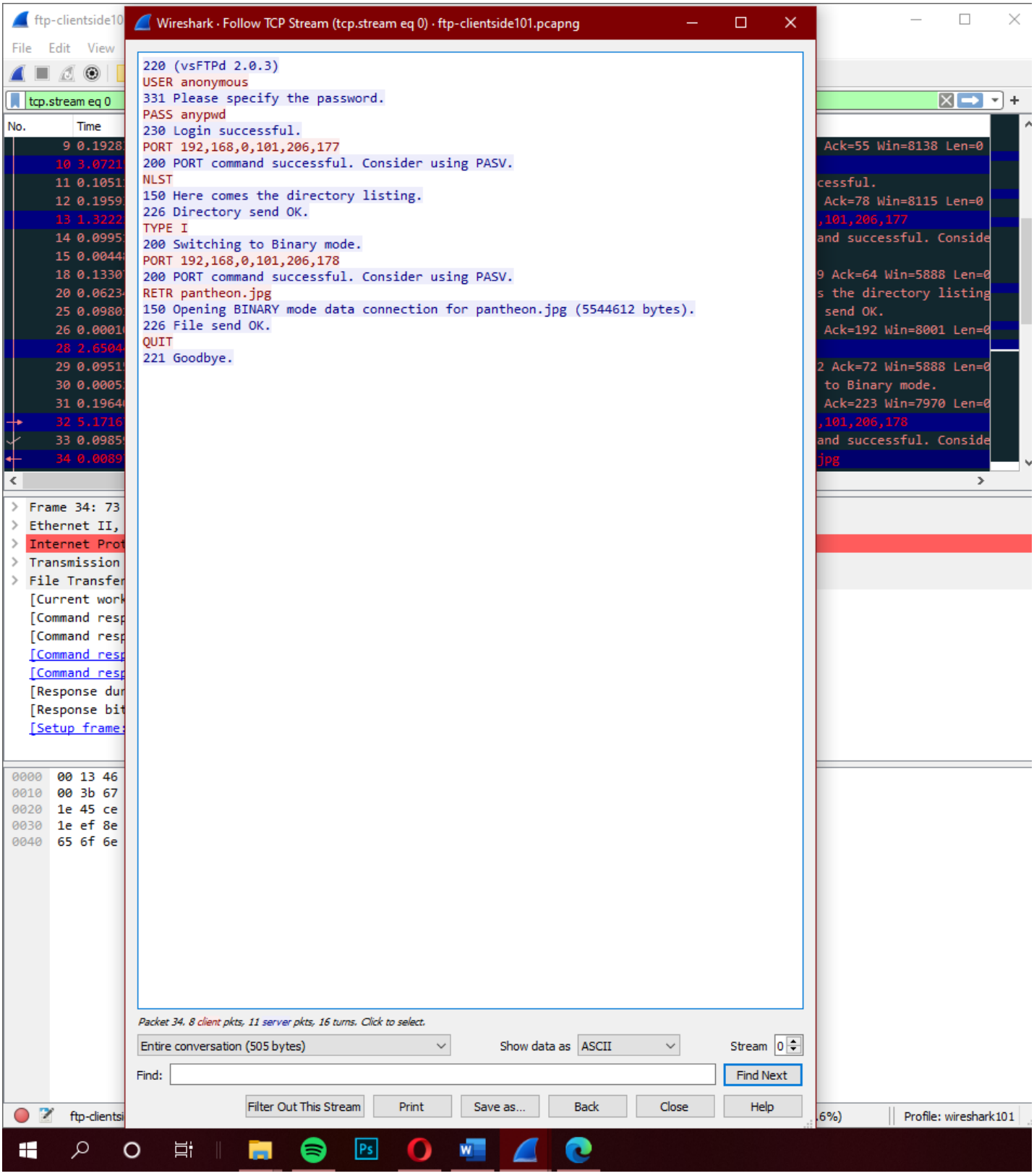
Paso 2:

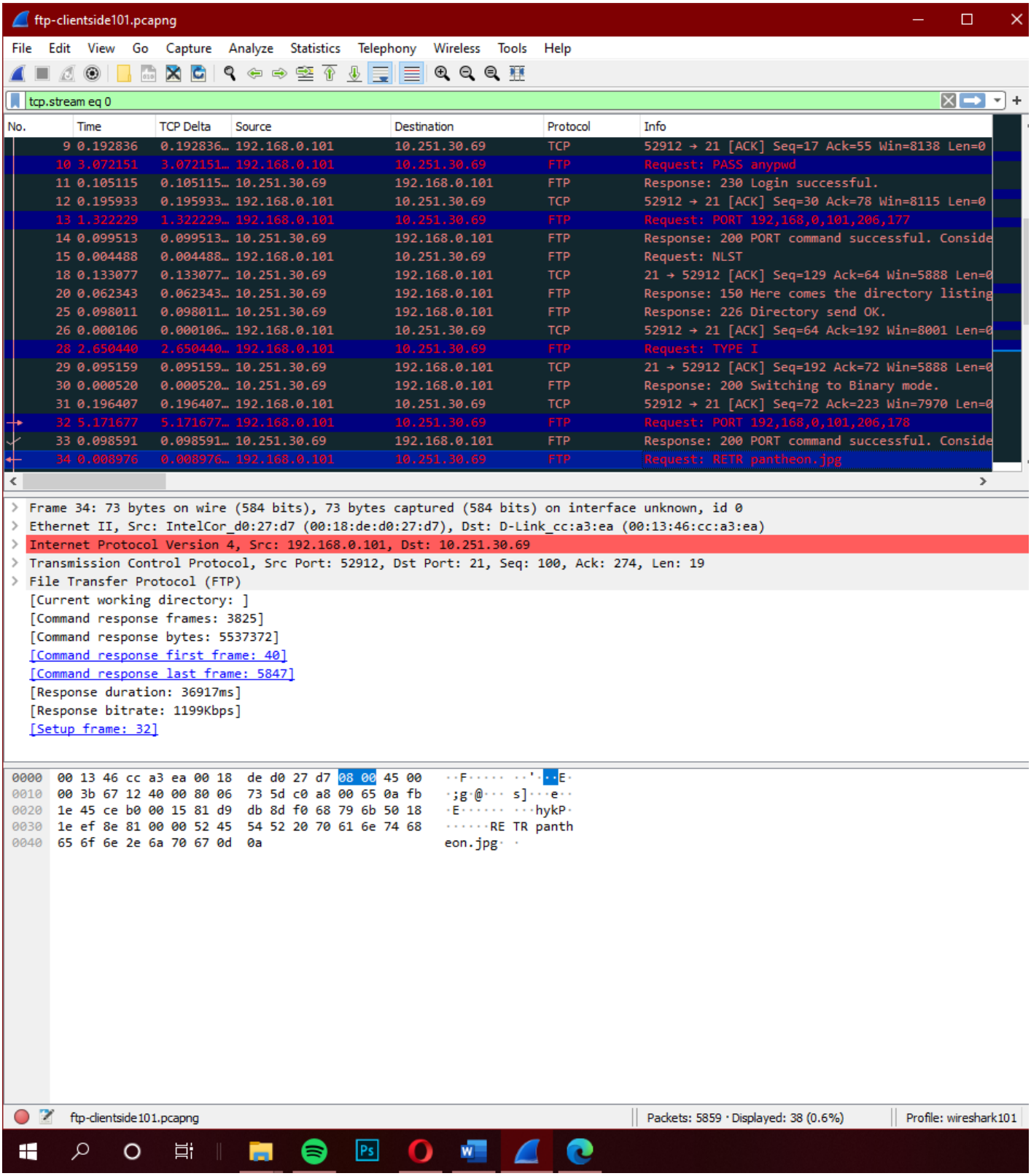

ftp-clientside101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time TCP Delta Source Destination Protocol Info
1 0.000000 0.000000… 192.168.0.101 10.251.30.69 TCP 52912 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
2 0.095003 0.095003… 10.251.30.69 192.168.0.101 TCP 21 → 52912 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len
3 0.000121 0.000121… 192.168.0.101 10.251.30.69 TCP 52912 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
4 0.101150 0.101150… 10.251.30.69 192.168.0.101 FTP Response: 220 (vsFTPd 2.0.3)
5 0.194645 0.194645… 192.168.0.101 10.251.30.69 TCP 52912 → 21 [ACK] Seq=1 Ack=21 Win=8172 Len=0
6 3.695004 3.695004… 192.168.0.101 10.251.30.69 FTP Request: USER anonymous
7 0.095841 0.095841… 10.251.30.69 192.168.0.101 TCP 21 → 52912 [ACK] Seq=21 Ack=17 Win=5888 Len=0
8 0.001838 0.001838… 10.251.30.69 192.168.0.101 FTP Response: 331 Please specify the password.
9 0.192836 0.192836… 192.168.0.101 10.251.30.69 TCP 52912 → 21 [ACK] Seq=17 Ack=55 Win=8138 Len=0
10 3.072151 3.072151… 192.168.0.101 10.251.30.69 FTP Request: PASS anypwd
11 0.105115 0.105115… 10.251.30.69 192.168.0.101 FTP Response: 230 Login successful.
12 0.195933 0.195933… 192.168.0.101 10.251.30.69 TCP 52912 → 21 [ACK] Seq=30 Ack=78 Win=8115 Len=0
13 1.322229 1.322229… 192.168.0.101 10.251.30.69 FTP Request: PORT 192,168,0,101,206,177
14 0.099513 0.099513… 10.251.30.69 192.168.0.101 FTP Response: 200 PORT command successful. Conside
15 0.004488 0.004488… 192.168.0.101 10.251.30.69 FTP Request: NLST
16 0.094934 0.000000… 10.251.30.69 192.168.0.101 TCP 20 → 52913 [SYN] Seq=0 Win=5840 Len=0 MSS=1460
17 0.000175 0.000175… 192.168.0.101 10.251.30.69 TCP 52913 → 20 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len
18 0.037968 0.133077… 10.251.30.69 192.168.0.101 TCP 21 → 52912 [ACK] Seq=129 Ack=64 Win=5888 Len=0
Frame 6: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface unknown, id 0
Ethernet II, Src: IntelCor_d0:27:d7 (00:18:de:d0:27:d7), Dst: D-Link_cc:a3:ea (00:13:46:cc:a3:ea)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 10.251.30.69
Transmission Control Protocol, Src Port: 52912, Dst Port: 21, Seq: 1, Ack: 21, Len: 16
File Transfer Protocol (FTP)
[Current working directory:]
0000 00 13 46 cc a3 ea 00 18 de d0 27 d7 08 00 45 00
0010 00 38 67 04 40 00 80 06 73 6e c0 a8 00 65 0a fb
0020 1e 45 ce b0 00 15 81 d9 db 2a f0 68 78 6e 50 18
0030 1f ec 53 05 00 00 55 53 45 52 20 61 6e 6f 6e 79
0040 6d 6f 75 73 0d 0a
mous
ftp-clientside101.pcapng
Packets: 5859 · Displayed: 5859 (100.0%)
Profile: wireshark101

Paso 3:

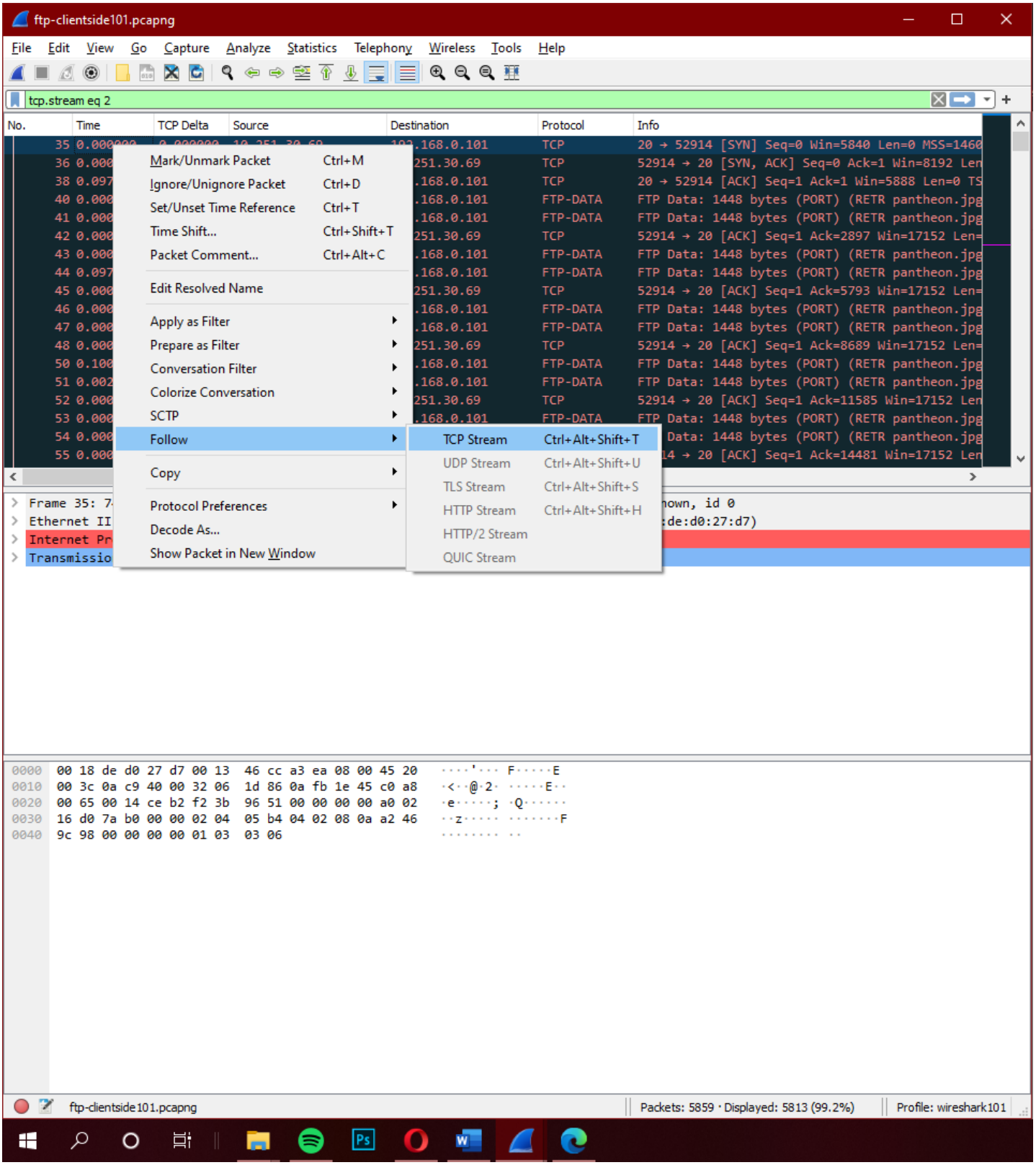

ftp-clientside101.pcapng
File Edit View
tcp.stream eq 0
No. Time
Wireshark · Follow TCP Stream (tcp.stream eq 0) · ftp-clientside101.pcapng
220 (vsFTPd 2.0.3)
USER anonymous
331 Please specify the password.
PASS anypwd
230 Login successful.
PORT 192,168,0,101,206,177
200 PORT command successful. Consider using PASV.
NLST
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 192,168,0,101,206,178
200 PORT command successful. Consider using PASV.
RETR pantheon.jpg
150 Opening BINARY mode data connection for pantheon.jpg (5544612 bytes).
226 File send OK.
QUIT
221 Goodbye.
8 client pkts, 11 server pkts, 16 turns.
Entire conversation (505 bytes)
Show data as ASCII
Stream 0
Find:
Find Next
Profile: wireshark101

Paso 4:

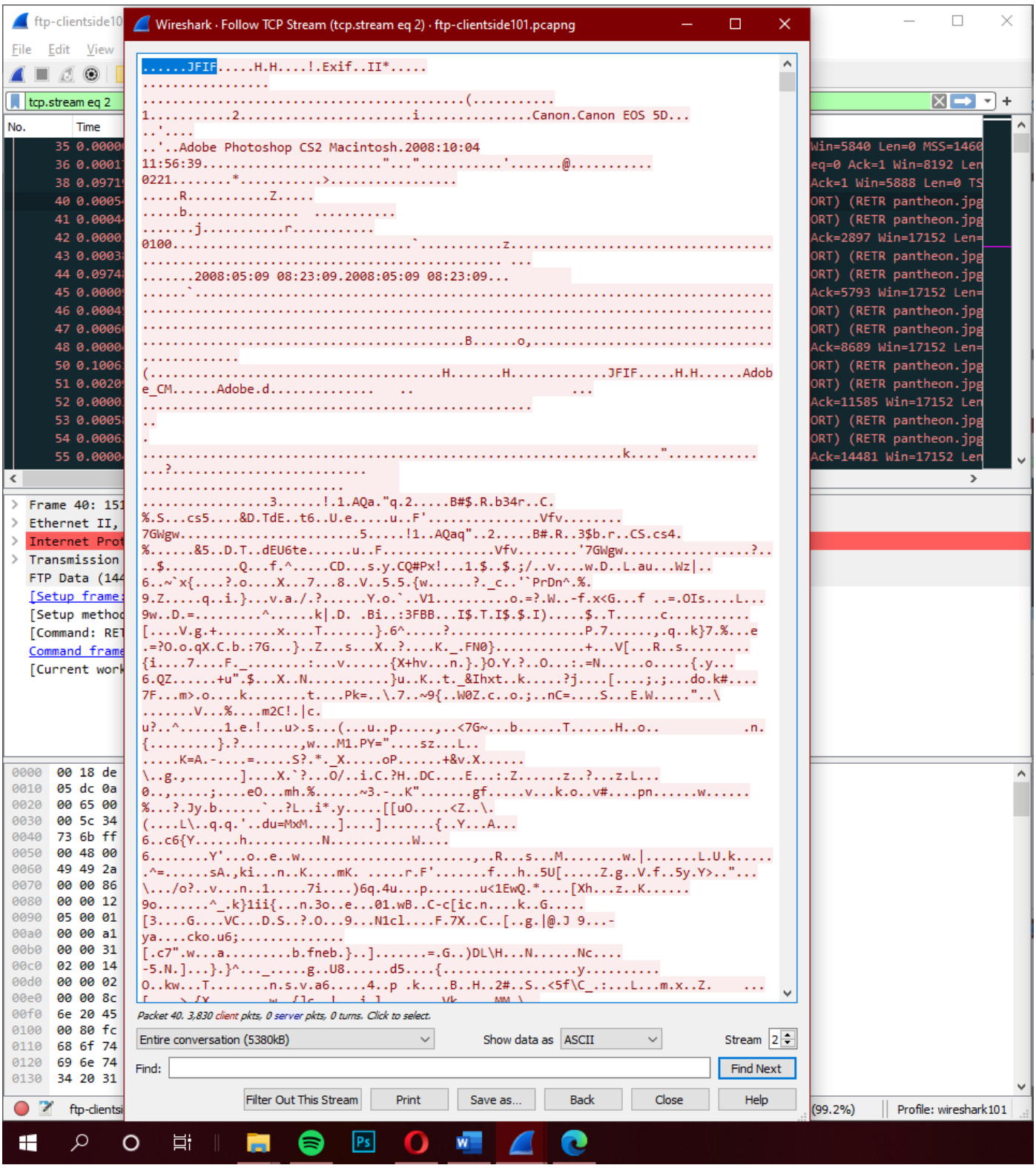

Wireshark · Follow TCP Stream (tcp.stream eq 0) · ftp-clientside101.pcapng
220 (vsFTPd 2.0.3)
USER anonymous
331 Please specify the password.
PASS anypwd
230 Login successful.
PORT 192,168,0,101,206,177
200 PORT command successful. Consider using PASV.
NLST
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 192,168,0,101,206,178
200 PORT command successful. Consider using PASV.
RETR pantheon.jpg
150 Opening BINARY mode data connection for pantheon.jpg (5544612 bytes).
226 File send OK.
QUIT
221 Goodbye.
Packet 34. 8 client pkts, 11 server pkts, 16 turns. Click to select.
Entire conversation (505 bytes)
Show data as ASCII
Stream 0
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help


ftp-clientside101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 0
No. Time TCP Delta Source Destination Protocol Info
9 0.192836 0.192836… 192.168.0.101 10.251.30.69 TCP 52912 → 21 [ACK] Seq=17 Ack=55 Win=8138 Len=0
10 3.072151 3.072151… 192.168.0.101 10.251.30.69 FTP Request: PASS anypwd
11 0.105115 0.105115… 10.251.30.69 192.168.0.101 FTP Response: 230 Login successful.
12 0.195933 0.195933… 192.168.0.101 10.251.30.69 TCP 52912 → 21 [ACK] Seq=30 Ack=78 Win=8115 Len=0
13 1.322229 1.322229… 192.168.0.101 10.251.30.69 FTP Request: PORT 192,168,0,101,206,177
14 0.099513 0.099513… 10.251.30.69 192.168.0.101 FTP Response: 200 PORT command successful. Conside
15 0.004488 0.004488… 192.168.0.101 10.251.30.69 FTP Request: NLST
18 0.133077 0.133077… 10.251.30.69 192.168.0.101 TCP 21 → 52912 [ACK] Seq=129 Ack=64 Win=5888 Len=0
20 0.062343 0.062343… 10.251.30.69 192.168.0.101 FTP Response: 150 Here comes the directory listing
25 0.098011 0.098011… 10.251.30.69 192.168.0.101 FTP Response: 226 Directory send OK.
26 0.000106 0.000106… 192.168.0.101 10.251.30.69 TCP 52912 → 21 [ACK] Seq=64 Ack=192 Win=8001 Len=0
28 2.650440 2.650440… 192.168.0.101 10.251.30.69 FTP Request: TYPE I
29 0.095159 0.095159… 10.251.30.69 192.168.0.101 TCP 21 → 52912 [ACK] Seq=192 Ack=72 Win=5888 Len=0
30 0.000520 0.000520… 10.251.30.69 192.168.0.101 FTP Response: 200 Switching to Binary mode.
31 0.196407 0.196407… 192.168.0.101 10.251.30.69 TCP 52912 → 21 [ACK] Seq=72 Ack=223 Win=7970 Len=0
32 5.171677 5.171677… 192.168.0.101 10.251.30.69 FTP Request: PORT 192,168,0,101,206,178
33 0.098591 0.098591… 10.251.30.69 192.168.0.101 FTP Response: 200 PORT command successful. Conside
34 0.008976 0.008976… 192.168.0.101 10.251.30.69 FTP Request: RETR pantheon.jpg
Frame 34: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface unknown, id 0
Ethernet II, Src: IntelCor_d0:27:d7 (00:18:de:d0:27:d7), Dst: D-Link_cc:a3:ea (00:13:46:cc:a3:ea)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 10.251.30.69
Transmission Control Protocol, Src Port: 52912, Dst Port: 21, Seq: 100, Ack: 274, Len: 19
File Transfer Protocol (FTP)
[Current working directory:]
[Command response frames: 3825]
[Command response bytes: 5537372]
[Command response first frame: 40]
[Command response last frame: 5847]
[Response duration: 36917ms]
[Response bitrate: 1199Kbps]
[Setup frame: 32]
0000 00 13 46 cc a3 ea 00 18 de d0 27 d7 08 00 45 00 ··F····· ··'···E·
0010 00 3b 67 12 40 00 80 06 73 5d c0 a8 00 65 0a fb ·;g·@··· s]···e··
0020 1e 45 ce b0 00 15 81 d9 db 8d f0 68 79 6b 50 18 ·E····· ···hykP·
0030 1e ef 8e 81 00 00 52 45 54 52 20 70 61 6e 74 68 ·····RE TR panth
0040 65 6f 6e 2e 6a 70 67 0d 0a eon.jpg· ·
ftp-clientside101.pcapng
Packets: 5859 · Displayed: 38 (0.6%)
Profile: wireshark101

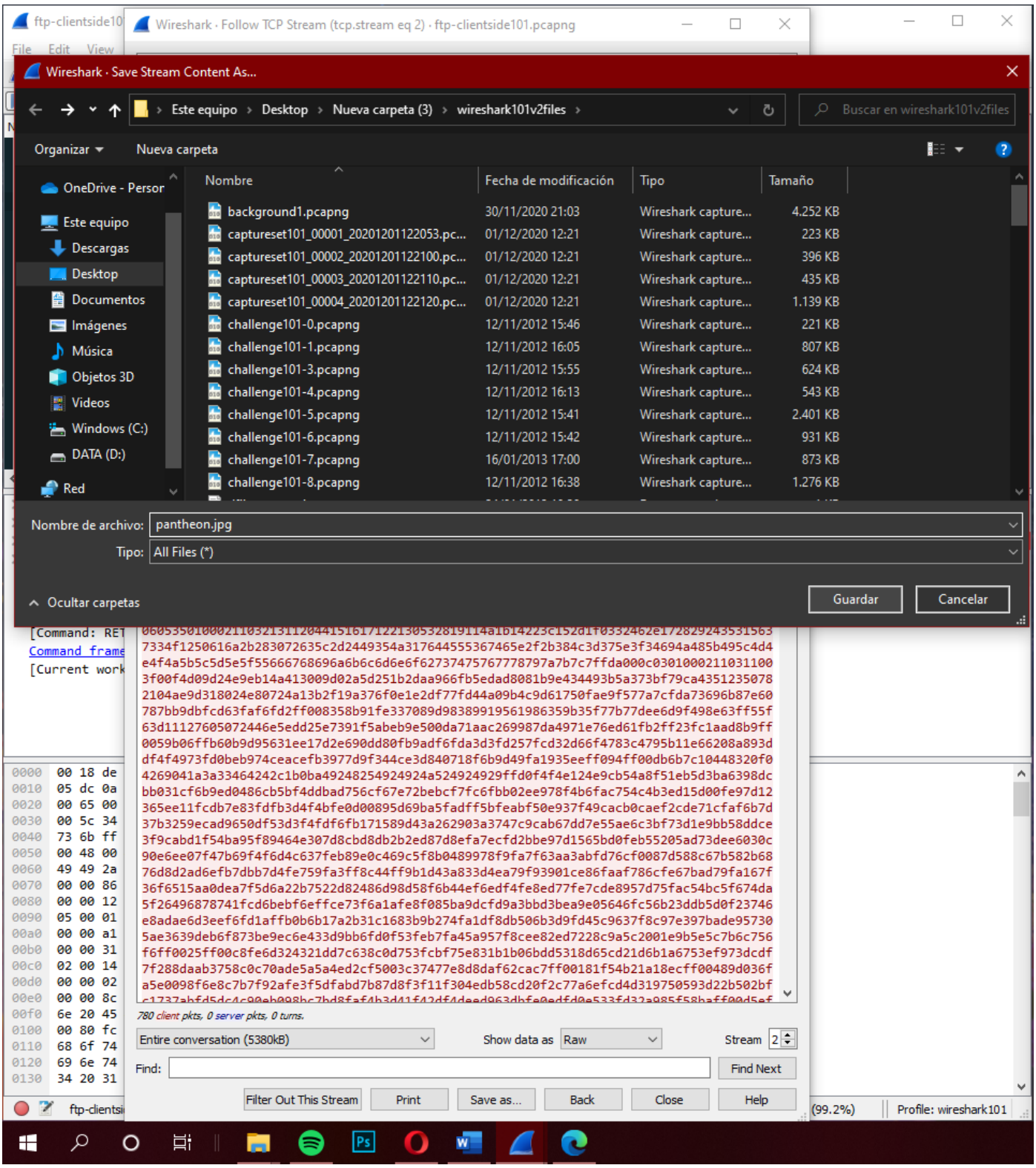
Paso 5:


ftp-clientside101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 2
No. Time TCP Delta Source Destination Protocol Info
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 35:
Ethernet II
Internet Pr
Transmissio
0000 00 18 de d0 27 d7 00 13 46 cc a3 ea 08 00 45 20
0010 00 3c 0a c9 40 00 32 06 1d 86 0a fb 1e 45 c0 a8
0020 00 65 00 14 ce b2 f2 3b 96 51 00 00 00 00 a0 02
0030 16 d0 7a b0 00 00 02 04 05 b4 04 02 08 0a a2 46
0040 9c 98 00 00 00 00 01 03 03 06
ftp-clientside101.pcapng
Packets: 5859 · Displayed: 5813 (99.2%)
Profile: wireshark101

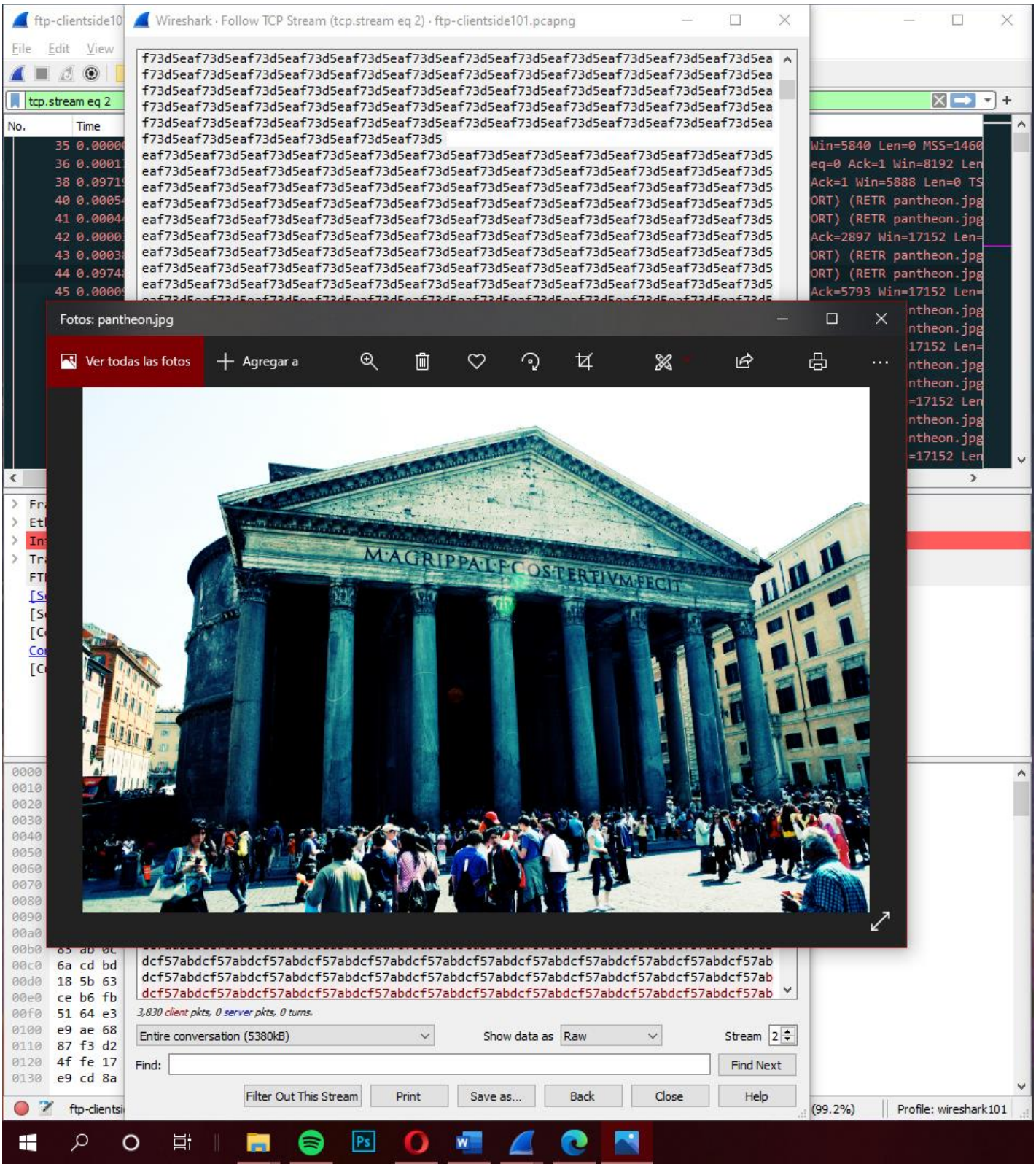
Paso 6:


Wireshark · Follow TCP Stream (tcp.stream eq 2) · ftp-clientside101.pcapng
Packet 40. 3,830 client pkts, 0 server pkts, 0 turns. Click to select.
Entire conversation (5380kB)
Show data as ASCII
Stream 2
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

Paso 7:


Wireshark · Follow TCP Stream (tcp.stream eq 2) · ftp-clientside101.pcapng
Wireshark · Save Stream Content As...
Este equipo › Desktop › Nueva carpeta (3) › wireshark101v2files ›
Buscar en wireshark101v2files
Organizar
Nueva carpeta
OneDrive - Persor
Este equipo
Descargas
Desktop
Documentos
Imágenes
Música
Objetos 3D
Videos
Windows (C:)
DATA (D:)
Red
Nombre
Fecha de modificación
Tipo
Tamaño
background1.pcapng 30/11/2020 21:03 Wireshark capture... 4.252 KB
captureset101_00001_20201201122053.pc... 01/12/2020 12:21 Wireshark capture... 223 KB
captureset101_00002_20201201122100.pc... 01/12/2020 12:21 Wireshark capture... 396 KB
captureset101_00003_20201201122110.pc... 01/12/2020 12:21 Wireshark capture... 435 KB
captureset101_00004_20201201122120.pc... 01/12/2020 12:21 Wireshark capture... 1.139 KB
challenge101-0.pcapng 12/11/2012 15:46 Wireshark capture... 221 KB
challenge101-1.pcapng 12/11/2012 16:05 Wireshark capture... 807 KB
challenge101-3.pcapng 12/11/2012 15:55 Wireshark capture... 624 KB
challenge101-4.pcapng 12/11/2012 16:13 Wireshark capture... 543 KB
challenge101-5.pcapng 12/11/2012 15:41 Wireshark capture... 2.401 KB
challenge101-6.pcapng 12/11/2012 15:42 Wireshark capture... 931 KB
challenge101-7.pcapng 16/01/2013 17:00 Wireshark capture... 873 KB
challenge101-8.pcapng 12/11/2012 16:38 Wireshark capture... 1.276 KB
Nombre de archivo: pantheon.jpg
Tipo: All Files (*)
Ocultar carpetas
Guardar
Cancelar
780 client pkts, 0 server pkts, 0 turns.
Entire conversation (5380kB)
Show data as Raw
Stream 2
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Profile: wireshark101

Paso 8:


Wireshark · Follow TCP Stream (tcp.stream eq 2) · ftp-clientside101.pcapng
Fotos: pantheon.jpg
Ver todas las fotos
Agregar a
M·AGRIPPA·L·F·COS·TERTIVM·FECIT
Entire conversation (5380kB)
Show data as
Raw
Stream
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help