

INSTITUTO TECNOLÓGICO 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:

The image shows a Windows desktop with the Wireshark application open. A dialog box titled "Wireshark - Open Capture File" is displayed, showing a list of files in the "wireshark101v2files" directory. The file "ftp-clientside101.pcapng" is selected. The dialog box includes a search bar, a list of files with columns for Name, Date modified, Type, and Size, and buttons for "Abrir", "Cancelar", and "Ayuda".

Nombre	Fecha de modificación	Tipo	Tamaño
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 18:55	Wireshark capture...	1.906 KB
ftp-download101.pca	03/11/2012 18:55	Wireshark capture...	24.344 KB
ftp-passwords101.pca	03/11/2012 18:55	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
hostinformation.csv	02/12/2020 22:50	Archivo de valores...	10 KB
http-au101b.pcapng	23/10/2012 17:09	Wireshark capture...	747 KB
http-browse101.pcapng	20/10/2012 17:50	Wireshark capture...	1.719 KB
http-browse101b.pcapng	08/11/2012 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
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

Nombre de archivo: ftp-clientside101.pcapng
Tipo de archivo: All Files
Read filter:
Format: Wireshark/... - pcapng
Size: 5998KB, 5859 data records
Start / elapsed: 2008-10-10 20:25:12 / 00:01:28

0000 00 13 46 cc a3 ea 00 18 de d0 27 d7 08 00 45 00 ..F....E.
0010 00 34 67 01 40 00 80 06 73 75 c0 a8 00 65 0a fb .4g.@..su.e.
0020 1e 45 ce b0 00 15 81 d9 db 29 00 00 00 00 80 02 .E.....)
0030 20 00 03 02 00 00 02 04 05 b4 01 03 03 00 01 01
0040 04 02 ..

ftp-clientside101.pcapng | Packets: 5859 · Displayed: 5859 (100.0%) | Profile: wireshark101

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=0
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	TCP	21 → 52912 [ACK] Seq=55 Ack=21 Win=5888 Len=0
12	0.195933	0.195933...	192.168.0.101	10.251.30.69	TCP	52912 → 21 [ACK] Seq=55 Ack=55 Win=8192 Len=0
13	1.322229	1.322229...	192.168.0.101	10.251.30.69	TCP	52912 → 21 [ACK] Seq=55 Ack=55 Win=8192 Len=0
14	0.099513	0.099513...	10.251.30.69	192.168.0.101	TCP	21 → 52912 [ACK] Seq=55 Ack=55 Win=8192 Len=0
15	0.004488	0.004488...	192.168.0.101	10.251.30.69	TCP	52912 → 21 [ACK] Seq=55 Ack=55 Win=8192 Len=0
16	0.094934	0.094934...	10.251.30.69	192.168.0.101	TCP	21 → 52912 [ACK] Seq=55 Ack=55 Win=8192 Len=0
17	0.000175	0.000175...	192.168.0.101	10.251.30.69	TCP	52912 → 21 [ACK] Seq=55 Ack=55 Win=8192 Len=0
18	0.037968	0.037968...	10.251.30.69	192.168.0.101	TCP	21 → 52912 [ACK] Seq=55 Ack=55 Win=8192 Len=0

Frame 1: 66 bytes on wire (528 bits) captured (0.000000 seconds) on interface 0
Ethernet II, Src: Realtek-80-00-00-00-00-00, Dst: Realtek-80-00-00-00-00-00
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 10.251.30.69
Transmission Control Protocol, Seq: 0, Win: 0, Len: 0

0000 00 13 46 cc a0 00 00 00 00 00 00 00 00 00 00 00
0010 00 34 67 01 40 00 00 00 00 00 00 00 00 00 00
0020 1e 45 ce b0 00 00 00 00 00 00 00 00 00 00 00
0030 20 00 03 02 00 00 00 00 00 00 00 00 00 00 00
0040 04 02

Wireshark - Preferences

SSDP
SSH
STANAG 5066
STANAG 5066
StarTeam
Steam IHS Di
STP
STT
STUN
SUA
SV
SYNC
SYNCHROPI
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 TCP streams (Whether subdissector can request TCP streams to be reassembled)

☒ Analyze TCP sequence numbers (Analyze TCP sequence numbers)

☒ Relative sequence numbers (Relative 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:

The image shows a Wireshark packet capture analysis of an FTP session. The main pane displays a list of 18 packets. The selected packet (No. 6) is an FTP request for the user 'anonymous'. The packet details pane shows the structure of the packet: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and File Transfer Protocol (FTP). The packet bytes pane shows the raw data in hexadecimal and ASCII.

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=0
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. Consider
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=0
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 ..F.....E..
0010 00 38 67 04 40 00 80 06 73 6e c0 a8 00 65 0a fb .8g.@...sn...e..
0020 1e 45 ce b0 00 15 81 d9 db 2a f0 68 78 6e 50 18 .E.....*..hxnP..
0030 1f ec 53 05 00 00 55 53 45 52 20 61 6e 6f 6e 79 ..S...US ER anony
0040 6d 6f 75 73 0d 0a mous..

Paso 3:

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:

The image shows a Wireshark window titled "Wireshark · Follow TCP Stream (tcp.stream eq 0) · ftp-clientside101.pcapng". The main pane displays the text of a TCP stream, which is an FTP session. The session starts with a 220 message from the server (vsFTPD 2.0.3) and a USER anonymous command from the client. This is followed by a 331 password prompt and a PASS anypwd command. The login is successful (230), and the client issues a PORT 192,168,0,101,206,177 command. The server responds with a 200 message and suggests using PASV. The client then issues an NLST command to request a directory listing. The server responds with a 150 message and the directory listing. The client issues a TYPE I command to switch to text mode, and the server responds with a 200 message. The client then issues a RETR pantheon.jpg command to retrieve a file. The server responds with a 150 message and opens a BINARY mode data connection. The client then issues a QUIT command, and the server responds with a 221 Goodbye message.

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

Profile: wireshark101

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. Consider
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. Consider
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 68RE 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:

The image shows the Wireshark network protocol analyzer interface. The main window displays a packet capture file named 'ftp-clientside101.pcapng'. The packet list pane on the left shows a list of captured packets, with packet 35 selected. A context menu is open over packet 35, and the 'Follow' option is selected, leading to a submenu where 'TCP Stream' is chosen. The packet details pane on the right shows the selected packet's structure, including the Ethernet II, Internet Protocol, and Transmission Control Protocol layers. The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	TCP Delta	Source	Destination	Protocol	Info
35	0.000000	0.000000	10.251.30.69	10.168.0.101	TCP	20 → 52914 [SYN] Seq=0 Win=5840 Len=0 MSS=1460
36	0.000000	0.000000	251.30.69	10.168.0.101	TCP	52914 → 20 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
38	0.007000	0.007000	10.168.0.101	10.168.0.101	TCP	20 → 52914 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TS=0
40	0.000000	0.000000	10.168.0.101	10.168.0.101	FTP-DATA	FTP Data: 1448 bytes (PORT) (RETR pantheon.jpg)
41	0.000000	0.000000	10.168.0.101	10.168.0.101	FTP-DATA	FTP Data: 1448 bytes (PORT) (RETR pantheon.jpg)
42	0.000000	0.000000	251.30.69	10.168.0.101	TCP	52914 → 20 [ACK] Seq=1 Ack=2897 Win=17152 Len=0
43	0.000000	0.000000	10.168.0.101	10.168.0.101	FTP-DATA	FTP Data: 1448 bytes (PORT) (RETR pantheon.jpg)
44	0.007000	0.007000	10.168.0.101	10.168.0.101	FTP-DATA	FTP Data: 1448 bytes (PORT) (RETR pantheon.jpg)
45	0.000000	0.000000	251.30.69	10.168.0.101	TCP	52914 → 20 [ACK] Seq=1 Ack=5793 Win=17152 Len=0
46	0.000000	0.000000	10.168.0.101	10.168.0.101	FTP-DATA	FTP Data: 1448 bytes (PORT) (RETR pantheon.jpg)
47	0.000000	0.000000	10.168.0.101	10.168.0.101	FTP-DATA	FTP Data: 1448 bytes (PORT) (RETR pantheon.jpg)
48	0.000000	0.000000	251.30.69	10.168.0.101	TCP	52914 → 20 [ACK] Seq=1 Ack=8689 Win=17152 Len=0
50	0.100000	0.100000	10.168.0.101	10.168.0.101	FTP-DATA	FTP Data: 1448 bytes (PORT) (RETR pantheon.jpg)
51	0.002000	0.002000	10.168.0.101	10.168.0.101	FTP-DATA	FTP Data: 1448 bytes (PORT) (RETR pantheon.jpg)
52	0.000000	0.000000	251.30.69	10.168.0.101	TCP	52914 → 20 [ACK] Seq=1 Ack=11585 Win=17152 Len=0
53	0.000000	0.000000	10.168.0.101	10.168.0.101	FTP-DATA	FTP Data: 1448 bytes (PORT) (RETR pantheon.jpg)
54	0.000000	0.000000	10.168.0.101	10.168.0.101	FTP-DATA	FTP Data: 1448 bytes (PORT) (RETR pantheon.jpg)
55	0.000000	0.000000	10.168.0.101	10.168.0.101	FTP-DATA	FTP Data: 1448 bytes (PORT) (RETR pantheon.jpg)

Frame 35: 7...
> Ethernet II
> Internet Protocol
> Transmission Control Protocol

0000 00 18 de d0 27 d7 00 13 46 cc a3 ea 08 00 45 20F.....E
0010 00 3c 0a c9 40 00 32 06 1d 86 0a fb 1e 45 c0 a8 <...@.2.....E..
0020 00 65 00 14 ce b2 f2 3b 96 51 00 00 00 00 a0 02 .e.....;..Q.....
0030 16 d0 7a b0 00 00 02 04 05 b4 04 02 08 0a a2 46 ..z.....F
0040 9c 98 00 00 00 00 01 03 03 06

ftp-clientside101.pcapng | Packets: 5859 · Displayed: 5813 (99.2%) | Profile: wireshark101

Paso 6:

The image shows a Wireshark packet capture analysis of an FTP session. The main window displays the packet list on the left, the packet details in the middle, and the packet bytes on the right. The packet list shows a sequence of packets, with packet 40 selected. The packet details pane shows the selected packet (40) and its contents, which are displayed in the packet bytes pane. The packet bytes pane shows the raw data of the selected packet, which is a file named 'pantheon.jpg'.

The packet list shows the following packets:

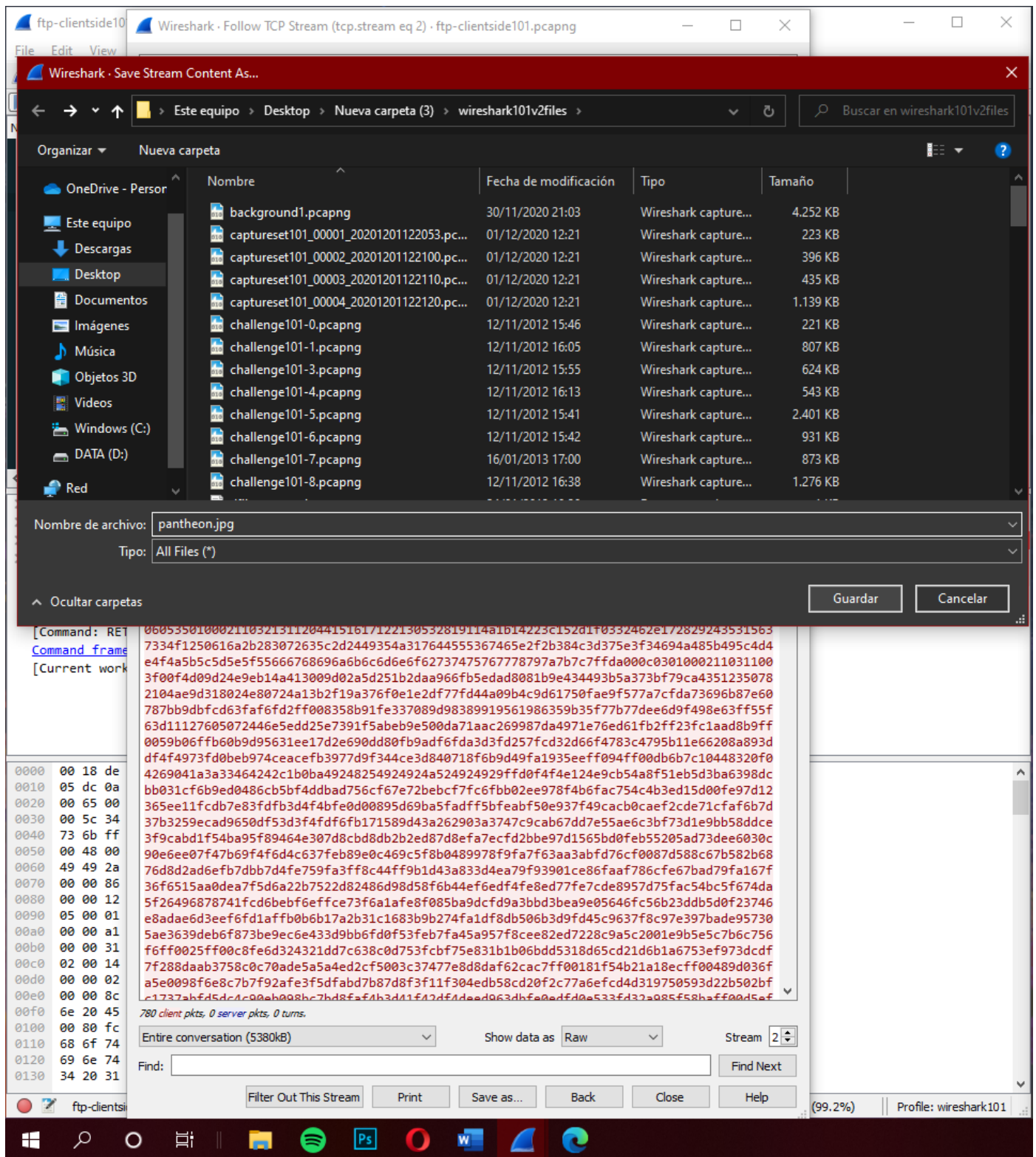
No.	Time	Source	Destination	Protocol	Length	Info
35	0.0000	192.168.1.101	192.168.1.1	FTP	144	DATA (144)
36	0.0001	192.168.1.101	192.168.1.1	FTP	144	DATA (144)
38	0.0971	192.168.1.101	192.168.1.1	FTP	144	DATA (144)
40	0.0005	192.168.1.101	192.168.1.1	FTP	144	DATA (144)
41	0.0004	192.168.1.101	192.168.1.1	FTP	144	DATA (144)
42	0.0000	192.168.1.101	192.168.1.1	FTP	144	DATA (144)
43	0.0003	192.168.1.101	192.168.1.1	FTP	144	DATA (144)
44	0.0974	192.168.1.101	192.168.1.1	FTP	144	DATA (144)
45	0.0000	192.168.1.101	192.168.1.1	FTP	144	DATA (144)
46	0.0004	192.168.1.101	192.168.1.1	FTP	144	DATA (144)
47	0.0006	192.168.1.101	192.168.1.1	FTP	144	DATA (144)
48	0.0000	192.168.1.101	192.168.1.1	FTP	144	DATA (144)
50	0.1006	192.168.1.101	192.168.1.1	FTP	144	DATA (144)
51	0.0020	192.168.1.101	192.168.1.1	FTP	144	DATA (144)
52	0.0000	192.168.1.101	192.168.1.1	FTP	144	DATA (144)
53	0.0005	192.168.1.101	192.168.1.1	FTP	144	DATA (144)
54	0.0006	192.168.1.101	192.168.1.1	FTP	144	DATA (144)
55	0.0000	192.168.1.101	192.168.1.1	FTP	144	DATA (144)

The packet details pane shows the selected packet (40) and its contents, which are displayed in the packet bytes pane. The packet bytes pane shows the raw data of the selected packet, which is a file named 'pantheon.jpg'.

The packet bytes pane shows the raw data of the selected packet, which is a file named 'pantheon.jpg'. The data is displayed in hexadecimal and ASCII format. The ASCII format shows the file name 'pantheon.jpg' and the file content.

The packet bytes pane shows the raw data of the selected packet, which is a file named 'pantheon.jpg'. The data is displayed in hexadecimal and ASCII format. The ASCII format shows the file name 'pantheon.jpg' and the file content.

Paso 7:



The screenshot shows a Windows desktop with several open applications. In the background, a Wireshark window displays a network capture on the 'tcp.stream eq 2' filter. The packet list shows a series of small, identical packets (35-45 bytes) with timestamps ranging from 0.0000 to 0.0974. The packet details pane shows a single packet with a length of 0 and a sequence number of 1. The packet bytes pane shows a series of hexadecimal values. In the foreground, a photo viewer window titled 'Fotos: pantheon.jpg' is open, displaying a photograph of the Pantheon in Rome. The photo shows the classical facade with its large columns and pediment, with a large crowd of people gathered in front. The photo viewer has a toolbar with various icons for viewing and editing the image. The taskbar at the bottom shows several open applications, including a file explorer, a web browser, and a terminal window.