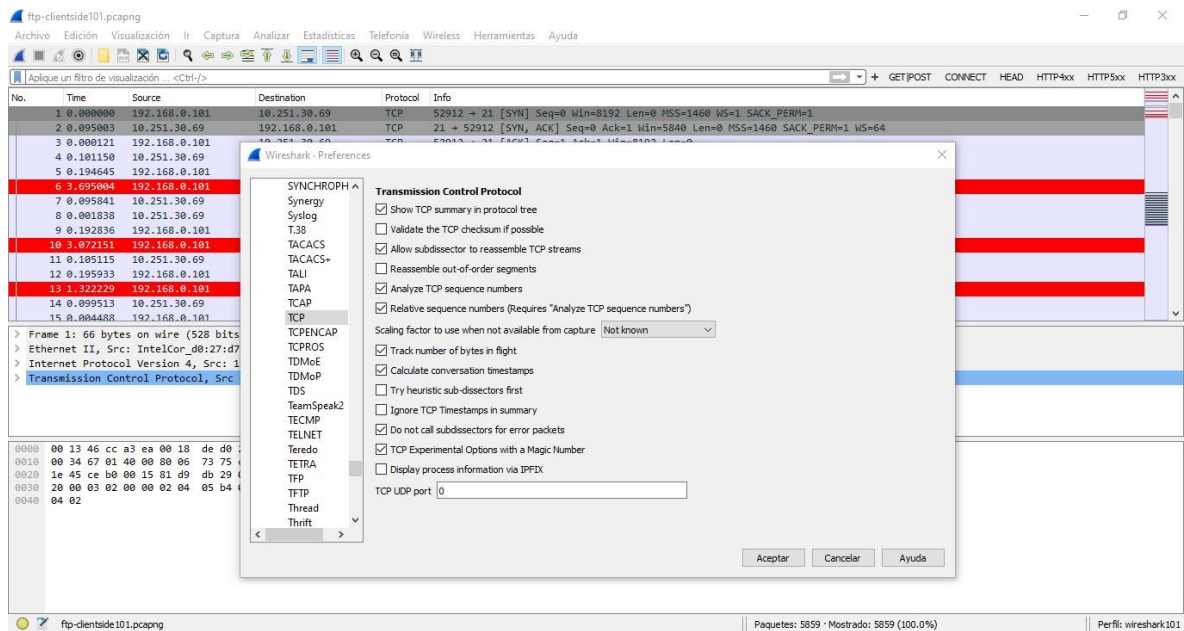
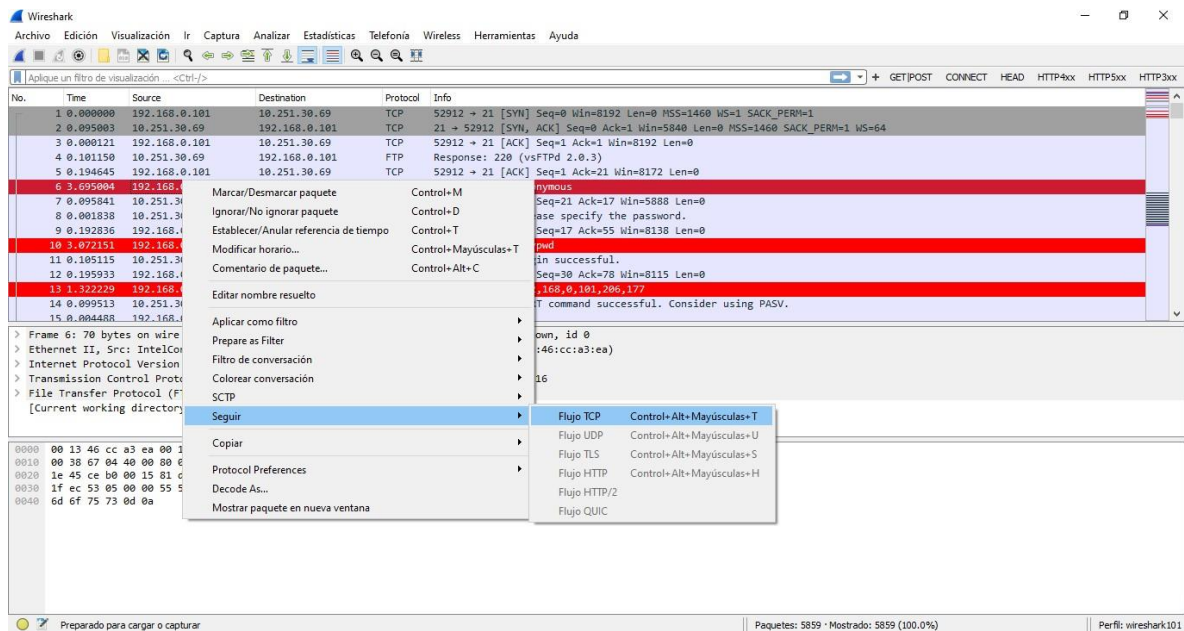


Lab38 - Extract a File from an HTTP File Transfer

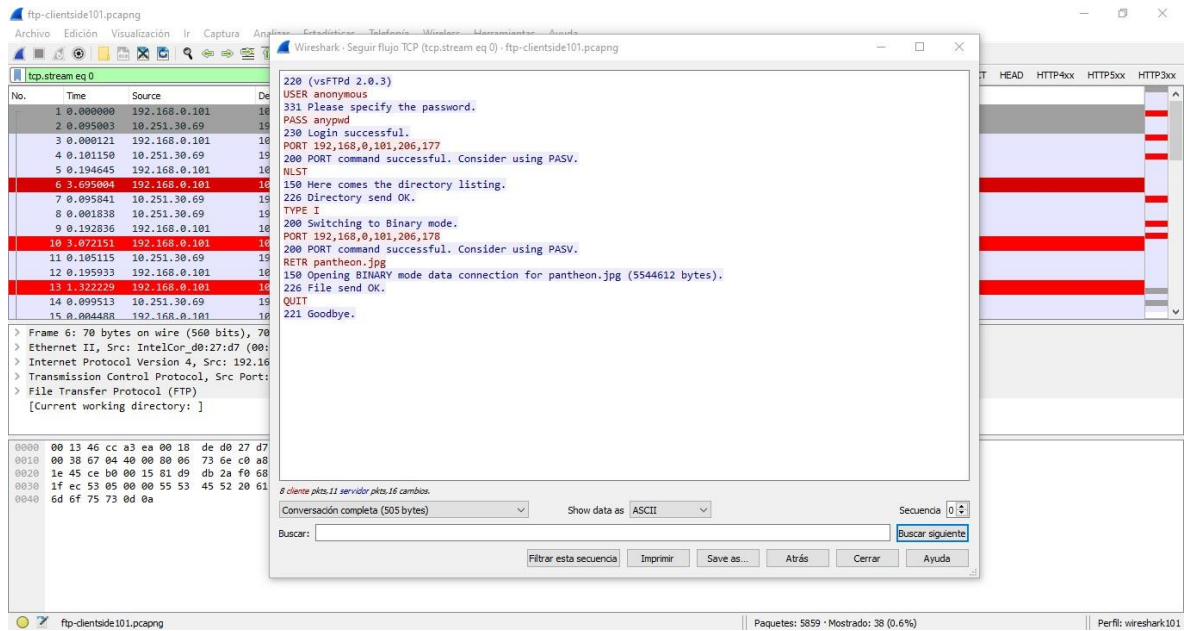
Abrimos el archivo ftp-clientside101.pcapng y verificamos que las preferencias de UTP este habilitado Allow Subdissector to reassemble TCP streams



1 y 3 En el paquete 6 click derecho Follow>TCP Streams



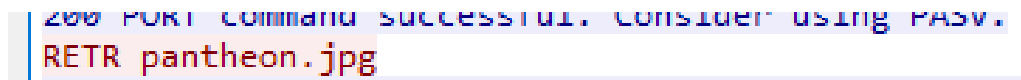
Podemos observar comandos y respuestas entre el cliente y el servidor



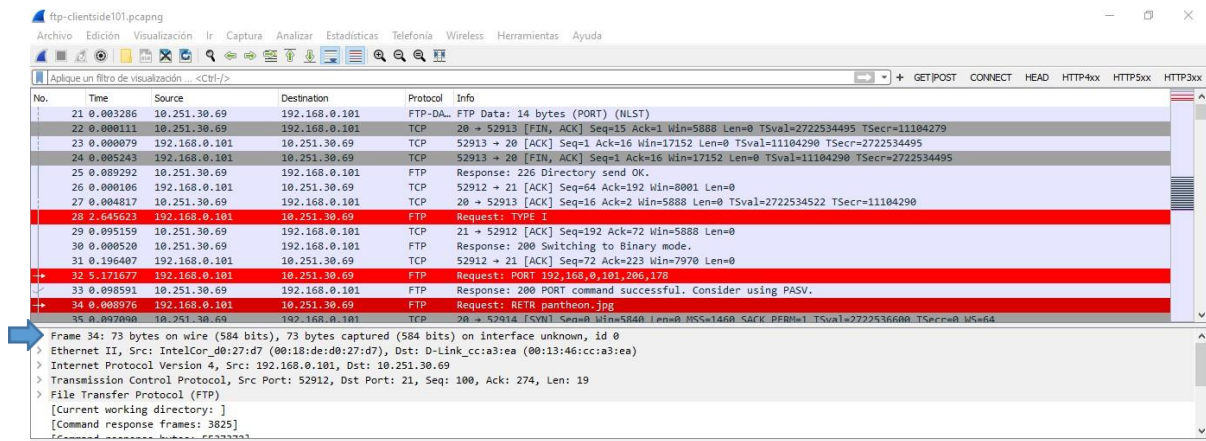
The image shows a Wireshark capture of an FTP session. The main window displays the packet list on the left, the packet details in the middle, and the packet bytes at the bottom. The packet list shows a sequence of FTP commands and responses. The packet details pane is expanded for packet 220, showing the FTP protocol structure. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.101	192.168.0.101	FTP	14	FTP Data: 14 bytes (PORT) (NLST)
2	0.095803	10.251.30.69	192.168.0.101	TCP	60	20 → 52913 [FIN, ACK] Seq=15 Ack=1 Win=5888 Len=0 TSval=2722534495 TSecr=11104279
3	0.000121	192.168.0.101	10.251.30.69	TCP	60	52913 → 20 [ACK] Seq=1 Ack=16 Win=17152 Len=0 TSval=11104290 TSecr=2722534495
4	0.101150	10.251.30.69	192.168.0.101	TCP	60	52913 → 20 [FIN, ACK] Seq=1 Ack=16 Win=17152 Len=0 TSval=11104290 TSecr=2722534495
5	0.194645	192.168.0.101	10.251.30.69	FTP	226	Response: 226 Directory send OK.
6	0.095841	10.251.30.69	192.168.0.101	TCP	60	52912 → 21 [ACK] Seq=64 Ack=192 Win=8081 Len=0 TSval=11104290 TSecr=2722534495
7	0.001838	10.251.30.69	192.168.0.101	TCP	60	52912 → 21 [ACK] Seq=64 Ack=192 Win=8081 Len=0 TSval=11104290 TSecr=2722534495
8	0.192836	192.168.0.101	10.251.30.69	FTP	20	Request: PORT 192,168,0,101,206,177
9	0.072151	192.168.0.101	10.251.30.69	FTP	20	Request: RETR pantheon.jpg
10	0.105115	10.251.30.69	192.168.0.101	TCP	60	21 → 52912 [ACK] Seq=192 Ack=72 Win=5888 Len=0 TSval=11104290 TSecr=2722534495
11	0.195933	192.168.0.101	10.251.30.69	FTP	200	Response: 200 PORT command successful. Consider using PASV.
12	0.195933	192.168.0.101	10.251.30.69	FTP	226	File send OK.
13	1.322229	192.168.0.101	10.251.30.69	FTP	221	Goodbye.
14	0.095513	10.251.30.69	192.168.0.101	TCP	60	20 → 52914 [CWIN] Seq=8 Win=5840 Len=0 HSeq=1468 SACK_PERM=1 TSval=2722534608 TSecr=815464
15	0.004488	192.168.0.101	10.251.30.69	TCP	60	52914 → 20 [ACK] Seq=1 Ack=16 Win=17152 Len=0 TSval=11104290 TSecr=2722534495

4 Le damos click en RETR pantheon.jpg



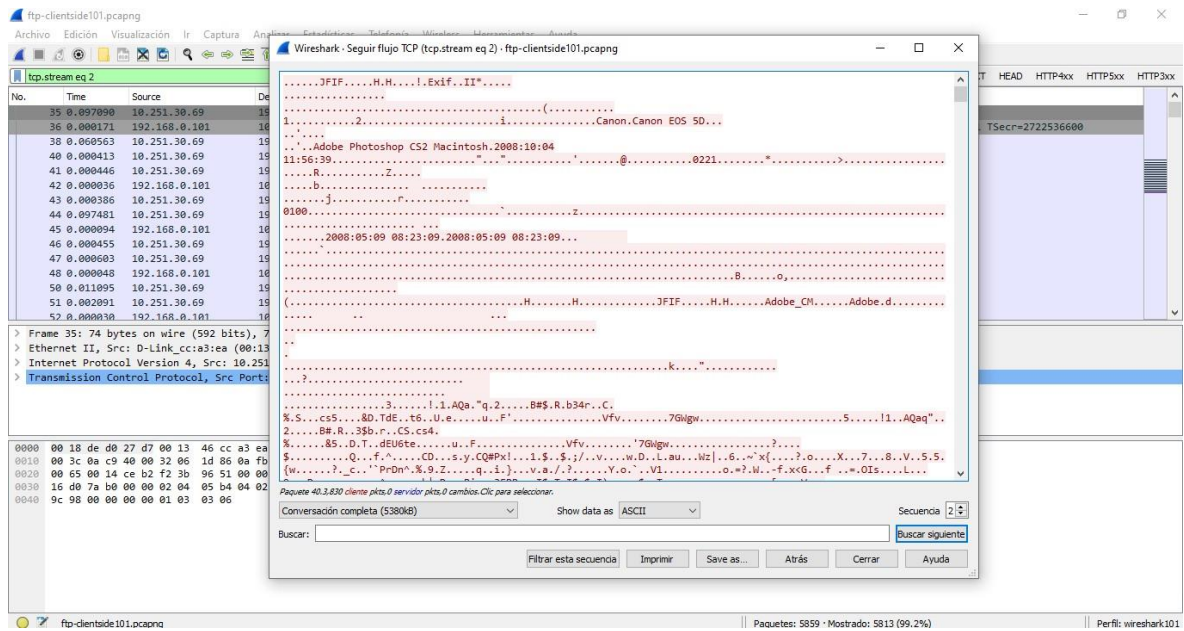
5 Eliminamos el filtro y debería de marcar el paquete 34.



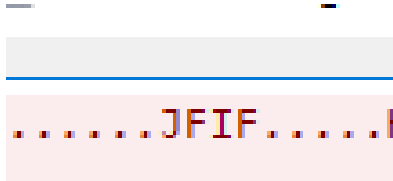
The image shows a Wireshark capture of an FTP session. The main window displays the packet list on the left, the packet details in the middle, and the packet bytes at the bottom. The packet list shows a sequence of FTP commands and responses. The packet details pane is expanded for packet 34, showing the FTP protocol structure. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
21	0.003286	10.251.30.69	192.168.0.101	FTP-DA	14	FTP Data: 14 bytes (PORT) (NLST)
22	0.000111	10.251.30.69	192.168.0.101	TCP	60	20 → 52913 [FIN, ACK] Seq=15 Ack=1 Win=5888 Len=0 TSval=2722534495 TSecr=11104279
23	0.000079	192.168.0.101	10.251.30.69	TCP	60	52913 → 20 [ACK] Seq=1 Ack=16 Win=17152 Len=0 TSval=11104290 TSecr=2722534495
24	0.005243	192.168.0.101	10.251.30.69	TCP	60	52913 → 20 [FIN, ACK] Seq=1 Ack=16 Win=17152 Len=0 TSval=11104290 TSecr=2722534495
25	0.009292	10.251.30.69	192.168.0.101	FTP	226	Response: 226 Directory send OK.
26	0.000106	192.168.0.101	10.251.30.69	TCP	60	52912 → 21 [ACK] Seq=64 Ack=192 Win=8081 Len=0 TSval=11104290 TSecr=2722534495
27	0.004817	10.251.30.69	192.168.0.101	TCP	60	20 → 52913 [ACK] Seq=16 Ack=2 Win=5888 Len=0 TSval=2722534522 TSecr=11104290
28	2.645623	192.168.0.101	10.251.30.69	FTP	20	Request: TYPE I
29	0.095159	10.251.30.69	192.168.0.101	TCP	60	21 → 52912 [ACK] Seq=192 Ack=72 Win=5888 Len=0 TSval=11104290 TSecr=2722534495
30	0.000520	10.251.30.69	192.168.0.101	FTP	200	Response: 200 Switching to Binary mode.
31	0.106407	192.168.0.101	10.251.30.69	TCP	60	52912 → 21 [ACK] Seq=72 Ack=223 Win=7970 Len=0 TSval=11104290 TSecr=2722534495
32	0.171677	192.168.0.101	10.251.30.69	FTP	200	Response: 200 PORT command successful. Consider using PASV.
33	0.098591	10.251.30.69	192.168.0.101	FTP	226	File send OK.
34	0.008276	192.168.0.101	10.251.30.69	FTP	20	Request: RETR pantheon.jpg
35	0.097098	10.251.30.69	192.168.0.101	TCP	60	20 → 52914 [CWIN] Seq=8 Win=5840 Len=0 HSeq=1468 SACK_PERM=1 TSval=2722534608 TSecr=815464

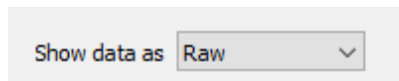
En el paquete 35 le damos click derecho Follow>TCP Streams y nos aparecerá lo siguiente



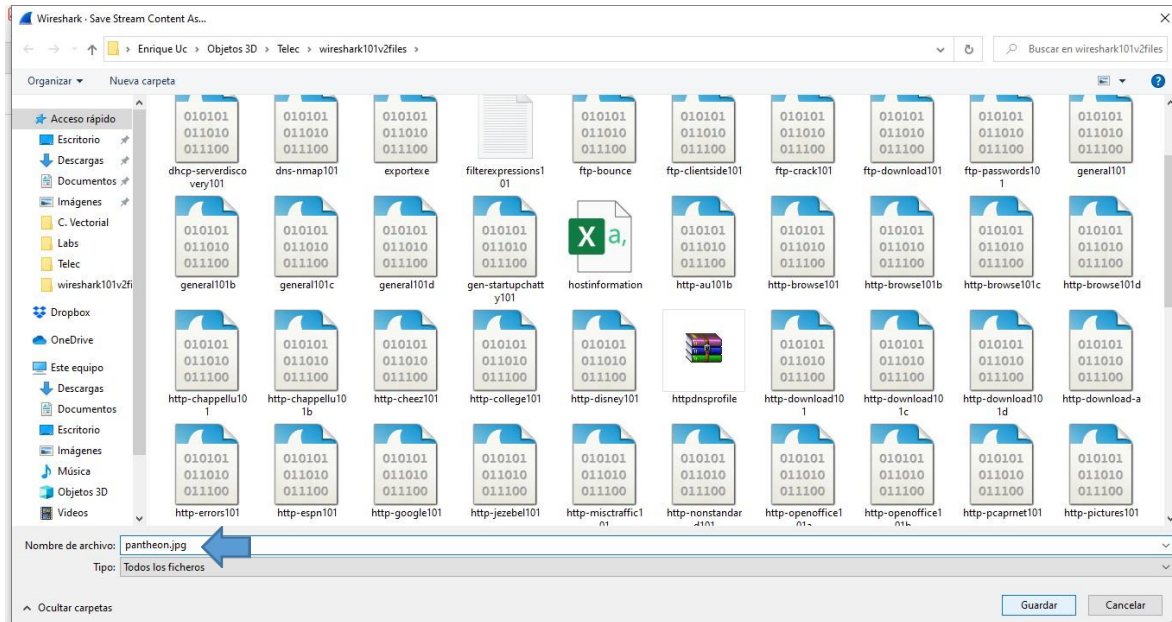
6 Podemos observar que el archivo identificado es .jpg(JFIF)



7 En showdata as ponemos Raw



Guardamos y le ponemos de nombre pantheon.jpg



Abrimos el archivo guardado y nos deberá aparecer la siguiente imagen.

