Covert Channel – Transfer

Write up by:

John Antone

835 COS

854 CPT

Covert Channel - Transfer

200

We heard that someone was transferring something important over the net. We think it might be the flag to this challenge, can you find it?

To start off with on this Pcap we look at the Protocol Hierarchy page:

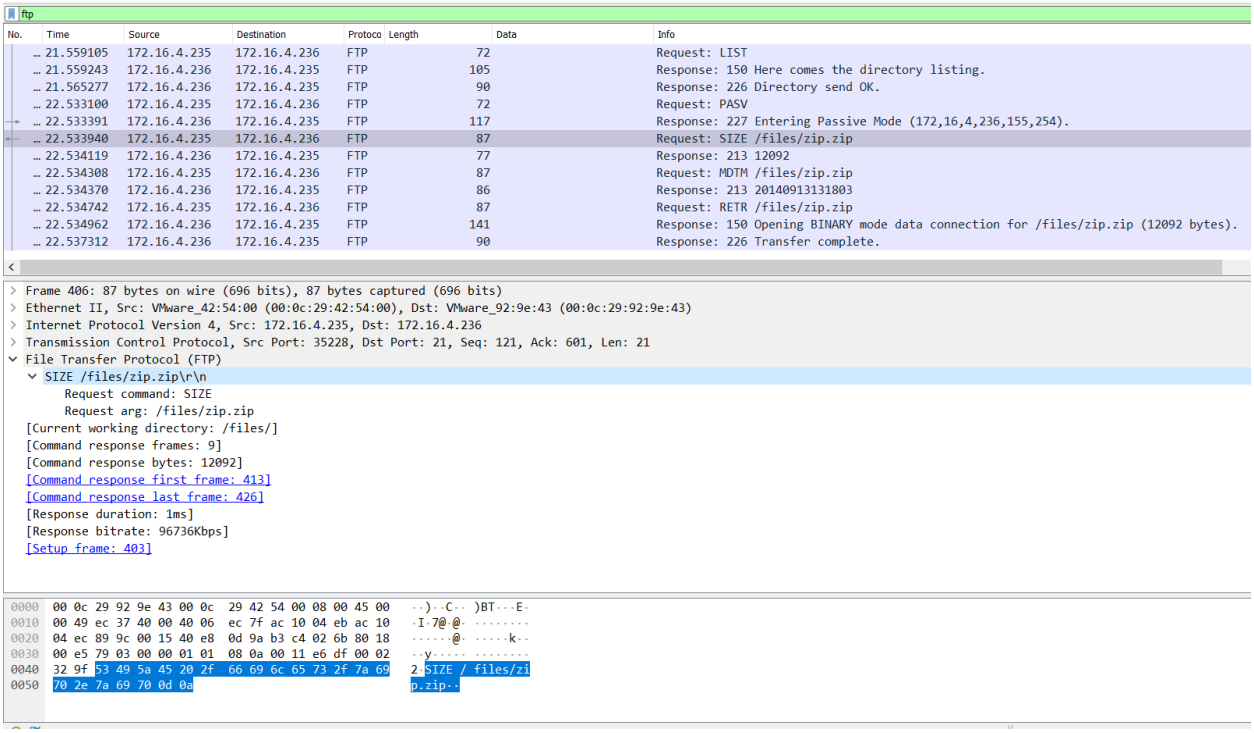
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	495	100.0	151940	38 k	0	0	0
Ethernet	100.0	495	4.6	6930	1770	0	0	0
Internet Protocol Version 4	98.4	487	6.4	9740	2488	0	0	0
User Datagram Protocol	12.9	64	0.3	512	130	0	0	0
Dynamic Host Configuration Protocol	0.4	2	0.4	600	153	2	600	153
Dropbox LAN sync Discovery Protocol	0.2	1	0.2	241	61	1	241	61
Domain Name System	12.1	60	2.6	4018	1026	60	4018	1026
Data	0.2	1	0.0	44	11	1	44	11
Transmission Control Protocol	73.3	363	82.6	125457	32 k	264	91852	23 k
Transport Layer Security	4.4	22	13.7	20888	5335	18	8657	2211
Hypertext Transfer Protocol	3.6	18	57.5	87322	22 k	10	2252	575
Line-based text data	1.6	8	148.6	225764	57 k	8	83515	21 k
FTP Data	2.2	11	8.0	12220	3121	9	0	0
Line-based text data	0.4	2	0.1	128	32	2	128	32
File Transfer Protocol (FTP)	10.5	52	0.7	1031	263	52	0	0
Internet Control Message Protocol	12.1	60	2.5	3840	980	60	3840	980
Address Resolution Protocol	1.6	8	0.2	314	80	8	314	80

We see the following protocols:

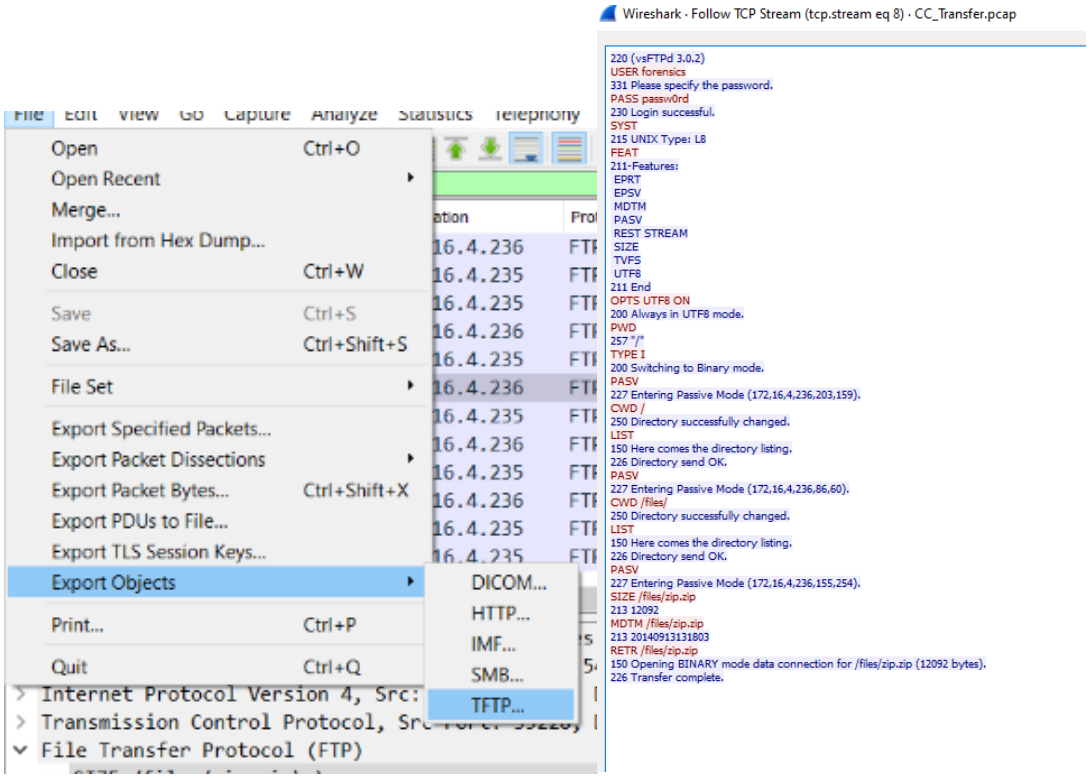
UDP: DHCP, DropBox LAN SYNC, DNS, Data

TCP: TLS, HTTP, FTP, ICMP

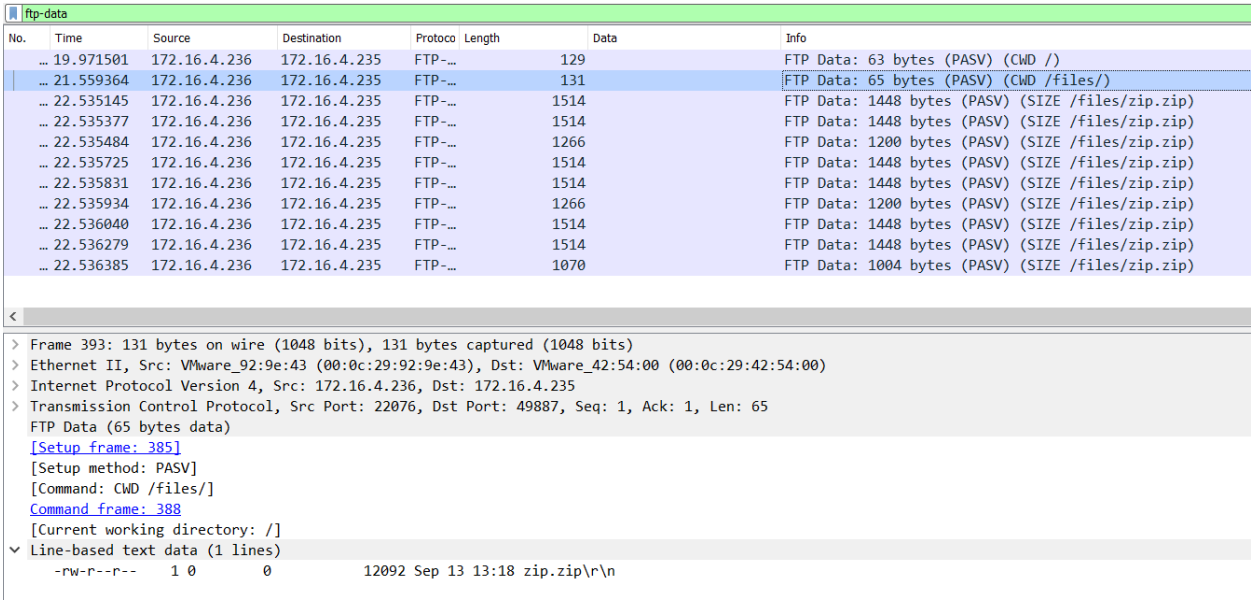
For this pcap we see FTP in plain text, so we can start off looking at that protocol first.



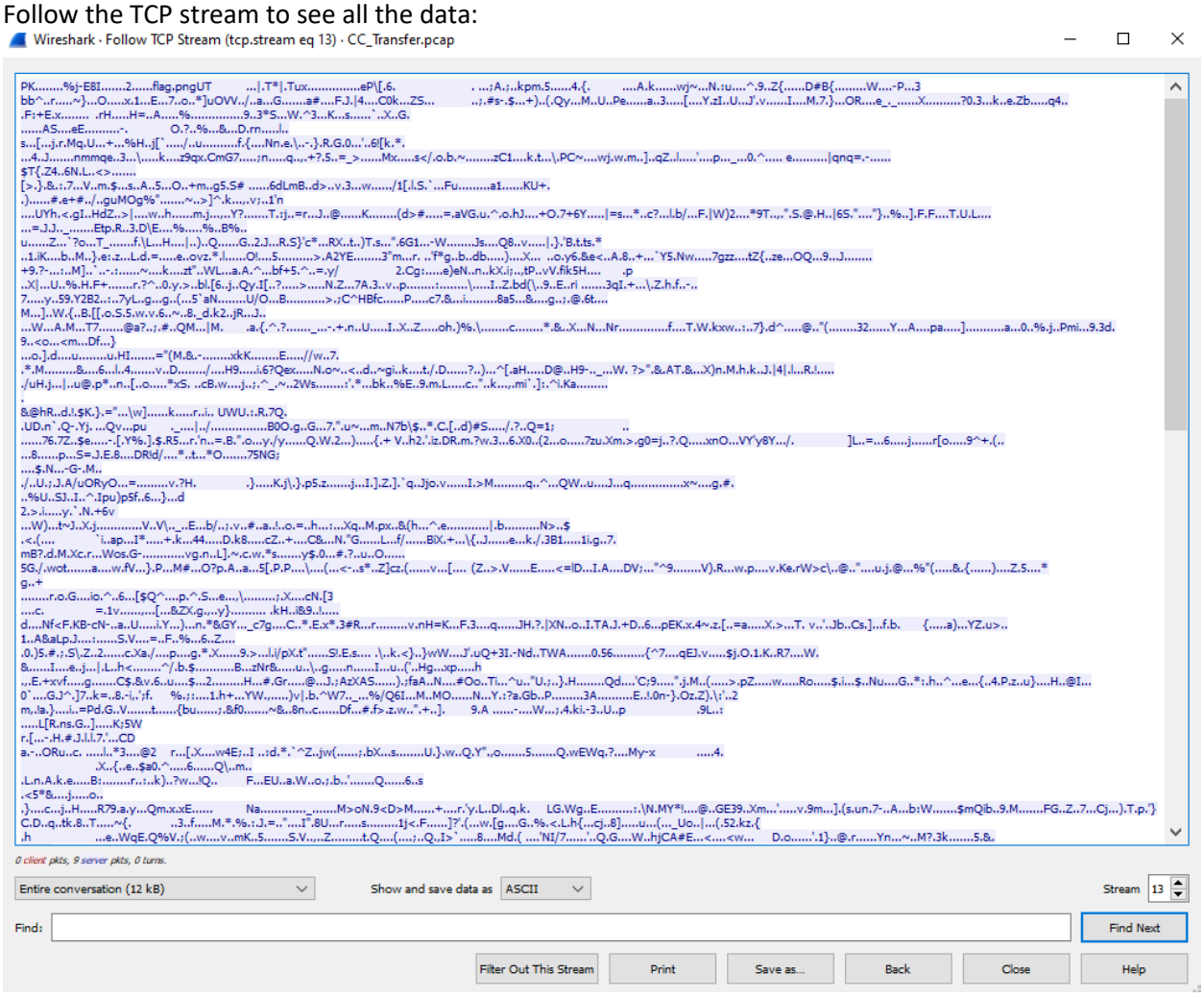
We see that there was a file downloaded named zip.zip, but when you go to find the data it seems to be missing. We cannot export the FTP data files and the TCP stream does not give us the data of the transfer either.



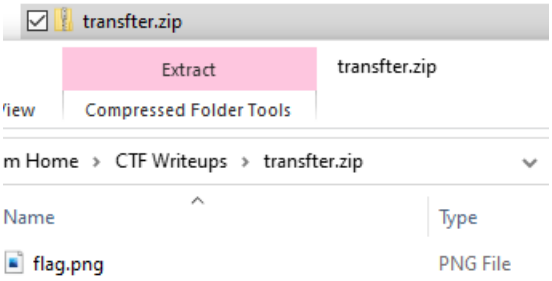
The answer is to switch the filter from ftp to ftp-data. We now see the data that was transferred.



Follow the TCP stream to see all the data:



Click on the Save as button to save the zip.zip file. We can see that the PK… is a Zip file and inside the zip file is a flag.png file.



We then open the flag.png file and we have our flag:

flag{91e02cd2b8621d0c05197f645668c5c4}