

# 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.

No.	Time	Source	Destination	Protocol	Length	Data	Info
...	21.559105	172.16.4.235	172.16.4.236	FTP	72		Request: LIST
...	21.559243	172.16.4.236	172.16.4.235	FTP	105		Response: 150 Here comes the directory listing.
...	21.565277	172.16.4.236	172.16.4.235	FTP	90		Response: 226 Directory send OK.
...	22.533100	172.16.4.235	172.16.4.236	FTP	72		Request: PASV
...	22.533391	172.16.4.236	172.16.4.235	FTP	117		Response: 227 Entering Passive Mode (172,16,4,236,155,254).
...	22.533940	172.16.4.235	172.16.4.236	FTP	87		Request: SIZE /files/zip.zip
...	22.534119	172.16.4.236	172.16.4.235	FTP	77		Response: 213 12092
...	22.534308	172.16.4.235	172.16.4.236	FTP	87		Request: MDTM /files/zip.zip
...	22.534370	172.16.4.236	172.16.4.235	FTP	86		Response: 213 20140913131803
...	22.534742	172.16.4.235	172.16.4.236	FTP	87		Request: RETR /files/zip.zip
...	22.534962	172.16.4.236	172.16.4.235	FTP	141		Response: 150 Opening BINARY mode data connection for /files/zip.zip (12092 bytes).
...	22.537312	172.16.4.236	172.16.4.235	FTP	90		Response: 226 Transfer complete.

> Frame 406: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)

> Ethernet II, Src: VMware\_42:54:00 (00:0c:29:42:54:00), Dst: VMware\_92:9e:43 (00:0c:29:92:9e:43)

> Internet Protocol Version 4, Src: 172.16.4.235, Dst: 172.16.4.236

> Transmission Control Protocol, Src Port: 35228, Dst Port: 21, Seq: 121, Ack: 601, Len: 21

> File Transfer Protocol (FTP)

> SIZE /files/zip.zip\r\n

Request command: SIZE

Request arg: /files/zip.zip

[Current working directory: /files/]

[Command response frames: 9]

[Command response bytes: 12092]

[Command response first frame: 413]

[Command response last frame: 426]

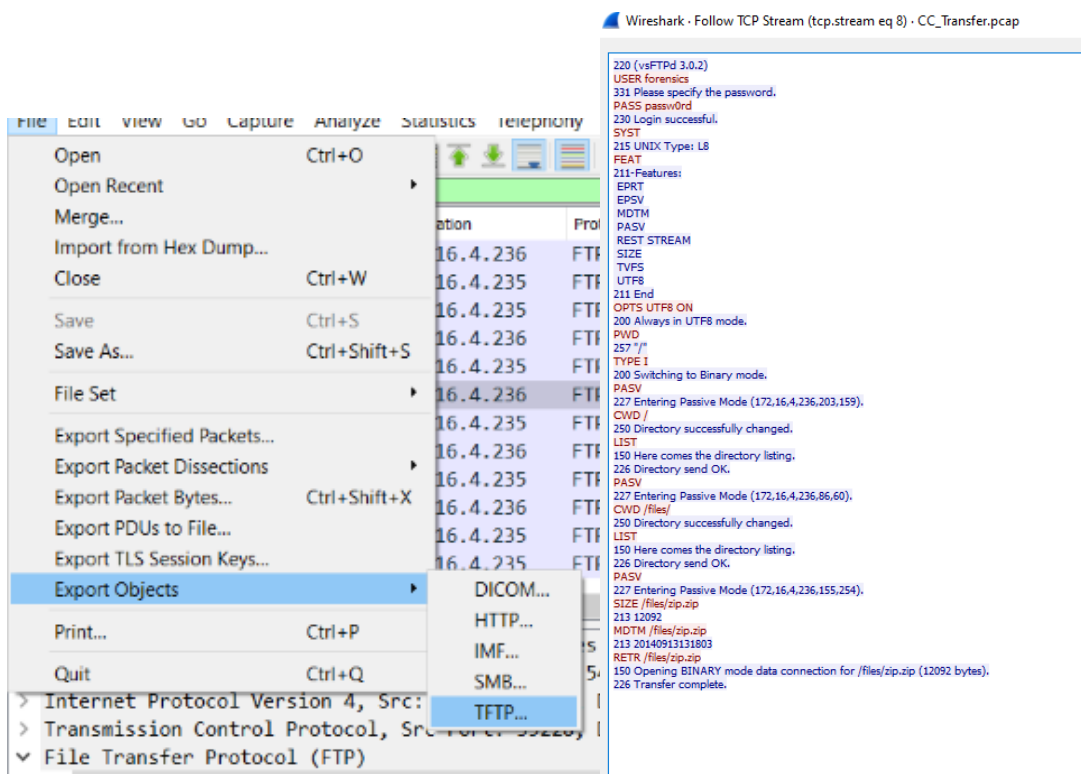
[Response duration: 1ms]

[Response bitrate: 96736Kbps]

[Setup frame: 403]

0000 00 0c 29 92 9e 43 00 0c 29 42 54 00 00 00 45 00 ..)C... )BT...E-  
0010 00 49 ec 37 40 00 00 06 ec 7f ac 10 04 eb ac 10 -I:7@\_@ .....  
0020 04 ec 89 9c 00 15 40 e8 0d 9a b3 c4 02 6b 80 18 .....@.....k-  
0030 00 e5 79 03 00 00 01 01 08 0a 00 11 e6 df 00 02 .....@.....k-  
0040 32 9f 53 49 5a 45 20 2f 66 69 6c 65 73 2f 7a 69 2.SIZE / files/zi  
0050 70 2e 7a 69 70 0d 0a p.zip..

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.

ftp-data						
No.	Time	Source	Destination	Protocol	Length	Data
...	19.971501	172.16.4.236	172.16.4.235	FTP-...	129	FTP Data: 63 bytes (PASV) (CWD /)
...	21.559364	172.16.4.236	172.16.4.235	FTP-...	131	FTP Data: 65 bytes (PASV) (CWD /files/)
...	22.535145	172.16.4.236	172.16.4.235	FTP-...	1514	FTP Data: 1448 bytes (PASV) (SIZE /files/zip.zip)
...	22.535377	172.16.4.236	172.16.4.235	FTP-...	1514	FTP Data: 1448 bytes (PASV) (SIZE /files/zip.zip)
...	22.535484	172.16.4.236	172.16.4.235	FTP-...	1266	FTP Data: 1200 bytes (PASV) (SIZE /files/zip.zip)
...	22.535725	172.16.4.236	172.16.4.235	FTP-...	1514	FTP Data: 1448 bytes (PASV) (SIZE /files/zip.zip)
...	22.535831	172.16.4.236	172.16.4.235	FTP-...	1514	FTP Data: 1448 bytes (PASV) (SIZE /files/zip.zip)
...	22.535934	172.16.4.236	172.16.4.235	FTP-...	1266	FTP Data: 1200 bytes (PASV) (SIZE /files/zip.zip)
...	22.536040	172.16.4.236	172.16.4.235	FTP-...	1514	FTP Data: 1448 bytes (PASV) (SIZE /files/zip.zip)
...	22.536279	172.16.4.236	172.16.4.235	FTP-...	1514	FTP Data: 1448 bytes (PASV) (SIZE /files/zip.zip)
...	22.536385	172.16.4.236	172.16.4.235	FTP-...	1070	FTP Data: 1004 bytes (PASV) (SIZE /files/zip.zip)

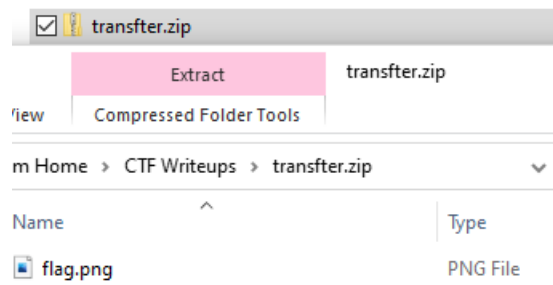
```
> Frame 393: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits)
> Ethernet II, Src: VMWare_92:9e:43 (00:0c:29:92:9e:43), Dst: VMWare_42:54:00 (00:0c:29:42:54:00)
> Internet Protocol Version 4, Src: 172.16.4.236, Dst: 172.16.4.235
> Transmission Control Protocol, Src Port: 22076, Dst Port: 49887, Seq: 1, Ack: 1, Len: 65
  FTP Data (65 bytes data)
    [Setup frame: 385]
    [Setup method: PASV]
    [Command: CWD /files/]
    [Command frame: 388]
    [Current working directory: /]
  Line-based text data (1 lines)
    -rw-r--r-- 1 0 0 12092 Sep 13 13:18 zip.zip\r\n
```

Follow the TCP stream to see all the data:

Wireshark · Follow TCP Stream (tcp.stream eq 13) · CC\_Transfer.pcap

Pk...%j;E8I...zennflag.pngUT...|.\*T\*.|Tux.....eP[.6... ..A.kpm.S...4... ..A.km.vjw....N..u...9.Z{...D#B...Wm...P.m3  
bb^r.f...O...x.L...E...o..?uOVV...f..a..G...e...F.J].4...COK...ZS... ..#s-+)...(Qy...M..U..Pe...e...a3...[...YzL.U...J.V...n...M.7)...OR...e...X...703.k.e.z.b...q4..  
.F+E...H=...A...e...9.3"S.W...c3...X.G... ..X.G... ..X.G...  
...AS...eE... ..O.7.%...&.D.rnm...  
s...[r.j.Mq.U...+%H.]... ..u...d...[...Nn...-.].R.G.O...s[k\*..  
...4...nnmqe...3...k...z9q.CmgG...njnqnq...+7.S.=\_...Mk...s</o.b...e...zC.I.k.t...l.PCv...wj.w.m...|qZ...p...m\_o^...e...[lqnq=-  
\$[?Z4.6L.<...  
[?]&.7.V.m.s.s.A.S...O.+m.g5.S#...6dLmB.d...v3...w...[I|.S'...Fu...a...KU+..  
...e#...+...gUMog%...>]'.k.u.v...1n  
...UTh...g.l.Hdz|=|W.h...m.m...Y?...T.t.j.=f.r.n.j...K...[d}&...=aVG...u...o.h.j...u.O.7+6Y...|=s...c7...lb/f.W)2...9T...S.@.H...[6S"...])%.j.F.F.T.U.L...  
...=J.J...Etp.R.3.D)...e.B9%..  
U...Z...7o...T...f(L.h.H...)|.Q...G.2.j...R.S)'c'...RX.t...T.S...'6G1...-W...m...Js...Q8...v...|).B.t.ts.\*  
...l.k.b.b.M...j.e.i.z.L.d...e.ovz...e...Ol...s...h...A2'E...3'm...r.'Pg.b.dbb...|X... ..oy.6.se{.A.8...+}'Y5.Nwn...7gz...tZ(.ze..OQ...9.j...  
+97...M... ..W...e...k.mzt'.W...l.A...b+f...s...=y/...2.Cg(...e)N.n.k.Xij...t.p.v.fikSH... ..p  
X|.U...H.F+...r?..0.y>b.l[.6j.Qy.I?](>...m.N.Z...7A.3...v...p... ..I..Z.bd[...]..S.E...f...3ql+...|Z.h.f...  
7mny.59.Y2B...7yL-g-g...[.s5...abN...U/O...B...>>c'HBC...P...c7&.s...m...8s5&.b...g...|@6t..  
M...|...[.B][...oS.S.w.v.6...&.d.k2..R...|..  
...W.a.M...7...@...j...QM...|M... ..a...?>...+...n.U.L.X.Z...oh%)%\... ..\*&.X...N.Nr...f...T.W.kcw...7).d^...@'^'(...32...Y...a...pa... ..a...0...%j.Pmi...9.3d.  
9...<o...cm...Df...  
...o...j...d...e...H...='(M&S...w...H...E...f...w/7..  
\*M...&.s...A...A...V...D.../...m...HB...6?Q...m...N.o...<d...gi.k...t/D...?)...[aH...D...H9...W.?>'&.AT&.S...Xn.M.h.k.|4|.l...R...  
/uH.j...|u@p^...h...[o...m]\*S...cB.W...n...j...^...2W...m...t...\*...bk,%E.3.m...m...e...k...m...|'.|^K...  
&@HR.d.{K}.'=[w]...m...f... UWU...:R.7Q..  
UD/n.^Q.Yj...Qv...pu \_...|/...m...BOO.g...G...7...u...m...N7b)\$...\*(C...d)]#S.../7..Q=1..  
...6.7z...S...-[Y%\$].\$R5...r...n...=B...<...y...f...y...Q.W.2...)(...+ V..h2'.izDR.m.7w3...6X0.(2...o...7zuXm...g0=j...7.Q...xmO...VYy8Y.../... ]L...=...6...m...[O...9^+(...  
...8...m...S=E.8...m...DRID...%...t...\*'O...m...7NSG)  
...S.N...-G-M...  
/U.U.j.A/uORYO...=...V?H... ..{...Kj}{.}p5.z...n...j...I.Z...|'.q;j)o.v...m...I>M...m...q...^QW...U...j...q...m...x...g.#..  
%U.S.J.L...l...ipujp5f.6...)..d  
2>...m...y...N.+6v  
...W)?...r...j...w...V.V...e...b...f...y...#...&.b...o...=...h...m...Xq.M.px.&(h...^...e...m...|b...m...N>...\$..  
...f... ..f... ..i...p...+...k...44...D...B...CZ...+...CS...N'-G...m...t...B...K...+...|...B...e...k...j3B1...lig.7..  
mB7.D.M.x.c...Vos.G...w...g...n...l...^...c...w...S...+...y...\$...0...#?...7...u...O...  
5G/(wot...a...w...f...v...|)...P...M...#O7p.A...a...S|.P.P...m...|...c...&\*...ZCZ(|...v...m...|... (Z>+V...m...E...<=|D...I.A...DV...?'...9...m...V)...R...w...v...KerW>c|...@...\*...u...j...%(%&...{...})...Z.S...\*  
g+..  
...m...f...o.G...b...d...&...j\$Q^...p...^...S...e...m...|...X...cN.[3  
...m...c... ..=Iv...m...|...&Z.G...y... ..k.H.I89...  
d...Nfc.F.KB-n...a.U...m...Y...|...n...\*BGY...c7g...C...\*.Ex\*3R#...m...v.nH=K...F.3...q...JH.7|XN...o.I.TA.J+D...6...PEKx4...z...[...a...X...>m...T...v...|'.b...Cs...|'.f.b... {...a)...YZu>..  
1.ABalp3...m...S.V...=F...6...Z...  
0.)5#...;S|.Z...c...X...a.../...p...g.\*X...9>...|/pX^...S...I.E.s...|'.k...<...)WW...J.U.Q+J.-Nd.TWA...0.56...{^7...qeE.V...s...|O.I.K.R7...W..  
8...m...f...o.G...b...d...&...j\$b...s...ZNr&B...t...|...g...f...m...|...H.g.Xp...  
...E...x...f...v...m...c...S&v...6...s...z...m...H...#...Gr...u...&J;Az(A.S...)|faA...N...#Oo...T...u...^...U...j...H...Q...d...C'9...\*j.M...(>...pZ...W...m...Ro...s...i...%N...G...\*...;h...^...e...{.4.P.z...u...|...H...@!1  
0''m.G...j7...k...&-...l...f... ..%...j...1...+...m...TW...m...|')b...l'W7...u...%Q61...M...MO...N...Y...?a.Gb...P...H...A...e...l0m^-Oz.Z)...|...2  
m...|a...|...=Pd.G.V...m...|...{bu...|&0...&...8...m...Drf...&f>z...w...f...r... 9A...m...W...n...4.ki-3...U...p... ..9...  
...U|R...G...j...K...SW  
r...|...-H...3Jl.7...CD  
a...OR...c...m...&...3...@2 [X...m...V4Ei...|...d...s'^Z...jw(m...bX...s...U...j).W.Q.Y^...o...m...S...Q...WEWq?...My\*x... ..4..  
X...{...e...\$a0...^...6...m...|...  
L.n.A.k.e...B...i...m...f...n...k...}.7wWQ... F...EU...a.W...o...j...b...l...Q...m...6.s  
<5%B...oj...  
C...d...j...m...R79...m...Qm...x...m... Na... ..m...>n>C>D>M...+...r...y.L.D.L.q.k LG.Wg.E...m...|'.N.MY?...@GE39...X...m...v...9m...|'.{sun-7...A...b...W...\$mqIb...9.M...FG...Z...7...C...}).T.p'}  
C.D...q.tk&8...T...m... ..3...f...m...M...%...j...=...I'BU...m...E...m...|<F...m...|7^...w...[g...g...%<L-h...c...j...8)...H...U...|...{.52.kz{  
.jh ...e...WqEQ%v...j...w...v...mk.S...S...V...m...t...Q...m...>...Q...|>...8...Md...|...NI'/...m...Q...G...W...h...jCA#E...<=<W... D...m...|...|...f...m...Y...m...M?3k...5.8.

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.



Name	Type
flag.png	PNG File

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

flag{91e02cd2b8621d0c05197f645668c5c4}