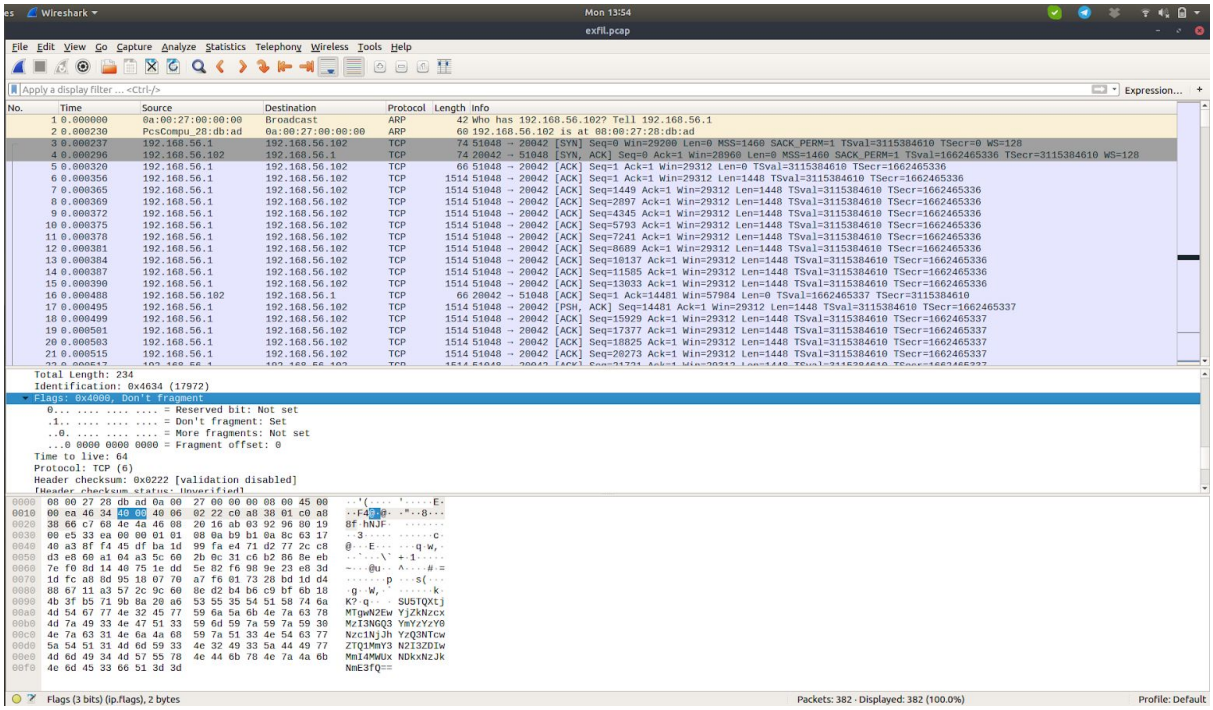
For: G-corp stage1

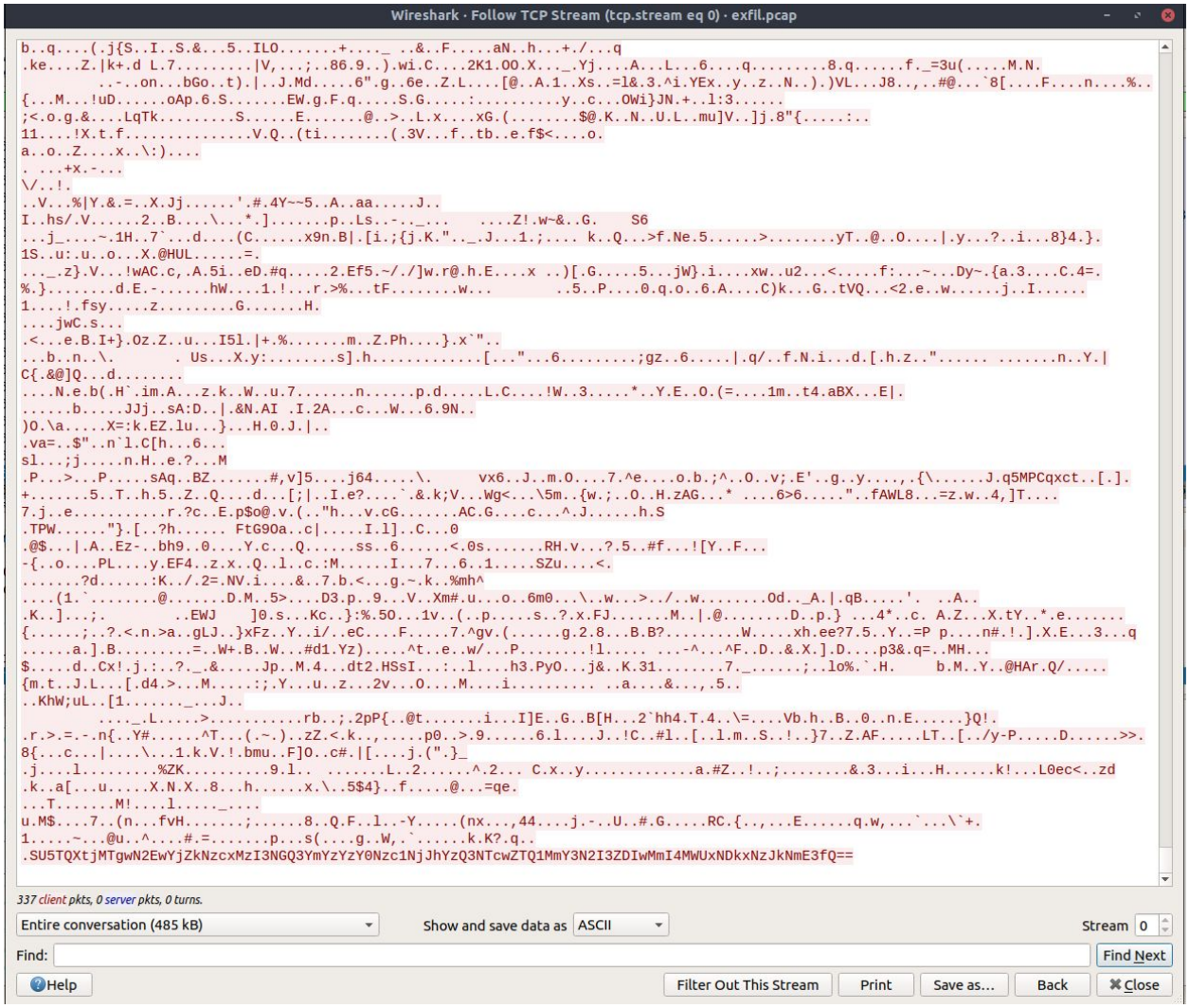
In this file we are asked to find sensible info inside a traffic package stream. We are given a “pcap” file, which can be opened with WireShark. We thus can open it, and the screen should looks like the the following:



Thanks to this tool we can easily see that, in this communication, only 2 protocols are involved (ARP and TCP), and 2 IPs as well (192.168.56.1 and 192.168.56.102).

In order to have a better overview of the communication, we can go to “*analyze / follow / TCP stream* ”, and this screen will show all of the messages. On the bottom, a base64 message is shown. We can decode it and reveal the flag:

INSA{c1807a0b6d7713274d7bf3c6477562ac47570e452f77b7d202b81e149172d6a7}


Wireshark · Follow TCP Stream (tcp.stream eq 0) · exfil.pcap
b..q....(.j{S..I..S.&...5..ILO.......+...._ ..&..F.....aN..h...+./...q
.ke....Z.|k+.d L.7.........|V,...;..86.9..).wi.C....2K1.OO.X..._.Yj....A...L...6....q.........8.q......f._=3u(.....M.N.
..-..on...bGo..t).|..J.Md.....6".g..6e..Z.L....[@..A.1..Xs..=l&.3.^i.YEx..y..z..N..).)VL...J8..,..#@...`8[....F....n....%..
{...M...!uD......oAp.6.S.......EW.g.F.q.....S.G.....:..........y..c...OWi}JN.+..l:3.....
;<.o.g.&....LqTk.........S......E.......@..>..L.x....xG.(........$@.K..N..U.L..mu]V..]j.8"{.....:..
11....!X.t.f..............V.Q..(ti........(.3V...f..tb..e.f$<....o.
a..o..Z....x..\:)....
. ...+x.-...
\/..!.
..V...%|Y.&.=..X.Jj......'.#.4Y~~5..A..aa.....J..
I..hs/.V......2..B....\...*.].......p..Ls..-..._...   ....Z!.w~&..G.   S6
...j_....~.1H..7`...d....(C......x9n.B|.[i.;{j.K."._.J...1.;.... k..Q...>f.Ne.5......>........yT..@..O....|.y...?..i...8}4.}.
1S..u:.u..o...X.@HUL......=.
..._.z}.V...!wAC.c,.A.5i..eD.#q.....2.Ef5.~/./]w.r@.h.E....x ..)[.G.....5...jW}.i....xw..u2...<.....f:...~...Dy~.{a.3....C.4=.
%.}........d.E.-......hW....1.!...r.>%...tF........w...   ..5..P....0.q.o..6.A....C)k...G..tVQ...<2.e..w......j..I......
1....!.fsy.....z.........G.......H.
....jwC.s...
.<...e.B.I+}.Oz.Z..u...I5l.|+.%.......m..Z.Ph....}.x`"..
...b..n..\.   . Us...X.y:........s].h.............[..."...6.........;gz..6.....|.q/..f.N.i...d.[.h.z.."...... ....n..Y.|
C{.&@]Q...d........
....N.e.b(.H`.im.A...z.k..W..u.7.......n......p.d.....L.C....!W..3.....*..Y.E..O.(=....1m..t4.aBX...E|.
......b.....JJj..sA:D..|.&N.AI .I.2A...c...W...6.9N..
)O.\a.....X=:k.EZ.lu...}...H.0.J.|..
.va=..$"..n`l.C[h...6...
sl...;j.....n.H..e.?...M
.P...>...P.....sAq..BZ.......#,v]5....j64.....\.   vx6..J..m.O....7.^e....o.b.;^..O..v;.E'..g..y....,.{\......J.q5MPCqxct..[.].
+.......5..T..h.5..Z..Q....d...[;|..I.e?....`.&.k;V...Wg<...\5m..{w.;..O..H.zAG...* ....6>6.....".fAWL8...=z.w..4,]T....
7.j..e...........r.?c..E.p$o@.v.(.."h...v.cG.......AC.G....c...^.J......h.S
.TPW......"}.[..?h..... FtG9Oa..c|.....I.l]..C...0
.@$...|.A..Ez-..bh9..0....Y.c...Q......ss..6......<.0s.......RH.v...?.5..#f...![Y..F...
-{..o....PL....y.EF4..z.x..Q..l..c.:M......I...7...6..1.....SZu....<.
.......?d......:K../.2=.NV.i....&..7.b.<...g.~.k..%mh^
....(1.`........@.......D.M..5>....D3.p..9...V..Xm#.u...o..6m0...\..w...>../..w........Od.._A.|.qB.....'. ..A..
.K..]...;.   ..EWJ   ]0.s...Kc..}:%.5O...1v..(..p.....s..?.x.FJ.......M..|.@........D..p.} ...4*..c. A.Z...X.tY..*.e.......
{......;..?.<.n.>a..gLJ..}xFz..Y..i/..eC....F.....7.^gv.(......g.2.8...B.B?.........W.....xh.ee?7.5..Y..=P p....n#.!.].X.E...3...q
......a.].B.........=..W+.B..W...#d1.Yz).....^t..e..w/...P........!l..... ...-^...^F..D..&.X.].D....p3&.q=..MH...
$.....d..Cx!.j.:..?._.&.....Jp..M.4...dt2.HSsI...:..l....h3.PyO...j&..K.31........7._.....;..lo%.`.H.   b.M..Y..@HAr.Q/.....
{m.t..J.L...[.d4.>...M.....;.Y...u..z...2v...O....M....i.......... ..a....&...,.5..
..KhW;uL..[1......._...J..
        ...._.L.....>...........rb..;.2pP{..@t......i...I]E..G..B[H...2`hh4.T.4..\=....Vb.h..B..0..n.E......}Q!.
.r.>.=.-.n{..Y#......^T...(.~.)..zZ.<.k.,.....p0..>.9......6.l....J..!C..#l..[..l.m..S..!..}7..Z.AF.....LT..[../y-P.....D......>>.
8{...c...|....\...1.k.V.!.bmu..F]O..c#.|[....j.(".}_
.j....l.........%ZK.........9.l.. ......L..2.....^.2... C.x..y.............a.#Z..!..;........&.3...i...H......k!...L0ec<..zd
.k..a[...u.....X.N.X..8...h......x.\..5$4}..f.....@...=qe.
...T.......M!....l....._....
u.M$....7..(n...fvH......;......8..Q.F..l..-Y.....(nx...,44....j.-..U..#.G.....RC.{..,...E......q.w,...`...\`+.
1.....~...@u..^....#.=.......p...s(....g..W,.`......k.K?.q..
.SU5TQXtjMTgwN2EwYjZkNzcxMzI3NGQ3YmYzYzY0Nzc1NjJhYzQ3NTcwZTQ1MmY3N2I3ZDIwMmI4MWUxNDkxNzJkNmE3fQ==
337 client pkts, 0 server pkts, 0 turns.
Entire conversation (485 kB)
Show and save data as
ASCII
Stream
0
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close