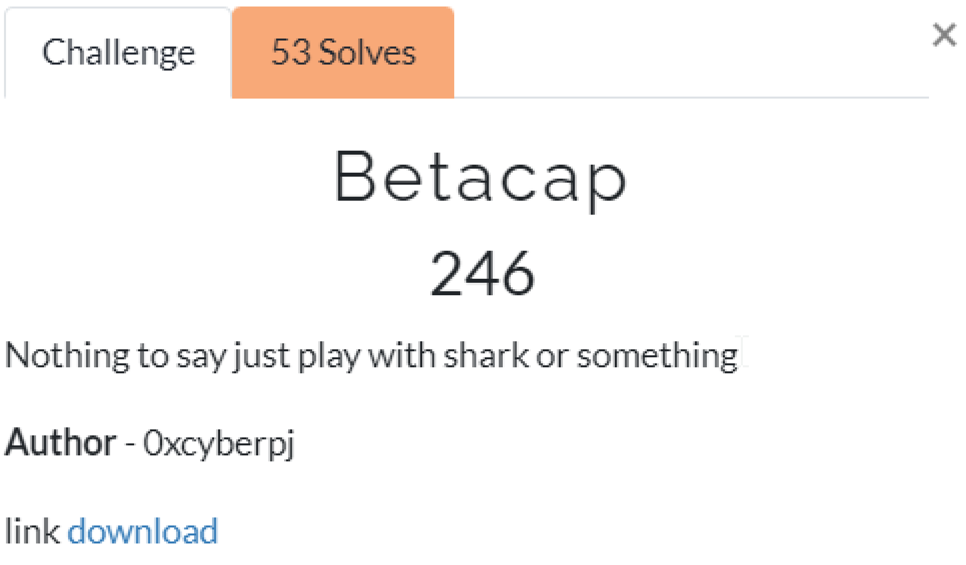
TamilCTF Betacap writeup.

Author : Paul jeremiah

Level : Medium -



Challenge | 53 Solves

Betacap

246

Nothing to say just play with shark or something

Author - 0xcyberpj

link download

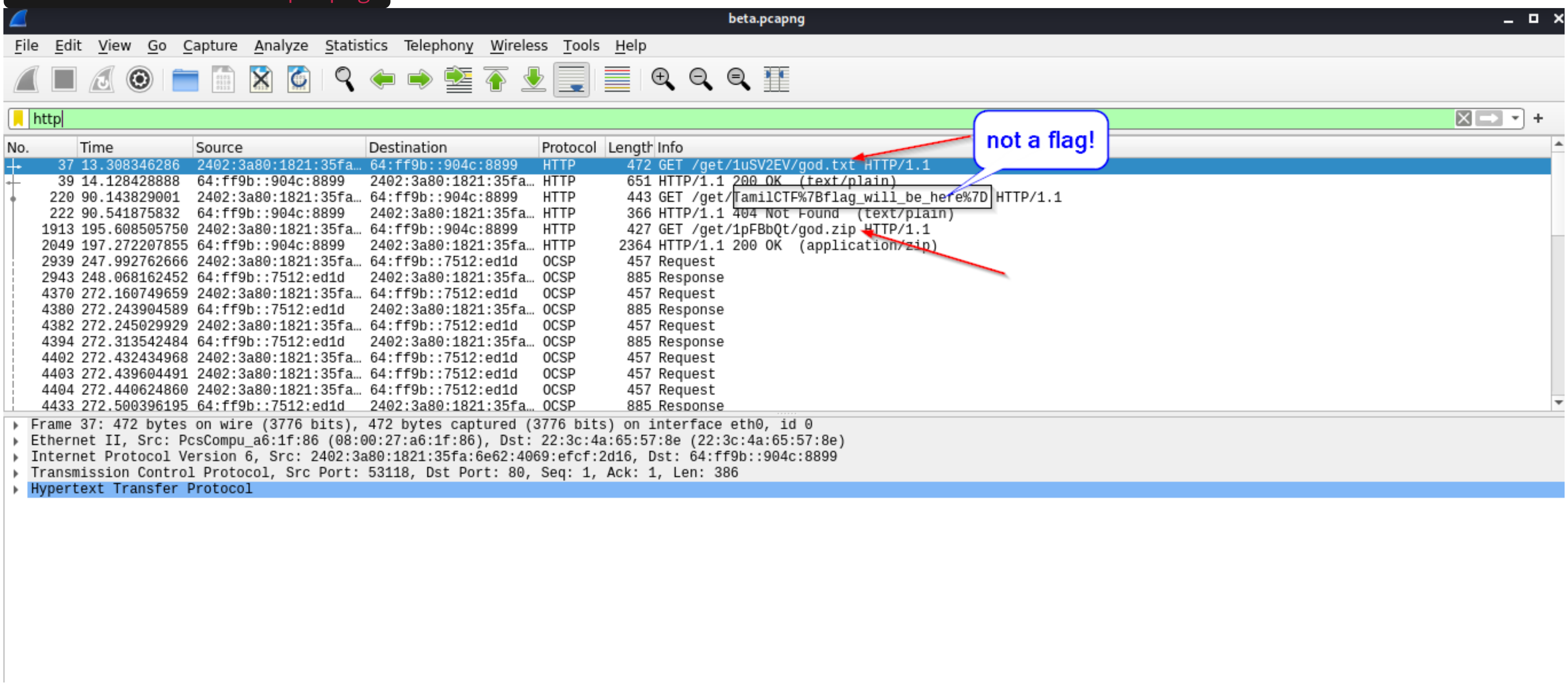
Given :
unzip

```
┌──(kali㉿kali)-[/tmp]
└─$ ⚡file beta.pcapng
beta.pcapng: pcapng capture file - version 1.0
```

Writeup →:

let's start with strings, nothing to be useful

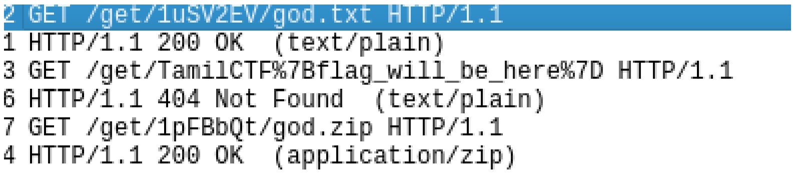
`sudo wireshark beta.pcapng`



beta.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

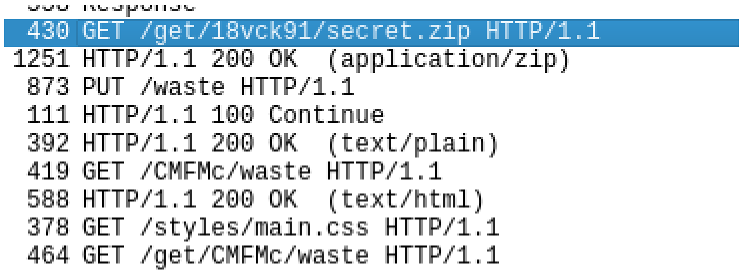
```
No.   Time          Source                  Destination             Protocol Length Info
   37 13.308346286  2402:3a80:1821:35fa…    64:ff9b::904c:8899      HTTP      472 GET /get/1uSV2EV/god.txt HTTP/1.1
   39 14.128428888  64:ff9b::904c:8899      2402:3a80:1821:35fa…    HTTP      651 HTTP/1.1 200 OK  (text/plain)
  220 90.143829001  2402:3a80:1821:35fa…    64:ff9b::904c:8899      HTTP      443 GET /get/TamilCTF%7Bflag_will_be_here%7D HTTP/1.1
  222 90.541875832  64:ff9b::904c:8899      2402:3a80:1821:35fa…    HTTP      366 HTTP/1.1 404 Not Found  (text/plain)
 1913 195.608505750 2402:3a80:1821:35fa…    64:ff9b::904c:8899      HTTP      427 GET /get/1pFBbQt/god.zip HTTP/1.1
 2049 197.272207855 64:ff9b::904c:8899      2402:3a80:1821:35fa…    HTTP     2364 HTTP/1.1 200 OK  (application/zip)
 2939 247.992762666 2402:3a80:1821:35fa…    64:ff9b::7512:ed1d      OCSP      457 Request
 2943 248.068162452 64:ff9b::7512:ed1d      2402:3a80:1821:35fa…    OCSP      885 Response
 4370 272.160749659 2402:3a80:1821:35fa…    64:ff9b::7512:ed1d      OCSP      457 Request
 4380 272.243904589 64:ff9b::7512:ed1d      2402:3a80:1821:35fa…    OCSP      885 Response
 4382 272.245029929 2402:3a80:1821:35fa…    64:ff9b::7512:ed1d      OCSP      457 Request
 4394 272.313542484 64:ff9b::7512:ed1d      2402:3a80:1821:35fa…    OCSP      885 Response
 4402 272.432434968 2402:3a80:1821:35fa…    64:ff9b::7512:ed1d      OCSP      457 Request
 4403 272.439604491 2402:3a80:1821:35fa…    64:ff9b::7512:ed1d      OCSP      457 Request
 4404 272.440624860 2402:3a80:1821:35fa…    64:ff9b::7512:ed1d      OCSP      457 Request
 4433 272.500396195 64:ff9b::7512:ed1d      2402:3a80:1821:35fa…    OCSP      885 Response

Frame 37: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_a6:1f:86 (08:00:27:a6:1f:86), Dst: 22:3c:4a:65:57:8e (22:3c:4a:65:57:8e)
Internet Protocol Version 6, Src: 2402:3a80:1821:35fa:6e62:4069:efcf:2d16, Dst: 64:ff9b::904c:8899
Transmission Control Protocol, Src Port: 53118, Dst Port: 80, Seq: 1, Ack: 1, Len: 386
Hypertext Transfer Protocol
```

so we got some files there



```
2 GET /get/1uSV2EV/god.txt HTTP/1.1
1 HTTP/1.1 200 OK  (text/plain)
3 GET /get/TamilCTF%7Bflag_will_be_here%7D HTTP/1.1
6 HTTP/1.1 404 Not Found  (text/plain)
7 GET /get/1pFBbQt/god.zip HTTP/1.1
4 HTTP/1.1 200 OK  (application/zip)
```

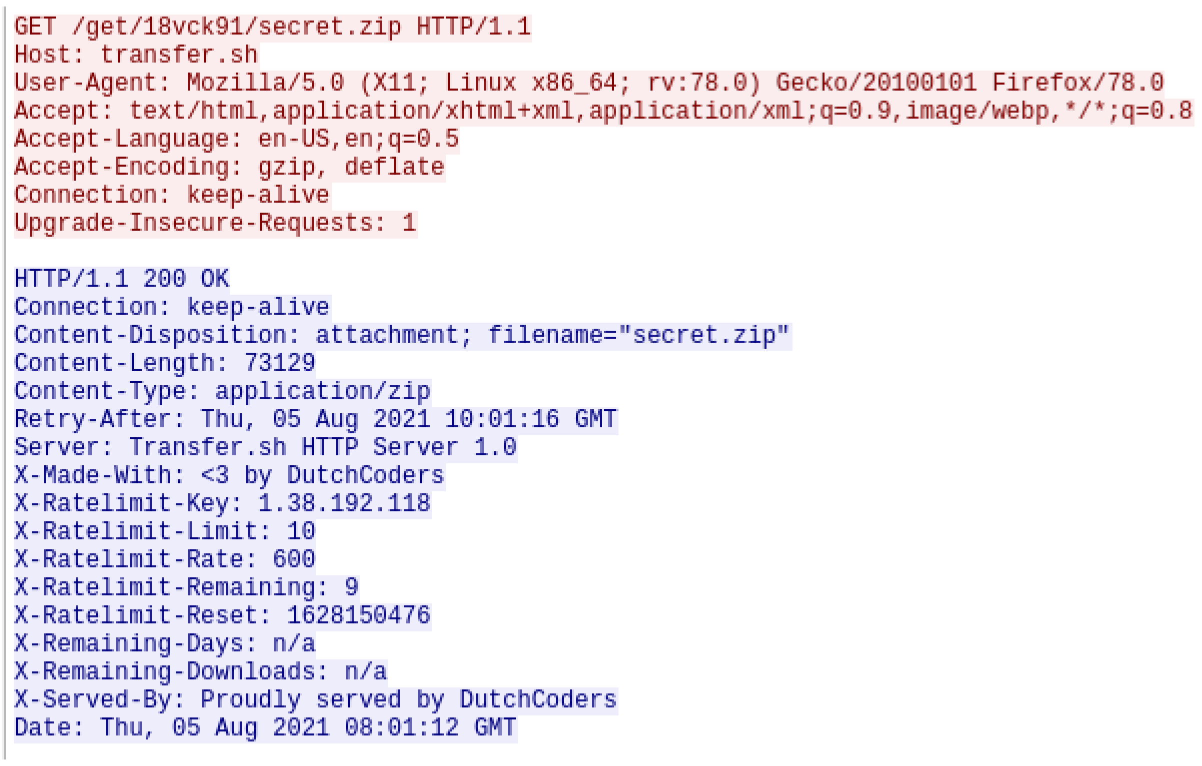
let's download them locally



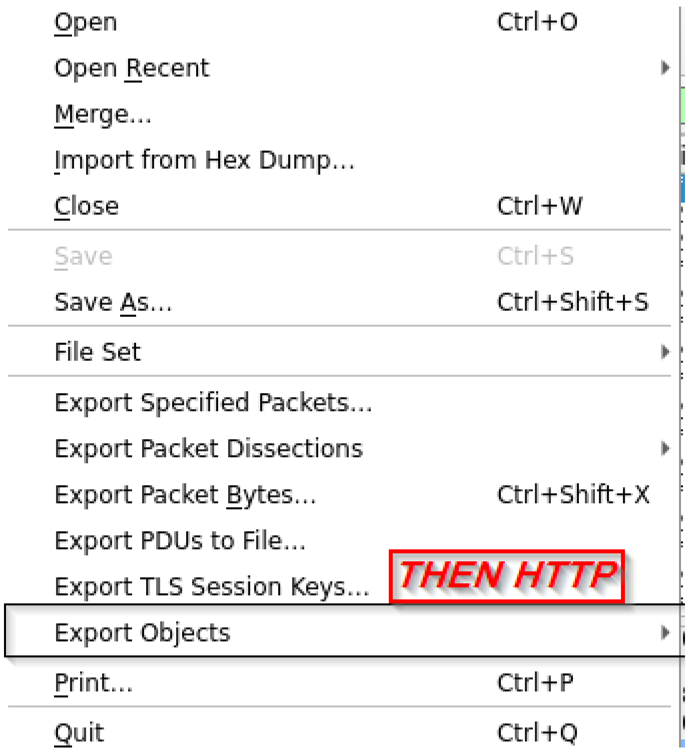
```
 430 GET /get/18vck91/secret.zip HTTP/1.1
1251 HTTP/1.1 200 OK  (application/zip)
 873 PUT /waste HTTP/1.1
 111 HTTP/1.1 100 Continue
 392 HTTP/1.1 200 OK  (text/plain)
 419 GET /CMFMc/waste HTTP/1.1
 588 HTTP/1.1 200 OK  (text/html)
 378 GET /styles/main.css HTTP/1.1
 464 GET /get/CMFMc/waste HTTP/1.1
```

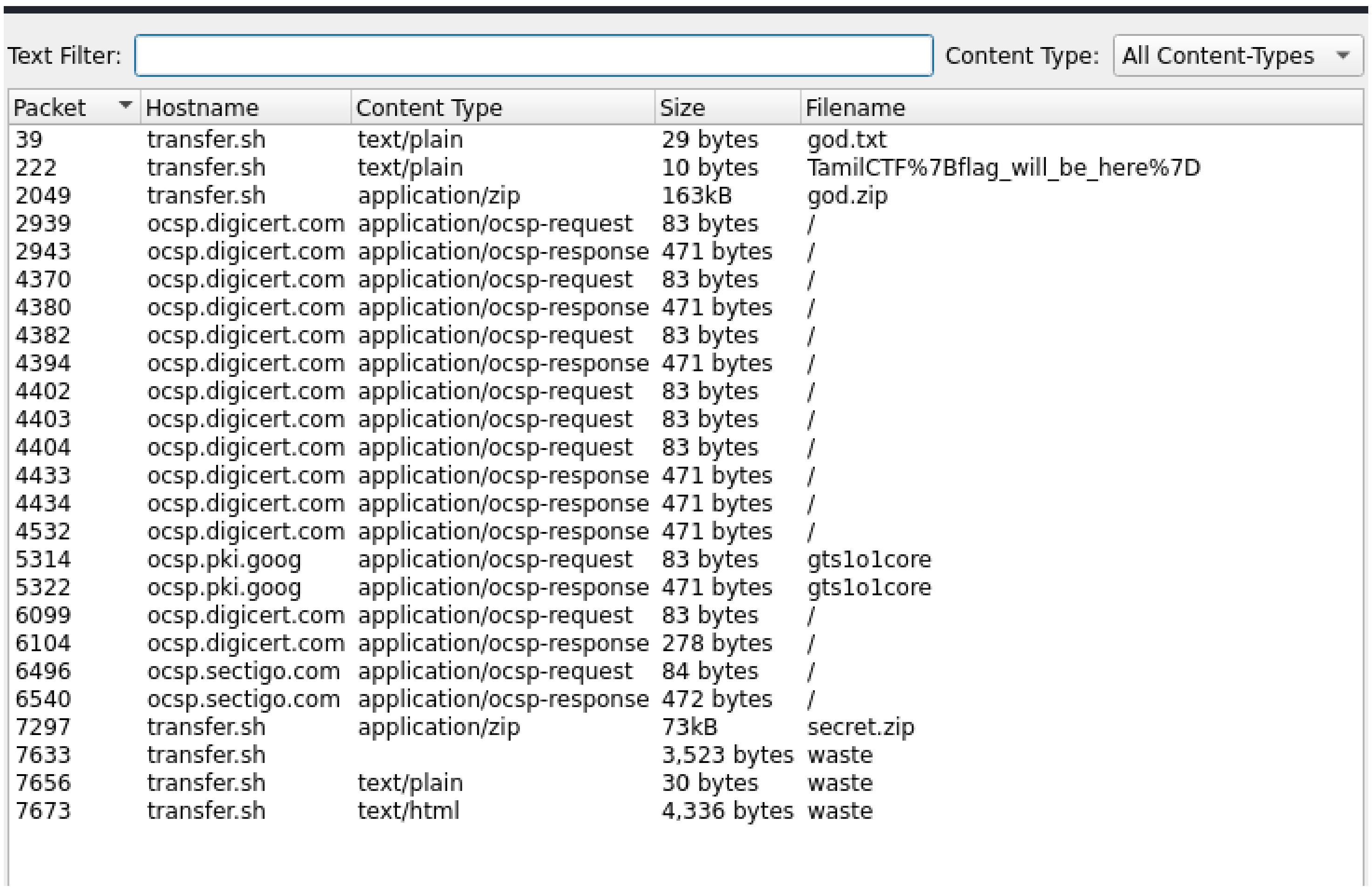
there are two methods to get them, here most of the files were from transfer.sh what if the links get expired!?

so here I'm going to extract the object from HTTP



```
GET /get/18vck91/secret.zip HTTP/1.1
Host: transfer.sh
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Connection: keep-alive
Content-Disposition: attachment; filename="secret.zip"
Content-Length: 73129
Content-Type: application/zip
Retry-After: Thu, 05 Aug 2021 10:01:16 GMT
Server: Transfer.sh HTTP Server 1.0
X-Made-With: <3 by DutchCoders
X-Ratelimit-Key: 1.38.192.118
X-Ratelimit-Limit: 10
X-Ratelimit-Rate: 600
X-Ratelimit-Remaining: 9
X-Ratelimit-Reset: 1628150476
X-Remaining-Days: n/a
X-Remaining-Downloads: n/a
X-Served-By: Proudly served by DutchCoders
Date: Thu, 05 Aug 2021 08:01:12 GMT
```

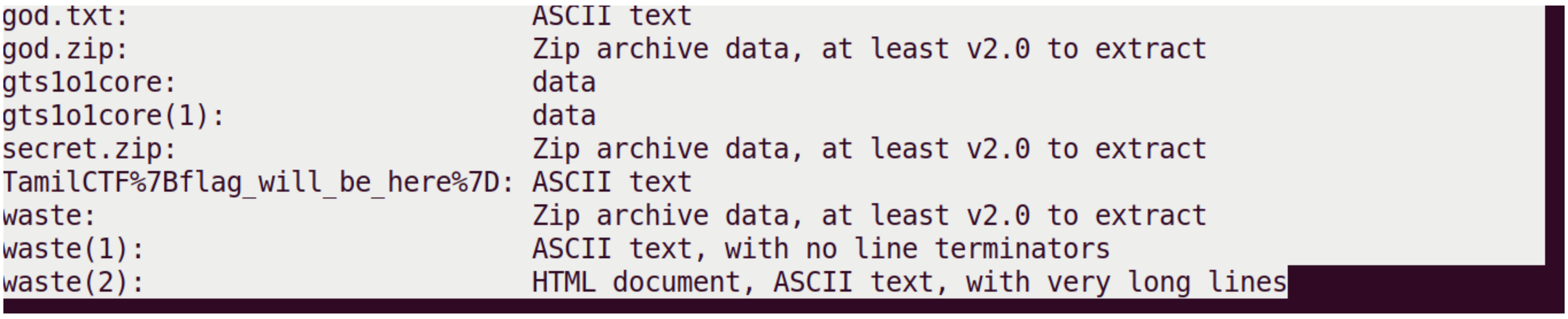




Text Filter: Content Type: All Content-Types

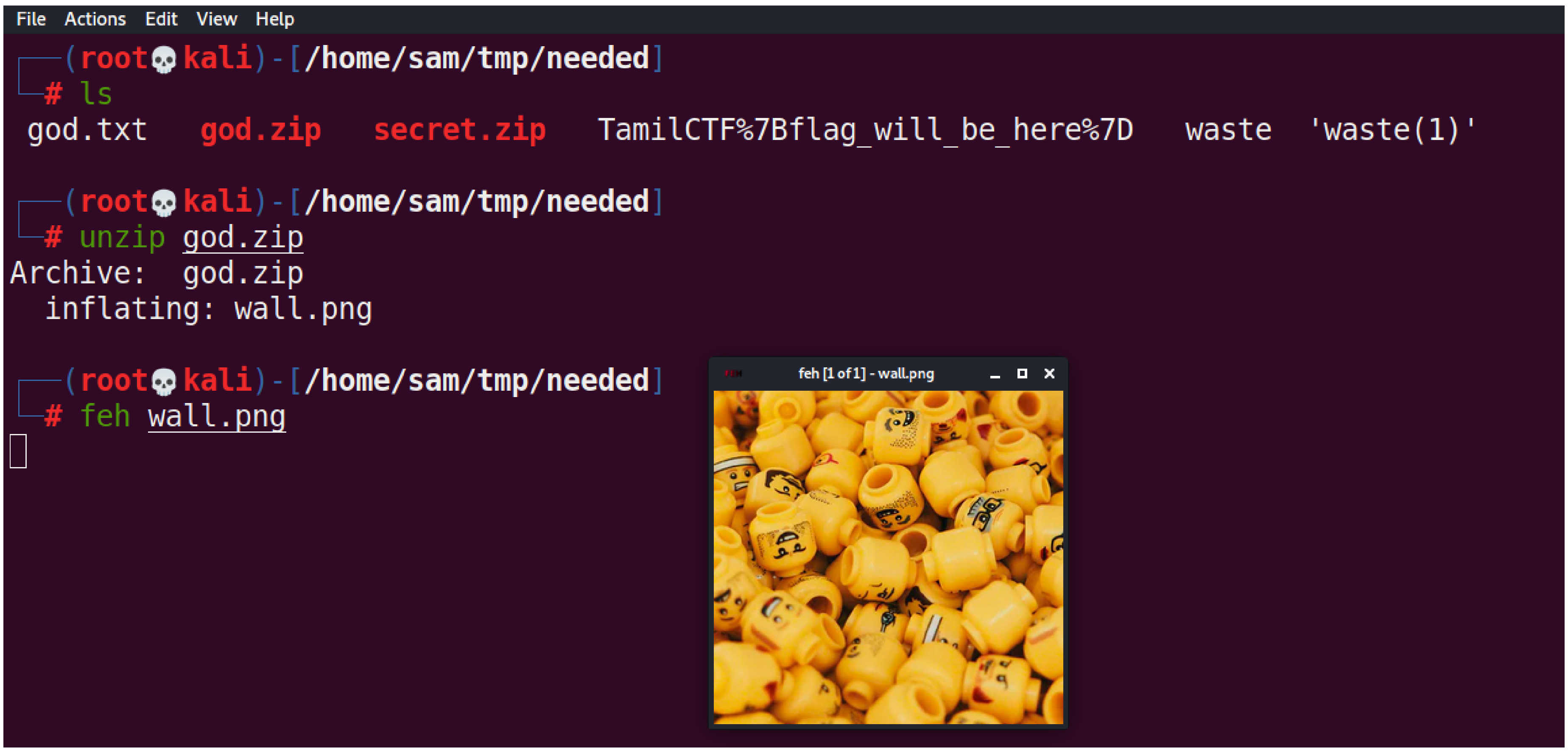
Packet	Hostname	Content Type	Size	Filename
39	transfer.sh	text/plain	29 bytes	god.txt
222	transfer.sh	text/plain	10 bytes	TamilCTF%7Bflag_will_be_here%7D
2049	transfer.sh	application/zip	163kB	god.zip
2939	ocsp.digicert.com	application/ocsp-request	83 bytes	/
2943	ocsp.digicert.com	application/ocsp-response	471 bytes	/
4370	ocsp.digicert.com	application/ocsp-request	83 bytes	/
4380	ocsp.digicert.com	application/ocsp-response	471 bytes	/
4382	ocsp.digicert.com	application/ocsp-request	83 bytes	/
4394	ocsp.digicert.com	application/ocsp-response	471 bytes	/
4402	ocsp.digicert.com	application/ocsp-request	83 bytes	/
4403	ocsp.digicert.com	application/ocsp-request	83 bytes	/
4404	ocsp.digicert.com	application/ocsp-request	83 bytes	/
4433	ocsp.digicert.com	application/ocsp-response	471 bytes	/
4434	ocsp.digicert.com	application/ocsp-response	471 bytes	/
4532	ocsp.digicert.com	application/ocsp-response	471 bytes	/
5314	ocsp.pki.goog	application/ocsp-request	83 bytes	gts1o1core
5322	ocsp.pki.goog	application/ocsp-response	471 bytes	gts1o1core
6099	ocsp.digicert.com	application/ocsp-request	83 bytes	/
6104	ocsp.digicert.com	application/ocsp-response	278 bytes	/
6496	ocsp.sectigo.com	application/ocsp-request	84 bytes	/
6540	ocsp.sectigo.com	application/ocsp-response	472 bytes	/
7297	transfer.sh	application/zip	73kB	secret.zip
7633	transfer.sh		3,523 bytes	waste
7656	transfer.sh	text/plain	30 bytes	waste
7673	transfer.sh	text/html	4,336 bytes	waste

save all →



```
god.txt:                         ASCII text
god.zip:                         Zip archive data, at least v2.0 to extract
gts1o1core:                      data
gts1o1core(1):                   data
secret.zip:                      Zip archive data, at least v2.0 to extract
TamilCTF%7Bflag_will_be_here%7D: ASCII text
waste:                           Zip archive data, at least v2.0 to extract
waste(1):                        ASCII text, with no line terminators
waste(2):                        HTML document, ASCII text, with very long lines
```

This is what we need!



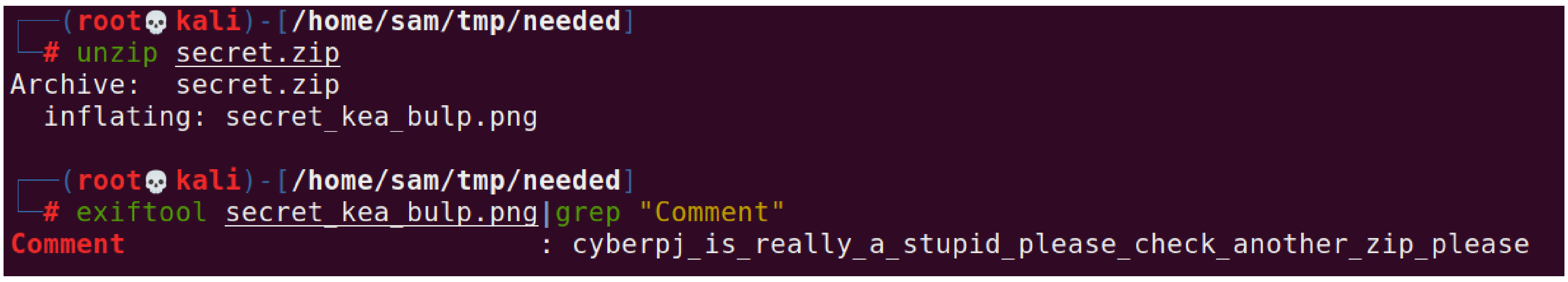
```
┌──(root💀kali)-[/home/sam/tmp/needed]
└─# ls
god.txt   god.zip   secret.zip   TamilCTF%7Bflag_will_be_here%7D   waste  'waste(1)'

┌──(root💀kali)-[/home/sam/tmp/needed]
└─# unzip god.zip
Archive:  god.zip
  inflating: wall.png

┌──(root💀kali)-[/home/sam/tmp/needed]
└─# feh wall.png
```

1. god.zip

```
┌──(root💀kali)-[/home/sam/tmp/needed]
└─# exiftool wall.png|grep Comment
Comment                         :
if_you_going_to_play_this_ctf_then_please_put_it_as_a_wallpaper_#godblessyou
```

lol just waste
just a comment

3.secret.zip

- 

```
┌──(root💀kali)-[/home/sam/tmp/needed]
└─# unzip secret.zip
Archive:  secret.zip
  inflating: secret_kea_bulp.png

┌──(root💀kali)-[/home/sam/tmp/needed]
└─# exiftool secret_kea_bulp.png|grep "Comment"
Comment                         : cyberpj_is_really_a_stupid_please_check_another_zip_please
```

  (let's check waste , waste is literally not a waste one)

4.waste
`file waste waste: Zip archive data, at least v2.0 to extract`

- extract

```
┌──(root💀kali)-[/home/sam/tmp/needed]
└─# unzip waste
Archive:  waste
  inflating: waste.png
```

```
┌──(root💀kali)-[/home/sam/tmp/needed]
└─# feh waste.png
feh WARNING: waste.png - Does not look like an image (magic bytes missing)
feh: No loadable images specified.
See 'man feh' for detailed usage information
```

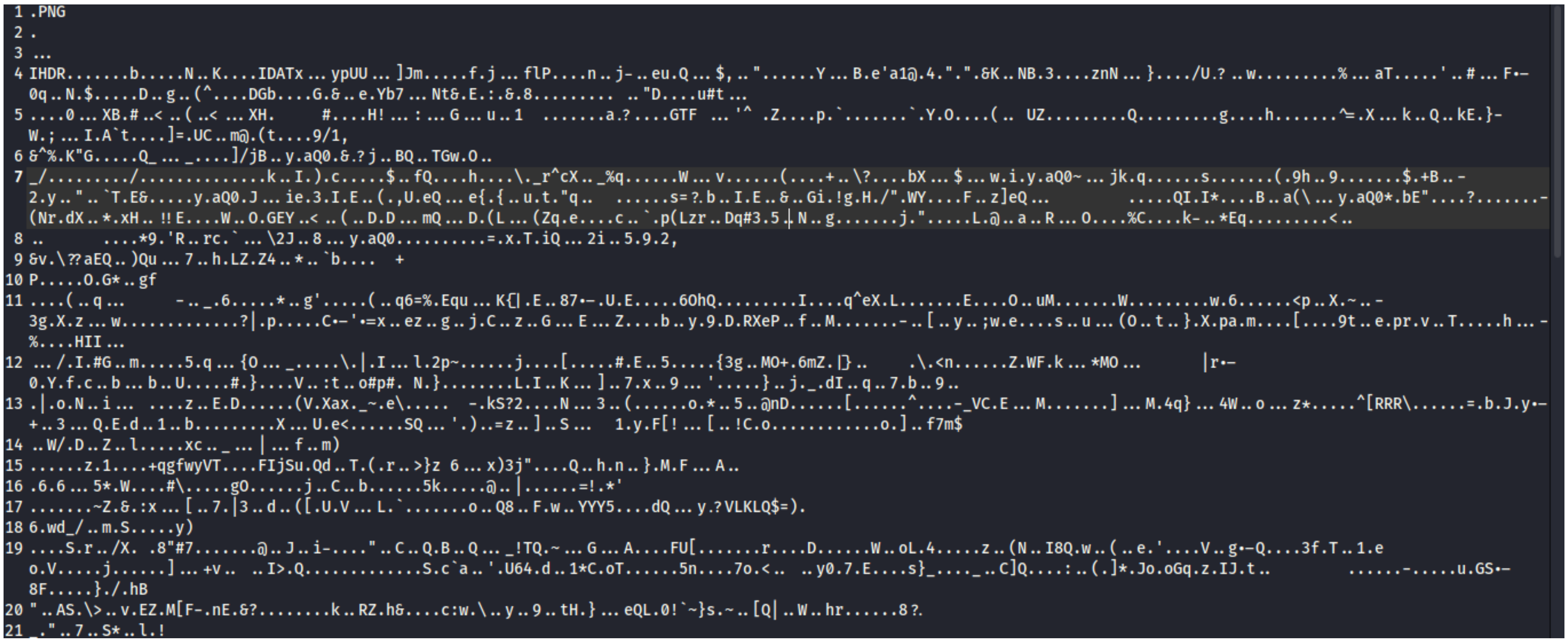
can't able to view it

> you guys going to correct the headers?
> or chunk data?

```
┌──(root💀kali)-[/home/sam/tmp/needed]
└─# file waste.png
waste.png: ASCII text, with very long lines
```

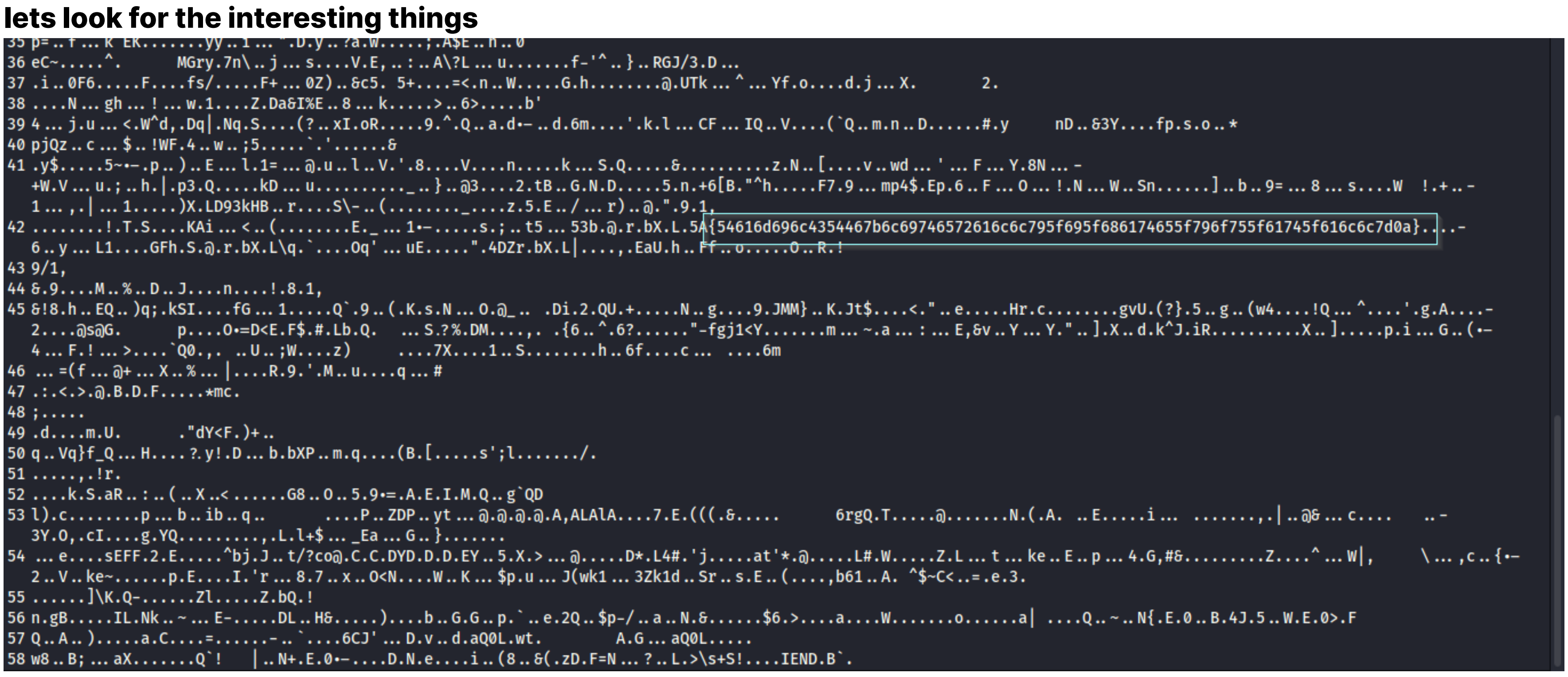
lol

- *any text editor*



```
.PNG
.
...
IHDR.......b.....N..K....IDATx...ypUU...]Jm.....f.j...flP....n..j-..eu.Q...$,.."......Y...B.e'a1@.4.".".&K..NB.3....znN...}..../U.?..w.........%...aT.....'..#...F•–
0q..N.$.....D..g..(^....DGb....G.&..e.Yb7...Nt&.E.:.&.8.........  .."D....u#t...
....0...XB.#..<..(..<...XH.     #....H!...:...G...u..1   .......a.?....GTF  ...'^ .Z....p.`.......`.Y.O....(..  UZ.........Q.........g....h.......^=.X...k..Q..kE.}-
W.;...I.A`t....]=.UC..m@.(t....9/1,
&^%.K"G.....Q_..._.....]/jB..y.aQ0.&.?j..BQ..TGw.O..
_/........./.............k..I.).c.....$..fQ....h....\._r^cX.._%q......W...v......(....+..\?....bX...$...w.i.y.aQ0~...jk.q......s.......(.9h..9.......$.+B..-
2.y.."..`T.E&.....y.aQ0.J...ie.3.I.E..(.,U.eQ...e{.{..u.t."q..   ......s=?.b..I.E..&..Gi.!g.H./".WY....F..z]eQ...          .....QI.I*....B..a(\...y.aQ0*.bE"....?.......-
(Nr.dX..*.xH..!!E....W..O.GEY..<..(..D.D...mQ...D.(L...(Zq.e....c..`.p(Lzr..Dq#3.5.N..g.......j.".....L.@..a..R...O....%C....k-..*Eq.........<..
..        ....*9.'R..rc.`...\2J..8...y.aQ0..........=.x.T.iQ...2i..5.9.2,
&v.\??aEQ..)Qu...7..h.LZ.Z4..*..`b....   +
P.....O.G*..gf
....(..q...      -.._.6.....*..g'.....(..q6=%.Equ...K{|.E..87•–.U.E.....6OhQ.........I....q^eX.L.......E....O..uM.......W.........w.6......<p..X.~..-
3g.X.z...w............?|.p.....C•–'•=x..ez..g..j.C..z..G...E...Z....b..y.9.D.RXeP..f..M.......-..[..y..;w.e....s..u...(O..t..}.X.pa.m....[....9t..e.pr.v..T.....h...-
%....HII...
.../.I.#G..m.....5.q...{O..._.....\.|.I...l.2p~......j....[.....#.E..5.....{3g..MO+.6mZ.|}..      .\.<n......Z.WF.k...*MO...        |r•–
0.Y.f.c..b...b..U.....#.}....V..:t..o#p#. N.}........L.I..K...]..7.x..9...'.....}..j._.dI..q..7.b..9..
.|.o.N..i...  ....z..E.D......(V.Xax._~.e\.....  -.kS?2....N...3..(......o.*..5..@nD......[......^....-_VC.E...M.......]...M.4q}...4W..o...z*.....^[RRR\......=.b.J.y•–
+..3...Q.E.d..1..b.........X...U.e<......SQ...'.)..=z..]..S...   1.y.F[!...[..!C.o............o.]..f7m$
..W/.D..Z..l.....xc.._...|...f..m)
......z.1....+qgfwyVT....FIjSu.Qd..T.(.r..>}z 6...x)3j"....Q..h.n..}.M.F...A..
.6.6...5*.W....#\.....gO......j..C..b......5k.....@..|......=!.*'
.......~Z.&.:x...[..7.|3..d..([.U.V...L.`.......o..Q8..F.w..YYY5....dQ...y.?VLKLQ$=).
6.wd_/..m.S.....y)
....S.r../X. .8"#7.......@..J..i-...."..C..Q.B..Q..._!TQ.~...G...A....FU[.......r....D......W..oL.4.....z..(N..I8Q.w..(..e.'....V..g•–Q....3f.T..1.e
o.V.....j......]...+v..  ..I>.Q............S.c`a..'.U64.d..1*C.oT......5n....7o.<..  ..y0.7.E....s}_...._..C]Q....:..(.]*.Jo.oGq.z.IJ.t..         ......-.....u.GS•–
8F.....}./.hB
"..AS.\>..v.EZ.M[F-.nE.&?........k..RZ.h&....c:w.\..y..9..tH.}...eQL.0!`~}s.~..[Q|..W..hr......8?.
_."..7..S*..l.!
```

lets look for the interesting things



```
p=..f...K EK.......yy..1..."..D.y..?a.W.....;.A$E..h..0
eC~.....^.      MGry.7n\..j...s....V.E,..:..A\?L...u.......f-'^..}..RGJ/3.D...
.i..0F6.....F....fs/.....F+...0Z)..&c5. 5+....=<.n..W.....G.h........@.UTk...^...Yf.o....d.j...X.        2.
....N...gh...!...w.1....Z.Da&I%E..8...k.....>..6>.....b'
4...j.u...<.W^d,.Dq|.Nq.S....(?..xI.oR.....9.^.Q..a.d•–..d.6m....'.k.l...CF...IQ..V....(`Q..m.n..D......#.y      nD..&3Y....fp.s.o..*
pjQz..c...$..!WF.4..w..;5.....`.'......&
.y$.....5~•–.p..)..E...l.1=...@.u..l..V.'.8....V....n.....k...S.Q.....&..........z.N..[....v..wd...'...F...Y.8N...-
+W.V...u.;..h.|.p3.Q.....kD...u.........._..}..@3....2.tB..G.N.D.....5.n.+6[B."^h.....F7.9...mp4$.Ep.6..F...O...!.N...W..Sn......]..b..9=...8...s....W  !.+..-
1...,.|...1.....)X.LD93kHB..r....S\-..(........_....z.5.E../...r)..@.".9.1,
........!.T.S....KAi...<..(........E._...1•–.....s.;..t5...53b.@.r.bX.L.5A{54616d696c4354467b6c69746572616c6c795f695f686174655f796f755f61745f616c6c7d0a}....-
6..y...L1....GFh.S.@.r.bX.L\q.`....Oq'...uE.....".4DZr.bX.L|....,.EaU.h..Ff..o.....O..R.!
9/1,
&.9....M..%..D..J....n....!.8.1,
&!8.h..EQ..)q;.kSI....fG...1.....Q`.9..(.K.s.N...O.@_..  .Di.2.QU.+.....N..g....9.JMM}..K.Jt$....<."..e.....Hr.c........gvU.(?}.5..g..(w4....!Q...^....'.g.A....-
2....@s@G.      p....O•=D<E.F$.#.Lb.Q.   ...S.?%.DM....,.  .{6..^.6?......"-fgj1<Y.......m...~.a...:...E,&v..Y...Y."..].X..d.k^J.iR..........X..].....p.i...G..(•–
4...F.!...>....`Q0.,.  ..U..;W....z)      ....7X....1..S........h..6f....c...  ....6m
...=(f...@+...X..%...|....R.9.'.M..u....q...#
.:.<.>.@.B.D.F.....*mc.
;.....
.d....m.U.       ."dY<F.)+..
q..Vq}f_Q...H....?.y!.D...b.bXP..m.q....(B.[.....s';l......./.
.....,.!r.
....k.S.aR..:..(..X..<......G8..O..5.9•=.A.E.I.M.Q..g`QD
l).c........p...b..ib..q..        ....P..ZDP..yt...@.@.@.@.A,ALAlA....7.E.(((.&.....       6rgQ.T.....@.......N.(.A.  ..E.....i...  .......,.|..@&...c....    ..-
3Y.O,.cI....g.YQ........,.L.l+$..._Ea...G..}.......
...e....sEFF.2.E.....^bj.J..t/?co@.C.C.DYD.D.D.EY..5.X.>...@.....D*.L4#.'j.....at'*.@.....L#.W.....Z.L...t...ke..E..p...4.G,#&.........Z....^...W|,      \...,c..{•–
2..V..ke~......p.E....I.'r...8.7..x..O<N....W..K...$p.u...J(wk1...3Zk1d..Sr..s.E..(....,b61..A.  ^$~C<..=.e.3.
......]\K.Q-......Zl.....Z.bQ.!
n.gB.....IL.Nk..~...E-.....DL..H&.....)....b..G.G..p.`..e.2Q..$p-/..a..N.&......$6.>....a....W.......o......a|  ....Q..~..N{.E.0..B.4J.5..W.E.0>.F
Q..A..).....a.C....=......-..`....6CJ'...D.v..d.aQ0L.wt.          A.G...aQ0L.....
w8..B;...aX.......Q`!    |..N+.E.0•–....D.N.e....i..(8..&(.zD.F=N...?..L.>\s+S!....IEND.B`.
```

#lookdeeper

copy it ⟶ decode

:)

```
┌──(root💀kali)-[/home/sam/tmp/needed]
└─# python3 -c
'print(bytearray.fromhex("54616d696c4354467b6c69746572616c6c795f695f686174655f796f755f61745f616c6c7d0a").decode

TamilCTF{literally_i_hate_you_at_all}
```

YEP

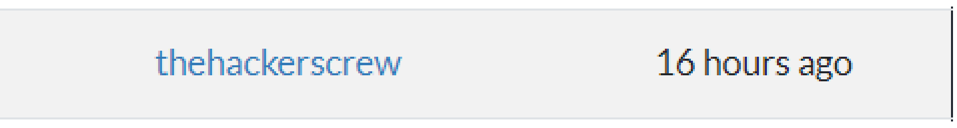
Flag:TamilCTF{literally_i_hate_you_at_all}

one_liner :

`python3 -c 'print(bytearray.fromhex("54616d696c4354467b6c69746572616c6c795f695f686174655f796f755f61745f616c6c7d0a").decode())'`

That's all

First Blood:



thehackerscrew 16 hours ago

@cyberpj