So you want to write a Tor pluggable transport

David Fifield
<dcf@torproject.org>

This is your Tor.

```
16 03 01 00 e4 01 00 00  e0 03 01 52 c0 22 24 61 ........ ...R."$a  ← TLSv1.0 Client Hello
a7 fd 88 c5 9e 87 d7 14  6d 0b 43 4e eb 24 1e 8d ........ m.CN.$..
e5 32 37 2e 4d 2a 3f cc  9e 0b 1e 00 00 48 c0 0a .27.M*?. .....H..  ← Ciphersuites
c0 14 00 88 00 87 00 39  00 38 c0 0f c0 05 00 84 .......9 .8......
00 35 c0 07 c0 09 c0 11  c0 13 00 45 00 44 00 33 .5...... ...E.D.3
00 32 c0 0c c0 0e c0 02  c0 04 00 96 00 41 00 04 .2...... .....A..
00 05 00 2f c0 08 c0 12  00 16 00 13 c0 0d c0 03 .../.... ........
fe ff 00 0a 00 ff 01 00  00 6f 00 00 00 22 00 20 ........ .o...".
00 00 1d 77 77 77 2e 72  32 34 6d 78 70 77 73 73 ...www.r 24mxpwss  ← Server name
34 6e 77 32 33 6f 72 77  6c 65 61 63 2e 63 6f 6d 4nw23orw leac.com
```

This is your Tor.

```
16 03 01 00 e4 01 00 00  e0 03 01 52 c0 22 24 61 ........ ...R."$a  ← TLSv1.0 Client Hello
a7 fd 88 c5 9e 87 d7 14  6d 0b 43 4e eb 24 1e 8d ........ m.CN.$..
e5 32 37 2e 4d 2a 3f cc  9e 0b 1e 00 00 48 c0 0a .27.M*?. .....H..  ← Ciphersuites
c0 14 00 88 00 87 00 39  00 38 c0 0f c0 05 00 84 .......9 .8......
00 35 c0 07 c0 09 c0 11  c0 13 00 45 00 44 00 33 .5...... ...E.D.3
00 32 c0 0c c0 0e c0 02  c0 04 00 96 00 41 00 04 .2...... .....A..
00 05 00 2f c0 08 c0 12  00 16 00 13 c0 0d c0 03 .../.... ........
fe ff 00 0a 00 ff 01 00  00 6f 00 00 00 22 00 20 ........ .o...".
00 00 1d 77 77 77 2e 72  32 34 6d 78 70 77 73 73 ...www.r 24mxpwss  ← Server name
34 6e 77 32 33 6f 72 77  6c 65 61 63 2e 63 6f 6d 4nw23orw leac.com
```

This is your Tor on obfs3.

```
86 14 46 4a b7 27 c1 07  9d 9a 21 b7 18 a0 f4 91 ..FJ.'.. ..!.....  ← Random junk
c7 39 d5 48 e7 31 f5 d6  6d 98 81 15 1d 2c f4 93 .9.H.1.. m....,..
33 e3 91 07 ec fd d7 be  a0 d5 df 6e b9 86 8f b7 3....... ...n....
91 b1 f2 80 ea ac 89 8f  0e b0 ec 78 16 ac 6f f0 ........ ...x..o.
34 c1 d5 e8 88 14 08 40  63 42 09 b3 72 64 a3 b9 4......@ cB..rd..
90 7c e1 69 23 40 07 57  73 9d 25 6a ac ca e9 4d .|.i#@.W s.%j...M
ca a6 f4 4c ac 5a aa 37  6a 66 2a 95 64 6d a1 56 ...L.Z.7 jf*.dm.V
```

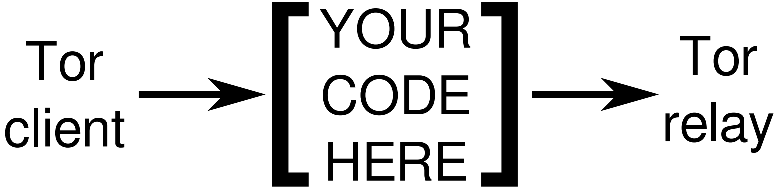
This is your Tor.

```
16 03 01 00 e4 01 00 00  e0 03 01 52 c0 22 24 61 ........ ...R."$a  ← TLSv1.0 Client Hello
a7 fd 88 c5 9e 87 d7 14  6d 0b 43 4e eb 24 1e 8d ........ m.CN.$..
e5 32 37 2e 4d 2a 3f cc  9e 0b 1e 00 00 48 c0 0a .27.M*?. .....H..  ← Ciphersuites
c0 14 00 88 00 87 00 39  00 38 c0 0f c0 05 00 84 .......9 .8......
00 35 c0 07 c0 09 c0 11  c0 13 00 45 00 44 00 33 .5...... ...E.D.3
00 32 c0 0c c0 0e c0 02  c0 04 00 96 00 41 00 04 .2...... .....A..
00 05 00 2f c0 08 c0 12  00 16 00 13 c0 0d c0 03 .../.... ........
fe ff 00 0a 00 ff 01 00  00 6f 00 00 00 22 00 20 ........ .o...". 
00 00 1d 77 77 77 2e 72  32 34 6d 78 70 77 73 73 ...www.r 24mxpwss  ← Server name
34 6e 77 32 33 6f 72 77  6c 65 61 63 2e 63 6f 6d 4nw23orw leac.com
```

This is your Tor on obfs3.

```
86 14 46 4a b7 27 c1 07  9d 9a 21 b7 18 a0 f4 91 ..FJ.'.. ..!.....  ← Random junk
c7 39 d5 48 e7 31 f5 d6  6d 98 81 15 1d 2c f4 93 .9.H.1.. m....,..
33 e3 91 07 ec fd d7 be  a0 d5 df 6e b9 86 8f b7 3....... ...n....
91 b1 f2 80 ea ac 89 8f  0e b0 ec 78 16 ac 6f f0 ........ ...x..o.
34 c1 d5 e8 88 14 08 40  63 42 09 b3 72 64 a3 b9 4......@ cB..rd..
90 7c e1 69 23 40 07 57  73 9d 25 6a ac ca e9 4d .|.i#@.W s.%j...M
ca a6 f4 4c ac 5a aa 37  6a 66 2a 95 64 6d a1 56 ...L.Z.7 jf*.dm.V
```

Any questions?



Tor client

YOUR CODE HERE

Tor relay

Pluggable transport libraries

- pyptlib for Python
- goptlib for Golang
- liballium for C

Further reading

- Pluggable transports wiki page https://trac.torproject.org/projects/tor/wiki/doc/PluggableTransports
- Pluggable transports specification (pt-spec.txt)
- tor-dev@lists.torproject.org
- #tor-dev on irc.oftc.net
  (PT meetings every other Friday)
- "Design of a blocking-resistant anonymity system" (23c3) and "How goverments have tried to block Tor" (28c3)

Come hack with us!