StegoTorus

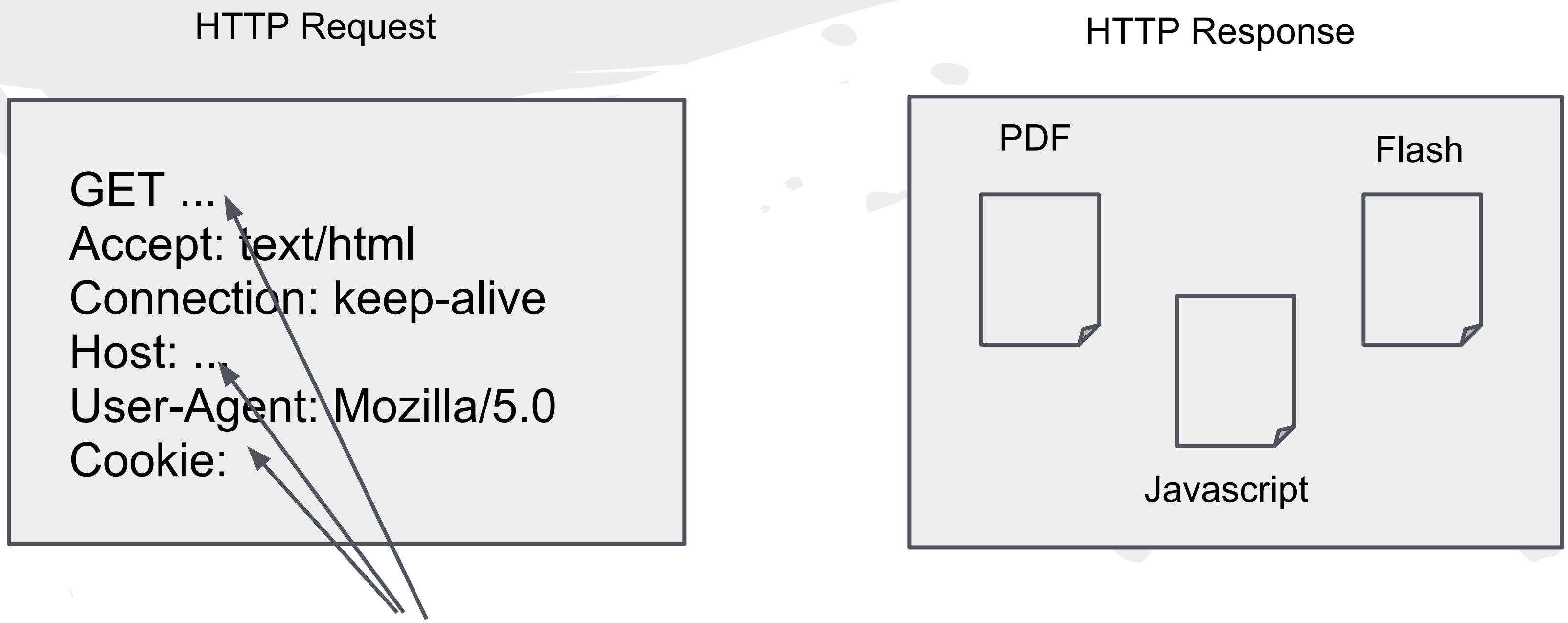
Camouflage for Tor

You Can't Take Our Freedom!

- Governments can easily inspect or manipulate most traffic that crosses their borders
- In 2011, Iran tried to block Tor traffic by scanning TLS handshakes.
- In 2012, Iran blocked all outbound https connections to many websites.

Let's Pretend

- Make Tor traffic look like HTTP



HTTP Request

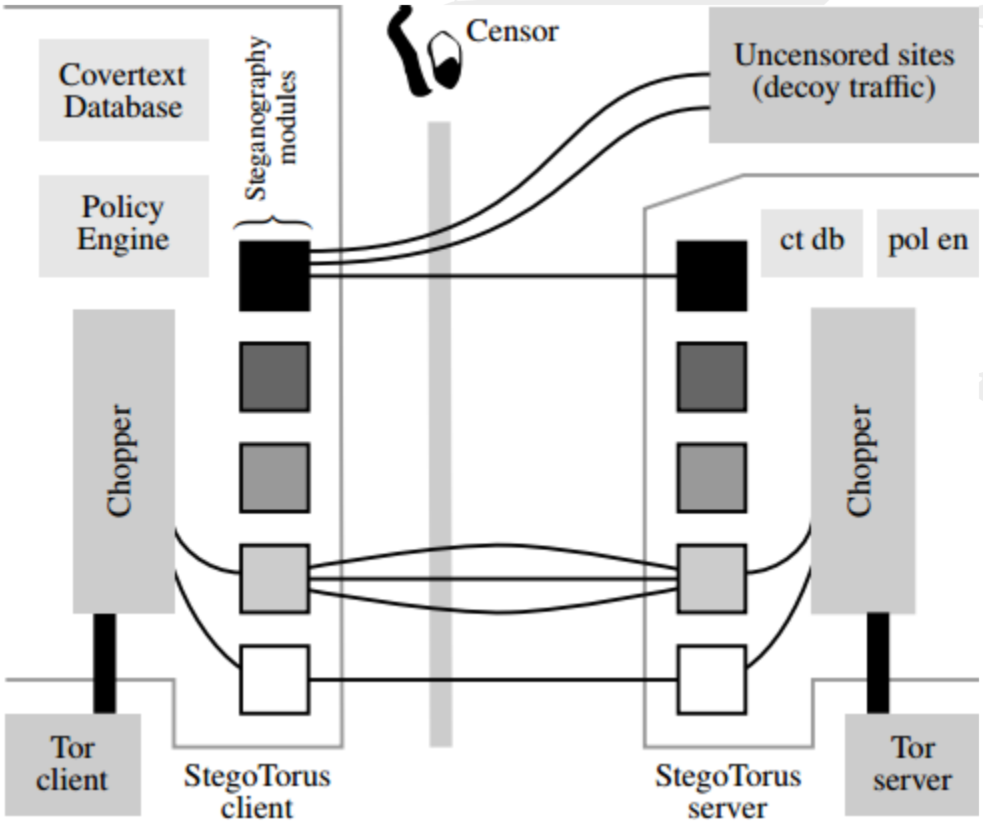
```
GET ...
Accept: text/html
Connection: keep-alive
Host: ...
User-Agent: Mozilla/5.0
Cookie:
```

HTTP Response

Insert encoded fragments of TOR message here

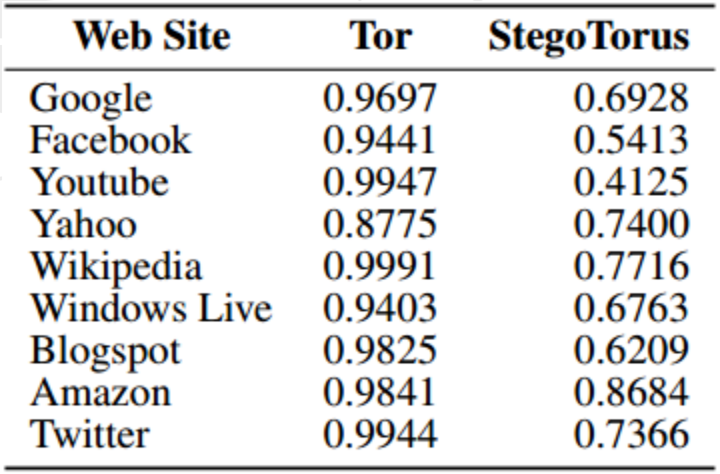
Sample files are mutated into carriers of encoded fragments of TOR message

Two Face


Covertext Database
Policy Engine
Steganography modules
Censor
Uncensored sites (decoy traffic)
ct db
pol en
Chopper
Chopper
Tor client
StegoTorus client
StegoTorus server
Tor server

Did I Fool You?

- No predictable packet sizes like TOR
- Maintain format rules
- Avoid probability classifiers



Web Site	Tor	StegoTorus
Google	0.9697	0.6928
Facebook	0.9441	0.5413
Youtube	0.9947	0.4125
Yahoo	0.8775	0.7400
Wikipedia	0.9991	0.7716
Windows Live	0.9403	0.6763
Blogspot	0.9825	0.6209
Amazon	0.9841	0.8684
Twitter	0.9944	0.7366