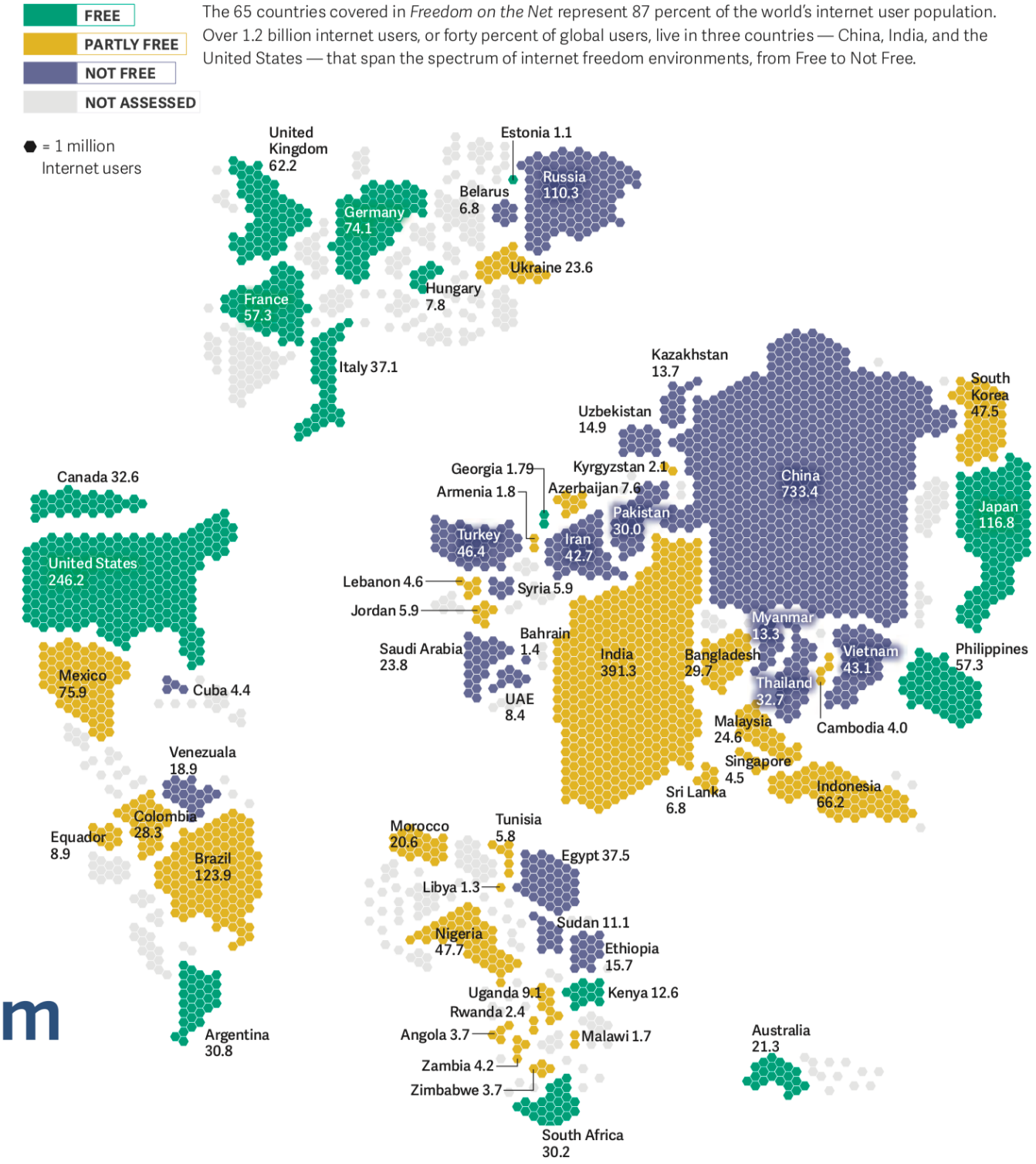
An ISP-Scale Deployment of TapDance

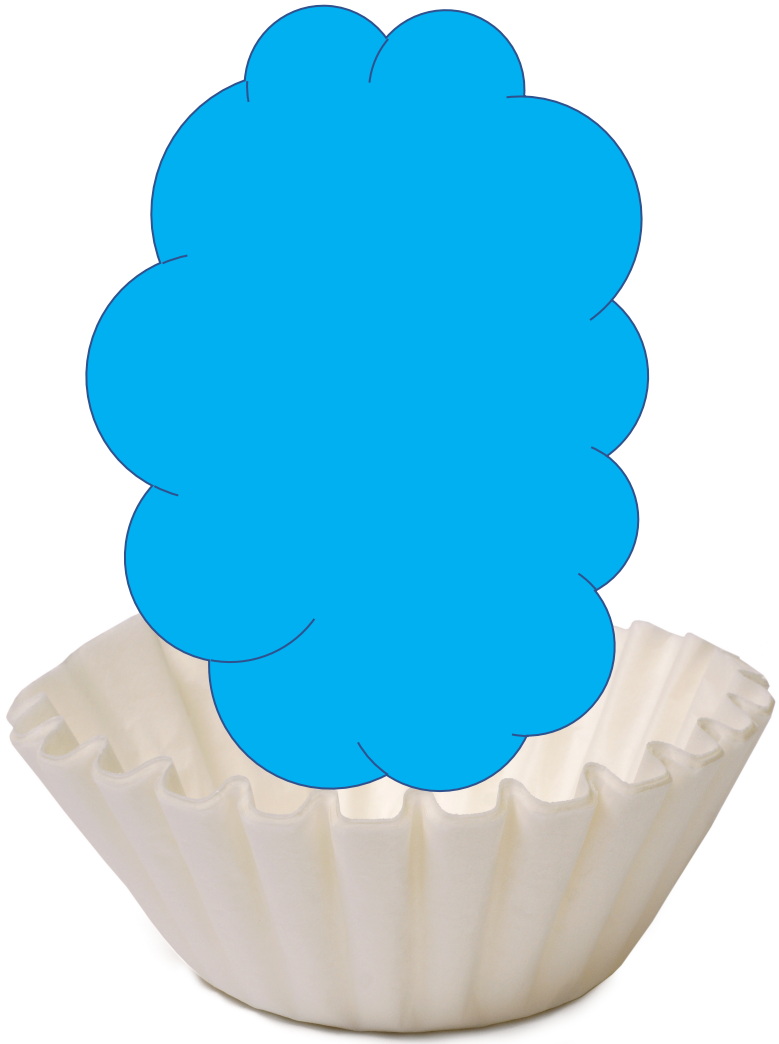
Presented by Nikita Borisov (@nikitab)

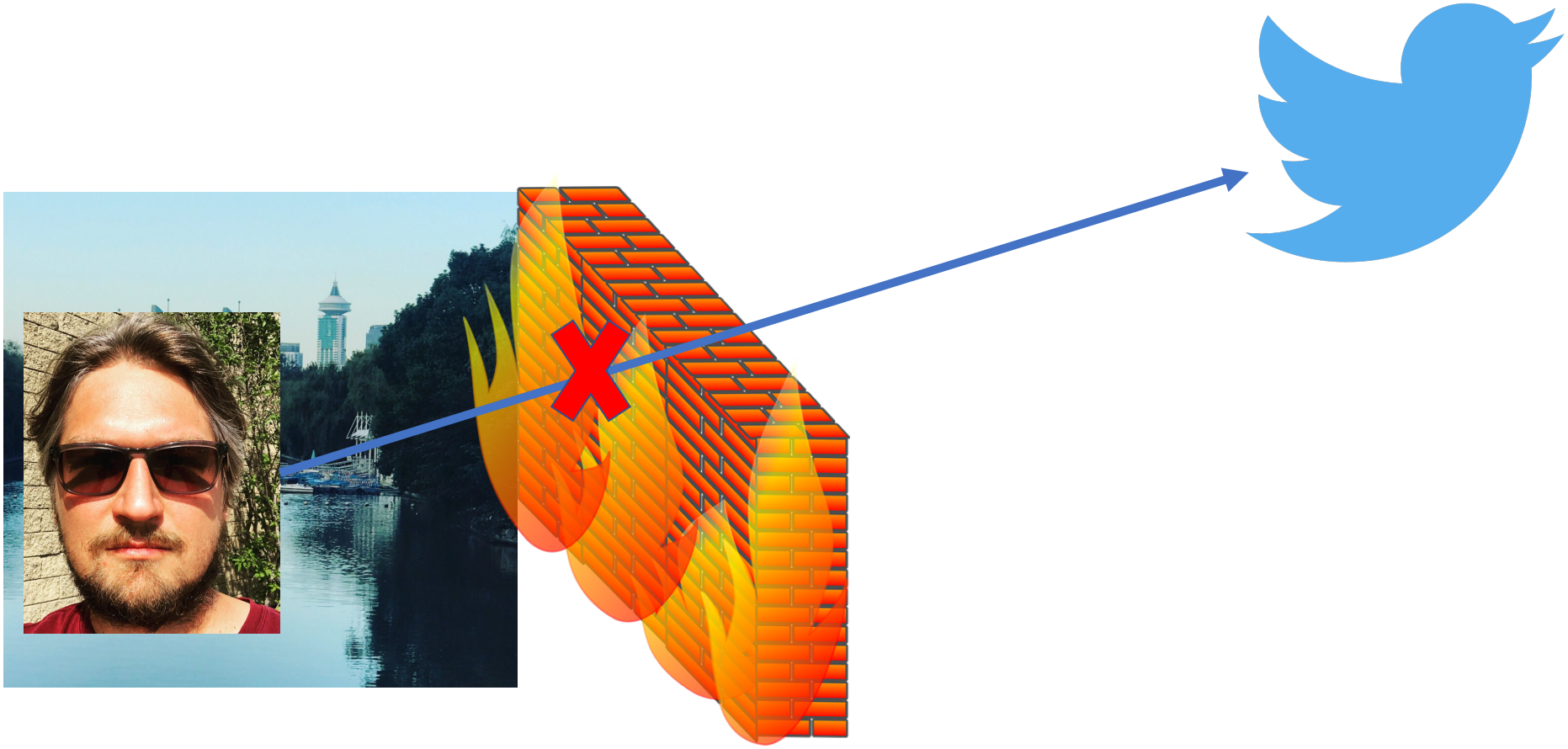
https://refraction.network/

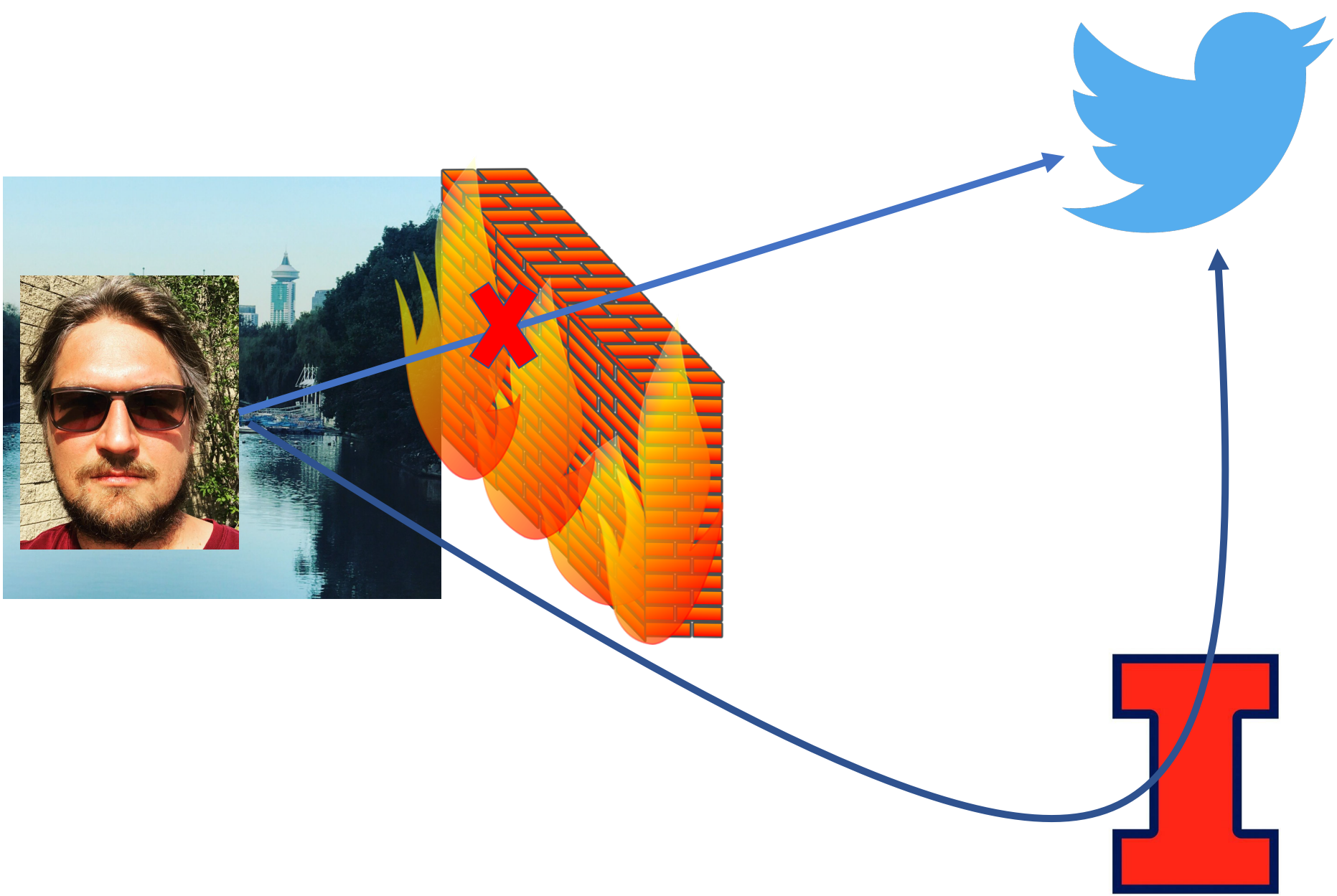

FREE
PARTLY FREE
NOT FREE
NOT ASSESSED
= 1 million Internet users
The 65 countries covered in *Freedom on the Net* represent 87 percent of the world's internet user population. Over 1.2 billion internet users, or forty percent of global users, live in three countries — China, India, and the United States — that span the spectrum of internet freedom environments, from Free to Not Free.
United Kingdom 62.2
Estonia 1.1
Russia 110.3
Belarus 6.8
Germany 74.1
Ukraine 23.6
Hungary 7.8
France 57.3
Italy 37.1
Kazakhstan 13.7
South Korea 47.5
Uzbekistan 14.9
Georgia 1.79
Kyrgyzstan 2.1
China 733.4
Armenia 1.8
Azerbaijan 7.6
Japan 116.8
Pakistan 30.0
Turkey 46.4
Iran 42.7
Canada 32.6
Lebanon 4.6
Syria 5.9
United States 246.2
Jordan 5.9
Myanmar 13.3
Bahrain 1.4
Saudi Arabia 23.8
India 391.3
Bangladesh 29.7
Vietnam 43.1
Philippines 57.3
Mexico 75.9
Cuba 4.4
UAE 8.4
Thailand 32.7
Cambodia 4.0
Malaysia 24.6
Venezuala 18.9
Singapore 4.5
Sri Lanka 6.8
Indonesia 66.2
Colombia 28.3
Morocco 20.6
Tunisia 5.8
Equador 8.9
Brazil 123.9
Egypt 37.5
Libya 1.3
Sudan 11.1
Nigeria 47.7
Ethiopia 15.7
Uganda 9.1
Kenya 12.6
Rwanda 2.4
Angola 3.7
Malawi 1.7
Australia 21.3
Zambia 4.2
Zimbabwe 3.7
Argentina 30.8
South Africa 30.2
Freedom House

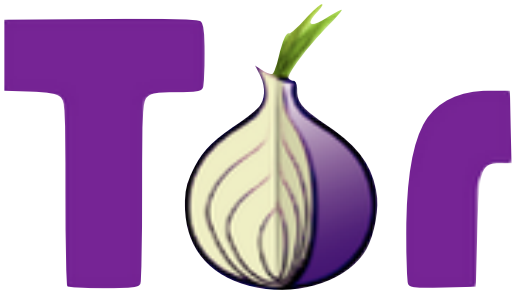
Internet Filtering

- Applies at many layers
  - DNS manipulation
  - BGP manipulation
  - DPI / content inspection
  - Packet filtering: IP/port









Anonymizer®

Ultrasurf

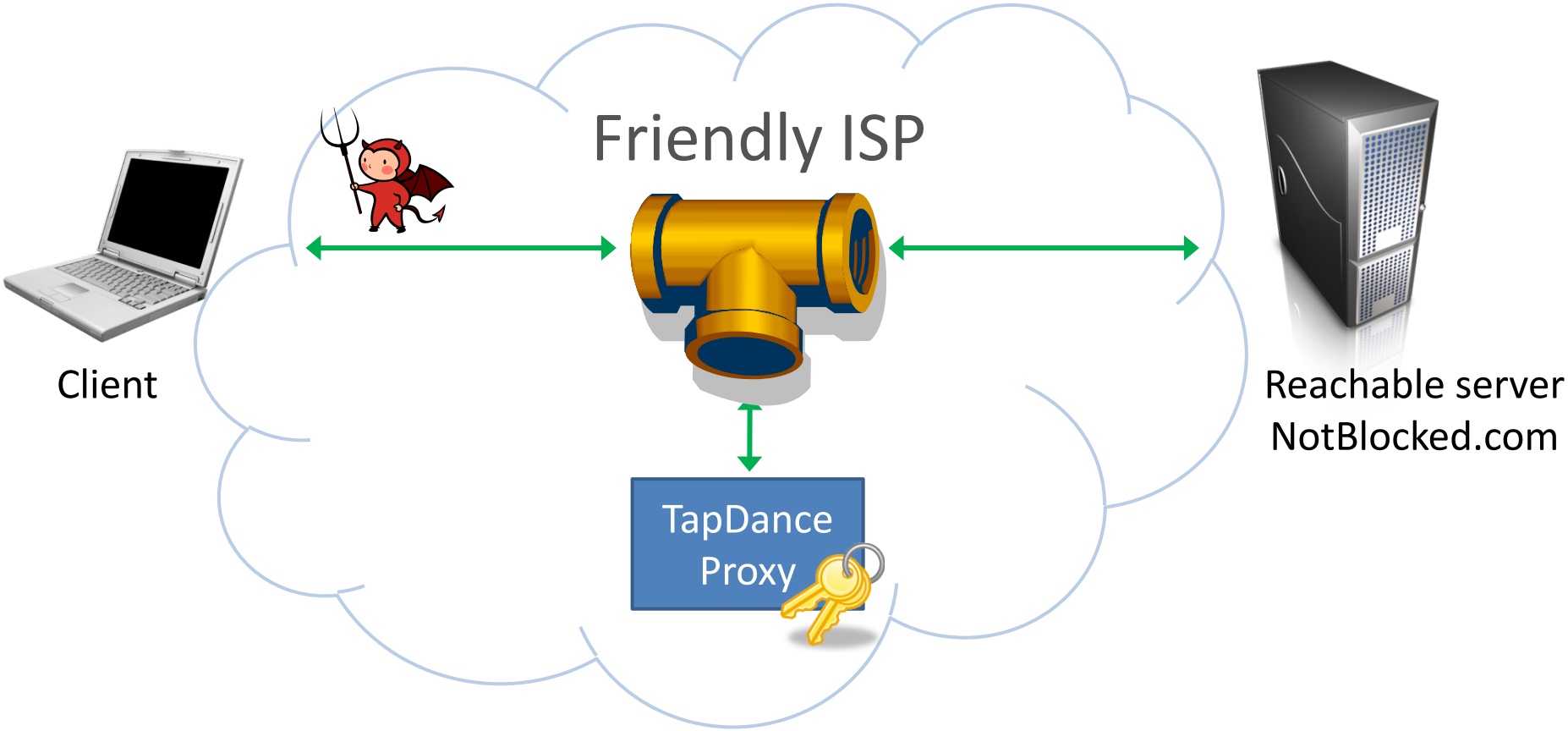
PRIVACY. SECURITY. FREEDOM.

psiphon

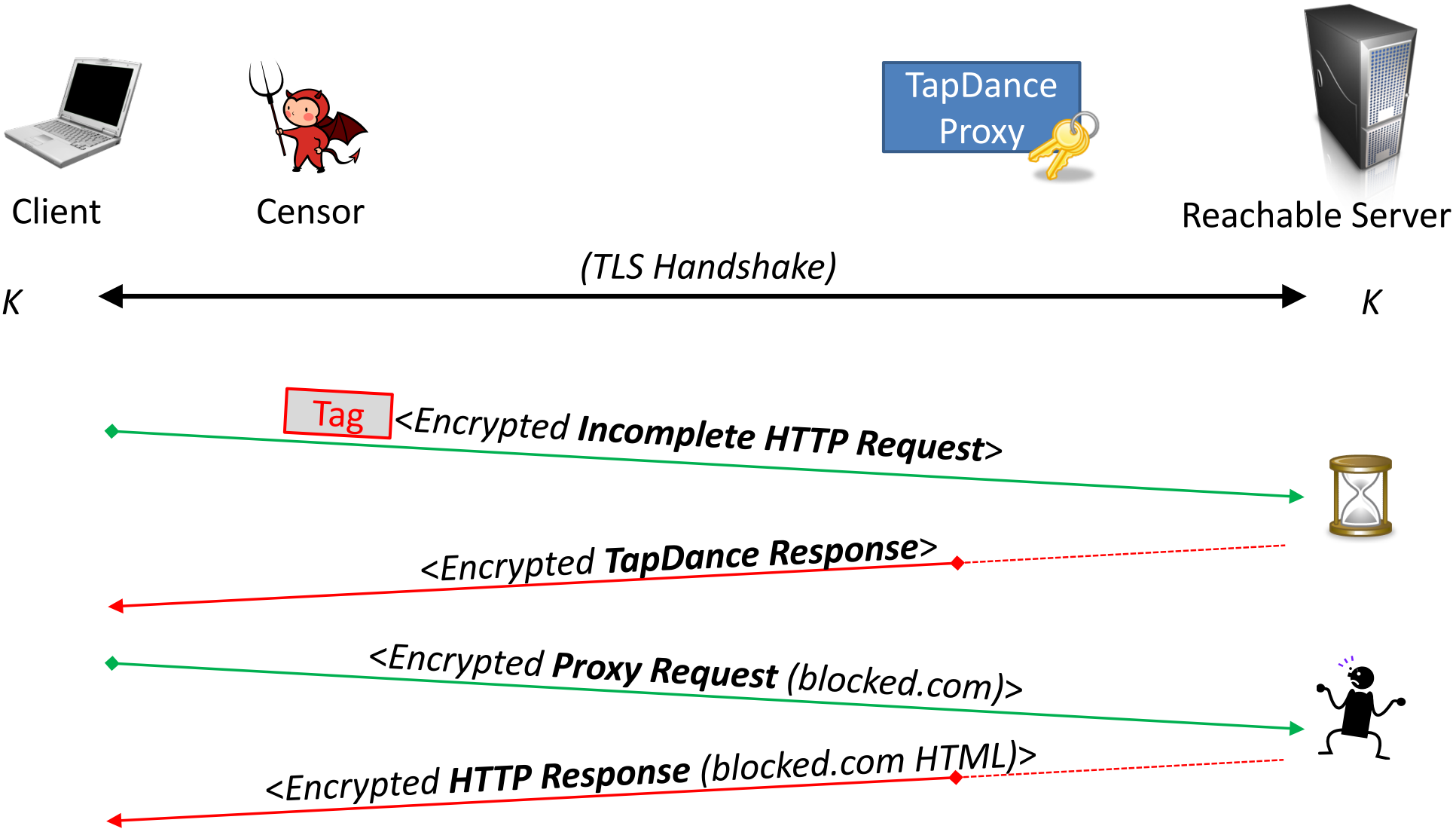
Cat-and-mouse game

- Censors **identify** and **block** proxies
- Circumventors **deploy** and **distribute** new proxies
- Advantage if proxies are:
  - Harder to find
  - Faster to deploy
  - Harder to block
  - Easier to distribute

TapDance: End-to-Middle Anticensorship without Flow Blocking



TapDance Protocol Overview

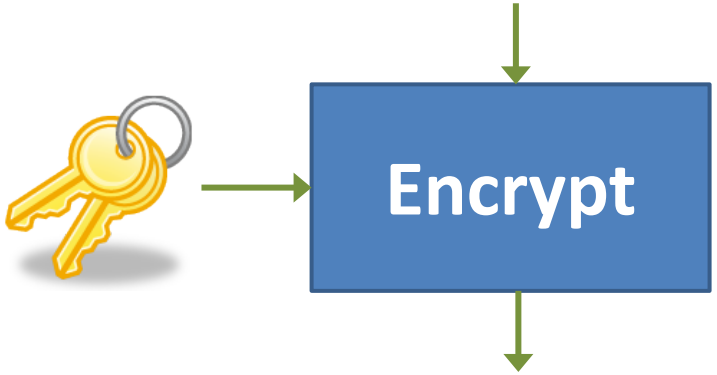


Incomplete HTTP request example

GET / HTTP/1.1\r\n

Host: www.site.com\r\n

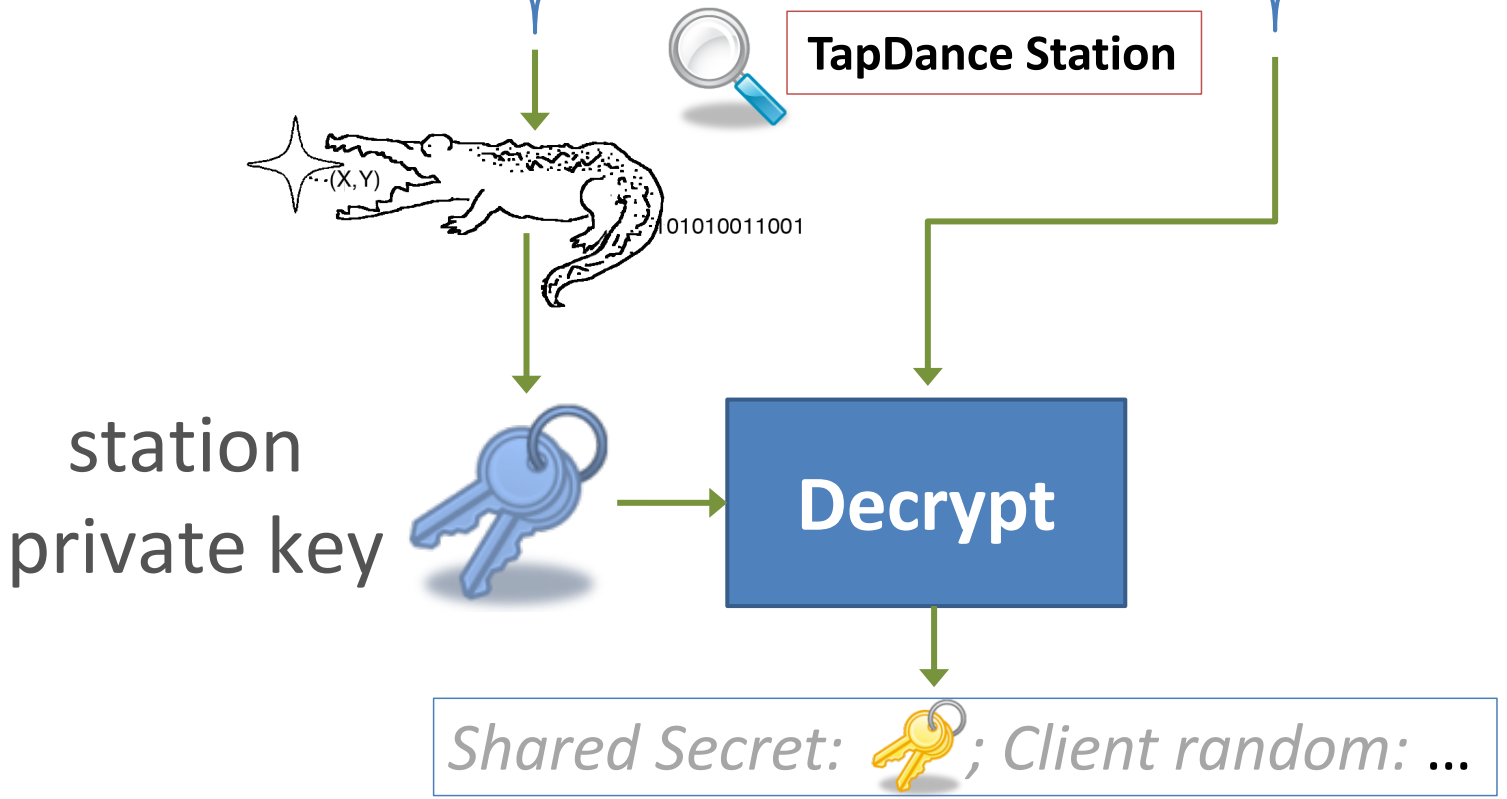
X-Ignore: u]DhsYGxVxEvuZEhESta…\r\n

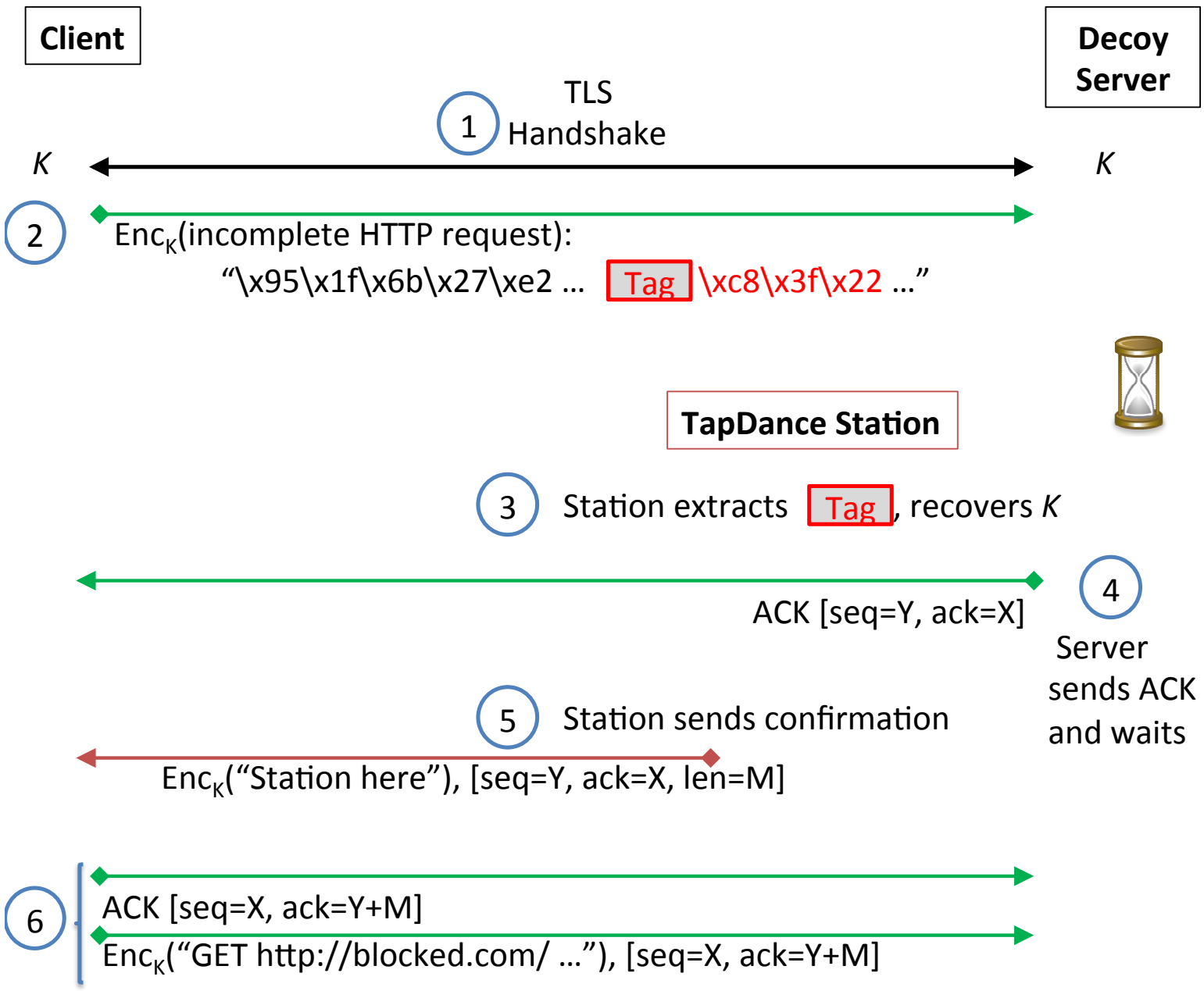


\x1e\x91\xb2\xce\x94\x8a\x6b\x3c\x78\x8c\x6f\x03
\x5e\xef\x97\x34\xf1\x2e\xc6\xe6\x7f\x10\xc8\x46
\xf9\x25\x6a\x0c\xff\x6d\x38 … \x70\xd7\x2c\x63 …

Incomplete HTTP request example

\x1e\x91\xb2\xce\x94\x8a\x6b\x3c\x78\x8c\x6f\x03
\x5e\xef\x97\x34\xf1\x2e\xc6\xe6\x7f\x10\xc8\x46
\xf9\x25\x6a\x0c\xff\x6d\x38 … \x70\xd7\x2c\x63 …



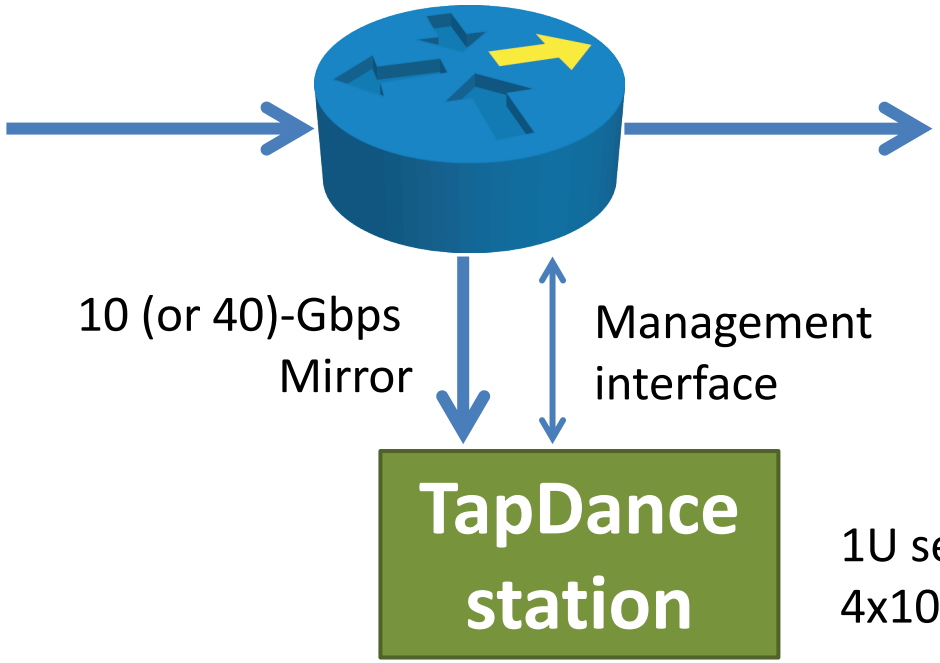

Client
Decoy Server
1
TLS Handshake
K
K
2
Enc_K(incomplete HTTP request):
"\x95\x1f\x6b\x27\xe2 … Tag \xc8\x3f\x22 …"
TapDance Station
3
Station extracts Tag, recovers K
ACK [seq=Y, ack=X]
4
Server sends ACK and waits
5
Station sends confirmation
Enc_K("Station here"), [seq=Y, ack=X, len=M]
6
ACK [seq=X, ack=Y+M]
Enc_K("GET http://blocked.com/ …"), [seq=X, ack=Y+M]

TapDance Trial Deployment

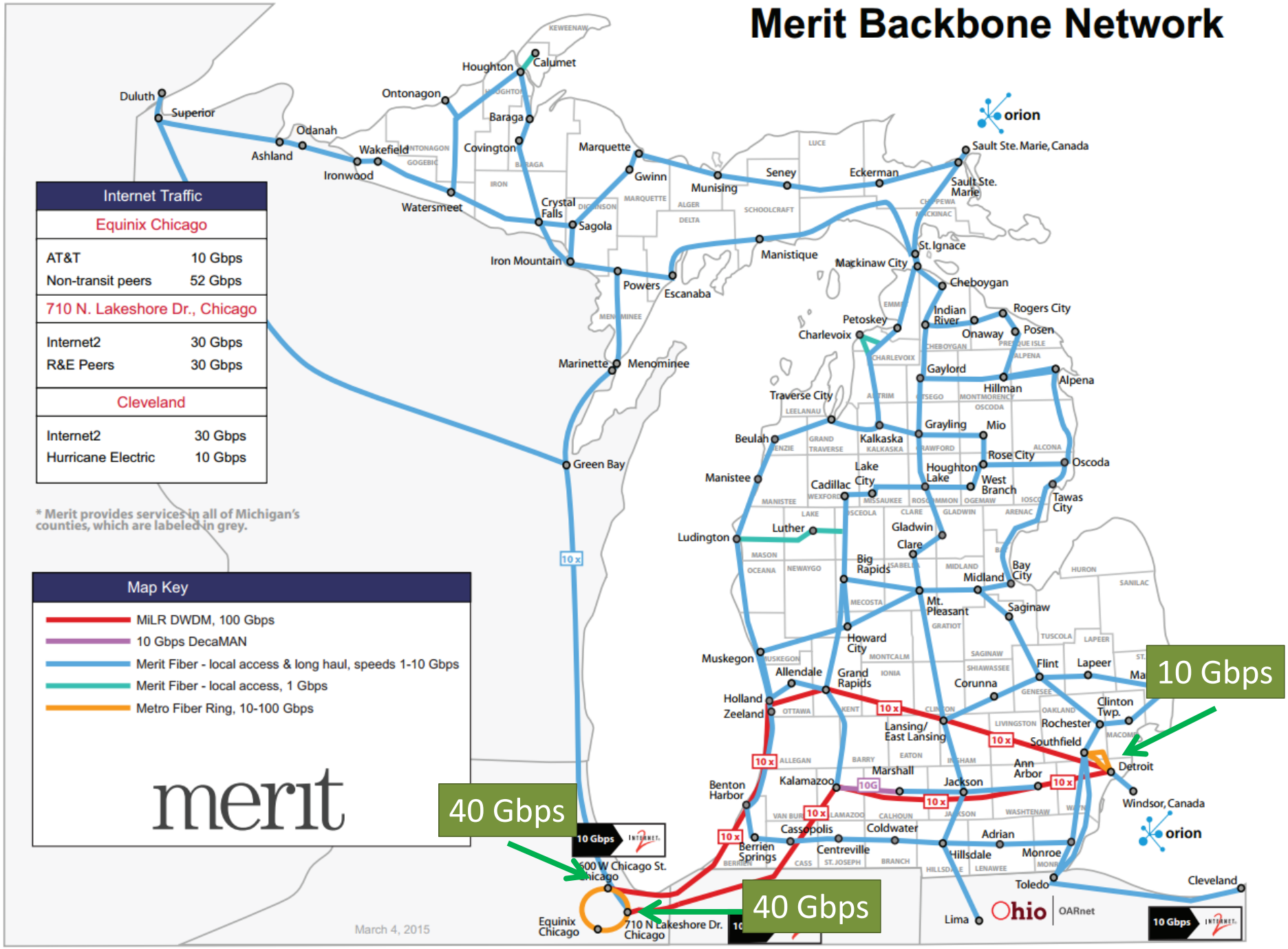
- Worked with two mid-size ISPs:

merit NETWORK

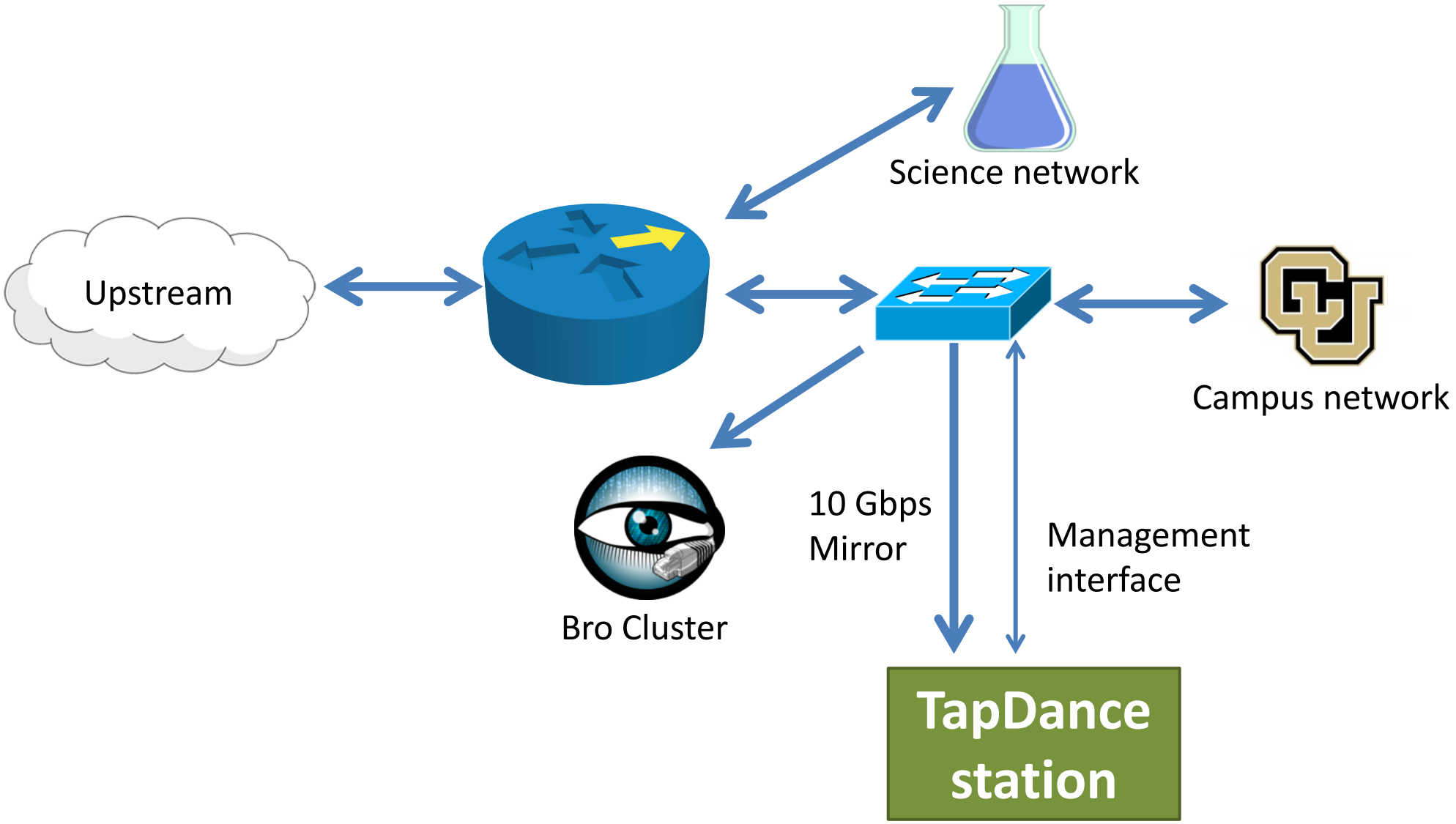
University of Colorado Boulder



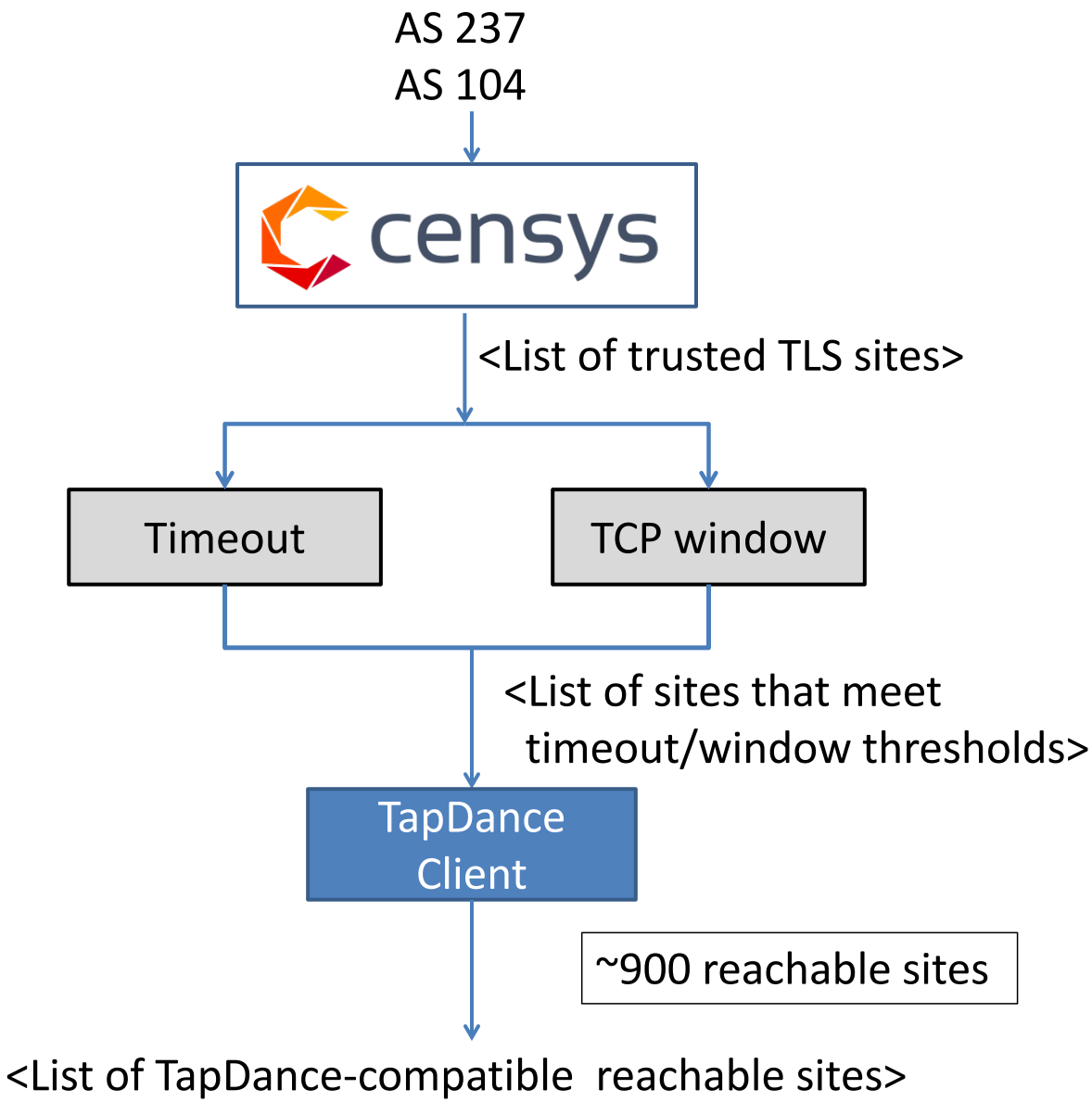
Merit Backbone Network



University of Colorado Network

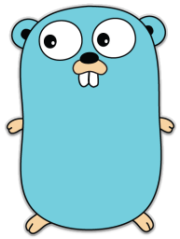


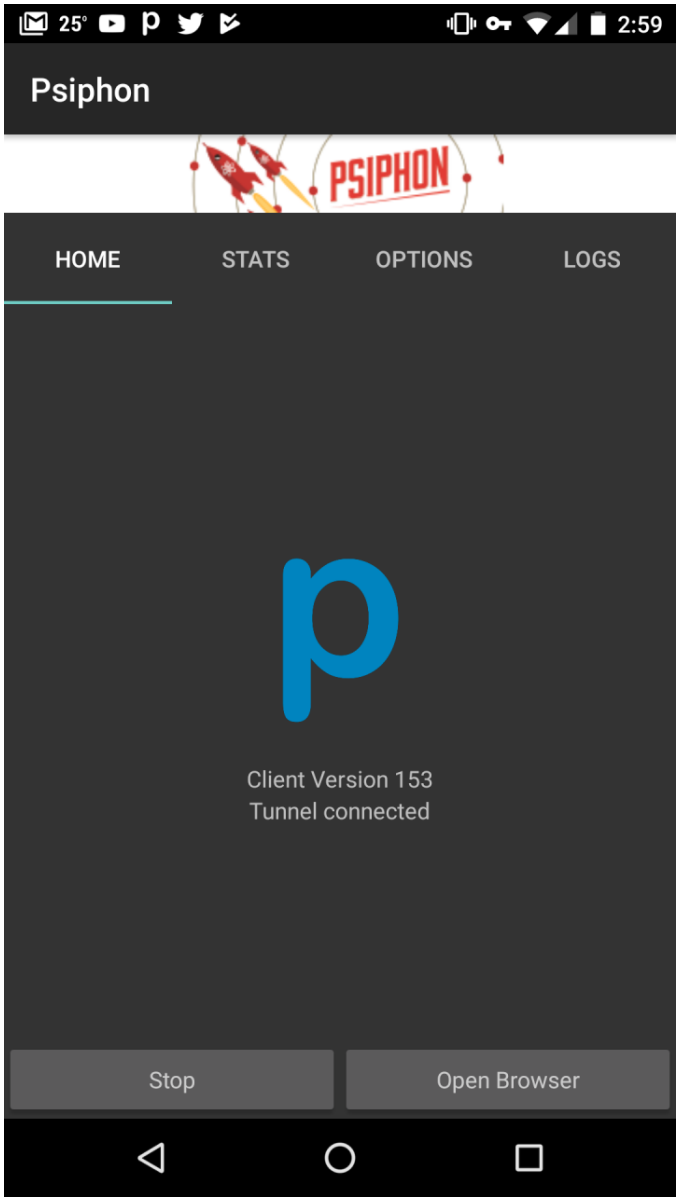
Reachable site discovery



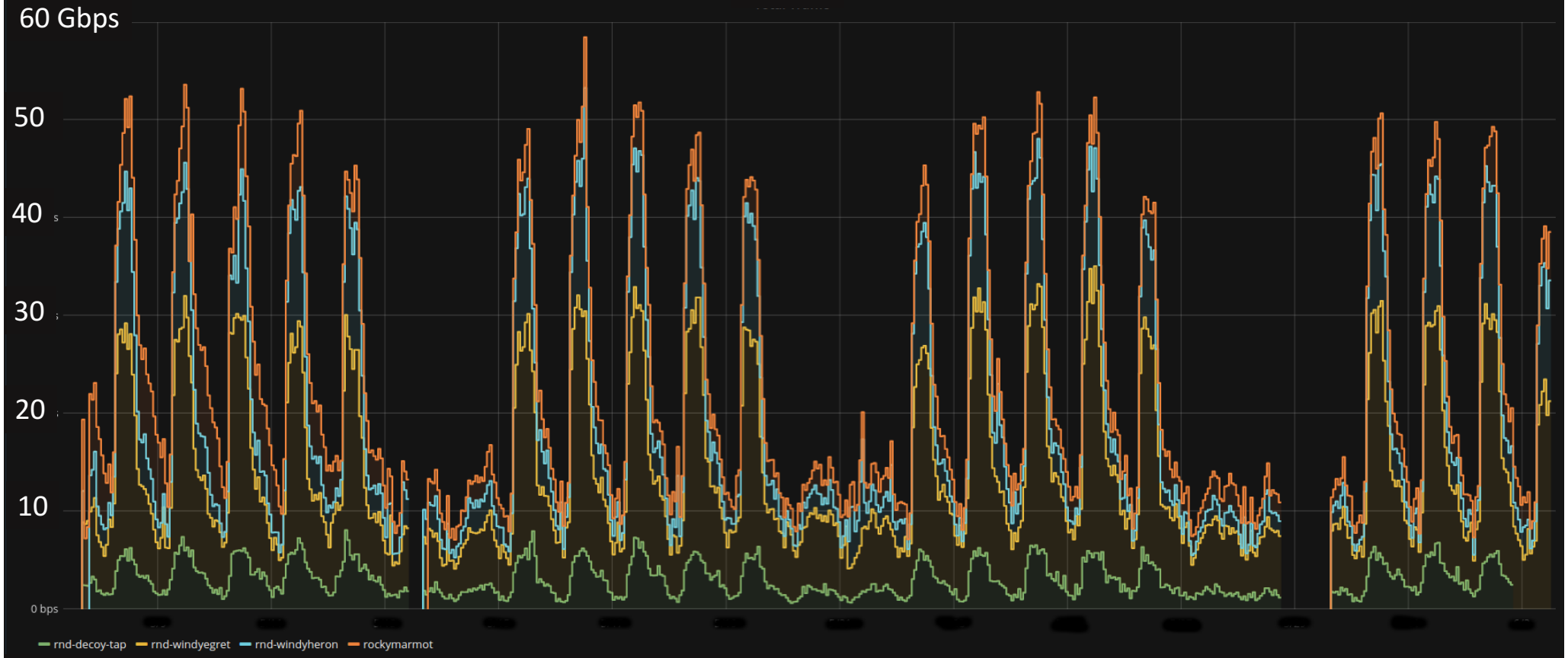
TapDance client

- 100% in **Go**
- Partnered with **Psiphon**
  - Integrated TapDance in Psiphon's Android app
  - Deployed to ~70K users in censored countries via remote update

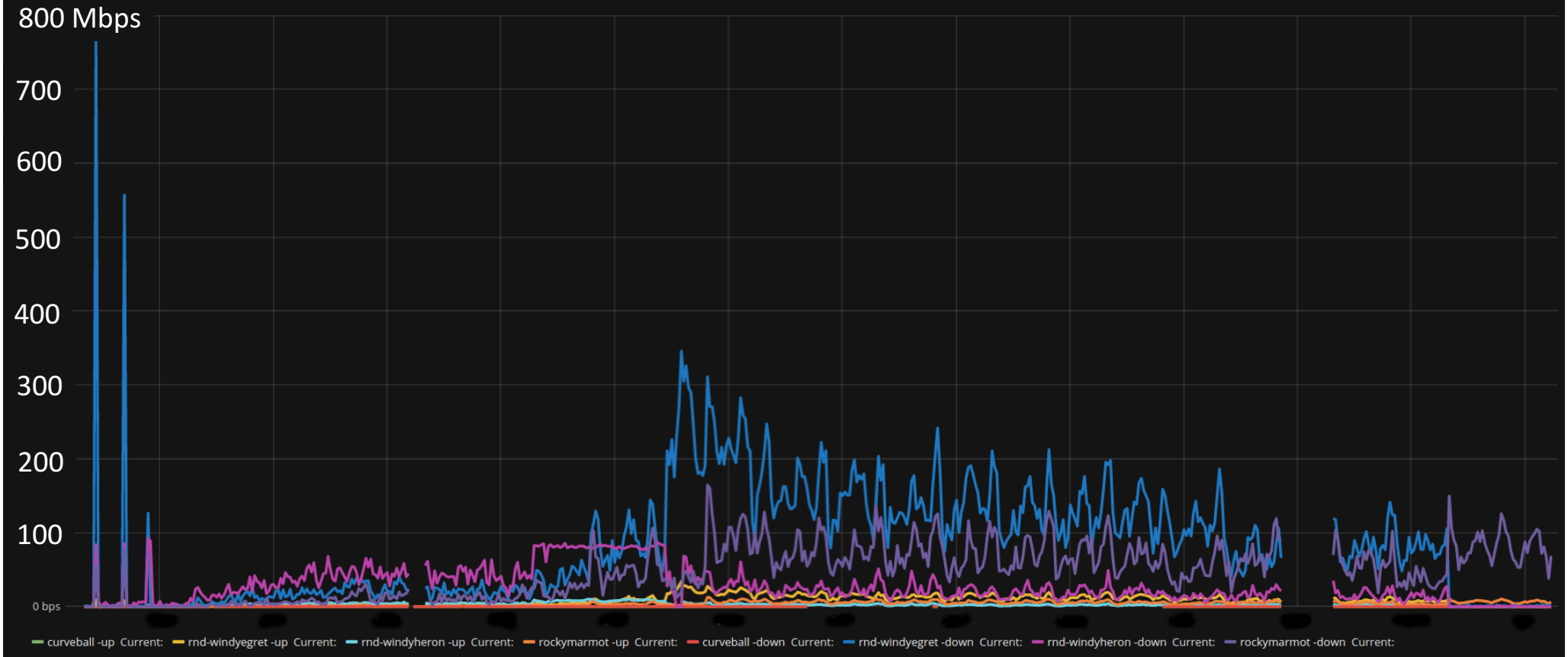




Total traffic



User traffic



Detectability

- A TapDance connection looks *different* from regular web browsing
  - DNS request
  - Connection scheduling
  - TLS negotiation (ClientHello, SNI)
  - HTTP request sizes

Detectability

- A TapDance connection looks *different* from regular web browsing
  - DNS request
    - DoH/DoT
  - Connection scheduling
    - QUIC / ORIGIN Frame
  - TLS negotiation (ClientHello, SNI)
    - Encrypted SNI
  - HTTP request/response sizes
    - HTTP/2 PUSH

Detectability

- A TapDance connection looks *different* from regular web browsing
  - DNS request
    - DoH/DoT
  - C
  - TLS negotiation (ClientHello, SNI)
    - Encrypted SNI
  - HTTP request/response sizes
    - HTTP/2 PUSH

Privacy from network observers makes censorship harder!

Looking for new ISP partners!

An ISP-Scale Deployment of TapDance

https://refraction.network/

merit NETWORK

University of Colorado Boulder

University of Michigan

Illinois
University of Illinois at Urbana-Champaign

Raytheon