Tracking Targets Through Proxies & Anonymizers (and the air speed velocity of an unladen swallow)

Also known as: TTTPaAatasvoaus

CLASSIFICATION

- Classification of this briefing is:

TS//SI//REL 5EYES

Agenda Items

- The issue at hand…(proxies, anonymizers & TOR, oh my!)
- What we do about, and how we approach, this issue…
- A couple examples of tracking targets through anonymizers (AnchorFree & Tor)
- Closing remarks and questions

Up Front Caveat

Before we begin this briefing, I want to set the stage by saying that there is no silver bullet for tracking target communications through anonymizers. Any methodology set forth in this briefing requires both manual analysis and (generally) luck.

With that out of the way…

The issue at hand…(proxies, anonymizers & Tor, oh my!)

- Targets generally don't like to have their communications tracked by government agencies or filtered by national firewalls.
- If they are tech-savvy enough, they will use anonymizers to try to mask their real IP/ location.
- This generally makes for sad analysts. ☹

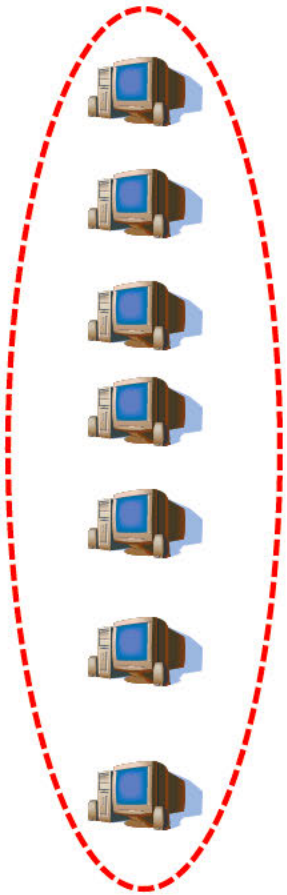
What we do about the issue at hand…

- The only way to track communications through anonymizers is if you understand how those anonymizers work. If you don't know what the traffic looks like, how will you recognize it in SIGINT?
- Generally our process is as follows:
  - Identify new proxy/anonymizer
  - Research/use anonymizer, document what happens, what does traffic look like, what client traffic does it pass through(if any)?
  - Create fingerprints in SIGINT to identify such proxy traffic
  - Correlate proxy traffic with known target activity

Anchorfree

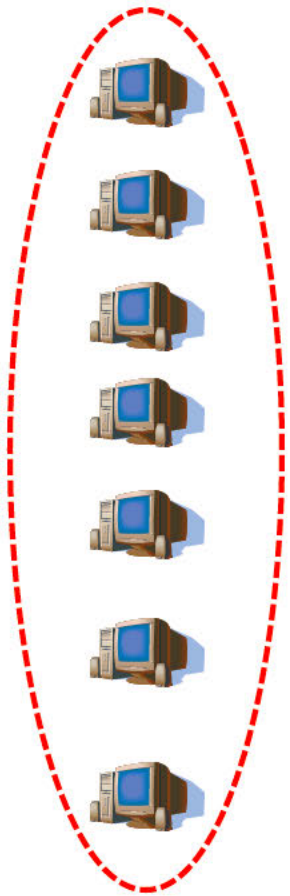
Anchorfree

AnchorFree owns a bunch of servers on the Internet.



Anchorfree

AnchorFree owns a bunch of servers on the Internet.

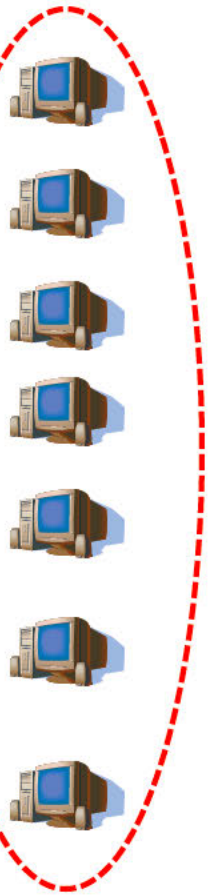


Then you have a user that downloads Hotspot Shield to proxy their traffic…

Anchorfree

AnchorFree owns a bunch of servers on the Internet.

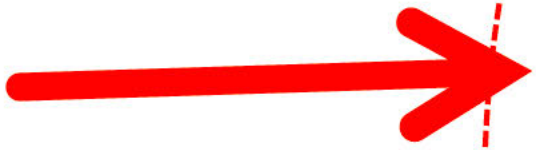
Then you have a user that downloads Hotspot Shield to proxy their traffic…

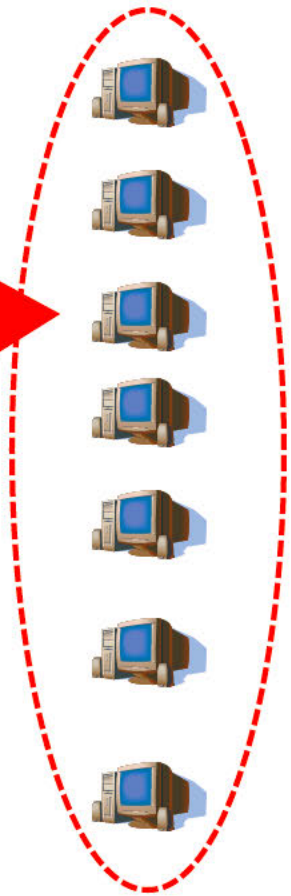


We'll pretend they want to go to Yahoo (or whereever else)

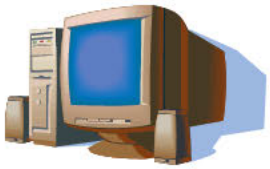
Anchorfree

AnchorFree owns a bunch of servers on the Internet.





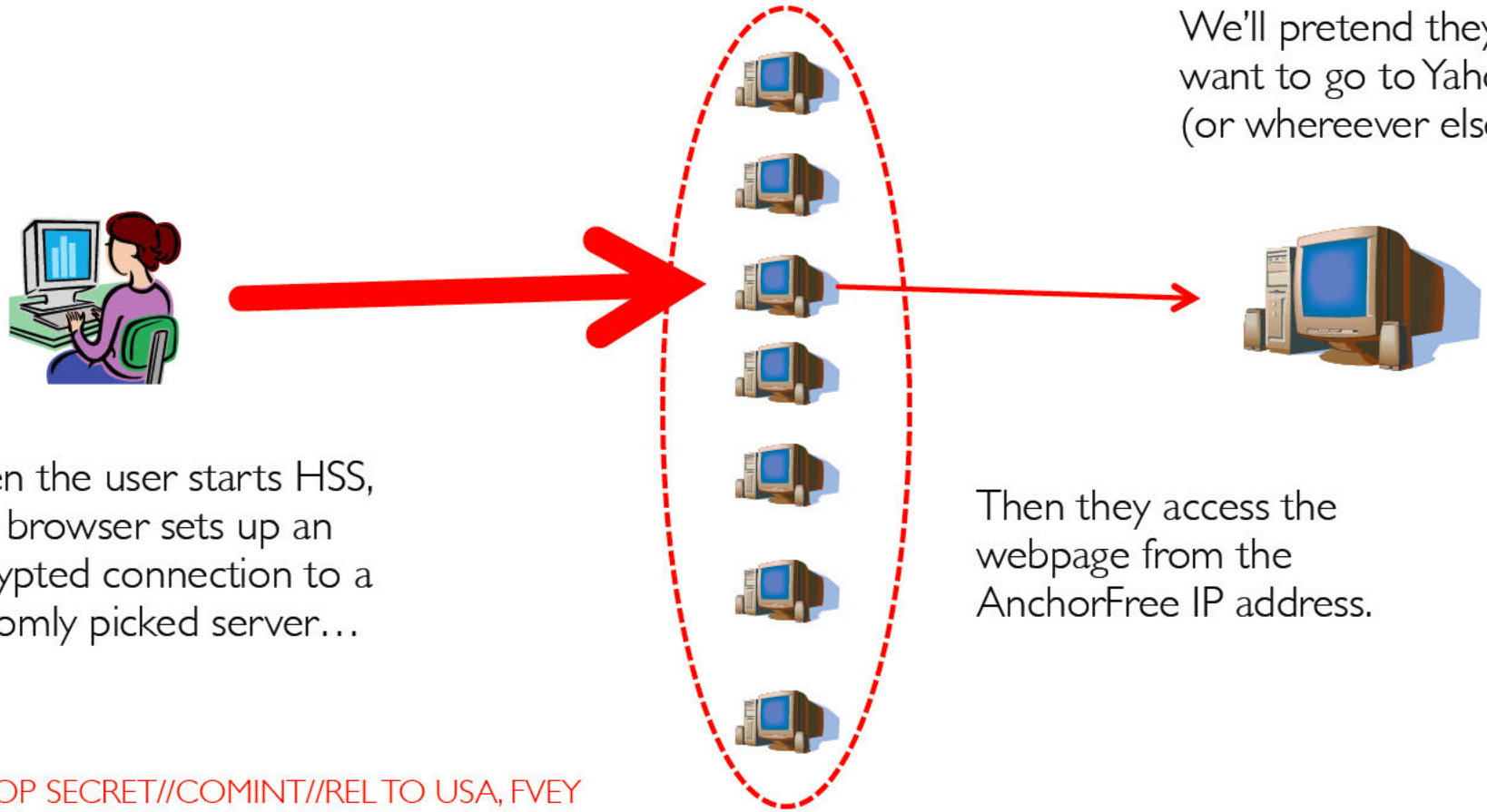
We'll pretend they want to go to Yahoo (or whereever else)



When the user starts HSS, their browser sets up an encrypted connection to a randomly picked server…

Anchorfree

AnchorFree owns a bunch of servers on the Internet.



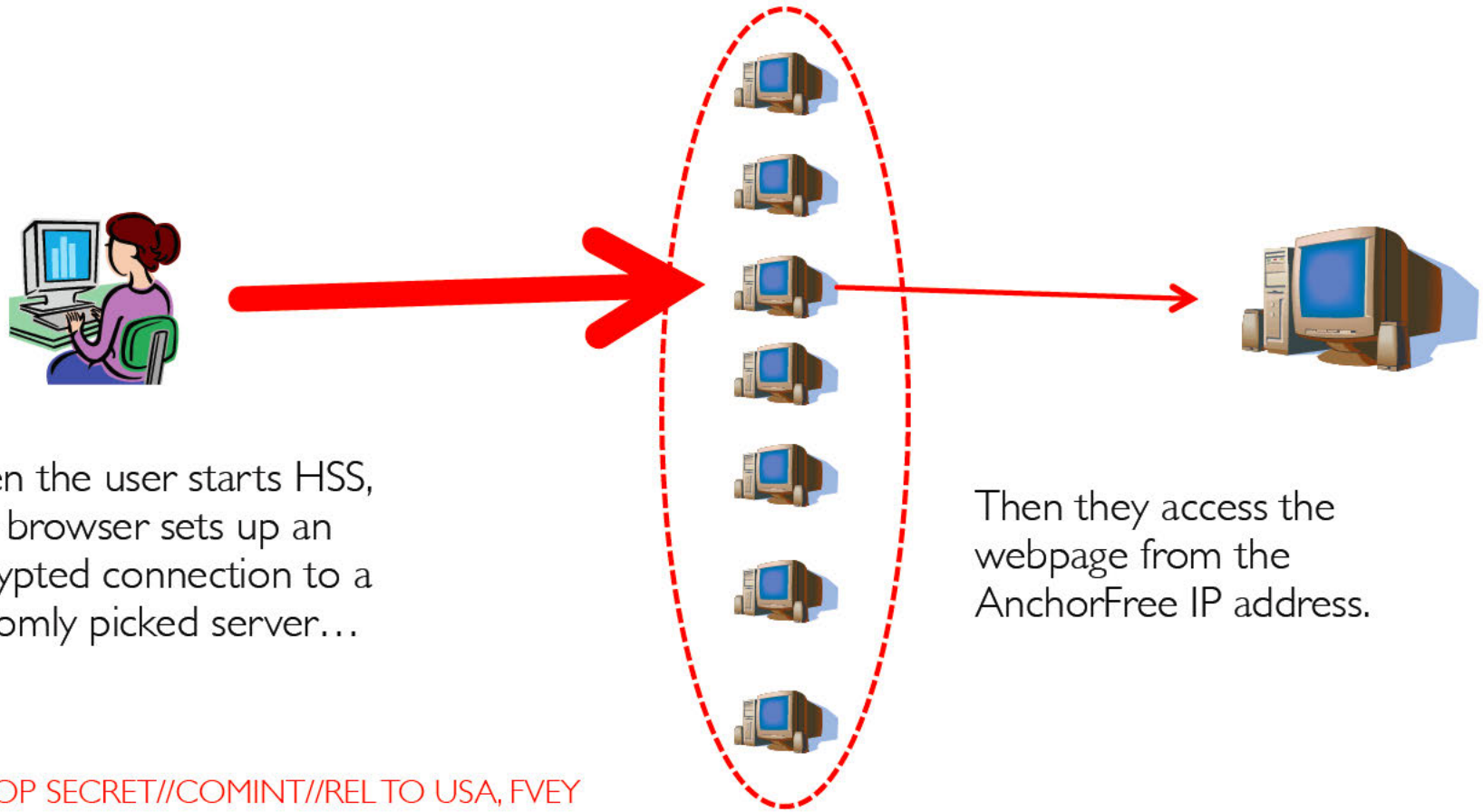
We'll pretend they want to go to Yahoo (or whereever else)

When the user starts HSS, their browser sets up an encrypted connection to a randomly picked server…

Then they access the webpage from the AnchorFree IP address.

Anchorfree

From testing, the IP address that the user connects to, and the IP they show up as are NOT the same. But there is a direct correlation between the two.



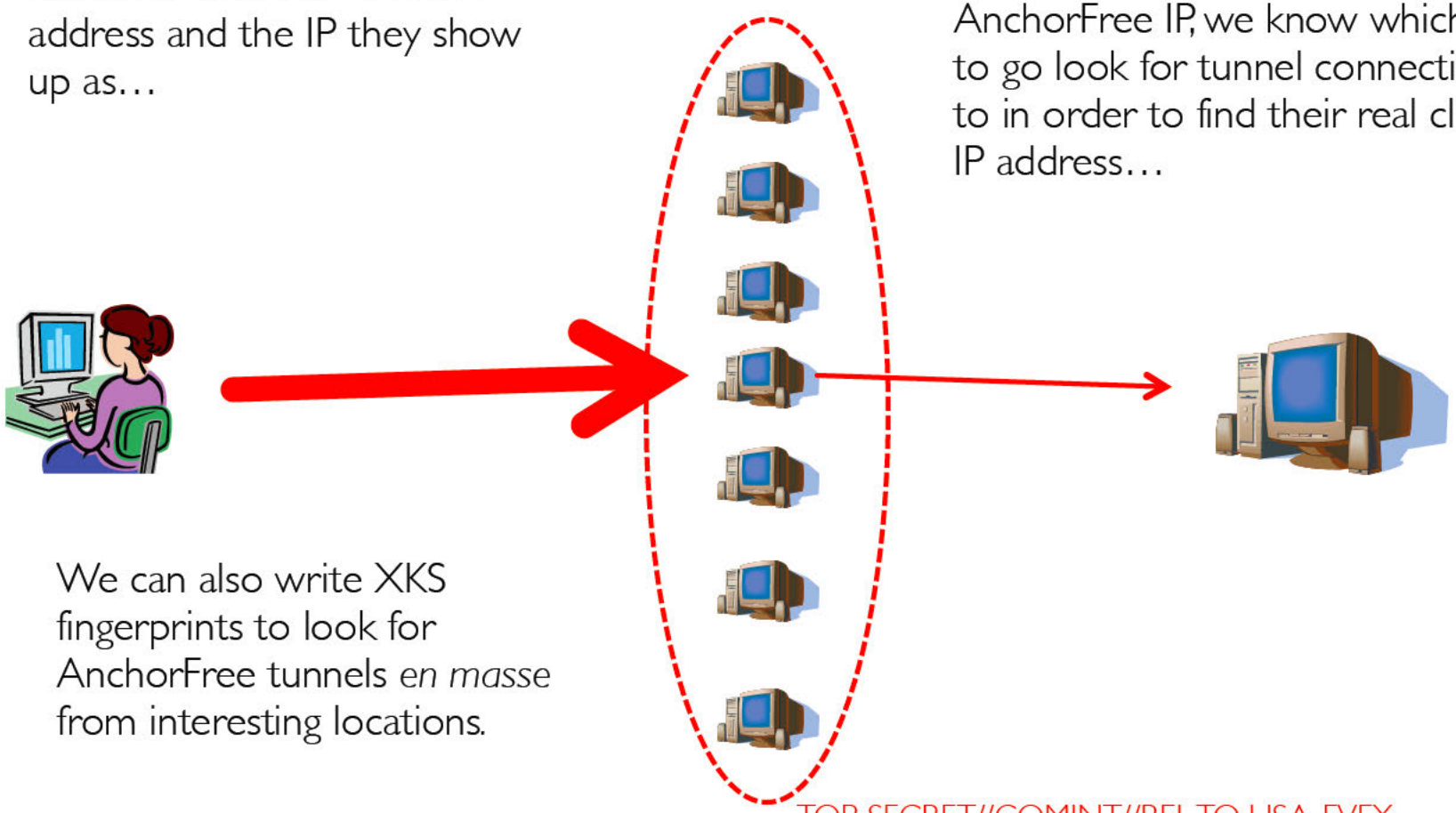
When the user starts HSS, their browser sets up an encrypted connection to a randomly picked server…

Then they access the webpage from the AnchorFree IP address.

AnchorFree….so what?

We can build static mappings between the inside/tunnel IP address and the IP they show up as…

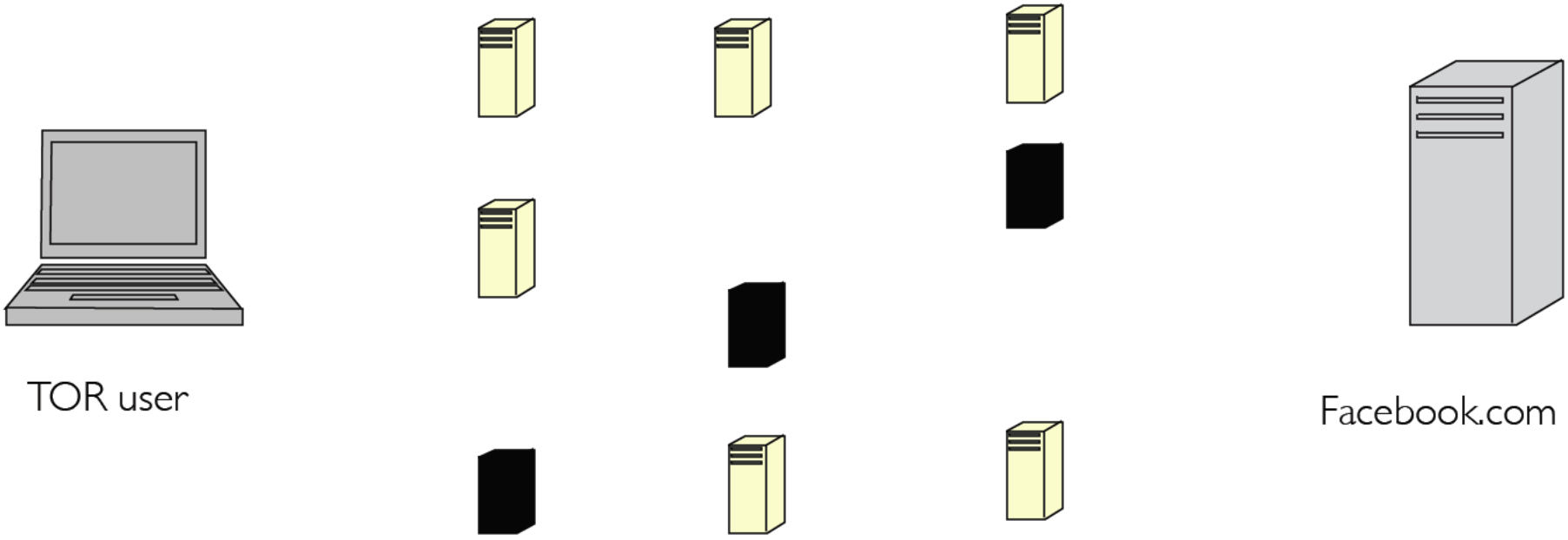
So when we see a target access their account from an AnchorFree IP, we know which IP to go look for tunnel connections to in order to find their real client IP address…



We can also write XKS fingerprints to look for AnchorFree tunnels *en masse* from interesting locations.

Tor

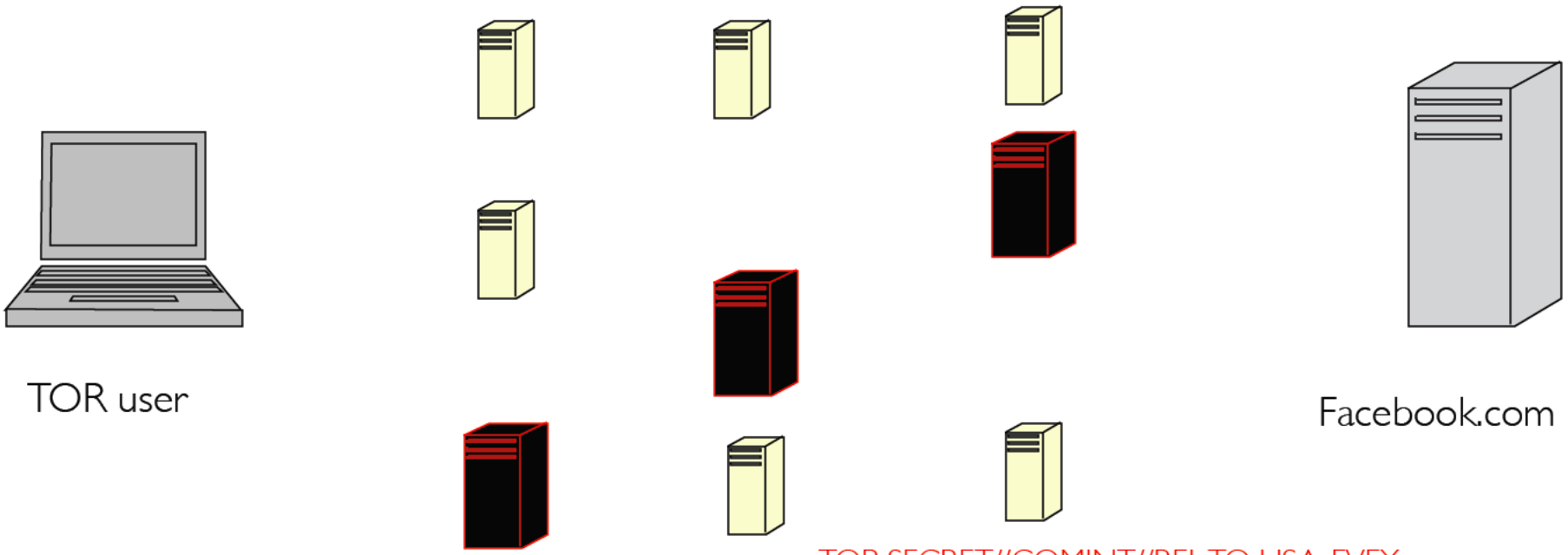
Example of Tor user connecting to facebook.com



Tor

Example of Tor user connecting to facebook.com

1) the user selects 3 relatively random Tor nodes to use.

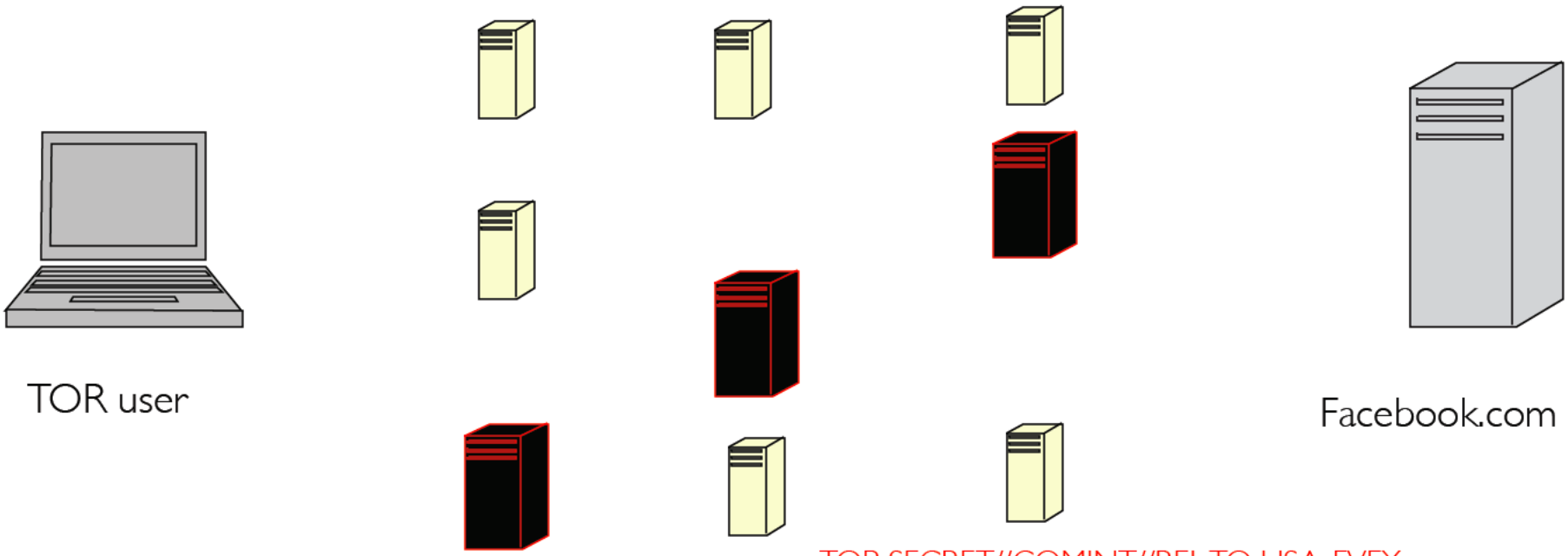


Tor

Example of Tor user connecting to facebook.com

1) the user selects 3 relatively random Tor nodes to use.

2) The user then sets up layers of SSL tunnels through them all to get to facebook. A layer is stripped off along each hop.

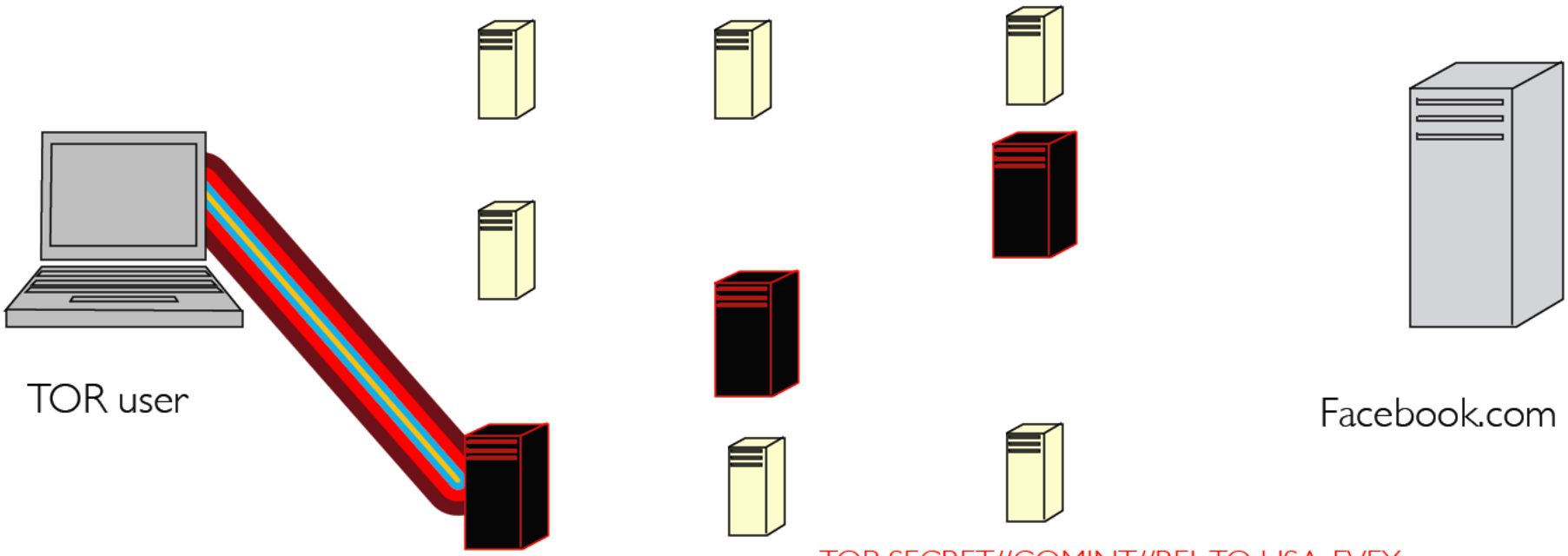


Tor

Example of Tor user connecting to facebook.com

1) the user selects 3 relatively random Tor nodes to use.

2) The user then sets up layers of SSL tunnels through them all to get to facebook. A layer is stripped off along each hop.

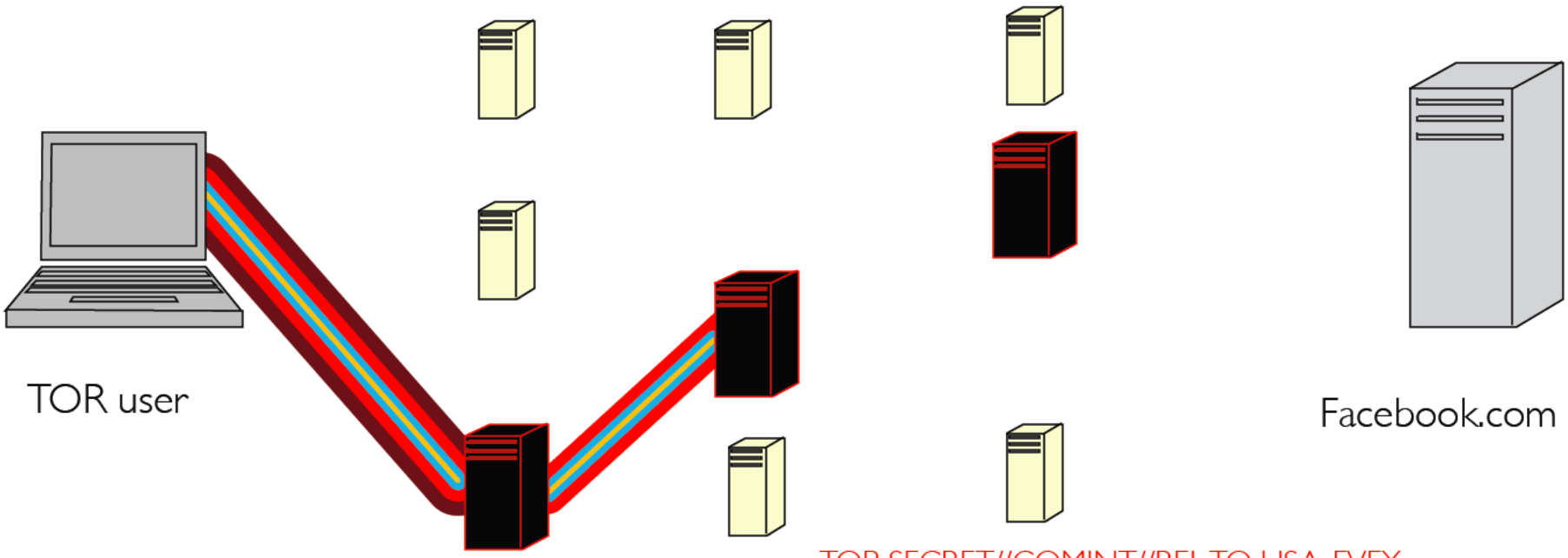


Tor

Example of Tor user connecting to facebook.com

1) the user selects 3 relatively random Tor nodes to use.

2) The user then sets up layers of SSL tunnels through them all to get to facebook. A layer is stripped off along each hop.

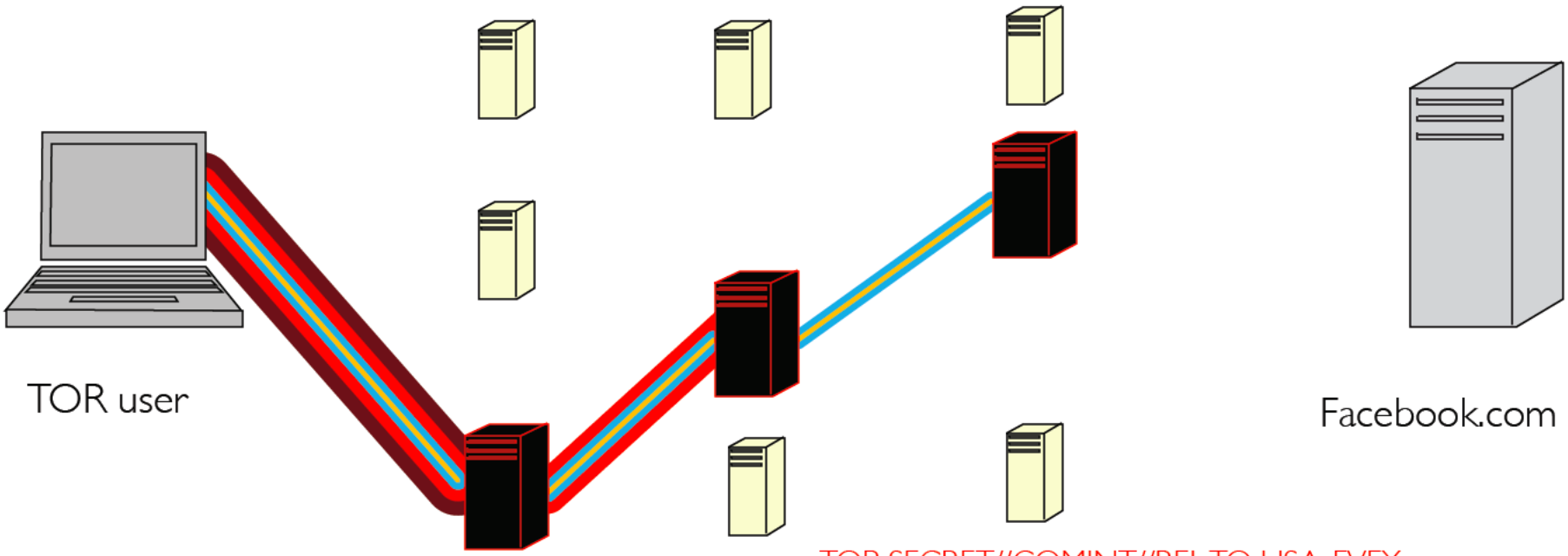


Tor

Example of Tor user connecting to facebook.com

1) the user selects 3 relatively random Tor nodes to use.

2) The user then sets up layers of SSL tunnels through them all to get to facebook. A layer is stripped off along each hop.

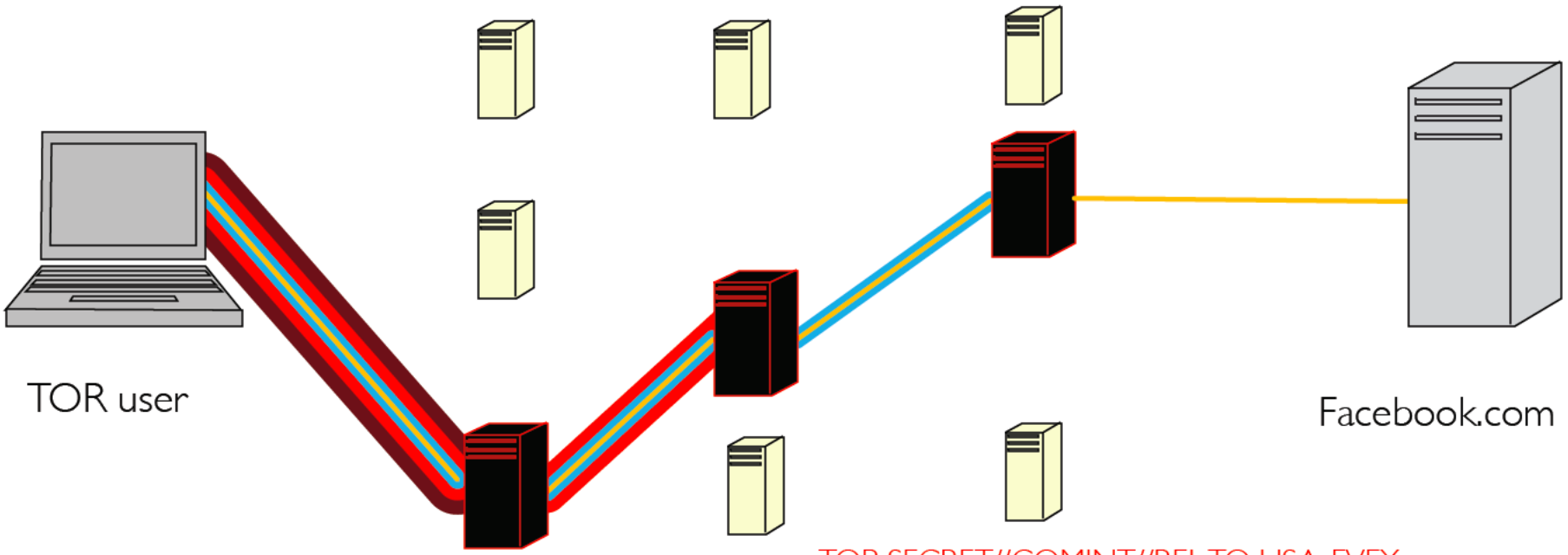


Tor

Example of Tor user connecting to facebook.com

1) the user selects 3 relatively random Tor nodes to use.

2) The user then sets up layers of SSL tunnels through them all to get to facebook. A layer is stripped off along each hop.



Interesting tidbits about Tor

- TOR uses SSL tunnels for encryption, we are able to identify what their SSL certificates look like (which allows us to identify Tor circuits in SIGINT).
- GOLDENFORTIN dataset and exit node traffic

And now for something completely different…

- A lot of research we do on anonymizers consists of open source research:
  - The Interwebz (forums, RFC's, 2010 Circumvention Tool Usage Report, etc)
  - Trial and Error / Wireshark
  - Basically RTFM'ing about how stuff works and translating that to the SIGINT system.

Contact Info

Questions?

NOBODY EXPECTS THE SPANISH INQUISITION!!!!