Understanding Tor
«A low-latency anonymity network»

Spyridon Antakis

A discussion based on ...

Tor: The Second-Generation Onion Router (2004)
Roger Dingledine, Nick Mathewson, Paul Syverson

... and today's challenges ...

November 10, 2013

... because sometimes I really wonder ...

anonymity, privacy, trust, data control, no-tracking, no-profiling

$\approx$

a luxury lost in the cloud

or

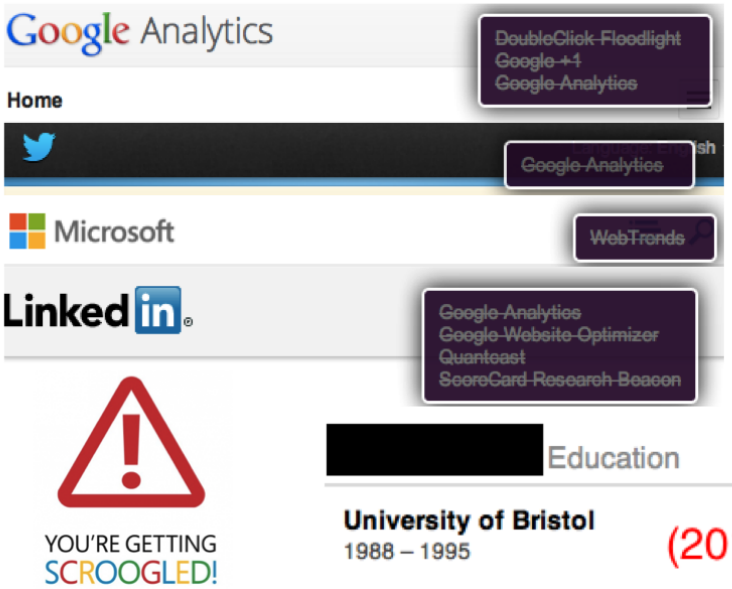
services under construction

?

... because awareness is missing ...

Recent activity:

Access Type [?] (Browser, mobile, POP3, etc.)	Location (IP address) [?]	Date/Time (Displayed in your time zone)
Browser (Safari) Show details	* Ireland ([redacted])	11:46 pm (0 minutes ago)
Browser (Safari) Show details	Ireland ([redacted])	11:43 pm (3 minutes ago)
Browser (Firefox) Show details	Ireland ([redacted])	8:47 pm (2.5 hours ago)
Browser (Firefox) Show details	Greece ([redacted])	5:53 pm (5 hours ago)
Browser (Firefox) Show details	Greece ([redacted])	5:10 pm (6 hours ago)
Browser (Firefox) Show details	Greece ([redacted])	4:03 pm (7 hours ago)
Browser (Safari) Show details	Ireland ([redacted])	1:50 pm (9 hours ago)
Browser (Firefox) Show details	Greece ([redacted])	1:25 pm (10 hours ago)
Browser (Firefox) Show details	Greece ([redacted])	12:10 pm (11 hours ago)
Browser (Firefox) Show details	Greece ([redacted])	11:33 am (12 hours ago)

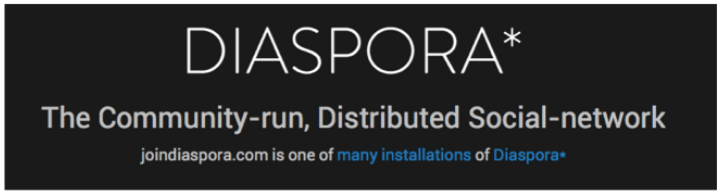


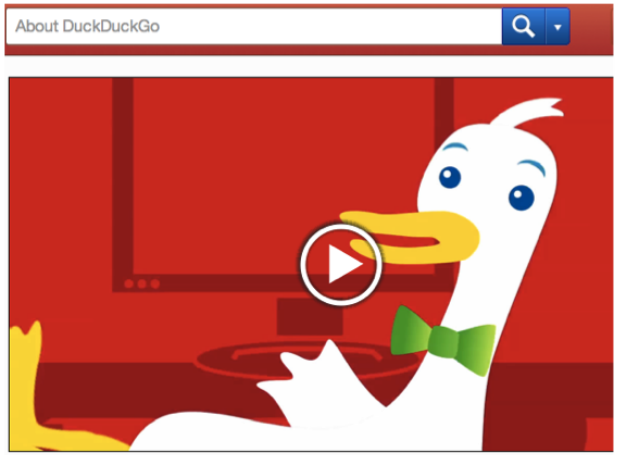
[redacted] Education

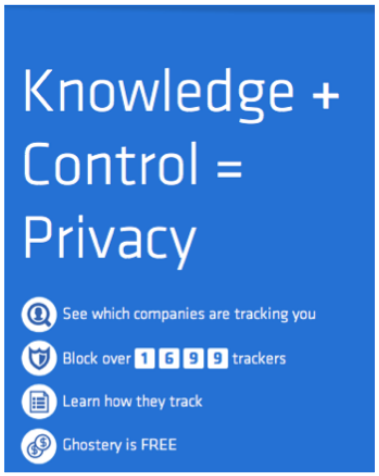
University of Bristol
1988 – 1995

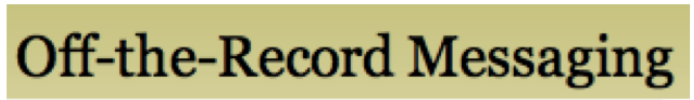
(2013-1988) + 18 = 43 years old ?

... because somebody has to care ...









RSA warns customers to stop using encryption algorithm over possible NSA backdoor

FBI Admits It Controlled Tor Servers Behind Mass Malware Attack

... because since 2008 I choose ...

My home server

LIGHTTPD
fly light.

POSTFIX

Not to have accounts on

twitter

facebook

Google

One account. All of Google.

LinkedIn

What is Tor ?

A **low-latency** anonymity system, proposed in 2004.

A design based on **Onion Routing**, developed by US Navy.

An **open-source** software that promises anonymity.

A **cross-platform** implementation with a strong community.

An **encrypted** overlay network with **trusted** directory servers.

What does Tor claim to achieve ?

Improvements*	Goals	Non Goals
Perfect forward secrecy	Deployability	Non peer-to-peer
Separating protocol cleaning	Usability	No protection against end-to-end attacks
No padding or traffic shaping	Flexibility	No protocol normalisation
Many TCP streams share one circuit	Simple Design	
Leaky-pipe circuit topology		
Congestion control and Integrity checking		
Exit policies and directory servers via HTTP		
Rendezvous points and hidden services		

∗ Over the Onion Routing design.

How overlay traffic looks like ?

Control Cells

circuit ID	cmd	payload
- 2 bytes -	- 1 byte -	- 509 bytes -

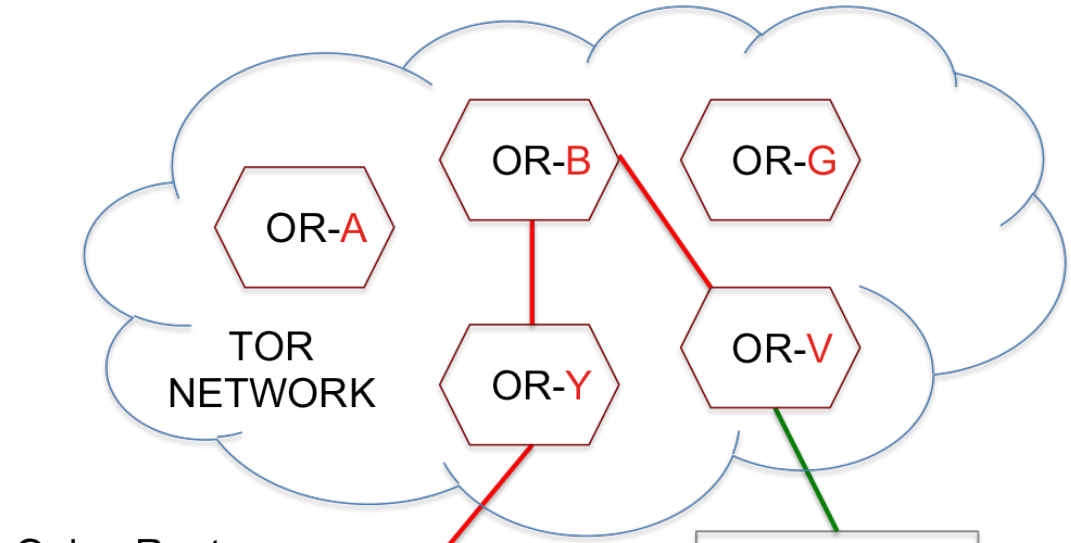
cmd-types = create, created, destroy, padding

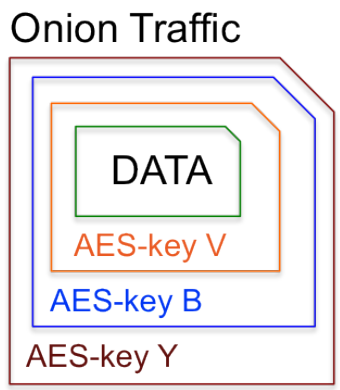
Relay Cells

circuit ID	relay	stream ID	digest	len	cmd	payload
- 2 bytes -	- 1 byte -	- 2 bytes -	- 6 bytes -	- 2 bytes -	- 1 byte -	- 498 bytes -

relay-cmd-types = data, begin, end, teardown, connected, extend, extended, truncate, truncated, sendme, drop

Communication process





Onion Routers have:

Identity keys: long-term keys (signing TLS certificates, more…)

Onion keys: short-term keys (encrypt request for new circuits)

TLS-Encrypted Non-Encrypted

... a lot more to understand ...

Attacks against Tor, such as traffic-analysis.

How **efficient** is the implementation?

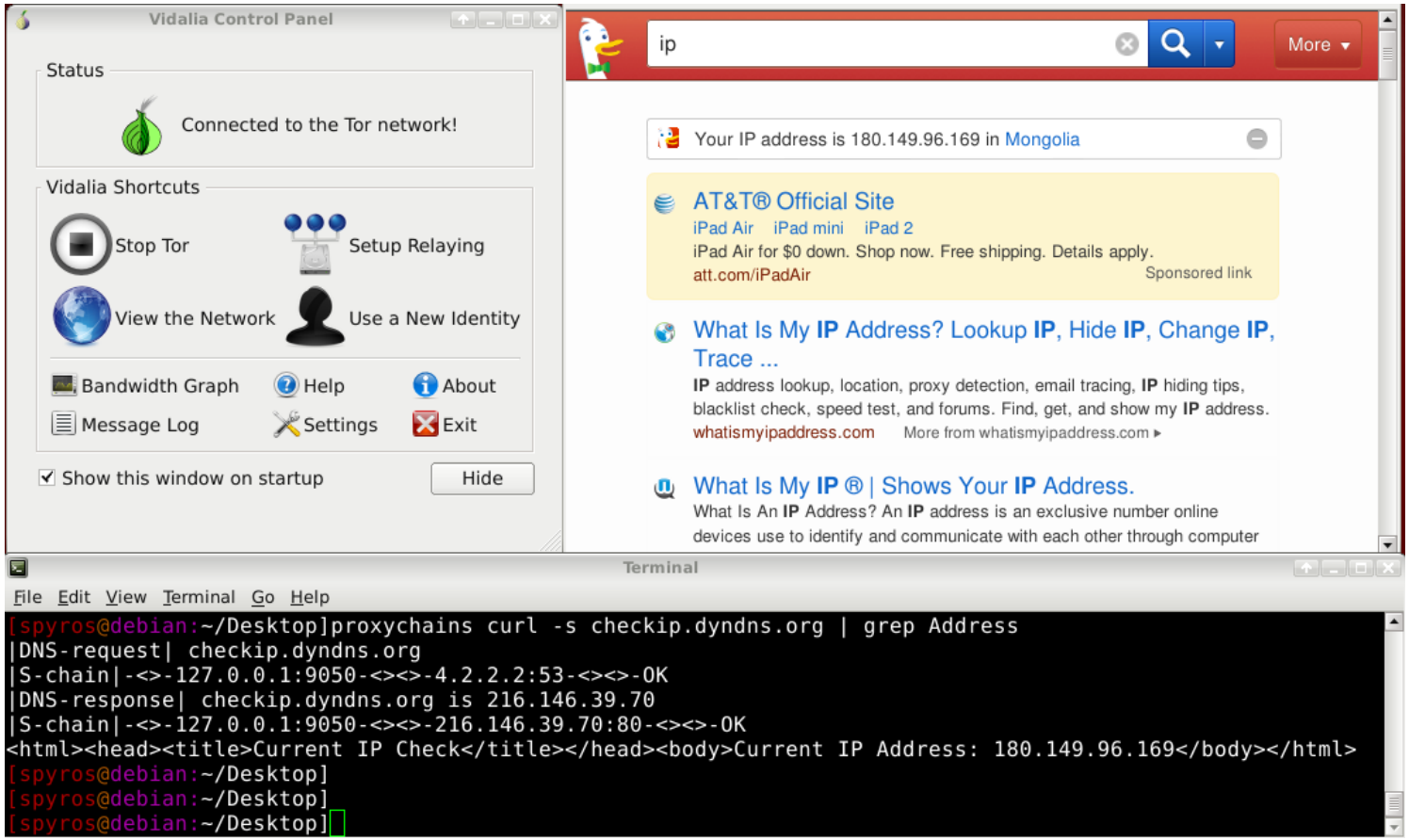
How traffic looks like on a **wireshark** trace?

Dive into the **source-code** and see exactly what happens.

... but let's discuss some personal observations ...

... early observations ...

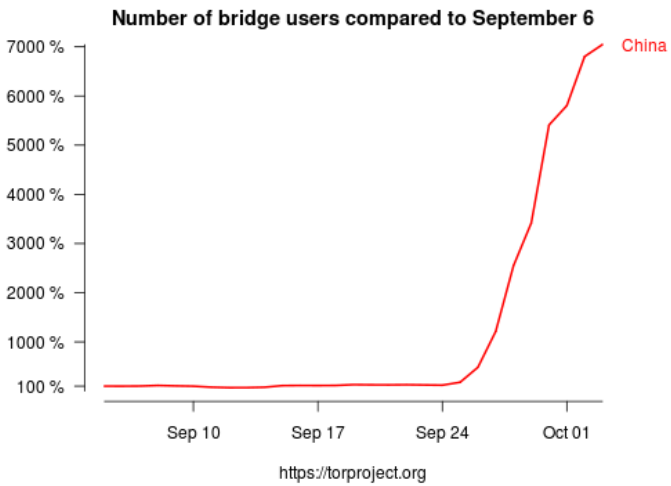
Proxychains allows direct usage of tools such as **curl, nmap.**

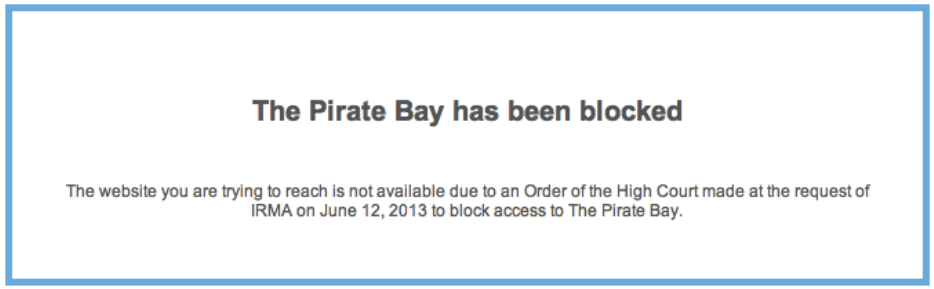


... early observations ...

Analytics are not polluted with Tor users, but IPs are still tracked.

Tor network becomes a workaround for censorship.





... if you want to read more ...

Design Paper

Tor: The Second-Generation Onion Router (2004)

Roger Dingledine, Nick Mathewson, Paul Syverson

https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf

More ...

https://www.torproject.org/

http://www.onion-router.net/

https://svn.torproject.org/

... questions ...