

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

≈

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 (██████████.3)	11:46 pm (0 minutes ago)
Browser (Safari) Show details	Ireland (4██████████.3)	11:43 pm (3 minutes ago)
Browser (Firefox) Show details	Ireland (4██████████.3)	8:47 pm (2.5 hours ago)
Browser (Firefox) Show details	Greece (8██████████.9)	5:53 pm (5 hours ago)
Browser (Firefox) Show details	Greece (8██████████.9)	5:10 pm (6 hours ago)
Browser (Firefox) Show details	Greece (8██████████.9)	4:03 pm (7 hours ago)
Browser (Safari) Show details	Ireland (1██████████.9)	1:50 pm (9 hours ago)
Browser (Firefox) Show details	Greece (8██████████.9)	1:25 pm (10 hours ago)
Browser (Firefox) Show details	Greece (8██████████.9)	12:10 pm (11 hours ago)
Browser (Firefox) Show details	Greece (8██████████.9)	11:33 am (12 hours ago)

Google Analytics

Home



Microsoft

LinkedIn



YOU'RE GETTING
SCROGGLED!

DoubleClick Floodlight
Google →
Google Analytics

Google Analytics

WebTrends

Google Analytics
Google Website Optimizer
Quantcast
ScoreCard Research Beacon

Education

University of Bristol
1988 – 1995

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



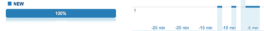
Right now

1

active visitors on site

Pageviews

Per minute



1.	Greece	110	
2.	Sweden	2	1.68%
3.	Cyprus	1	0.84%
4.	Netherlands	1	0.84%
5.	Turkey	1	0.84%
6.	United States	1	0.84%

... because somebody has to care ...

DIASPORA*
The Community-run, Distributed Social-network
*joindiaspora.com is one of many installations of Diaspora**



HOW IT WORKS

Knowledge +
Control =
Privacy

- See which companies are tracking you
- Block over 1000 trackers
- Learn how they track
- Ghostery is FREE

Silent Circle

Company

Silent Circle is an encrypted communications firm providing secure multiplatform communication services for mobile devices, desktop and email. Launched October 16, 2012, the company is privately funded. [Wikipedia](#)

Founded: October 16, 2012

Founders: Phil Zimmermann, Mike Janke



NoScript

Developer(s) [Giorgio Maone](#)

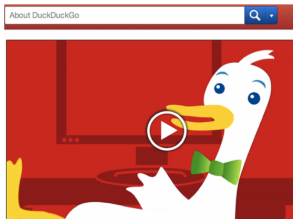
Stable release [2.6.8.4](#) / October 24, 2013;
0 days ago

Available in [48 Languages](#)

Type [Mozilla extension](#)

License [GPL](#)

Website [NoScript.net](#)



We believe in better search and real privacy

Off-the-Record Messaging

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



Not to have accounts on



Google

One account. All of Google.



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.

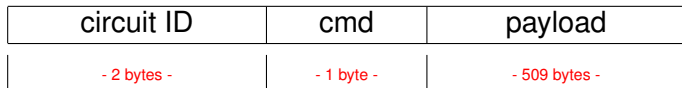
What does Tor claim to achieve ?

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.

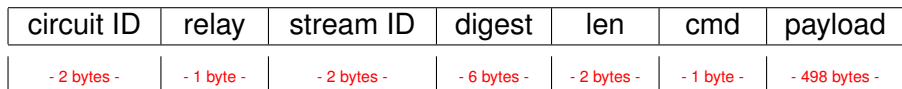
How overlay traffic looks like ?

Control Cells



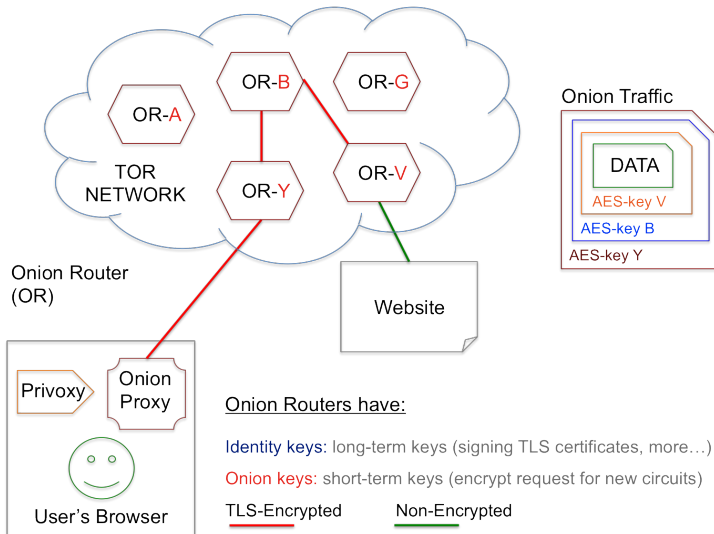
cmd-types = create, created, destroy, padding

Relay Cells



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)

... a lot more to understand ...

Attacks against Tor, such as traffic-analysis.

How **efficient** is the implementation?

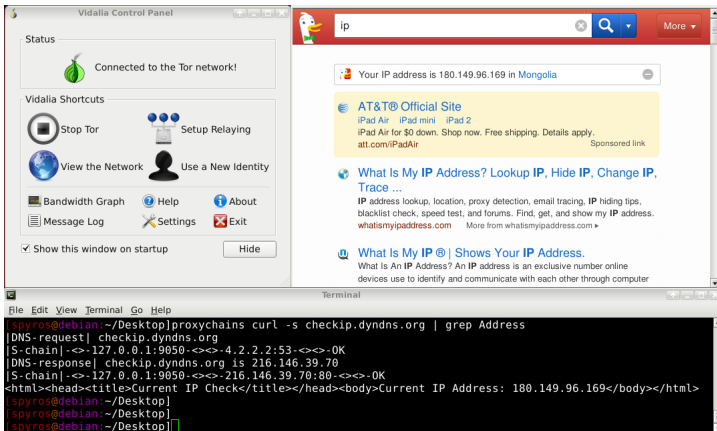
How traffic looks like on a **wireshark** trace?

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**.



The screenshot displays a Linux desktop environment. On the left is the Vidalia Control Panel, which shows the status as 'Connected to the Tor network!' and provides shortcuts for 'Stop Tor', 'Setup Relaying', 'View the Network', 'Use a New Identity', 'Bandwidth Graph', 'Help', 'About', 'Message Log', 'Settings', and 'Exit'. Below the shortcuts, there is a checkbox for 'Show this window on startup' and a 'Hide' button.

In the center is a web browser window with the address bar set to 'ip'. The page content includes a search bar, a notification that 'Your IP address is 180.149.96.169 in Mongolia', and several search results. The first result is 'AT&T® Official Site' with a sponsored link. The second result is 'What is My IP Address? Lookup IP, Hide IP, Change IP, Trace ...' from whatismyipaddress.com. The third result is 'What is My IP @ | Shows Your IP Address.' from whatismyipaddress.com.

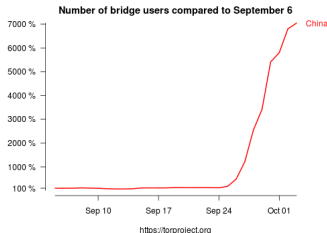
At the bottom is a terminal window with the following commands and output:

```
[spyros@debian:~/Desktop]proxychains curl -s checkip.dyndns.org | grep Address
[DNS-request] checkip.dyndns.org
[S-chain]-<-127.0.0.1:9050-<-<-4.2.2.2:53-<-<-OK
[DNS-response] checkip.dyndns.org is 216.146.39.70
[S-chain]-<-127.0.0.1:9050-<-<-216.146.39.70:80-<-<-OK
<html><head><title>Current IP Check</title></head><body>Current IP Address: 180.149.96.169</body></html>
[spyros@debian:~/Desktop]
[spyros@debian:~/Desktop]
[spyros@debian:~/Desktop]
```

... early observations ...

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

Tor network becomes a workaround for **censorship**.



The Pirate Bay has been blocked

The website you are trying to reach is not available due to an Order of the High Court made at the request of IRMA on June 12, 2013 to block access to The Pirate Bay.

... 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 ...

