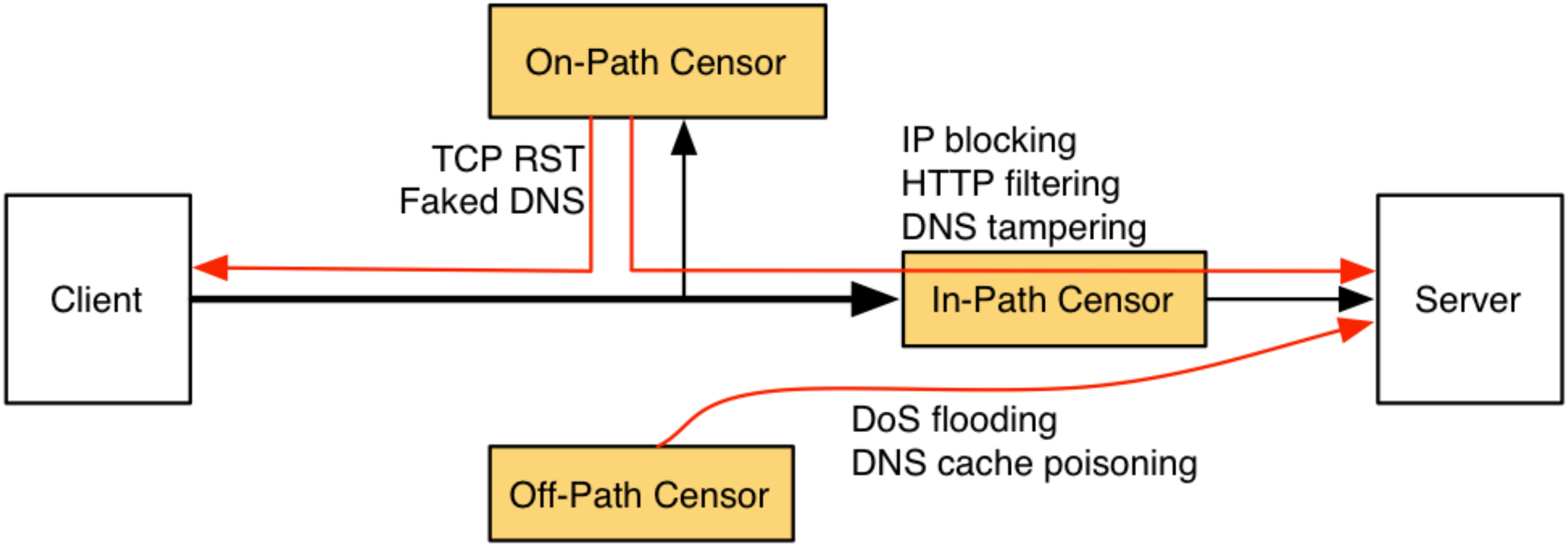
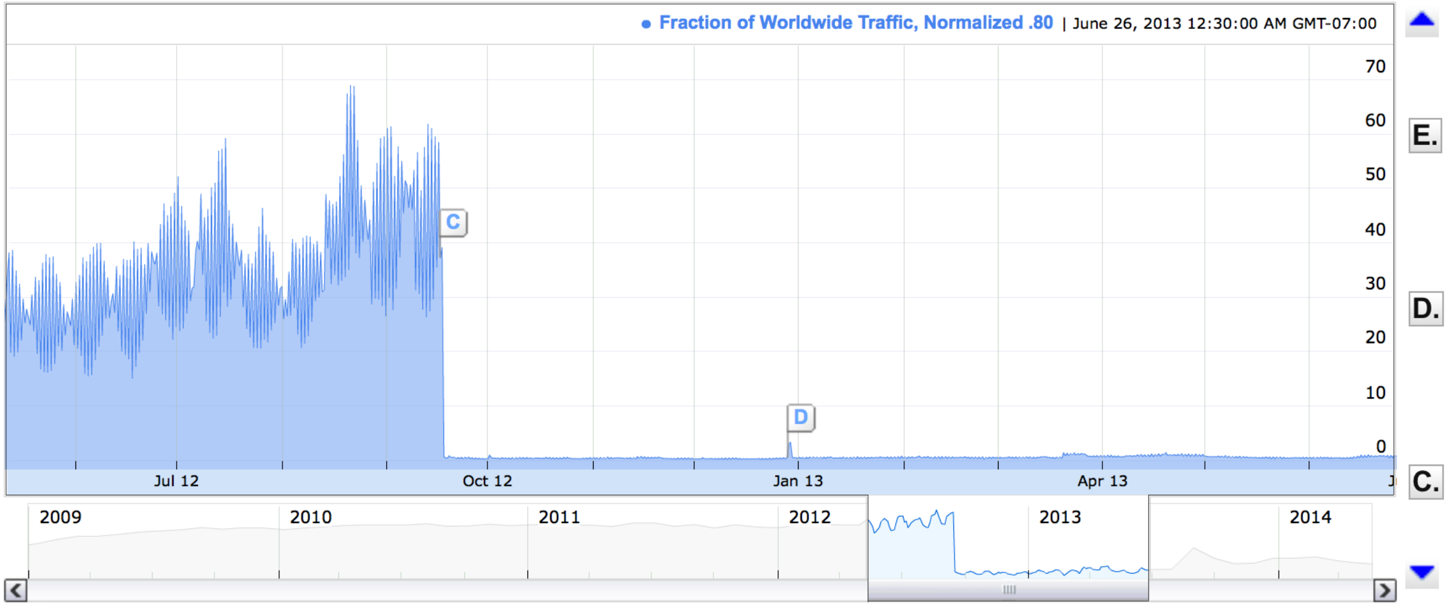

On-Path Censor
TCP RST
Faked DNS
IP blocking
HTTP filtering
DNS tampering
Client
In-Path Censor
Server
DoS flooding
DNS cache poisoning
Off-Path Censor

Browse real-time traffic to Google products and services

This page provides near real-time information about traffic to our products and services around the world. Each graph shows historic traffic patterns for a given geographic region and product. For more information, see our FAQ.

Pakistan ⬍ YouTube ⬍

Fraction of Worldwide Traffic, Normalized



Data after this point are still being finalized. Interpret them with caution.

2014-5-13

Pakistan Lifts YouTube Ban, for 3 Minutes – New York Times [Read More]

2012-12-28

Pakistan blocks YouTube over anti-Islam film – AFP [Read More]

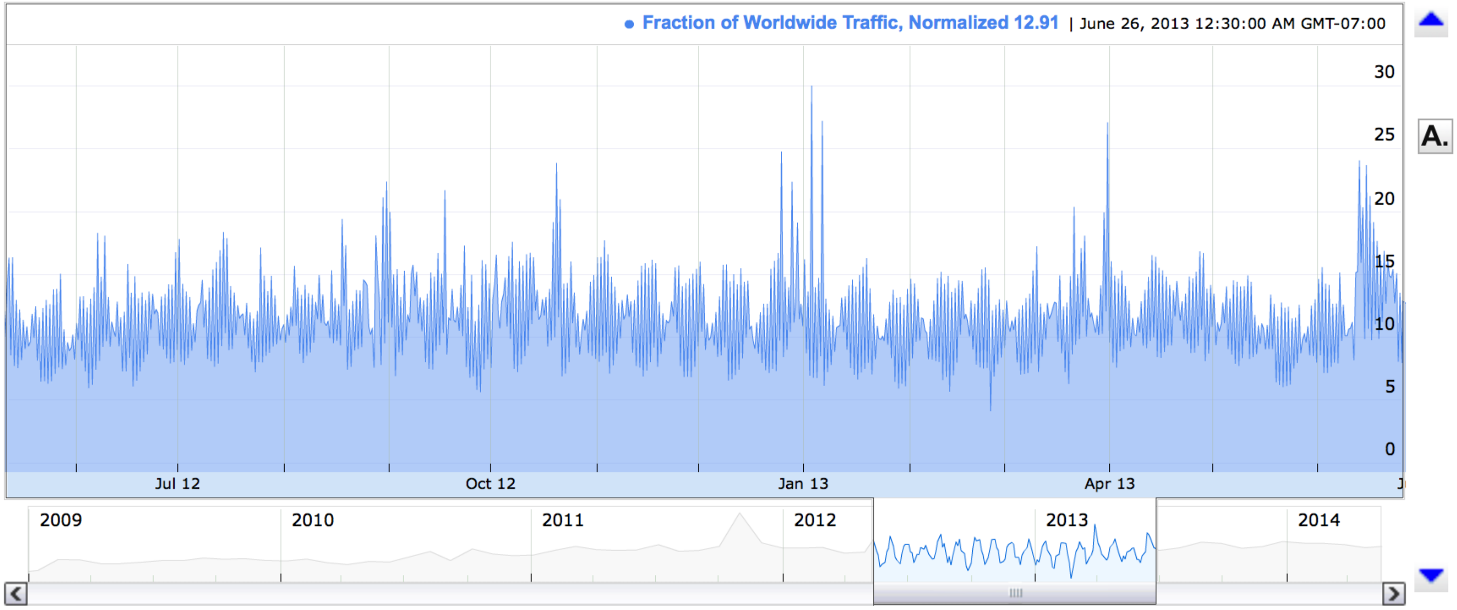
2012-9-17

Browse real-time traffic to Google products and services

This page provides near real-time information about traffic to our products and services around the world. Each graph shows historic traffic patterns for a given geographic region and product. For more information, see our FAQ.

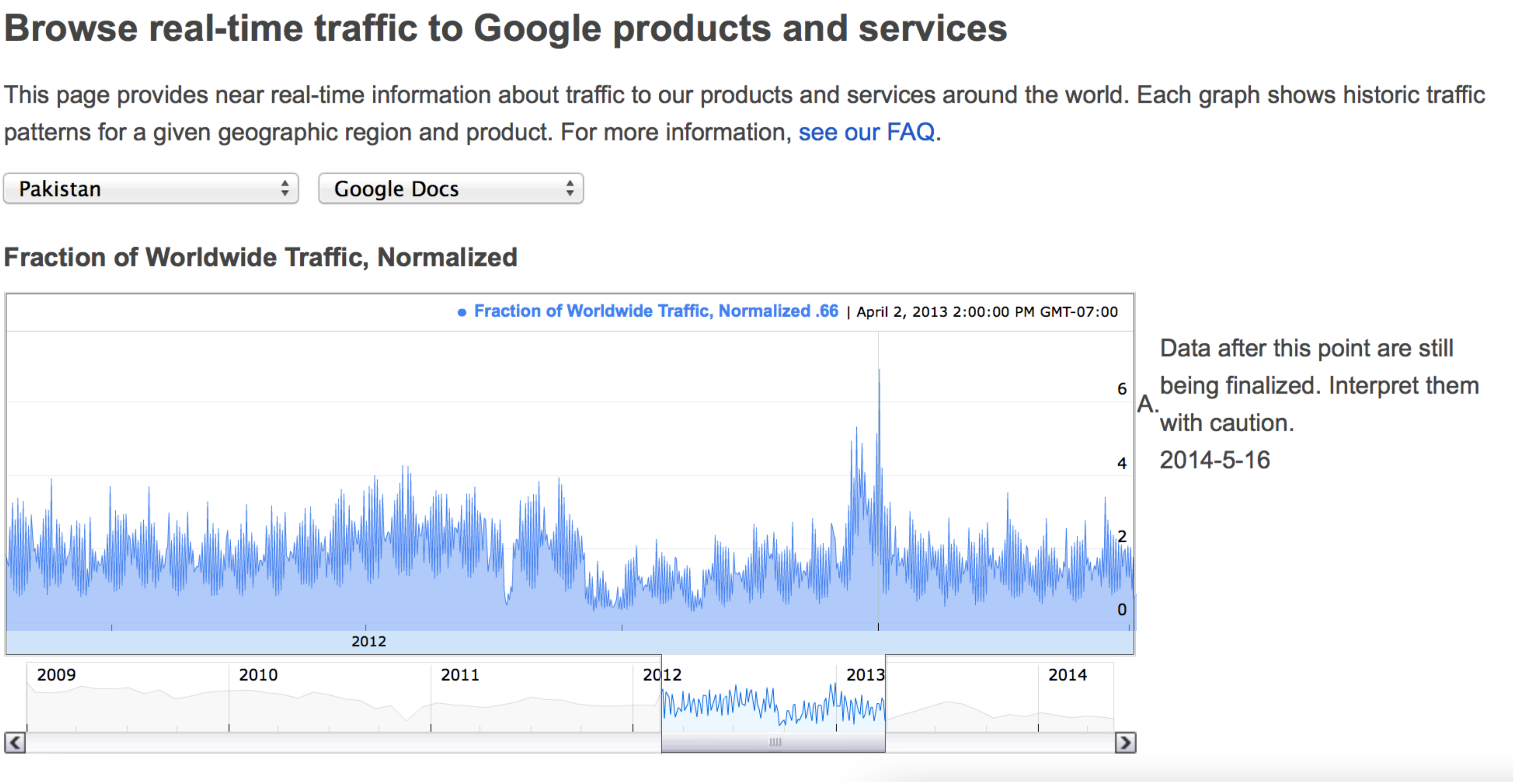
Pakistan ⬍ Blogger ⬍

Fraction of Worldwide Traffic, Normalized



A. Data after this point are still being finalized. Interpret them with caution.

2014-5-13



Browse real-time traffic to Google products and services

This page provides near real-time information about traffic to our products and services around the world. Each graph shows historic traffic patterns for a given geographic region and product. For more information, see our FAQ.

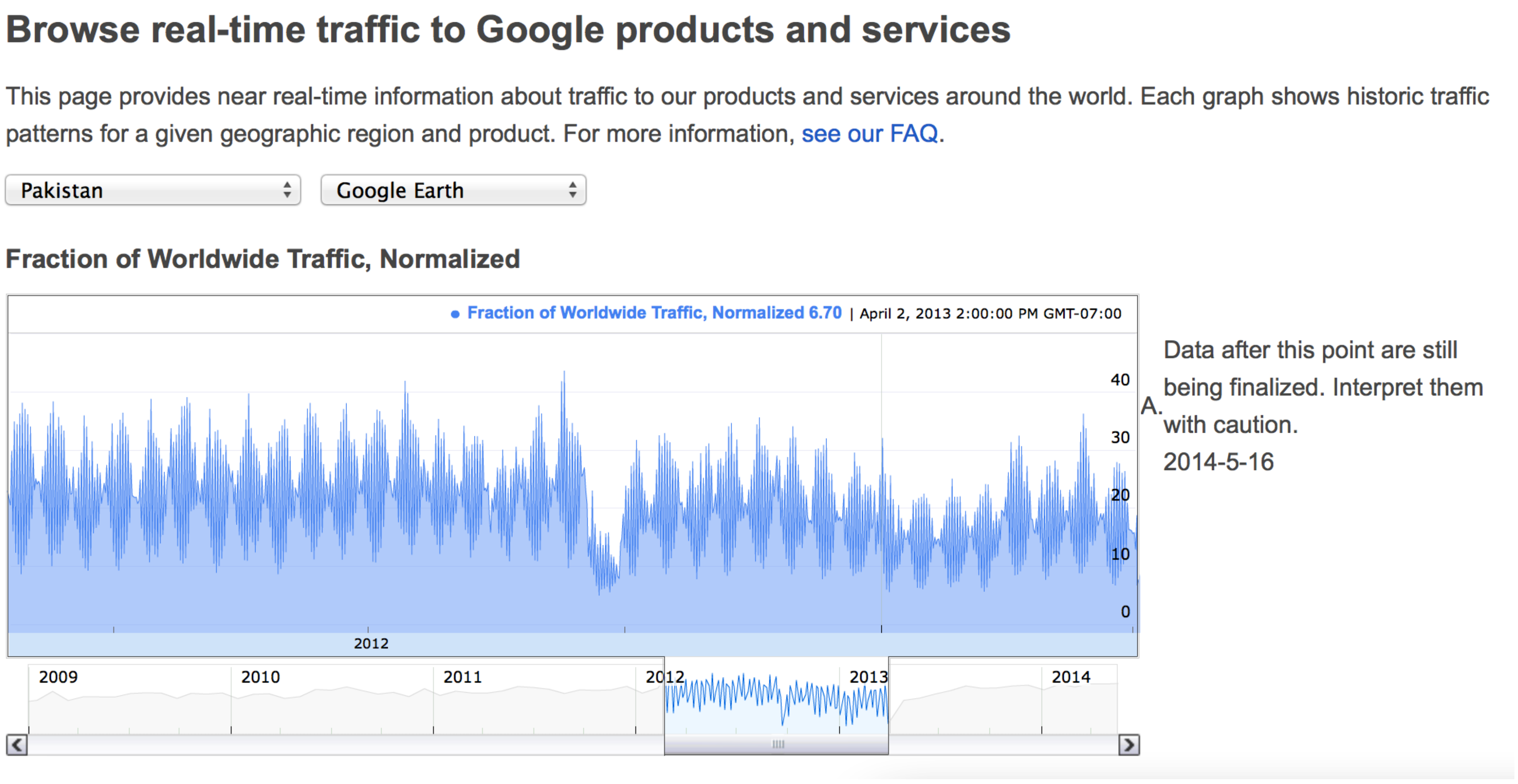
Pakistan ⇕ Google Docs ⇕

Fraction of Worldwide Traffic, Normalized

● Fraction of Worldwide Traffic, Normalized .66 | April 2, 2013 2:00:00 PM GMT-07:00
6
4
2
0
2012
A.
2009
2010
2011
2012
2013
2014

Data after this point are still being finalized. Interpret them with caution.

2014-5-16



Browse real-time traffic to Google products and services

This page provides near real-time information about traffic to our products and services around the world. Each graph shows historic traffic patterns for a given geographic region and product. For more information, see our FAQ.

Pakistan

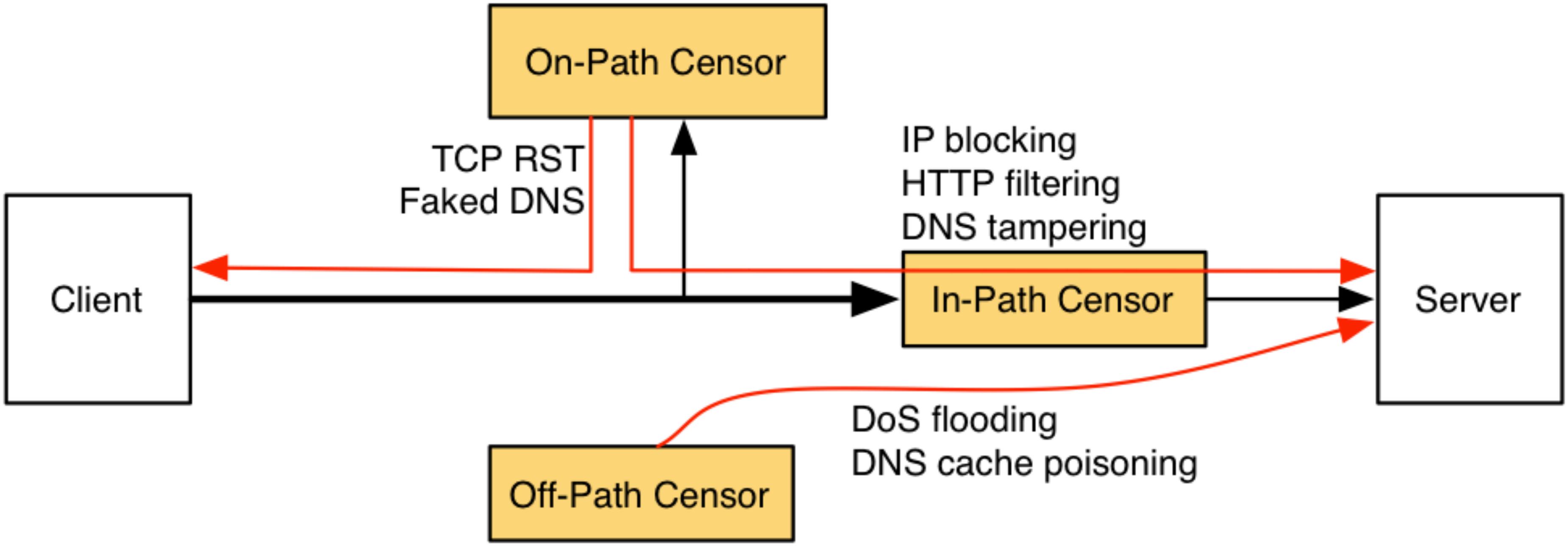
Google Earth

Fraction of Worldwide Traffic, Normalized

● Fraction of Worldwide Traffic, Normalized 6.70 | April 2, 2013 2:00:00 PM GMT-07:00

Data after this point are still being finalized. Interpret them with caution.

2014-5-16

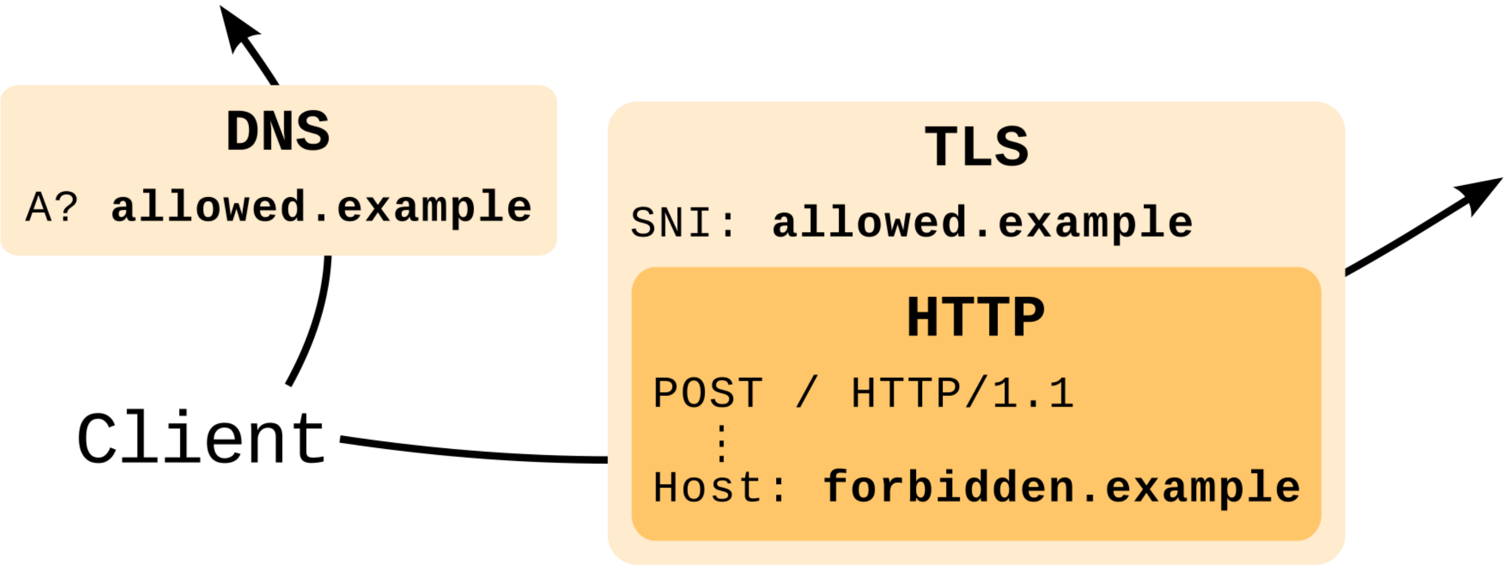

On-Path Censor
TCP RST
Faked DNS
IP blocking
HTTP filtering
DNS tampering
Client
In-Path Censor
Server
DoS flooding
DNS cache poisoning
Off-Path Censor

Identified Source	Signature
Identified Injector	
Sandvine	Multipacket: First Packet IPID += 4, second packet SEQ + 12503, IPID += 5
Bezeqint	Multipacket: Constant sequence, `RST_ACK_CHANGE`, IPID = 16448
Yournet	`SYN_RST`: Only on SMTP, TTL usually +3 to +5, unrelated IPID
Victoria	Multipacket: Sequence Increment 1500, IPID = 305, TTL += 38
IPID 256	Single packet: Usually less TTL, IPID = 256
IPID 64	Multipacket: IPID = 64, often sequence increment of 1460
IPID -26	Multipacket: First IPID -= 26, often sequence increment of 1460
SEQ 1460	Multipacket: Sequence increment always 1460
RAE	Single packet: Sets RST, ACK and ECN nonce sum (control bit 8)
Go Away	Single packet: Payload on RST of "`Go Away, We're Not Home`"
Optonline	Multipacket: No fingerprint, all activity from a single ISP
Identified Non-Injected Source	
SYN/RST 128	`SYN_RST` with RST TTL += 128
SYN/RST 65259	`SYN_RST` with RST IPID = 65259
0-Seq RST	Reset with SEQ = 0
IPID 0	IPID = 0, multiple RSTs, limited range
IPID 0 Solo	IPID = 0, spurious RST (often ignored)
Stale RST	RST belonging to a previous connection (port reuse)
Spambot SR	Spam source sending payload packets with SYN and RST flags
DNS `SYN_RST`	Normal DNS servers aborting connections at initiation

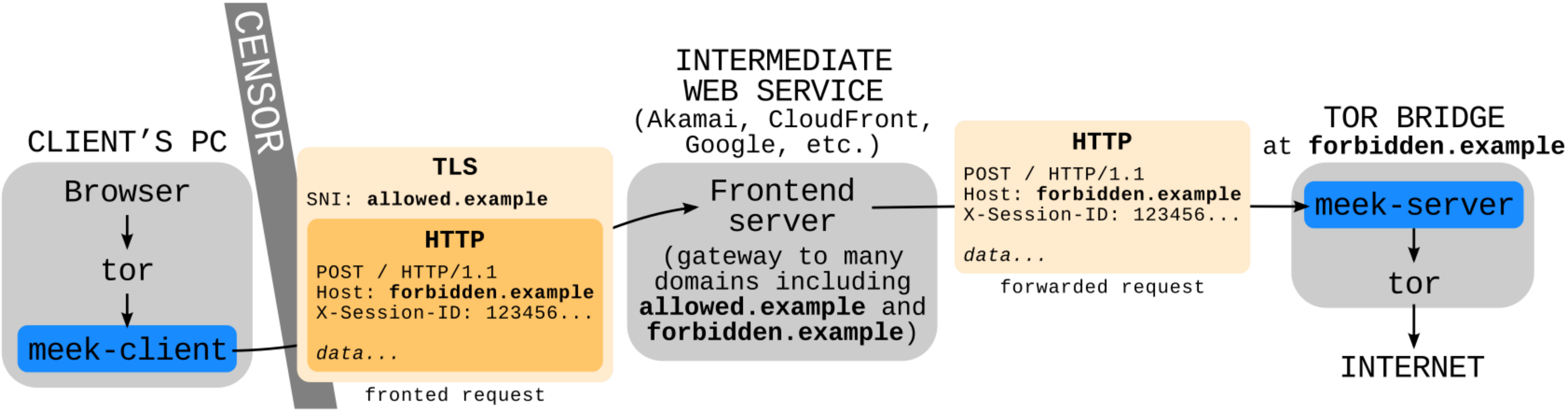
Table 1. Features for both identified RST injectors and identified non-injected sources.

Test	Evasion Class	Description	Circumvention Opportunities	Fixing Cost	Receiver Dependent?
IP1	Ambiguity	$_{IP(TTL=<low>)}p(Bad) \implies reset$	Insertion	High	
IP2	Reassembly	Overlapping fragment processing	Insertion	High	✓
TCP1	TCB creation	$_{IP(TTL=<low>)}p_i^S, \quad p_{i+1}^S, \quad p_{i+2}(Bad) \quad \wedge \quad (tuple(p_i) = tuple(p_{i+1})) \wedge (seq(p_i) \neq seq(p_{i+1})) \implies \neg\, reset$	Insertion-Evasion	Low	
TCP2	Incompleteness	$_{IP(ack=<bad>)}p(Bad) \implies reset$	Insertion	Low	
TCP3	Incompleteness	$_{IP(chksum=<bad>)}p(Bad) \implies reset$	Insertion	Low	
TCP4	Incompleteness	$p^{\neg A}(Bad) \implies reset$	Insertion	Low	
TCP5	Reassembly	Overlapping segment processing	Insertion	High	✓
TCP6[a]	TCB Teardown	$_{IP(TTL=<low>)}p_i^{R(A)}, p_{i+1}(Bad) \implies \neg\, reset$	Insertion-Evasion	High	
TCP6[b]	TCB Teardown	$_{IP(TTL=<low>)}\ p_i^F, p_{i+1}(Bad) \implies \neg\, reset$	Insertion-Evasion	Low	
TCP7	State Management	$\tau(\leq\ \approx 10\text{ hr}), p_i(Bad) \implies reset$	State exhaust.	High	
TCP8	State Management	$(p_i(Good)^+ \wedge \delta(Good) \leq\ \approx 1\text{ GB}), p_{i+1}(Bad) \implies reset$	State exhaust.	High	
TCP9	State Management	$hole, \ (p_i(Good)^+ \wedge \delta(Good) \geq 1\ \text{ KB} \wedge abovehole(p_i)), p_{i+1}(Bad) \implies \neg reset$	State exhaust.	High	✓
TCP10	State Management	$hole, \tau(y) \geq 60\text{ min}, (p_i(Bad) \wedge abovehole(p_i)) \implies \neg reset$	State exhaust.	High	✓
HTTP1	Ambiguity	GET with >1 space between method and URI $\implies \neg\, reset$	Evasion	Low	
HTTP2	Incompleteness	GET with keyword at location $> 2048 \implies \neg\, reset$	Evasion	Low	
HTTP3	Incompleteness	GET with keyword in $\geq$ 2nd of multiple requests in single segment $\implies \neg\, reset$	Evasion	Low	
HTTP4	Incompleteness	GET with URL encoded (except %-encoding) $\implies \neg\, reset$	Evasion	Low	✓

Table 1: Evasion opportunities in GFW's analysis of network traffic.



```
POST / HTTP/1.1
  ⋮
Host: forbidden.example
```

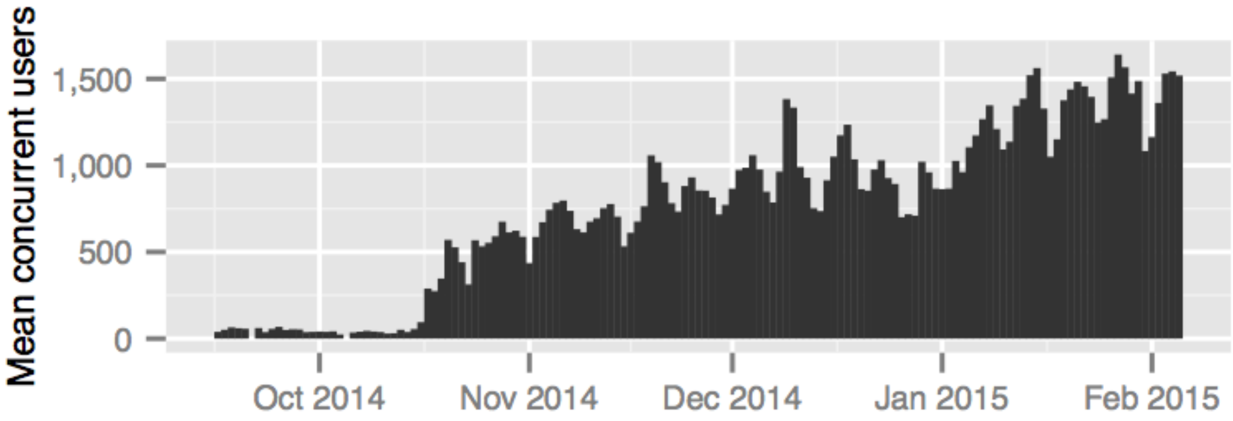


```
POST / HTTP/1.1
Host: forbidden.example
X-Session-ID: 123456...

data...
```

```
POST / HTTP/1.1
Host: forbidden.example
X-Session-ID: 123456...

data...
```



	App Engine		CloudFront		Azure (est.)	
	GB	cost	GB	cost	GB	cost
early 2014	37	$4.28	31	$3.10	0	$0.00
Sep 2014	34	$4.02	36	$4.59	47	$5.53
Oct 2014	289	$40.85	479	$130.29	298	$35.04
Nov 2014	1375	$224.67	1269	$362.60	500	$58.80
Dec 2014	2132	$326.81	1579	$417.31	512	$60.21
Jan 2015	2944	$464.37	2449	$669.02	638	$75.03
total	6811	$1065.00	5843	$1586.91	1995	$267.30

	Who	What	How
Polymorphism	**Tor bridges**, **Flash Proxy** [99], **VPN Gate** [177]	**Obfs2/3/4**, **ScrambleSuit** [247], Dust [241]	**Tor Jun, 2012**[1]
Steganography	Cirripede [118], Decoy routing [142], **GoAgent**, **Meek** [221], OSS [100], TapDance [249], Telex [250], CloudTransport [46]	**FTE** [85], Infranet [96], SkyF2F [54], Collage [49], CensorSpoofer [229], DEFIANCE [156], SkypeMorph [166], StegoTorus [237], Freewave [119], Identity-based Steganographic Tagging [196], Message In A Bottle [126], SWEET [255], Facade [137], Trist [65], Facet [155], DenaLi [171]	**Tor Jan, 2011**[2], **Tor Sep, 2011**[3] [17]

Table 1: Prior research on evading network-based censorship using obfuscation, organized by primary obfuscation method. Columns show the primary type of feature obfuscated. **Bold** denotes deployed tools.

Attacks	**List type**	**Target**	**Seen: Description**
Website blocking	Blacklist	Who	Thailand 2006: DNS filtering Tor website [80]; Iran & Saudi Arabia 2007: Block GET request pattern with `/tor/` [80]; China 2008, Iran 2012: Block Tor website [34, 154].
Block by default	Whitelist	Who	Tunisia 2009: Only allow ports 80/443 [80]; Iran 2013: TCP reset all non-HTTP [33].
SSL throttling/blocking	Blacklist	Who	Iran 2009, 2011 [30,153] SSL throttled to 2 Kb/s; Iran 2012: Block port 443 [154].
IP address blocking	Blacklist	Who	China 2009: Block public relays and directory authorities [151]; China 2010: Block bridges [152]; Iran 2014: Block directory authorities [31].
Deep packet inspection (DPI)	Blacklist	How	Iran 2011: On Diffie–Hellman parameter in SSL handshake [80]; Iran 2011, Iran 2013: On SSL certificate lifetime [79, 153]; Syria 2011 and 2012: On TLS renegotiation [80]; China 2011: On TLS cipher list in "Client Hello" [239]; Iran 2012, UAE 2012: On TLS handshake [154,200]; Iran 2012: On TLS client key exchange [33]; Ethiopia 2012, Kazakhstan 2012: On TLS "Server Hello" [198,199]; Philippines 2012: On TLS cipher suite [242].
Active probing	(Blacklist)	How	Probing is used to populate a blacklist. China 2011, 2013 [120, 243].
Unplug Internet	N/A	N/A	Egypt 2011, Libya 2011 [21], Syria 2012 [61].

Table 2: Survey of Known Tor Censorship Incidents