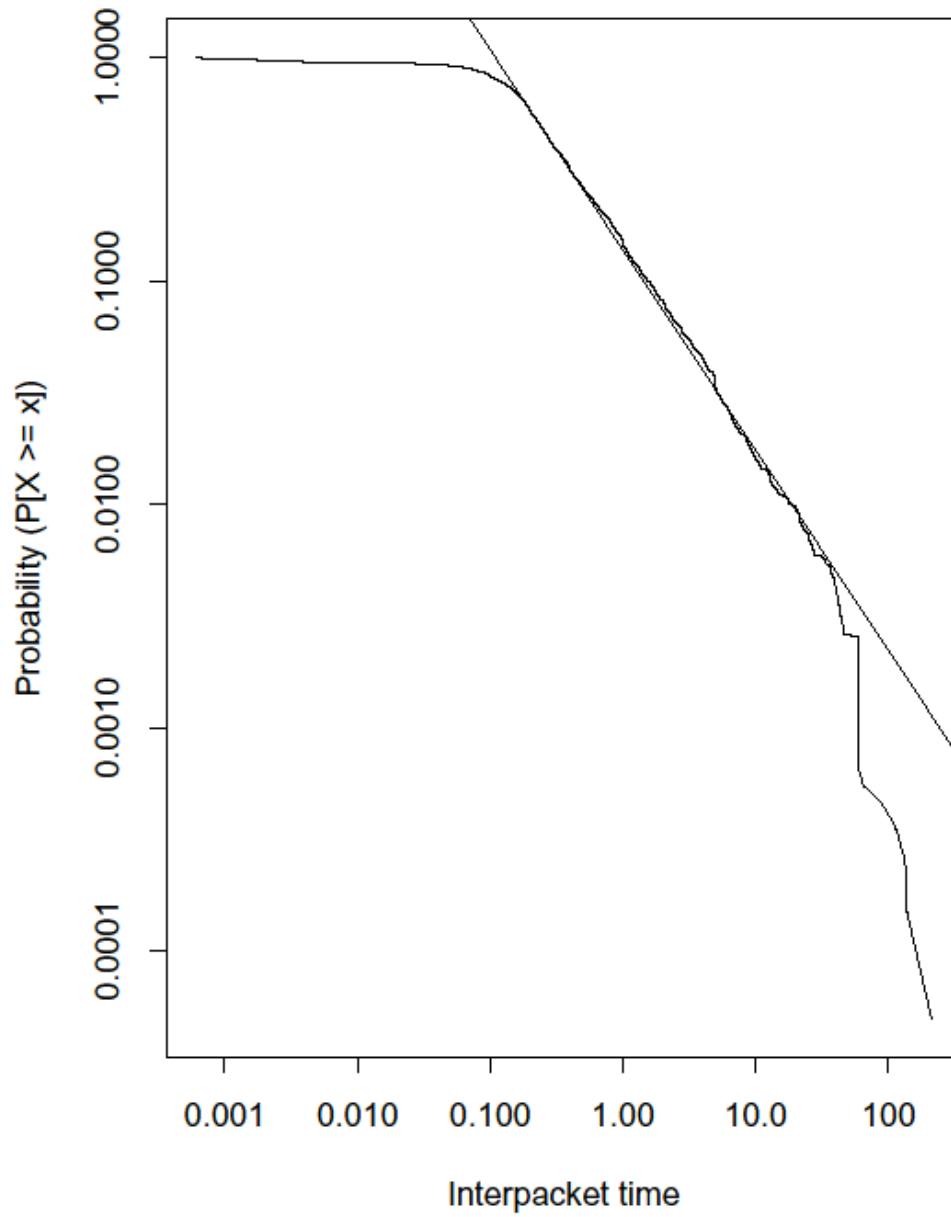


Log-Log plot of Telnet packet interarrivals



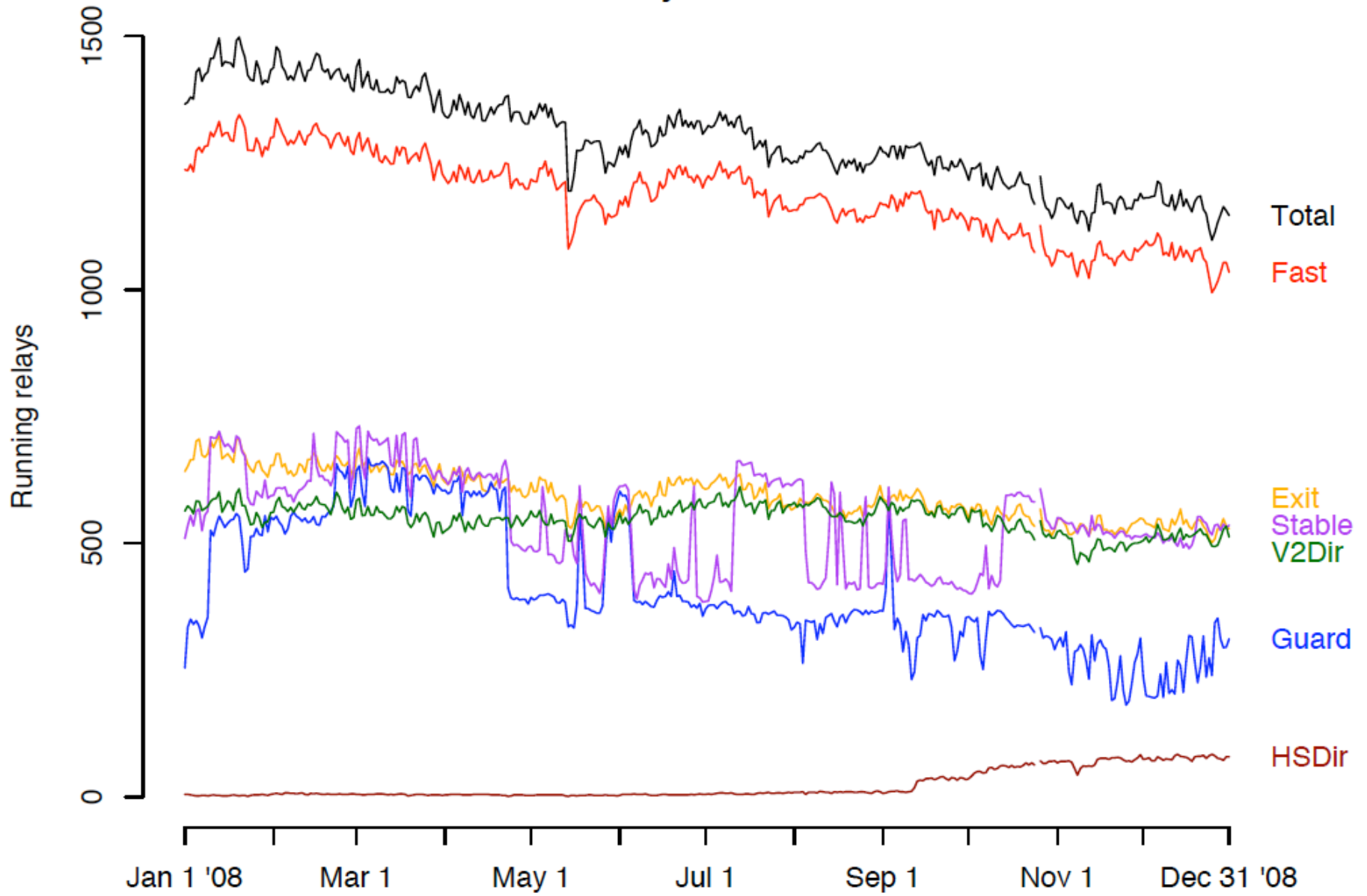
Port	Number of Exit Nodes
22	211
53	216
80	226
110	210
143	208
443	238
5190	184
6667	172

Port	Number of Exit Nodes
25	4
119	25
135–139	6
445	6
465	12
587	13
1214	7
4661–4666	5
6699	9

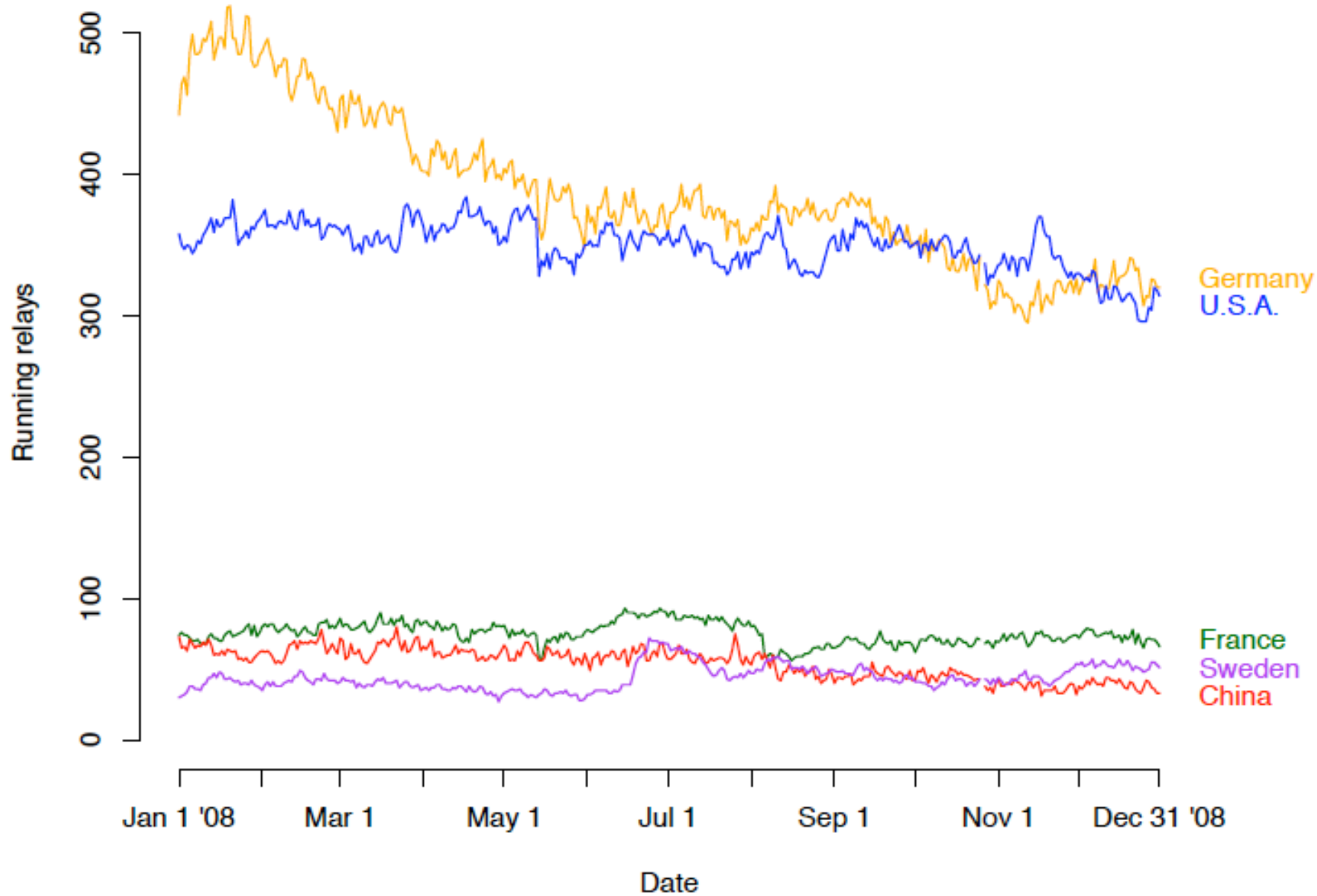
**Table 1.** Exit traffic protocol distribution by number of TCP connections, size, and number of unique destination hosts.

<b>Protocol</b>	<b>Connections</b>	<b>Bytes</b>	<b>Destinations</b>
HTTP	12,160,437 (92.45%)	411 GB (57.97%)	173,701 (46.01%)
SSL	534,666 (4.06%)	11 GB (1.55%)	7,247 (1.91%)
BitTorrent	438,395 (3.33%)	285 GB (40.20%)	194,675 (51.58%)
Instant Messaging	10,506 (0.08%)	735 MB (0.10%)	880 (0.23%)
E-Mail	7,611 (0.06%)	291 MB (0.04%)	389 (0.10%)
FTP	1,338 (0.01%)	792 MB (0.11%)	395 (0.10%)
Telnet	1,045 (0.01%)	110 MB (0.02%)	162 (0.04%)
<b>Total</b>	<b>13,154,115</b>	<b>709 GB</b>	<b>377,449</b>

# Relay statuses



## Relay locations

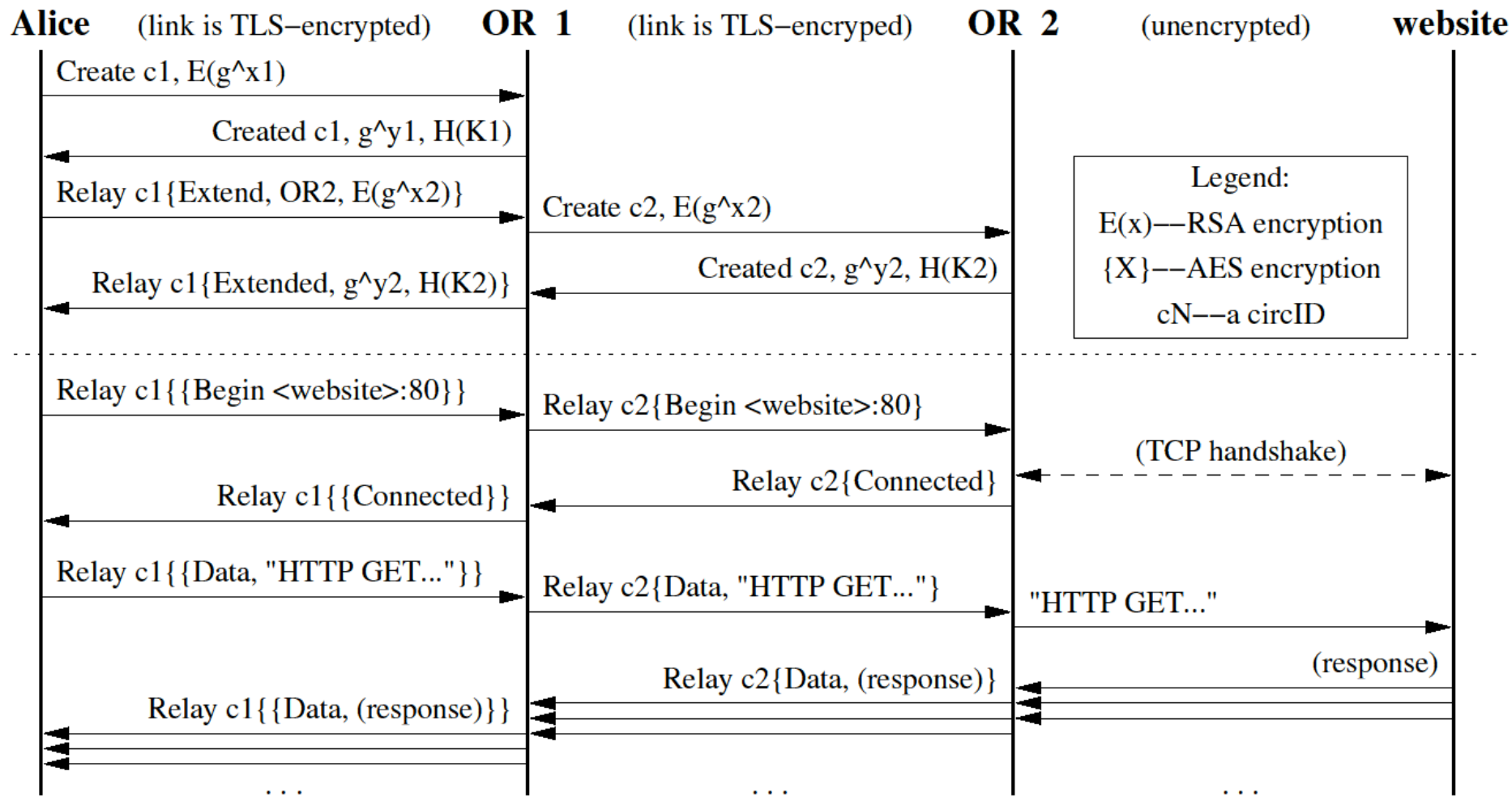


<b>Client Distribution</b>		<b>Router Distribution</b>	
<i>Country</i>	<i>Total</i>	<i>Country</i>	<i>Total</i>
Germany	2,304	Germany	374
China	988	United States	326
United States	864	France	69
Italy	254	China	40
Turkey	221	Italy	36
United Kingdom	170	Netherlands	35
Japan	155	Sweden	35
France	150	Finland	25
Russia	146	Austria	24
Brazil	134	United Kingdom	24

<b>Relative Tor Usage</b>	
<i>Country</i>	<i>Ratio</i>
Germany	7.73
Turkey	2.47
Italy	1.37
Russia	0.89
China	0.84
France	0.77
United Kingdom	0.75
United States	0.62
Brazil	0.56
Japan	0.32

2	1	509 bytes
CircID	CMD	DATA

2	1	2	6	2	1	498
CircID	Relay	StreamID	Digest	Len	CMD	DATA





FIELD	(IP_verhl,	1,	KEEP)
FIELD	(IP_tos,	1,	KEEP)
FIELD	(IP_len,	2,	KEEP)
FIELD	(IP_id,	2,	KEEP)
FIELD	(IP_frag,	2,	KEEP)
FIELD	(IP_ttl,	1,	KEEP)
FIELD	(IP_proto,	1,	KEEP)
PUTOFF_FIELD	(IP_cksum,	2,	ZERO)
FIELD	(IP_src,	4,	anonymize_ip_addr)
FIELD	(IP_dst,	4,	anonymize_ip_addr)
FIELD	(IP_options,	VARLEN,	anonymize_ip_options)
PICKUP_FIELD	(IP_cksum,	0,	recompute_ip_checksum)
FIELD	(IP_data,	VARLEN,	anonymize_ip_data)

**Figure 1: Specification for IP header anonymization.**

CASE	(TCPOPT_eol,	0, 1,	KEEP)
CASE	(TCPOPT_nop,	1, 1,	KEEP)
CASE	(TCPOPT_mss,	2, 4,	KEEP)
CASE	(TCPOPT_wsopt,	3, 3,	KEEP)
CASE	(TCPOPT_sackperm,	4, 2,	KEEP)
CASE	(TCPOPT_sack,	5, VARLEN,	KEEP)
CASE	(TCPOPT_tsopt,	8, 10,	renumber_tcp_timestamp)
CASE	(TCPOPT_cc,	11, VARLEN,	KEEP)
CASE	(TCPOPT_ccnew,	12, VARLEN,	KEEP)
DEFAULT_CASE	(TCPOPT_other,	VARLEN,	TCPOPT_alert_and_replace_with_NOP)

**Figure 2: TCP option anonymization specification.**

Section	Meta-Data
§ 3.1	Packets found in the original trace with bad checksums are flagged in the meta-data, with a version of the packet with a bad checksum placed in the anonymized trace.
§ 3.1	Truncated packets found in the original trace are noted in the meta-data. The packet inserted into the anonymized trace has a corrected checksum based on the sanitized packet.
§ 3.2	The meta-data includes a rough frequency table of Ethernet vendor codes.
§ 3.3	The meta-data contains a list of the anonymized prefix and size of each internal subnet found in the trace, along with the subnet's gateway and broadcast addresses.
§ 3.3	The anonymized IP address of detected scanners is included in the meta-data. The anonymization maps addresses for the target in traffic involving scanners differently than addresses in non-scanning traffic.
§ 3.3	The meta-data lists addresses that are part of LBNL's address space, but not from a valid LBNL subnet.
§ 3.4	Hosts for which <code>tcpmkpub</code> could not determine the endianness of TCP's timestamp option are flagged in the meta-data. The order of the timestamps for these hosts is based on the order in which the packets arrive at the tracing location, rather than the time at which they were transmitted.
§ 6	The meta-data gives the number of packets completely removed from the traces due to policy considerations.
§ 6	The meta-data includes a tag indicating the anonymization key used to conduct the transformations. All traces with the same tag are uniformly anonymized.
§ 6	The meta-data includes a checksum digest of the anonymized packet trace to ensure that the traces and meta-data can be properly paired.

**Table 1: Meta-data accompanying the anonymized traces.**