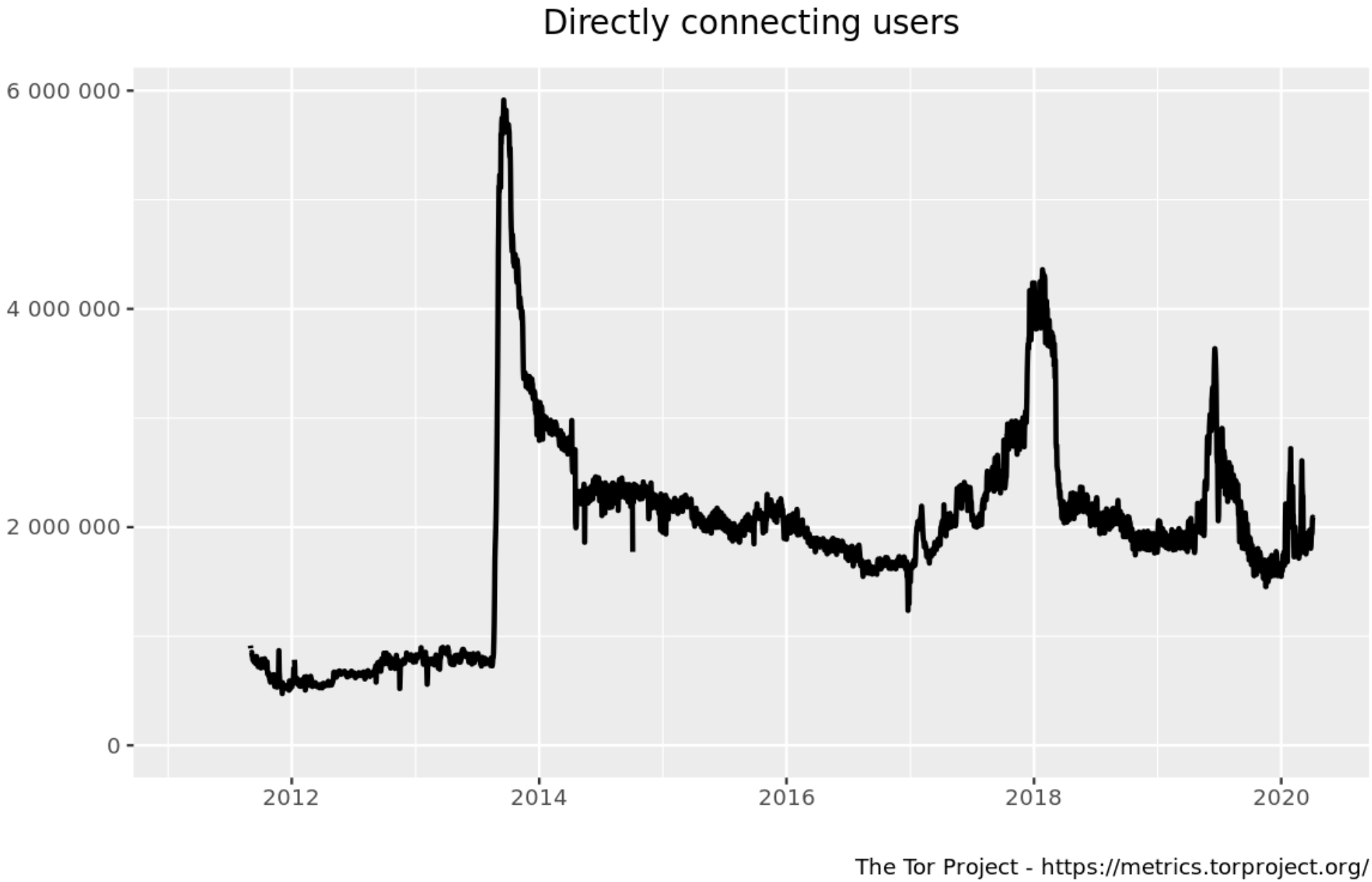
Lecture Outline

- Feedback from Bill Marczak's lecture?

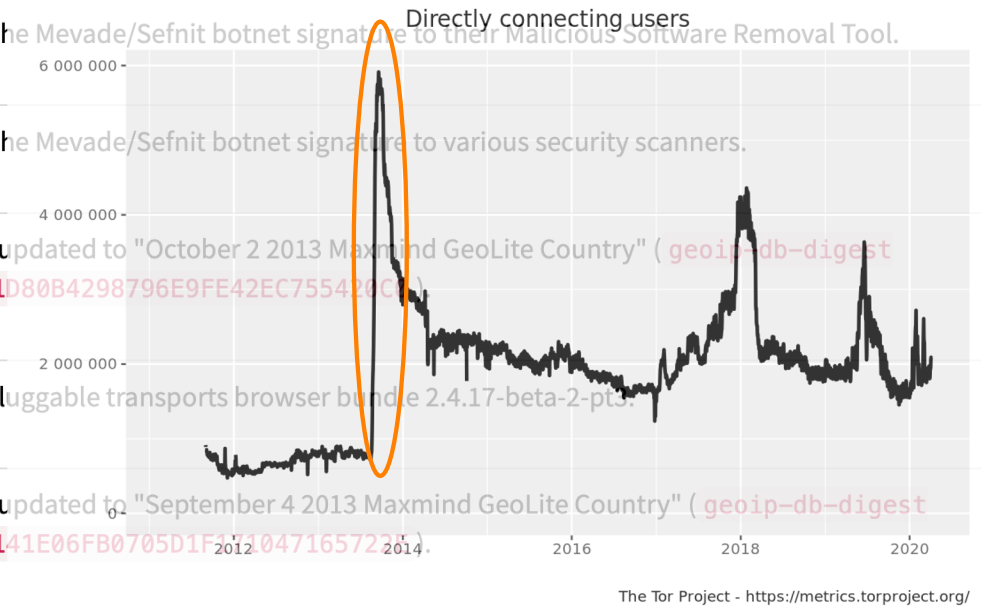
- A bit about Anonymity:
  - Brief look at Tor's evolution …
  - … plus a "teachable moment"

- The problem of Spam
  - *Measurement* of a botmaster's spamming operations
  - DNSBLs and *counter-intelligence*
  - Spammer $$

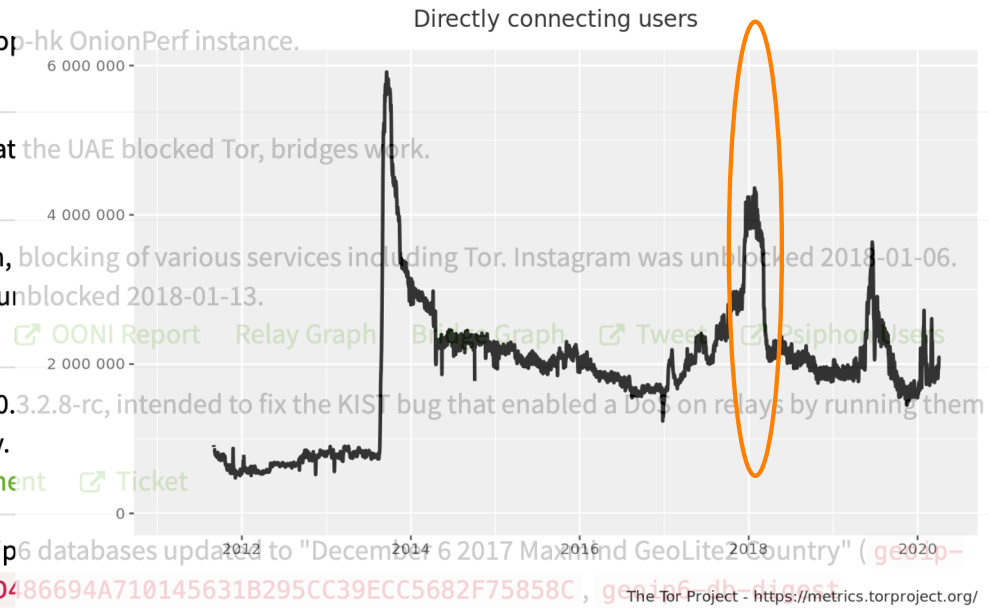
Tor's Evolution


Directly connecting users
6 000 000
4 000 000
2 000 000
0
2012
2014
2016
2018
2020
The Tor Project - https://metrics.torproject.org/

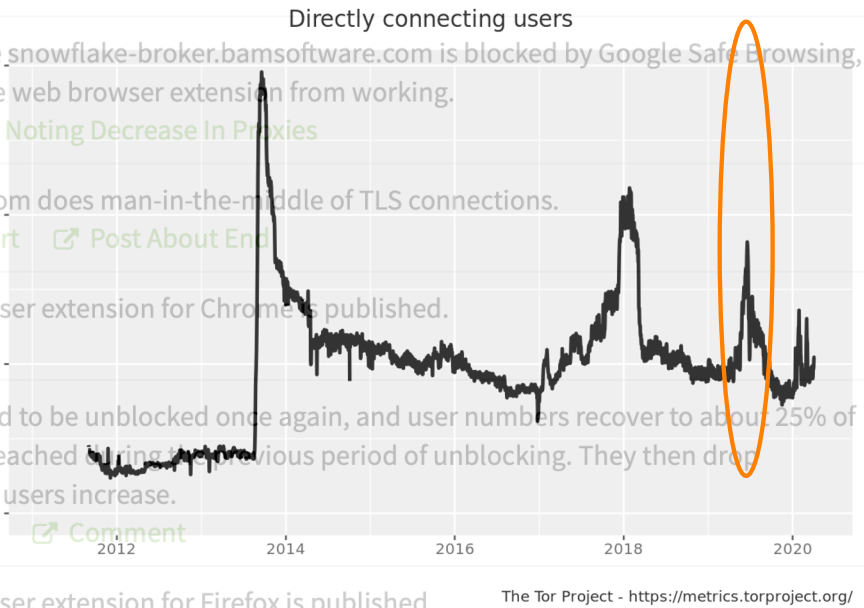
2013-11-03	<OR> Relays	Microsoft adds the Mevade/Sefnit botnet signature to their Malicious Software Removal Tool. Blog Post
2013-10-27	<OR> Relays	Microsoft adds the Mevade/Sefnit botnet signature to various security scanners. Blog Post
2013-10-11	ipv4	geoip database updated to "October 2 2013 Maxmind GeoLite Country" (`geoip-db-digest` `A28267CED18A1D80B4298796E9FE42EC7554...`). Commit
2013-09-23	flashproxy obfs2 obfs3	Release of the pluggable transports browser bundle 2.4.17-beta-2-pt3. Blog Post
2013-09-10	ipv4	geoip database updated to "September 4 2013 Maxmind GeoLite Country" (`geoip-db-digest` `CB632F60547F141E06FB0705D1F...`). Commit
2013-08-19 to 2014-04-28	<OR> Relays	Relay users increase globally from about 800K to over 5M, when computers in the Mevade/Sefnit botnet began using Tor to communicate. The user count decreased in the following months through efforts to clean up the botnet. Sometime in 2014-04, the botnet switched from using Tor to using SSH. Blog Post Tech Report Analysis Switch To SSH
2013-08-12	ipv4	geoip database updated to "August 7 2013 Maxmind GeoLite Country" (`geoip-db-digest` `83CCB5AF823A5CCF3C86C3CA33AF801D4E8996EC`). Commit
2013-08-10	flashproxy obfs2 obfs3	Release of the pluggable transports browser bundle 2.4.15-beta-2-pt1. Blog Post
2013-07-08	ipv4	geoip database updated to "July 3 2013 Maxmind GeoLite Country" (`geoip-db-digest` `4D558EA73DD91A0361DE3FA3E83171DCD38D1A2D`). Commit
2013-06-05	ipv4	geoip database updated to "June 5 2013 Maxmind GeoLite Country" (`geoip-db-digest` `5E570BB92DBEE1D517E35DAA4A52F58FDA6BB44E`). Commit
2013-06-02	flashproxy obfs2 obfs3	Release of the pluggable transports browser bundle 2.4.12-alpha-2-pt1. Blog Post

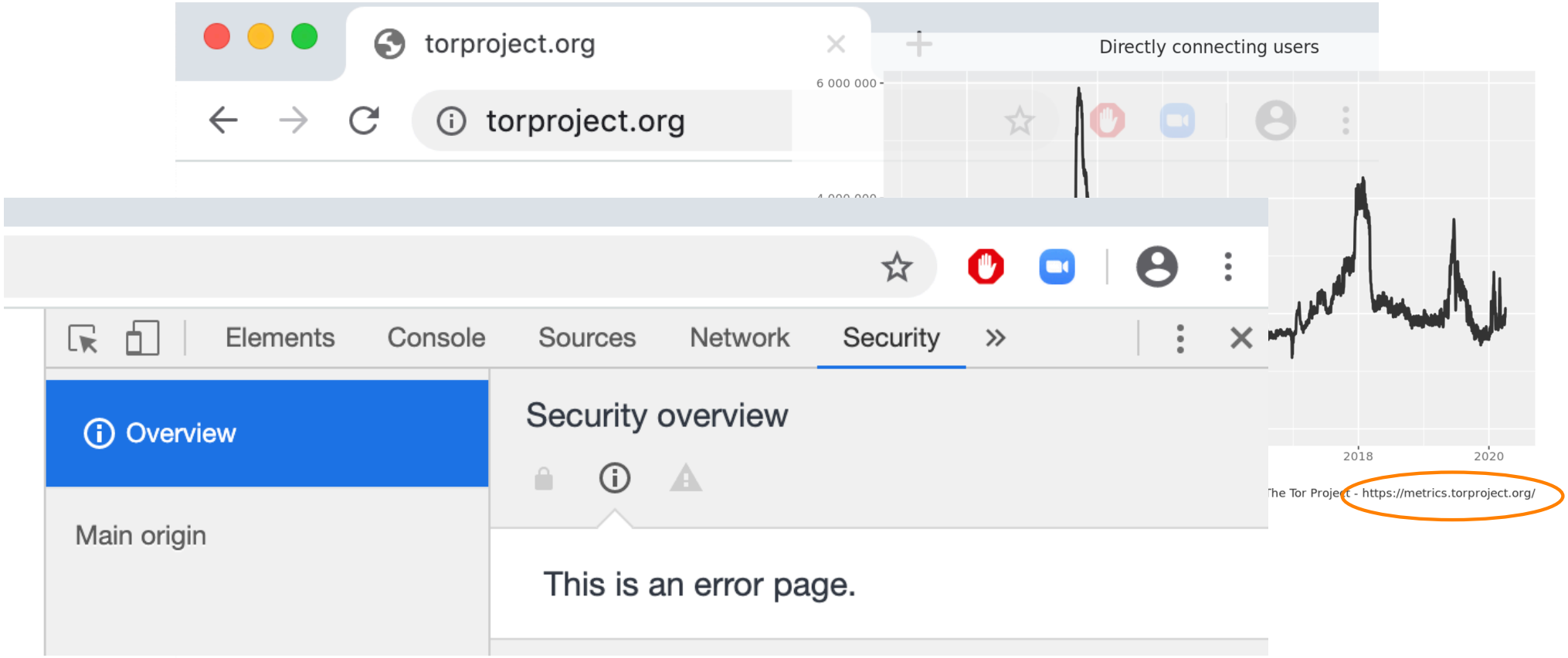


2018-01-05 to present		Outage of the op-hk OnionPerf instance. Op-Hk Graph
2018-01-01	United Arab Emirates Relays	User report that the UAE blocked Tor, bridges work. Comment
2017-12-28 to 2018-01-13	Iran	Protests in Iran, blocking of various services including Tor. Instagram was unblocked 2018-01-06. Telegram was unblocked 2018-01-13. Wikipedia OONI Report Relay Graph Bridge Graph Tweet Psiphon Users
2017-12-21		Release of tor 0.3.2.8-rc, intended to fix the KIST bug that enabled a DoS on relays by running them out of memory. Announcement Ticket
2017-12-20	ipv4 ipv6	geoip and geoip6 databases updated to "December 6 2017 MaxMind GeoLite2 Country" (`geoip-db-digest 1D486694A710145631B295CC39ECC5682F75858C` , `geoip6-db-digest F33231CAC761A71F7C19273DB1E11CEE01E2D982`). Commit
2017-12-16 to 2017-12-17	Bridges Unknown	Drop in the number of measured bridges. Graph Mailing List Post
2017-12-12 to 2018-01-18	meek	Outage of the meek.bamsoftware.com (unthrottled for public use), meek.bamsoftware.com:7443 (former meek-azure, now unused), and gaeuploader.meek.bamsoftware.com (used by GAEuploader) bridges.
2017-12-12 to 2018-01-10	France <OR> Relays Unknown	Temporary tripling of relay users in France. Bridges not affected. Graph
2017-12-10 to 2018-02-01	Germany <OR> Relays Unknown	Further, slow increase of relay users in Germany, from 500k to over 1.5M. Graph Reddit Thread Ticket
2017-12-09	<OR> ipv6 Relays	Release of Tor Browser 7.0.11, containing tor 0.3.1.9, which adds an IPv6 address for the bridge authority bastet. Blog Post
2017-12-09	<OR> ipv6 Relays	Release of Tor Browser 7.5a9, containing tor 0.3.2.6-alpha, which adds an IPv6 address for the bridge authority bastet. Blog Post



2019-07-23	snowflake	The broker dom ain name snowflake-broker.bamsoftware.com is blocked by Google Safe Browsing, preventing the S nowflake web browser extensio n from working. Ticket C omment Noting Decrease In Proxies
2019-07-18 to 2019-08-07	Kazakhstan	The Kazakh ISP KazTelecom does man-in-the-m iddle of TLS connections. Censored Pla net Report Post About End
2019-07-03	snowflake	The Snowflake v web browser extension for Chrome is published. Comment
2019-07-02 to 2019-08-26	Iran <OR> Relays Bridges	Relays in Iran ar e reported to be unblocked once again, and user numbers recover to about 25% of the maximum th ey had reached during the previous period of unblocking. They then drop precipitously, a nd bridge users increase. Ticket C omment Comment
2019-06-26	snowflake	The Snowflake v web browser extension for Firefox is published. Comment
2019-06-21 to present	Burma	Internet shutdown in parts of Myanmar. Report
2019-06-20	obfs4	A call to set up new obfs4 bridges is posted to the tor-relays mailing list. Mailing List Thread Thread Continues
2019-05-28		Failure of network equipment at site of op-ab OnionPerf instance (equipment now replaced) Onionperf Timeouts Graph
2019-05-22	fte	Release of Tor Browser 9.0a1, removes support for FTE. Blog Post Ticket
2019-05-17	ipv4 ipv6	geoip and geoip6 databases updated to "May 13 2019 Maxmind GeoLite2 Country" (`geoip-db-digest 35DFDA2D06D2A0467EF37D60A67B438B11952B74` , `geoip6-db-digest C0193A1D086819353FABBF70AADB15866B7B2525`). Commit
2019-05-16 to 2019-06-23	Iran Relays	Tor becomes directly accessible in Iran, leading to an explosion in relay users up to about 1.5 million, before being blocked again. Ticket Comment About End Tor-Talk Thread Reddit Thread Comment Reddit Thread





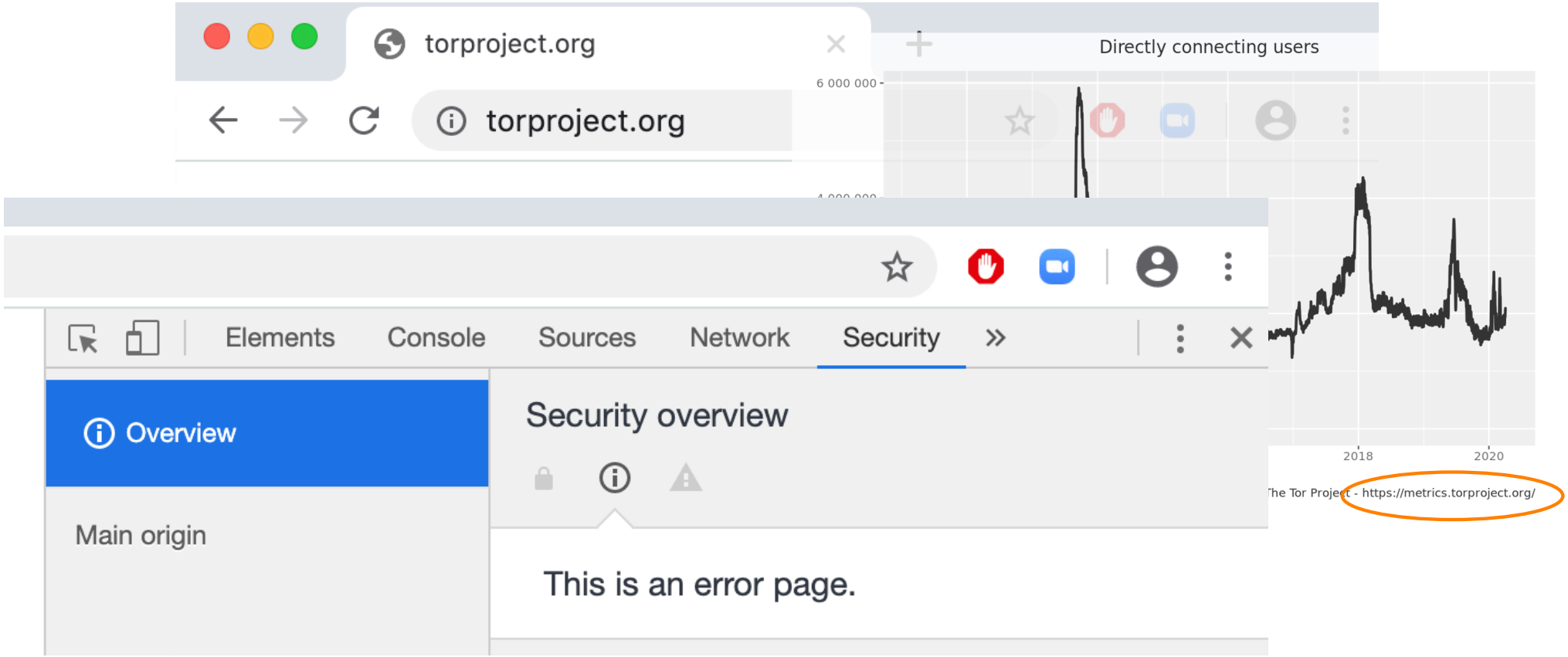
This site can't provide a secure connection

torproject.org sent an invalid response.

ERR_SSL_PROTOCOL_ERROR

None of my browsers can get to `torproject.org` from my home

Reload



This site can't provide a secure connection

torproject.org sent an invalid response.

ERR_SSL_PROTOCOL_ERROR

But it works through campus VPN

Reload

Users

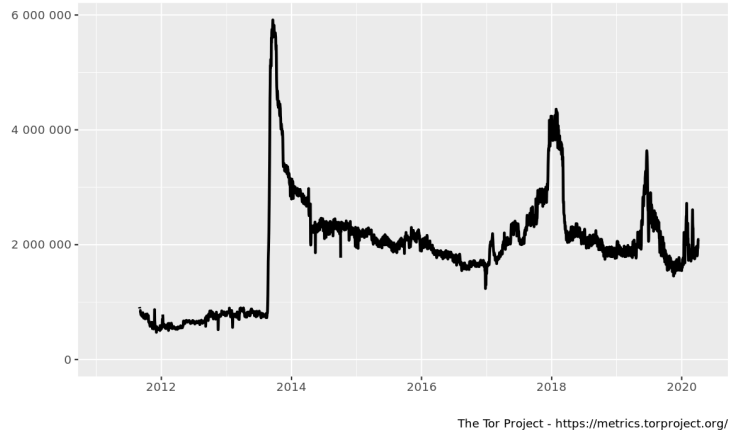
We estimate the number of users by analyzing the requests induced by clients to relays and bridges.

Relay users | Bridge users by country | Bridge users by transport | Bridge users by country and transport | Bridge users by IP version

BridgeDB requests by requested transport | BridgeDB requests by distributor | Top-10 countries by relay users

Top-10 countries by possible censorship events | Top-10 countries by bridge users | "The anonymous Internet"

Directly connecting users



Start date: 2010-01-01

End date: 2020-04-07

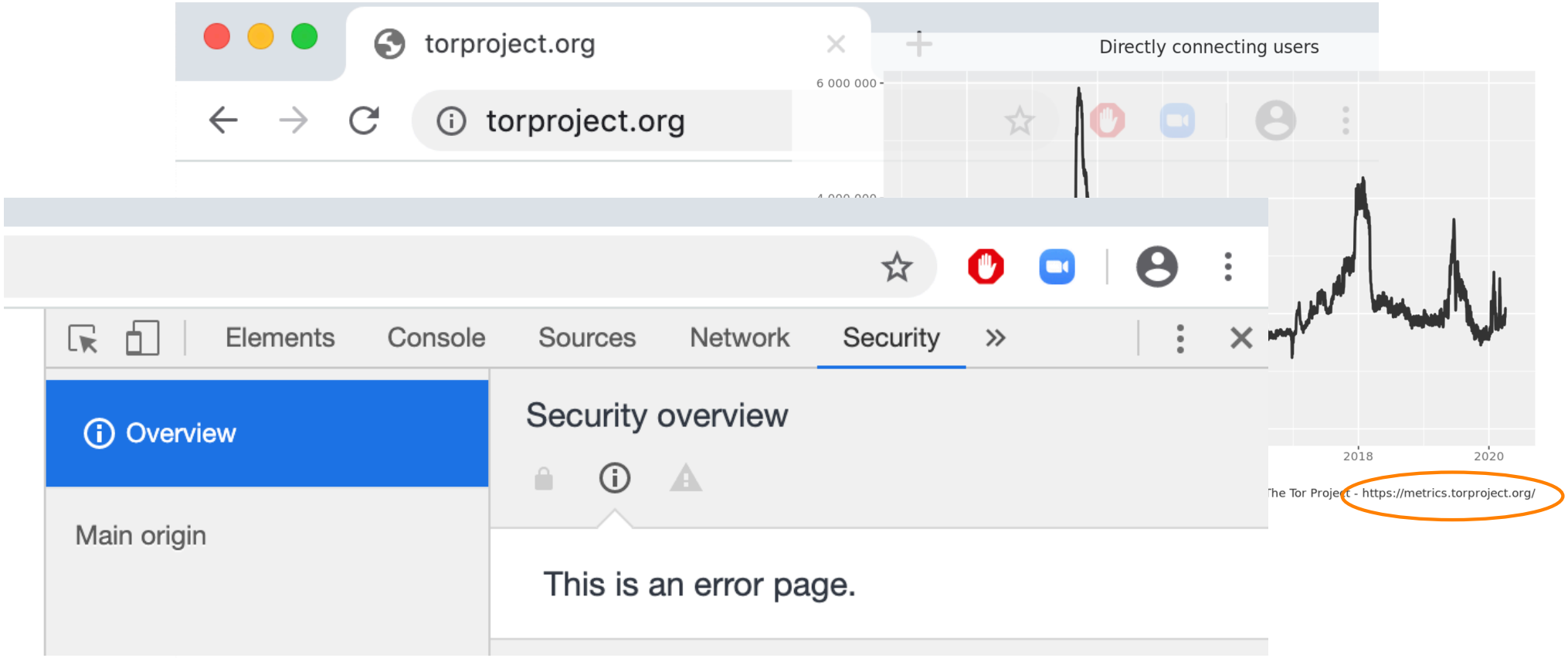
Source: All users

Show possible censorship events if available: Off

Update graph

Download graph as PNG or PDF.

This graph shows the estimated number of directly-connecting clients; that is, it excludes clients connecting via



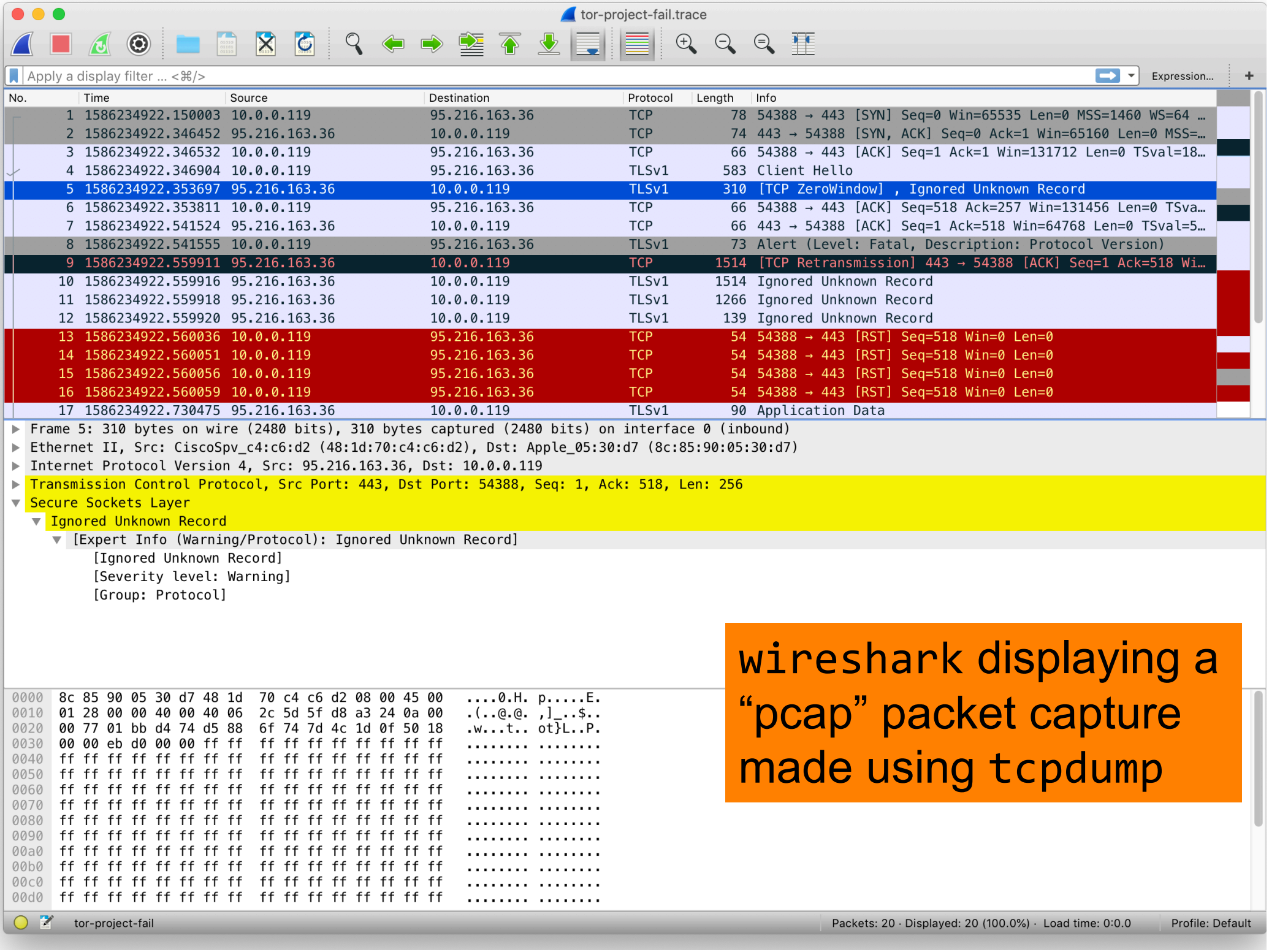
This site can't provide a secure connection

torproject.org sent an invalid response.

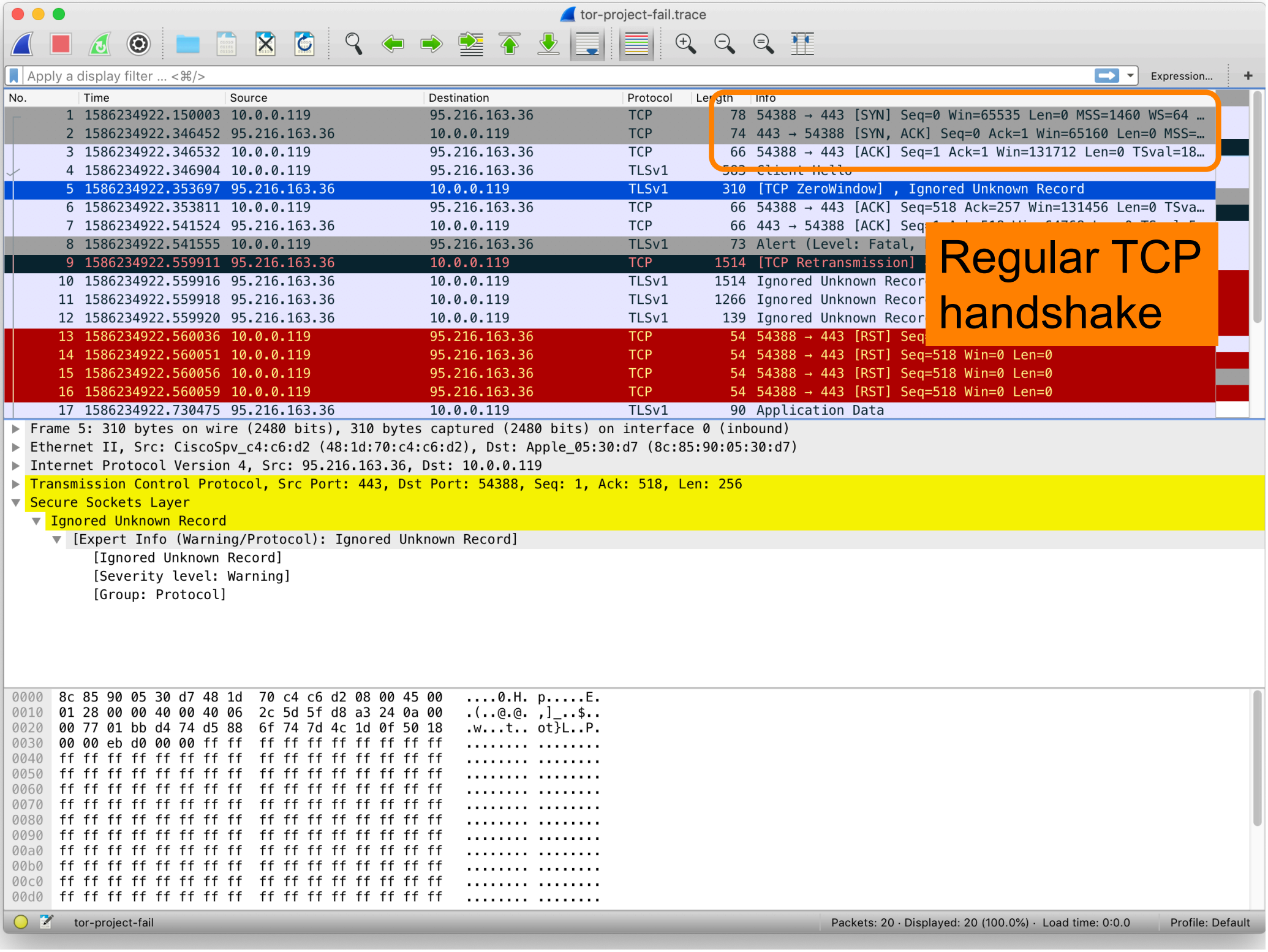
ERR_SSL_PROTOCOL_ERROR

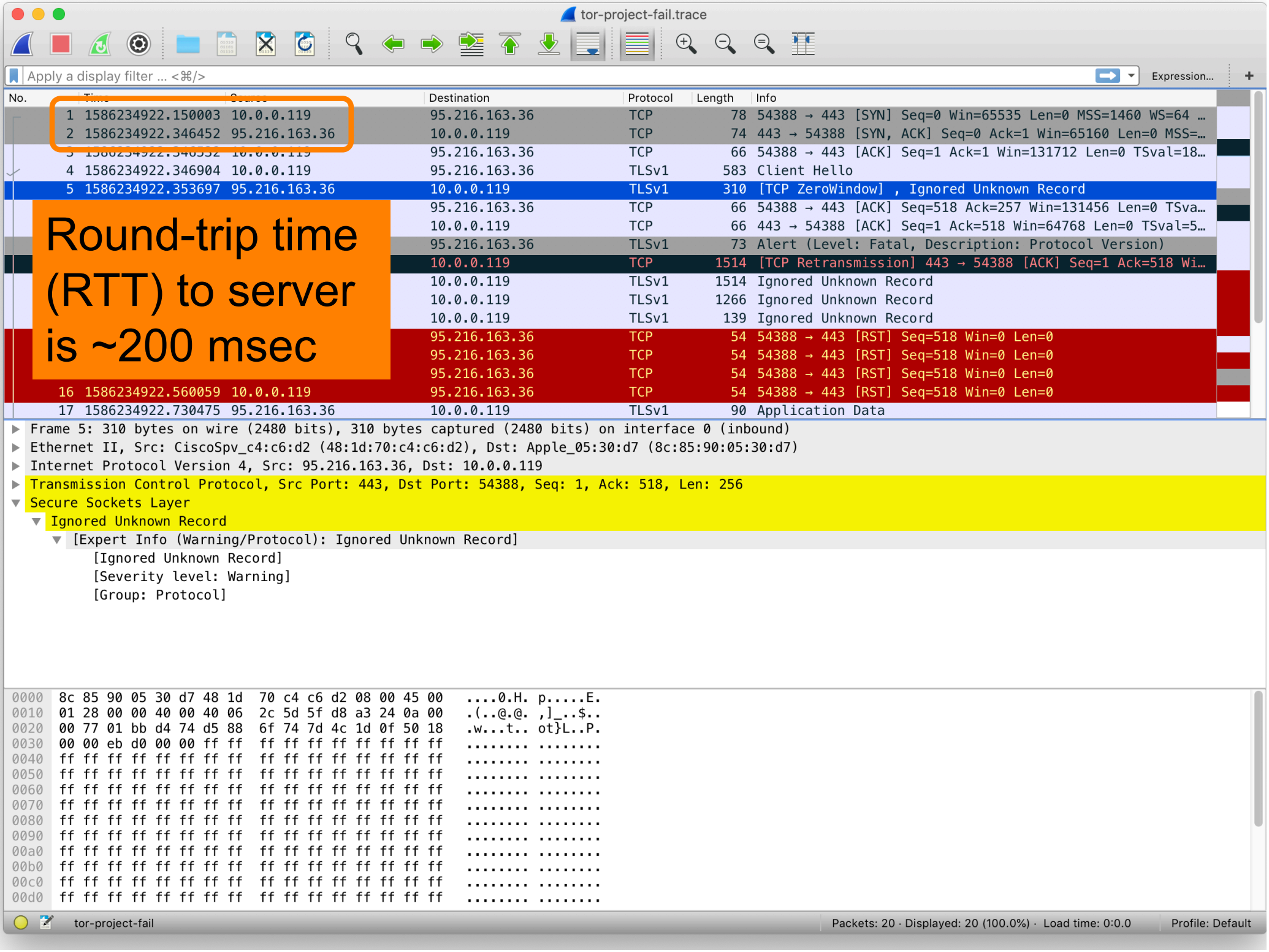
How do we diagnose this failure?

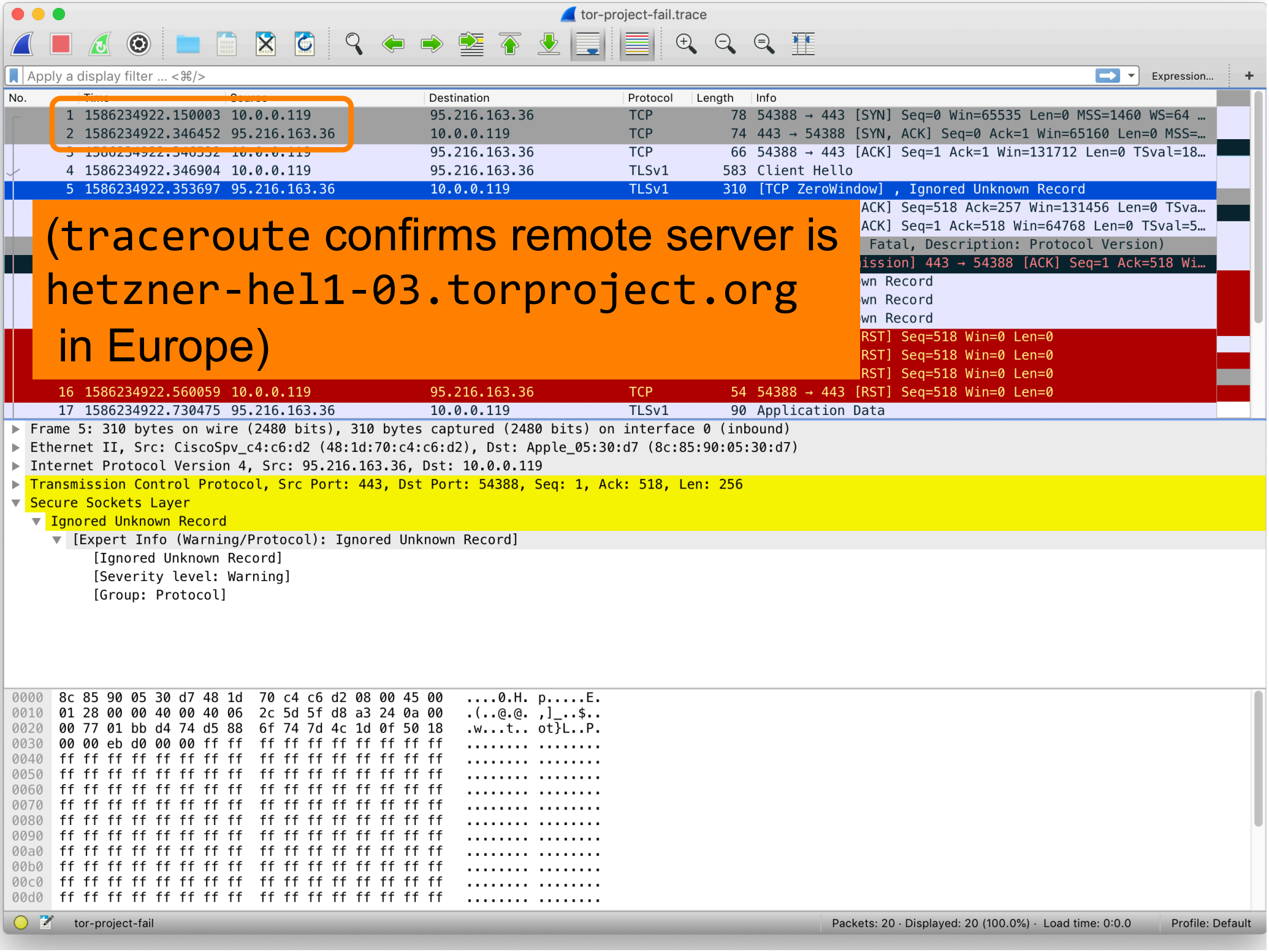
Reload

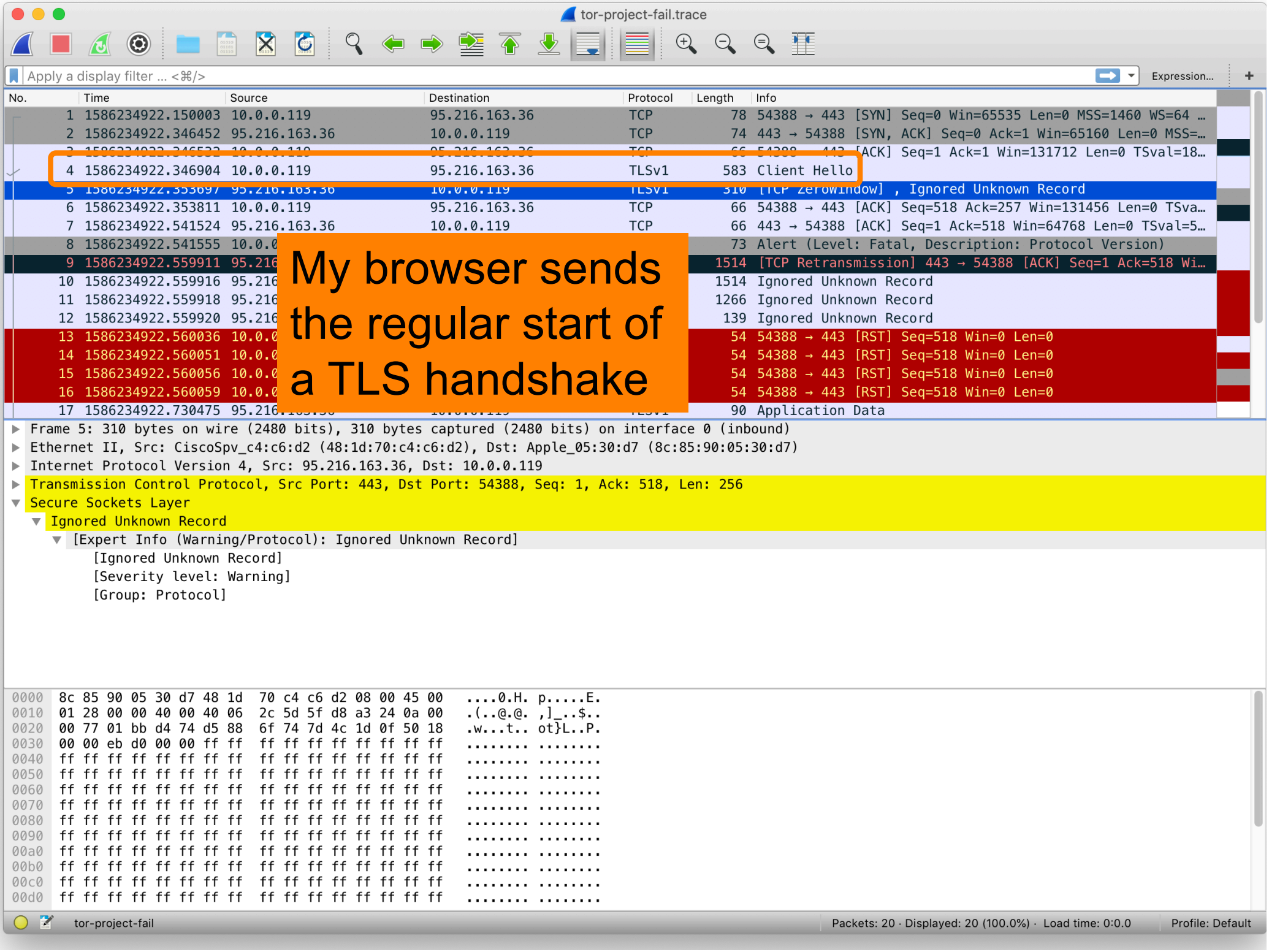


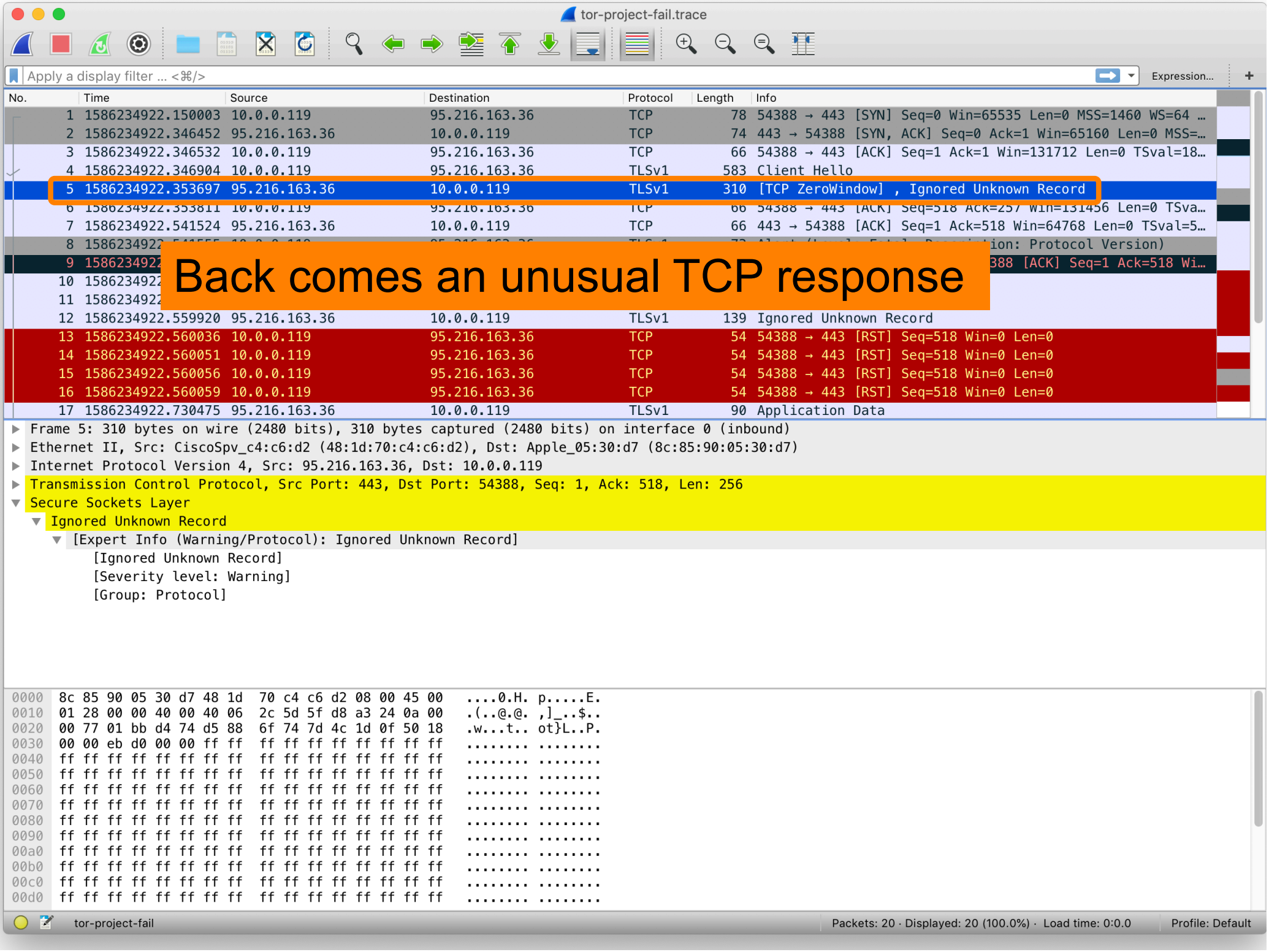
wireshark displaying a "pcap" packet capture made using tcpdump

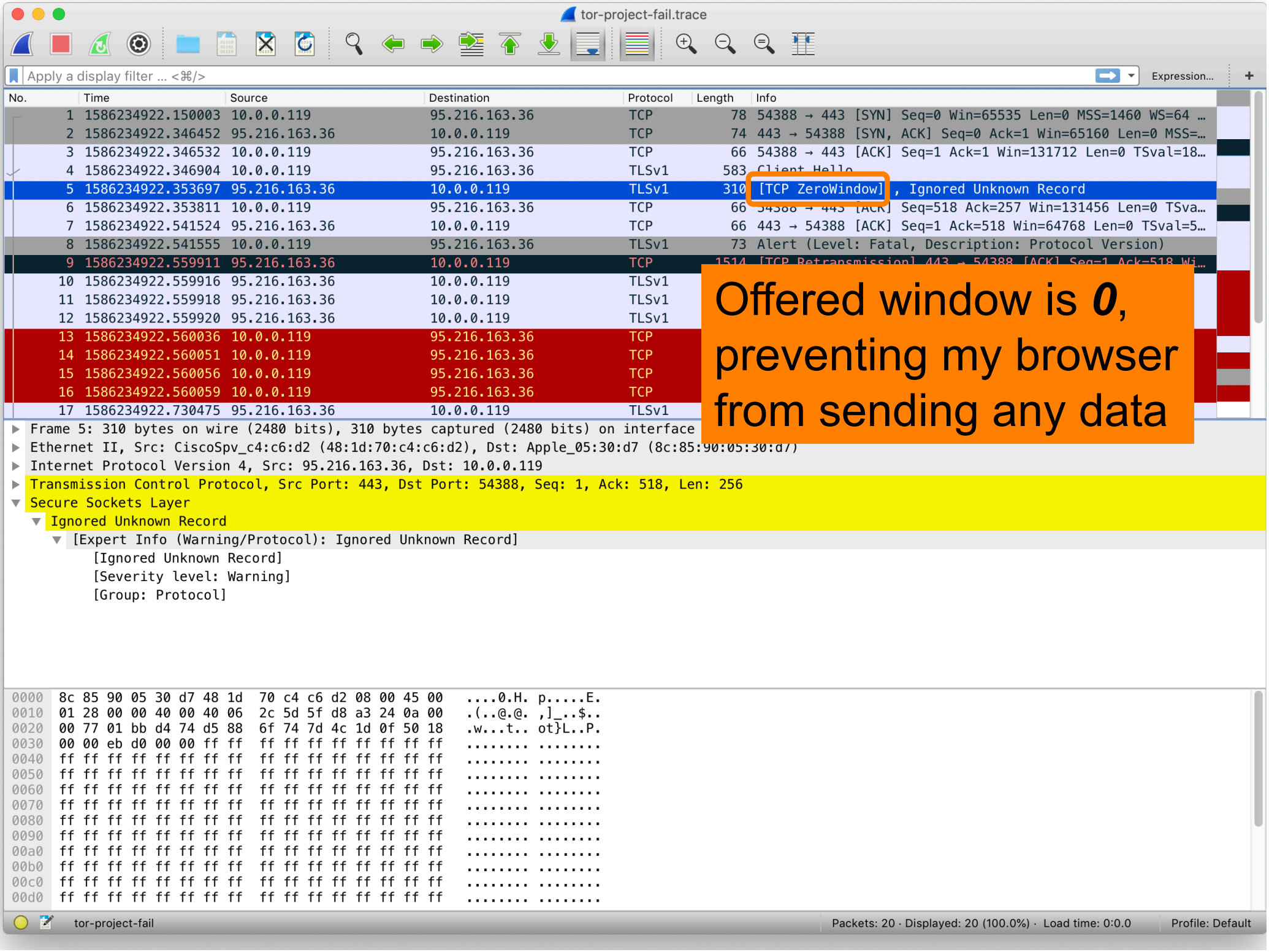

tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3 1586234922.346532 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
6 1586234922.353811 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq
8 1586234922.541555 10.0.0.119 95.216.163.36 TLSv1 73 Alert (Level: Fatal,
9 1586234922.559911 95.216.163.36 10.0.0.119 TCP 1514 [TCP Retransmission]
10 1586234922.559916 95.216.163.36 10.0.0.119 TLSv1 1514 Ignored Unknown Recor
11 1586234922.559918 95.216.163.36 10.0.0.119 TLSv1 1266 Ignored Unknown Recor
12 1586234922.559920 95.216.163.36 10.0.0.119 TLSv1 139 Ignored Unknown Recor
13 1586234922.560036 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq
14 1586234922.560051 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
15 1586234922.560056 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
16 1586234922.560059 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
17 1586234922.730475 95.216.163.36 10.0.0.119 TLSv1 90 Application Data
Regular TCP handshake
Frame 5: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface 0 (inbound)
Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)
Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119
Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256
Secure Sockets Layer
Ignored Unknown Record
[Expert Info (Warning/Protocol): Ignored Unknown Record]
[Ignored Unknown Record]
[Severity level: Warning]
[Group: Protocol]
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 01 28 00 00 40 00 40 06 2c 5d 5f d8 a3 24 0a 00 .(..@.@. ,]_..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 50 18 .w...t.. ot}L..P.
0030 00 00 eb d0 00 00 ff ff ff ff ff ff ff ff ff ff ....
0040 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0050 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0060 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0070 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0080 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0090 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00a0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00b0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00c0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00d0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
tor-project-fail
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.0
Profile: Default

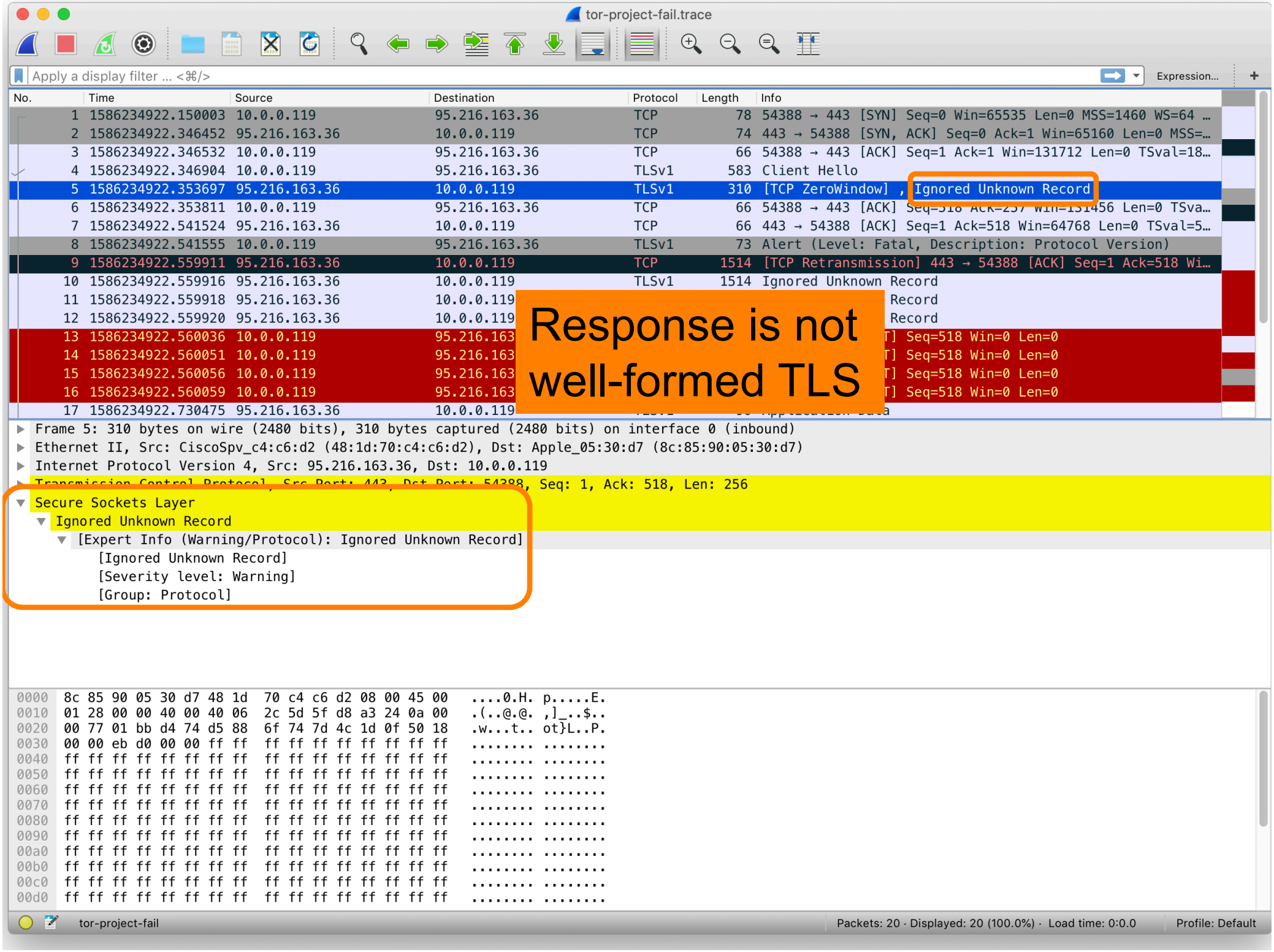

tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
95.216.163.36 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
10.0.0.119 TCP 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10.0.0.119 TLSv1 1514 Ignored Unknown Record
10.0.0.119 TLSv1 1266 Ignored Unknown Record
10.0.0.119 TLSv1 139 Ignored Unknown Record
95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
16 1586234922.560059 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
17 1586234922.730475 95.216.163.36 10.0.0.119 TLSv1 90 Application Data
Round-trip time (RTT) to server is ~200 msec
Frame 5: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface 0 (inbound)
Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)
Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119
Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256
Secure Sockets Layer
Ignored Unknown Record
[Expert Info (Warning/Protocol): Ignored Unknown Record]
[Ignored Unknown Record]
[Severity level: Warning]
[Group: Protocol]
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 01 28 00 00 40 00 40 06 2c 5d 5f d8 a3 24 0a 00 .(..@.@. ,]_..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 50 18 .w...t.. ot}L..P.
0030 00 00 eb d0 00 00 ff ff ff ff ff ff ff ff ff ff ....
0040 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0050 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0060 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0070 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0080 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0090 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00a0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00b0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00c0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00d0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
tor-project-fail
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.0
Profile: Default

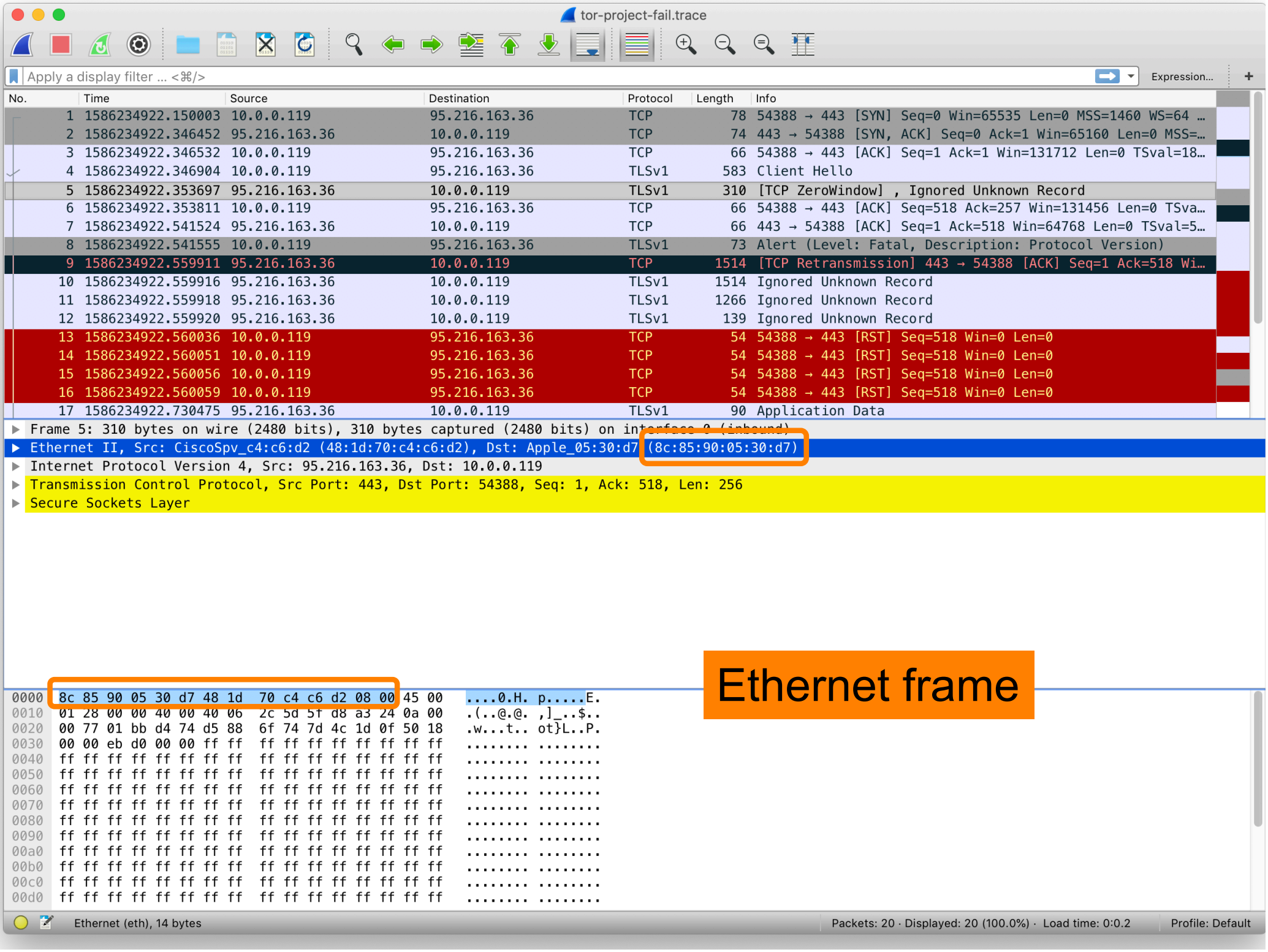

tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
(traceroute confirms remote server is hetzner-hel1-03.torproject.org in Europe)
16 1586234922.560059 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
17 1586234922.730475 95.216.163.36 10.0.0.119 TLSv1 90 Application Data
Frame 5: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface 0 (inbound)
Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)
Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119
Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256
Secure Sockets Layer
Ignored Unknown Record
[Expert Info (Warning/Protocol): Ignored Unknown Record]
[Ignored Unknown Record]
[Severity level: Warning]
[Group: Protocol]
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 01 28 00 00 40 00 40 06 2c 5d 5f d8 a3 24 0a 00 .(..@.@. ,]_..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 50 18 .w...t.. ot}L..P.
0030 00 00 eb d0 00 00 ff ff ff ff ff ff ff ff ff ff ....
0040 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0050 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0060 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0070 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0080 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0090 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00a0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00b0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00c0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00d0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
tor-project-fail
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.0
Profile: Default

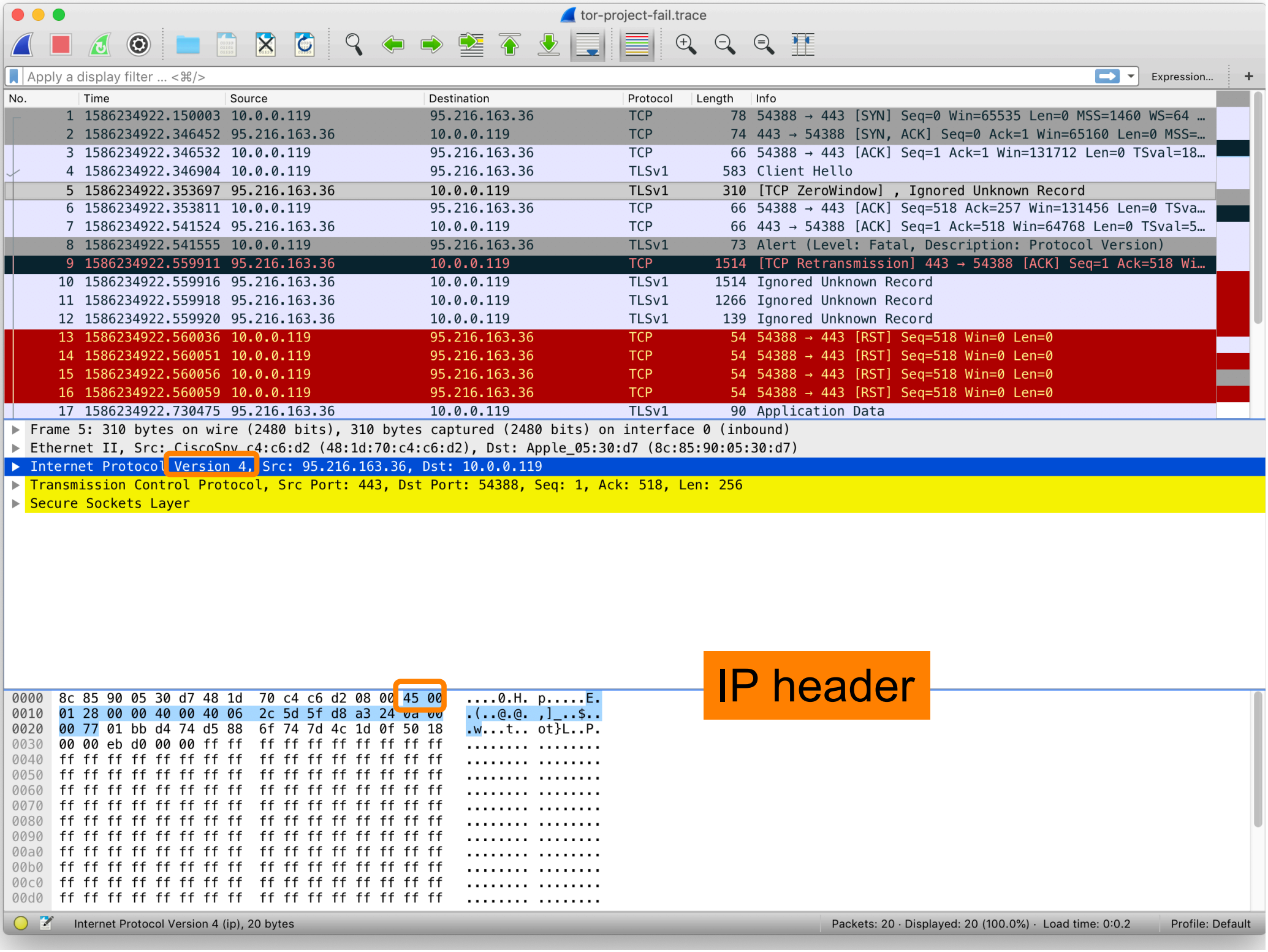

tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
6 1586234922.353811 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8 1586234922.541555 10.0.0 73 Alert (Level: Fatal, Description: Protocol Version)
9 1586234922.559911 95.216 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10 1586234922.559916 95.216 1514 Ignored Unknown Record
11 1586234922.559918 95.216 1266 Ignored Unknown Record
12 1586234922.559920 95.216 139 Ignored Unknown Record
13 1586234922.560036 10.0.0 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
14 1586234922.560051 10.0.0 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
15 1586234922.560056 10.0.0 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
16 1586234922.560059 10.0.0 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
17 1586234922.730475 95.216 90 Application Data
My browser sends the regular start of a TLS handshake
Frame 5: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface 0 (inbound)
Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)
Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119
Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256
Secure Sockets Layer
Ignored Unknown Record
[Expert Info (Warning/Protocol): Ignored Unknown Record]
[Ignored Unknown Record]
[Severity level: Warning]
[Group: Protocol]
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 01 28 00 00 40 00 40 06 2c 5d 5f d8 a3 24 0a 00 .(..@.@. ,]_..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 50 18 .w...t.. ot}L..P.
0030 00 00 eb d0 00 00 ff ff ff ff ff ff ff ff ff ff ....
0040 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0050 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0060 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0070 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0080 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0090 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00a0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00b0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00c0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00d0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
tor-project-fail
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.0
Profile: Default

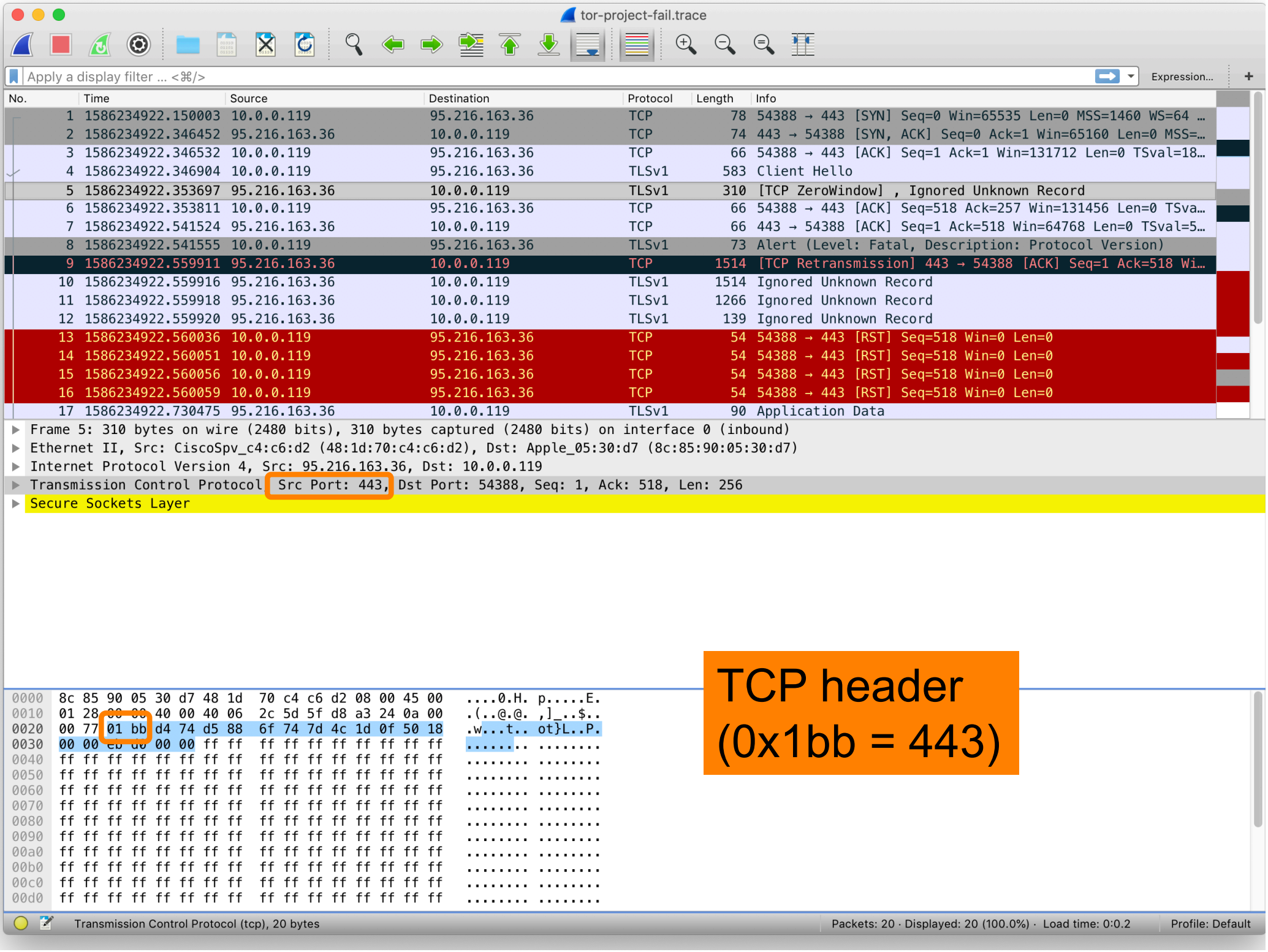

tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3 1586234922.346532 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
12 1586234922.559920 95.216.163.36 10.0.0.119 TLSv1 139 Ignored Unknown Record
13 1586234922.560036 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
14 1586234922.560051 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
15 1586234922.560056 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
16 1586234922.560059 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
17 1586234922.730475 95.216.163.36 10.0.0.119 TLSv1 90 Application Data
Back comes an unusual TCP response
Frame 5: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface 0 (inbound)
Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)
Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119
Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256
Secure Sockets Layer
Ignored Unknown Record
[Expert Info (Warning/Protocol): Ignored Unknown Record]
[Ignored Unknown Record]
[Severity level: Warning]
[Group: Protocol]
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 01 28 00 00 40 00 40 06 2c 5d 5f d8 a3 24 0a 00 .(..@.@. ,]_..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 50 18 .w...t.. ot}L..P.
0030 00 00 eb d0 00 00 ff ff ff ff ff ff ff ff ff ff ....
0040 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0050 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0060 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0070 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0080 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0090 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00a0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00b0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00c0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00d0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
tor-project-fail
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.0
Profile: Default

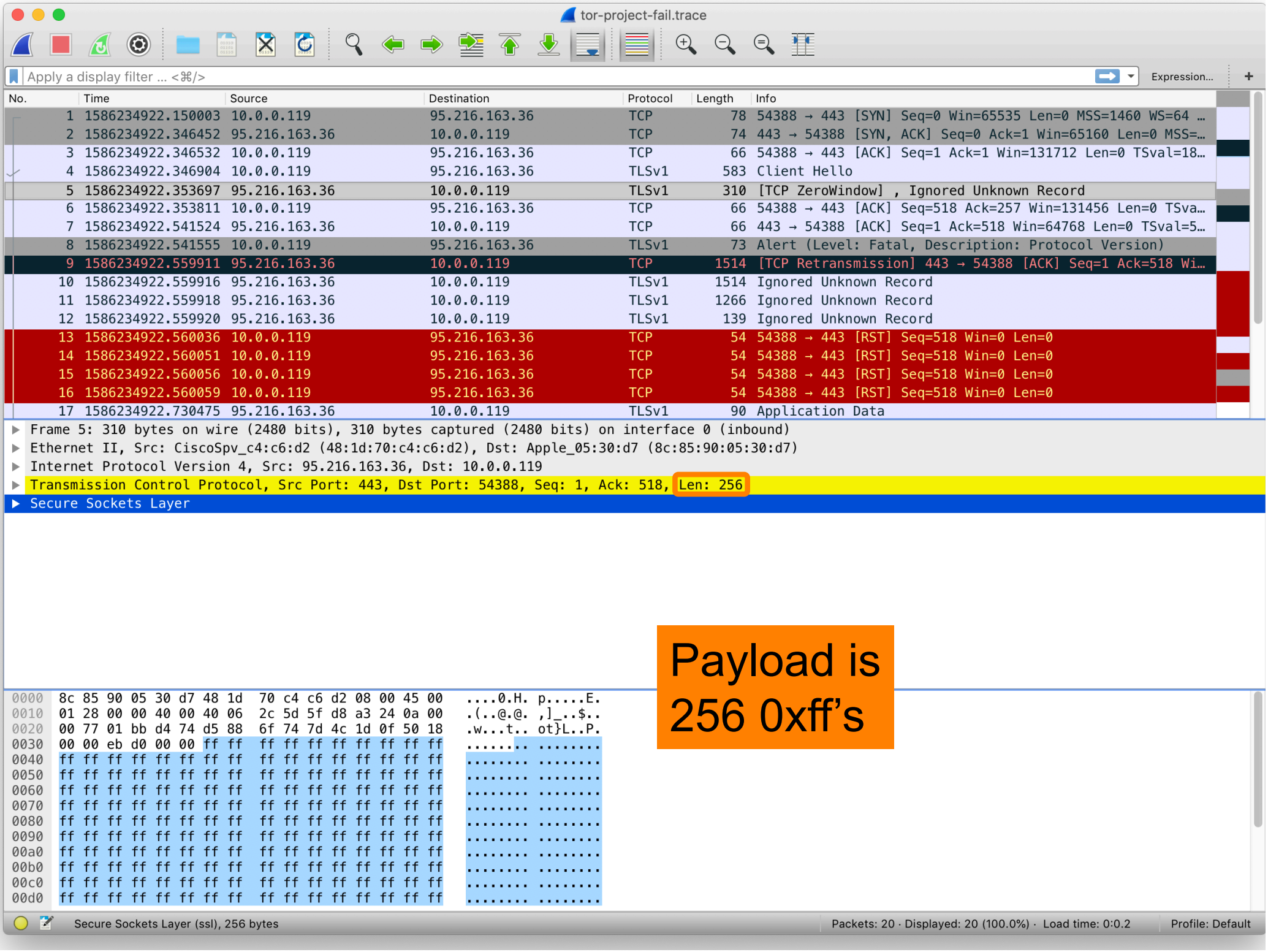

tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3 1586234922.346532 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
6 1586234922.353811 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8 1586234922.541555 10.0.0.119 95.216.163.36 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
9 1586234922.559911 95.216.163.36 10.0.0.119 TCP 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10 1586234922.559916 95.216.163.36 10.0.0.119 TLSv1
11 1586234922.559918 95.216.163.36 10.0.0.119 TLSv1
12 1586234922.559920 95.216.163.36 10.0.0.119 TLSv1
13 1586234922.560036 10.0.0.119 95.216.163.36 TCP
14 1586234922.560051 10.0.0.119 95.216.163.36 TCP
15 1586234922.560056 10.0.0.119 95.216.163.36 TCP
16 1586234922.560059 10.0.0.119 95.216.163.36 TCP
17 1586234922.730475 95.216.163.36 10.0.0.119 TLSv1
Offered window is 0, preventing my browser from sending any data
Frame 5: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface
Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)
Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119
Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256
Secure Sockets Layer
Ignored Unknown Record
[Expert Info (Warning/Protocol): Ignored Unknown Record]
[Ignored Unknown Record]
[Severity level: Warning]
[Group: Protocol]
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 01 28 00 00 40 00 40 06 2c 5d 5f d8 a3 24 0a 00 .(..@.@. ,]_..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 50 18 .w...t.. ot}L..P.
0030 00 00 eb d0 00 00 ff ff ff ff ff ff ff ff ff ff ....
0040 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0050 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0060 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0070 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0080 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0090 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00a0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00b0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00c0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00d0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
tor-project-fail
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.0
Profile: Default

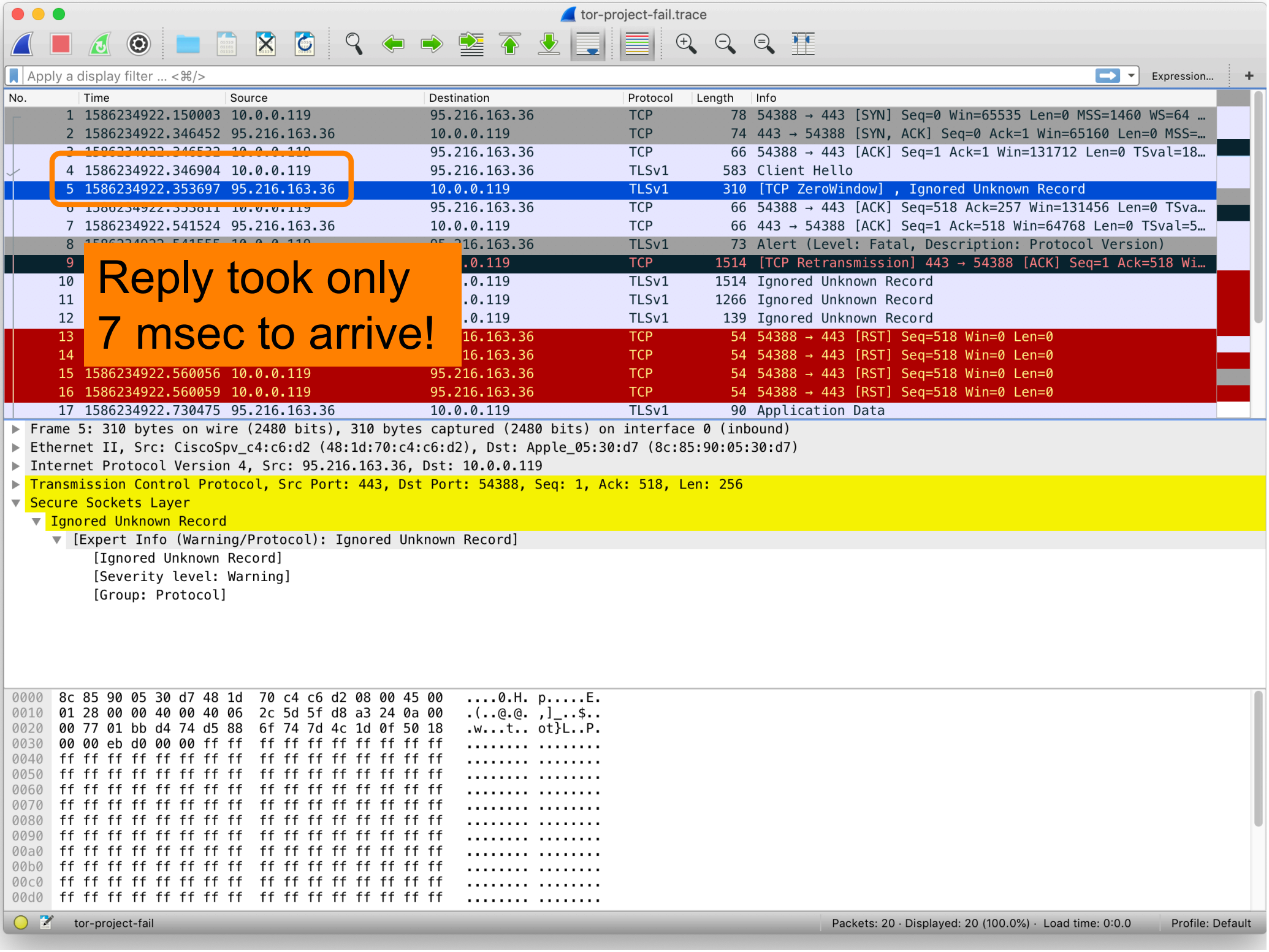

tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3 1586234922.346532 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
6 1586234922.353811 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8 1586234922.541555 10.0.0.119 95.216.163.36 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
9 1586234922.559911 95.216.163.36 10.0.0.119 TCP 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10 1586234922.559916 95.216.163.36 10.0.0.119 TLSv1 1514 Ignored Unknown Record
11 1586234922.559918 95.216.163.36 10.0.0.119 Record
12 1586234922.559920 95.216.163.36 10.0.0.119 Record
13 1586234922.560036 10.0.0.119 95.216.163 T] Seq=518 Win=0 Len=0
14 1586234922.560051 10.0.0.119 95.216.163 T] Seq=518 Win=0 Len=0
15 1586234922.560056 10.0.0.119 95.216.163 T] Seq=518 Win=0 Len=0
16 1586234922.560059 10.0.0.119 95.216.163 T] Seq=518 Win=0 Len=0
17 1586234922.730475 95.216.163.36 10.0.0.119
Response is not well-formed TLS
Frame 5: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface 0 (inbound)
Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)
Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119
Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256
Secure Sockets Layer
Ignored Unknown Record
[Expert Info (Warning/Protocol): Ignored Unknown Record]
[Ignored Unknown Record]
[Severity level: Warning]
[Group: Protocol]
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 01 28 00 00 40 00 40 06 2c 5d 5f d8 a3 24 0a 00 .(..@.@. ,]_..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 50 18 .w...t.. ot}L..P.
0030 00 00 eb d0 00 00 ff ff ff ff ff ff ff ff ff ff ....
0040 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0050 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0060 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0070 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0080 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0090 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00a0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00b0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00c0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00d0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
tor-project-fail
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.0
Profile: Default

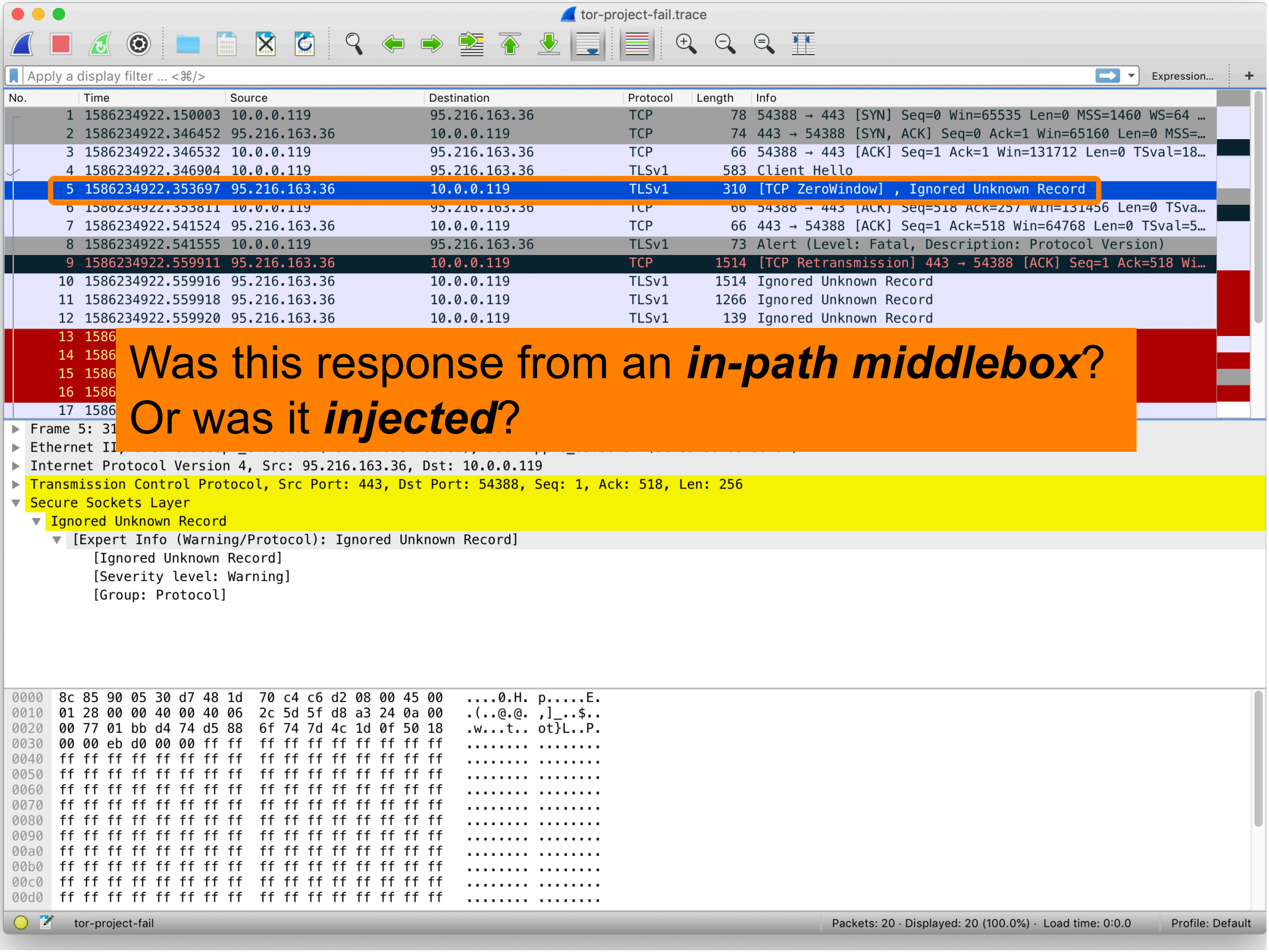

tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3 1586234922.346532 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
6 1586234922.353811 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8 1586234922.541555 10.0.0.119 95.216.163.36 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
9 1586234922.559911 95.216.163.36 10.0.0.119 TCP 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10 1586234922.559916 95.216.163.36 10.0.0.119 TLSv1 1514 Ignored Unknown Record
11 1586234922.559918 95.216.163.36 10.0.0.119 TLSv1 1266 Ignored Unknown Record
12 1586234922.559920 95.216.163.36 10.0.0.119 TLSv1 139 Ignored Unknown Record
13 1586234922.560036 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
14 1586234922.560051 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
15 1586234922.560056 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
16 1586234922.560059 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
17 1586234922.730475 95.216.163.36 10.0.0.119 TLSv1 90 Application Data
Frame 5: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface 0 (inbound)
Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)
Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119
Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256
Secure Sockets Layer
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 01 28 00 00 40 00 40 06 2c 5d 5f d8 a3 24 0a 00 .(..@.@. ,]_..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 50 18 .w...t.. ot}L..P.
0030 00 00 eb d0 00 00 ff ff ff ff ff ff ff ff ff ff ....
0040 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0050 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0060 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0070 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0080 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0090 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00a0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00b0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00c0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00d0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
Ethernet frame
Ethernet (eth), 14 bytes
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.2
Profile: Default

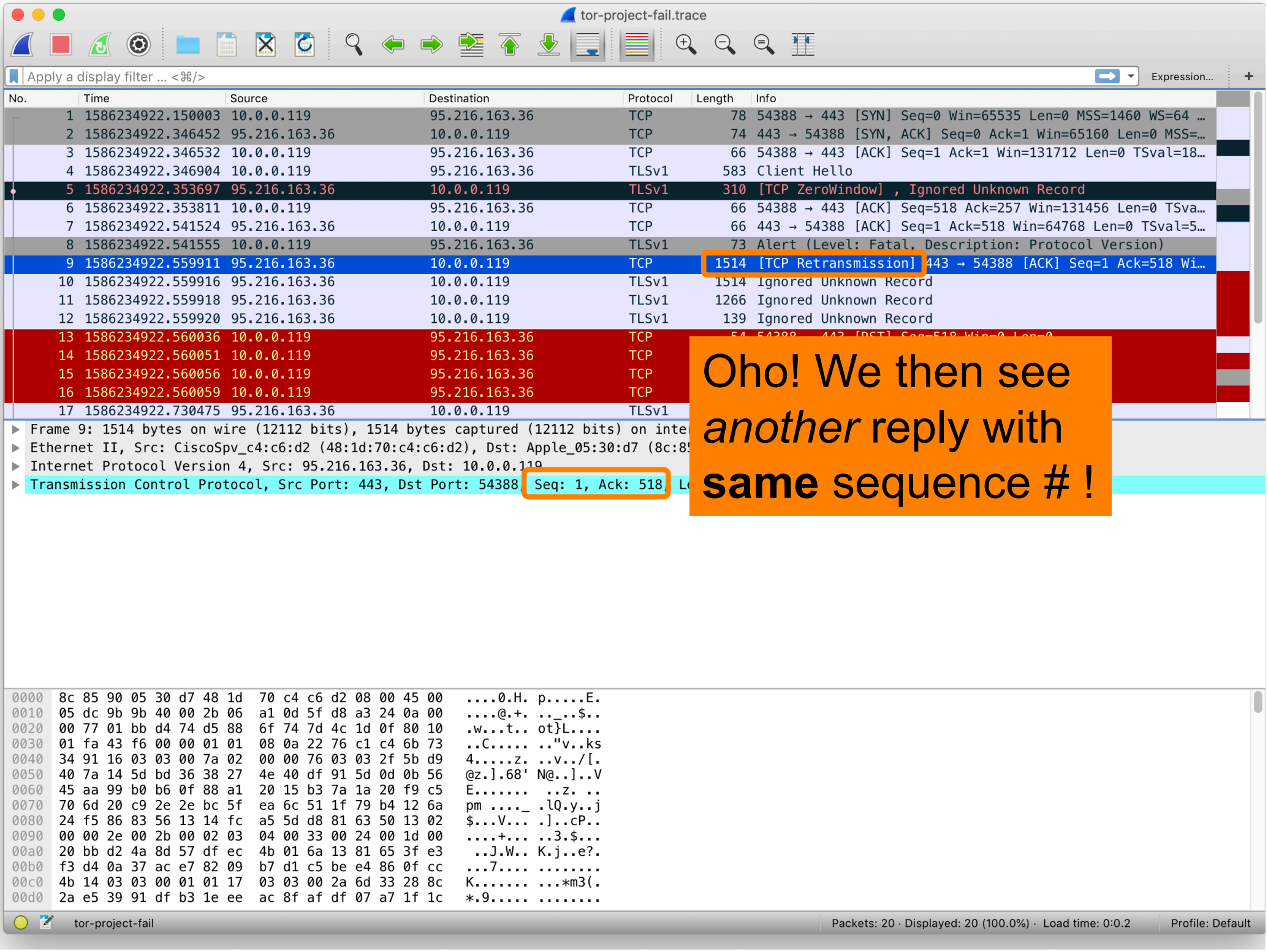

tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3 1586234922.346532 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
6 1586234922.353811 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8 1586234922.541555 10.0.0.119 95.216.163.36 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
9 1586234922.559911 95.216.163.36 10.0.0.119 TCP 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10 1586234922.559916 95.216.163.36 10.0.0.119 TLSv1 1514 Ignored Unknown Record
11 1586234922.559918 95.216.163.36 10.0.0.119 TLSv1 1266 Ignored Unknown Record
12 1586234922.559920 95.216.163.36 10.0.0.119 TLSv1 139 Ignored Unknown Record
13 1586234922.560036 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
14 1586234922.560051 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
15 1586234922.560056 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
16 1586234922.560059 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
17 1586234922.730475 95.216.163.36 10.0.0.119 TLSv1 90 Application Data
Frame 5: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface 0 (inbound)
Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)
Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119
Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256
Secure Sockets Layer
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 01 28 00 00 40 00 40 06 2c 5d 5f d8 a3 24 0a 00 .(..@.@. ,]_..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 50 18 .w...t.. ot}L..P.
0030 00 00 eb d0 00 00 ff ff ff ff ff ff ff ff ff ff ....
0040 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0050 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0060 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0070 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0080 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0090 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00a0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00b0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00c0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00d0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
IP header
Internet Protocol Version 4 (ip), 20 bytes
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.2
Profile: Default

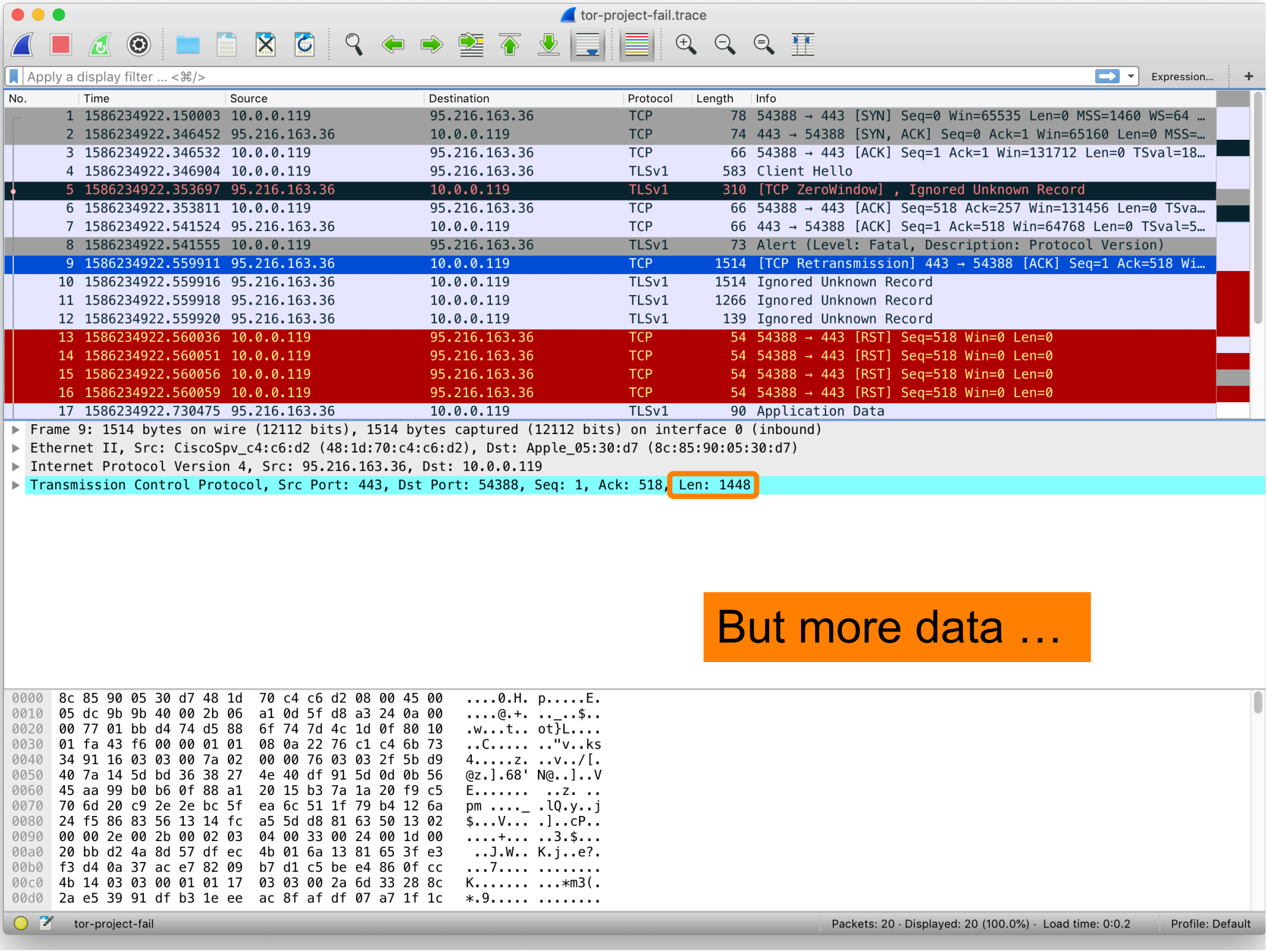

tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3 1586234922.346532 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
6 1586234922.353811 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8 1586234922.541555 10.0.0.119 95.216.163.36 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
9 1586234922.559911 95.216.163.36 10.0.0.119 TCP 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10 1586234922.559916 95.216.163.36 10.0.0.119 TLSv1 1514 Ignored Unknown Record
11 1586234922.559918 95.216.163.36 10.0.0.119 TLSv1 1266 Ignored Unknown Record
12 1586234922.559920 95.216.163.36 10.0.0.119 TLSv1 139 Ignored Unknown Record
13 1586234922.560036 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
14 1586234922.560051 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
15 1586234922.560056 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
16 1586234922.560059 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
17 1586234922.730475 95.216.163.36 10.0.0.119 TLSv1 90 Application Data
Frame 5: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface 0 (inbound)
Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)
Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119
Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256
Secure Sockets Layer
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 01 28 .. .. 40 00 40 06 2c 5d 5f d8 a3 24 0a 00 .(..@.@. ,]_..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 50 18 .w...t.. ot}L..P.
0030 00 00 .. .. 00 00 ff ff ff ff ff ff ff ff ff ff ....
0040 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0050 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0060 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0070 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0080 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0090 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00a0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00b0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00c0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00d0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
TCP header
(0x1bb = 443)
Transmission Control Protocol (tcp), 20 bytes
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.2
Profile: Default

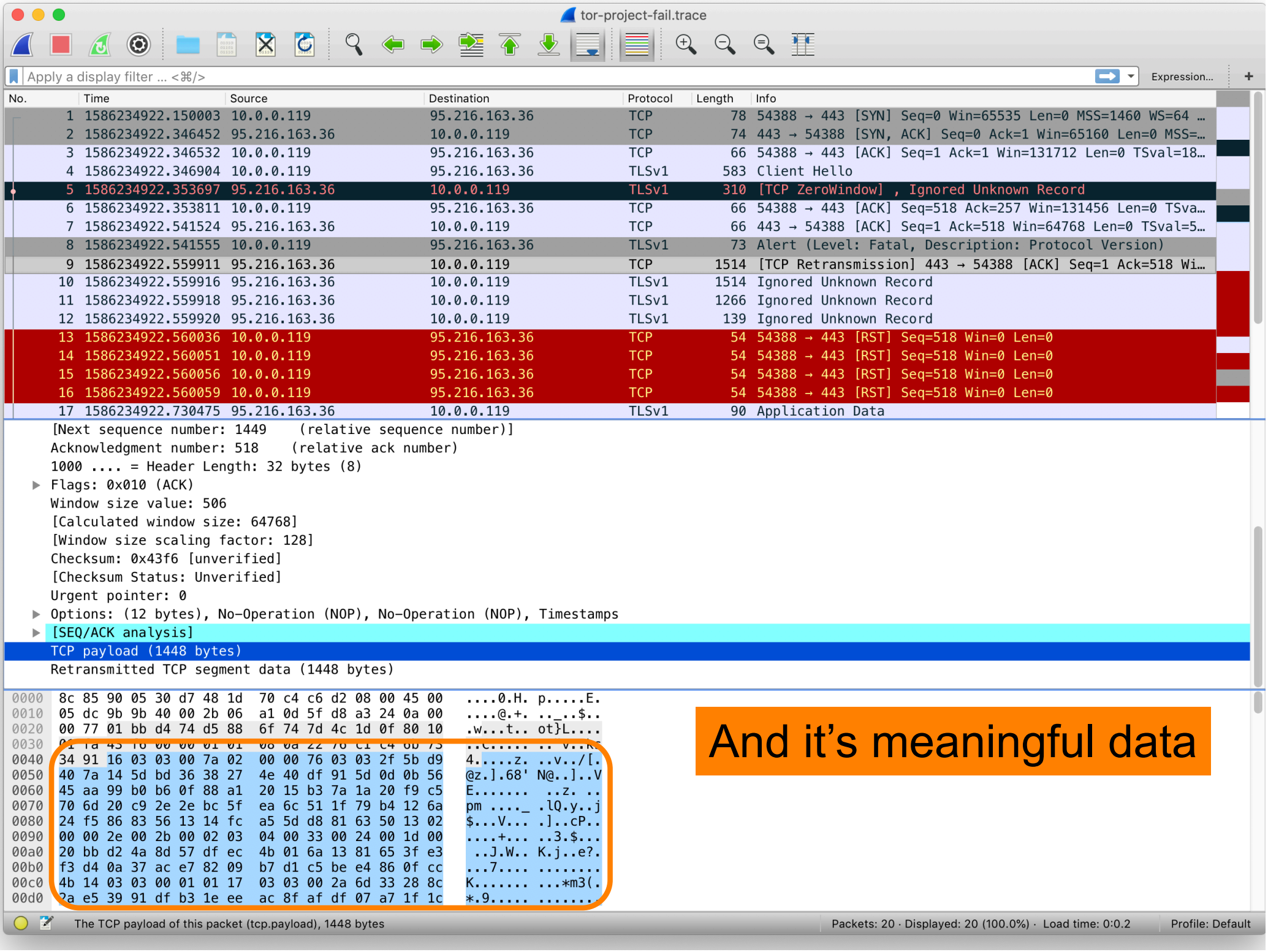

tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3 1586234922.346532 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
6 1586234922.353811 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8 1586234922.541555 10.0.0.119 95.216.163.36 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
9 1586234922.559911 95.216.163.36 10.0.0.119 TCP 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10 1586234922.559916 95.216.163.36 10.0.0.119 TLSv1 1514 Ignored Unknown Record
11 1586234922.559918 95.216.163.36 10.0.0.119 TLSv1 1266 Ignored Unknown Record
12 1586234922.559920 95.216.163.36 10.0.0.119 TLSv1 139 Ignored Unknown Record
13 1586234922.560036 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
14 1586234922.560051 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
15 1586234922.560056 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
16 1586234922.560059 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
17 1586234922.730475 95.216.163.36 10.0.0.119 TLSv1 90 Application Data
Frame 5: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface 0 (inbound)
Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)
Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119
Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256
Secure Sockets Layer
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 01 28 00 00 40 00 40 06 2c 5d 5f d8 a3 24 0a 00 .(..@.@. ,]_..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 50 18 .w...t.. ot}L..P.
0030 00 00 eb d0 00 00 ff ff ff ff ff ff ff ff ff ff ....
0040 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0050 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0060 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0070 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0080 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0090 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00a0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00b0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00c0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00d0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
Payload is 256 0xff's
Secure Sockets Layer (ssl), 256 bytes
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.2
Profile: Default

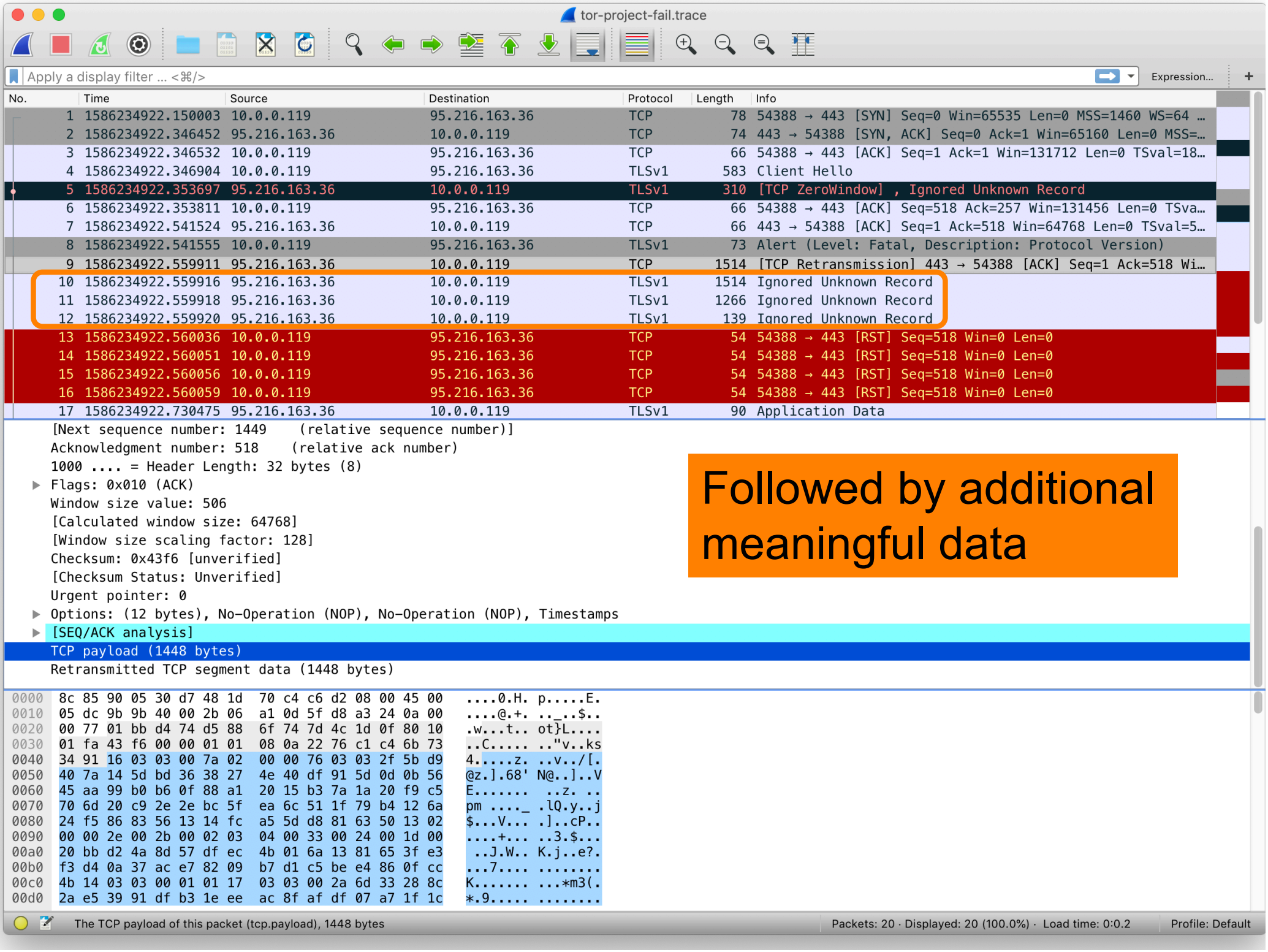

tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
9 TCP 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10 TLSv1 1514 Ignored Unknown Record
11 TLSv1 1266 Ignored Unknown Record
12 TLSv1 139 Ignored Unknown Record
13 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
14 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
15 1586234922.560056 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
16 1586234922.560059 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
17 1586234922.730475 95.216.163.36 10.0.0.119 TLSv1 90 Application Data
Reply took only
7 msec to arrive!
Frame 5: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface 0 (inbound)
Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)
Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119
Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256
Secure Sockets Layer
Ignored Unknown Record
[Expert Info (Warning/Protocol): Ignored Unknown Record]
[Ignored Unknown Record]
[Severity level: Warning]
[Group: Protocol]
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 01 28 00 00 40 00 40 06 2c 5d 5f d8 a3 24 0a 00 .(..@.@. ,]_..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 50 18 .w...t.. ot}L..P.
0030 00 00 eb d0 00 00 ff ff ff ff ff ff ff ff ff ff ....
0040 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0050 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0060 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0070 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0080 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0090 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00a0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00b0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00c0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00d0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
tor-project-fail
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.0
Profile: Default

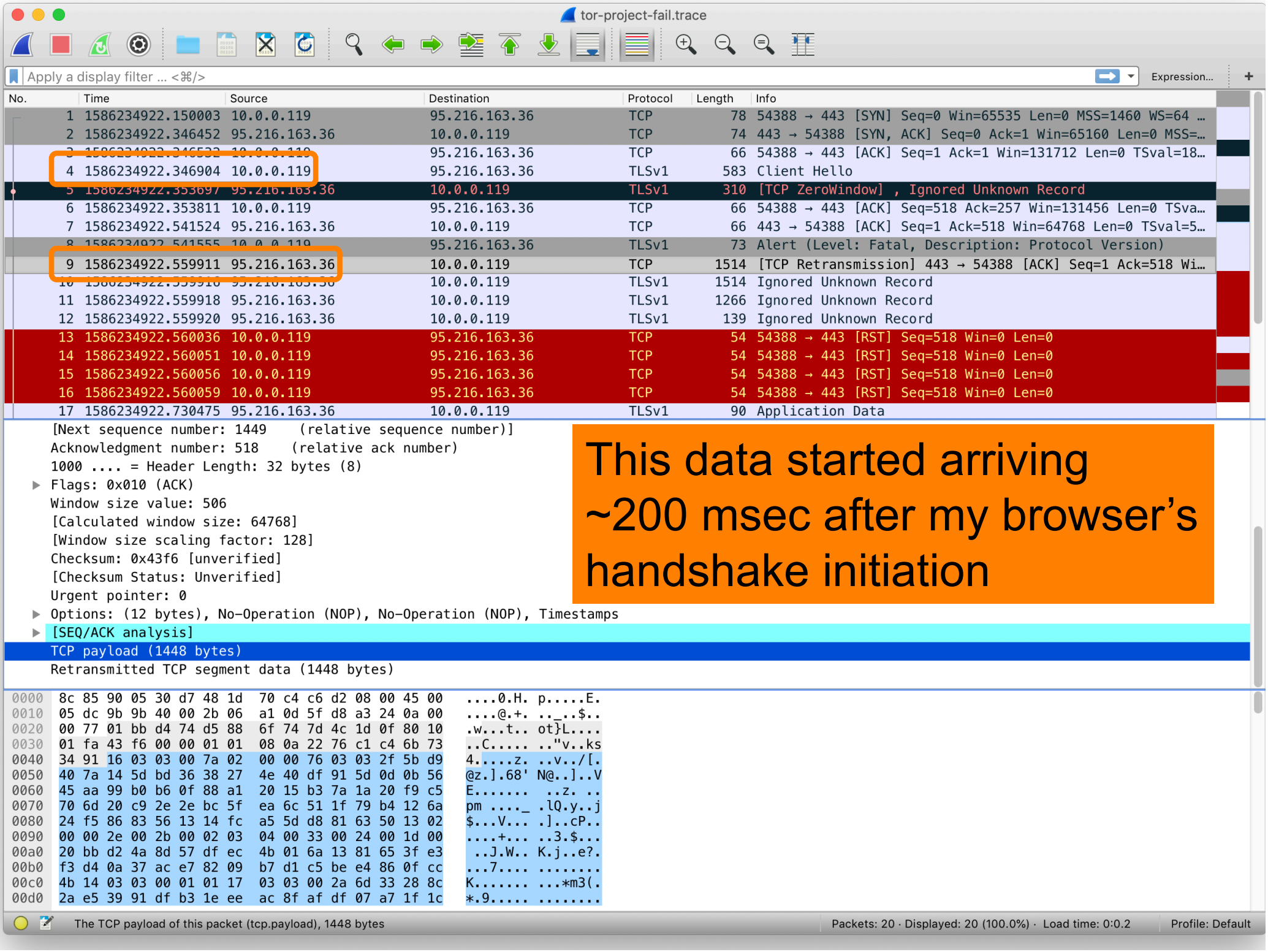

tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3 1586234922.346532 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8 1586234922.541555 10.0.0.119 95.216.163.36 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
9 1586234922.559911 95.216.163.36 10.0.0.119 TCP 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10 1586234922.559916 95.216.163.36 10.0.0.119 TLSv1 1514 Ignored Unknown Record
11 1586234922.559918 95.216.163.36 10.0.0.119 TLSv1 1266 Ignored Unknown Record
12 1586234922.559920 95.216.163.36 10.0.0.119 TLSv1 139 Ignored Unknown Record
13 1586
14 1586
15 1586
16 1586
17 1586
Was this response from an *in-path middlebox*?
Or was it *injected*?
Frame 5: 31
Ethernet II,
Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119
Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256
Secure Sockets Layer
Ignored Unknown Record
[Expert Info (Warning/Protocol): Ignored Unknown Record]
[Ignored Unknown Record]
[Severity level: Warning]
[Group: Protocol]
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 01 28 00 00 40 00 40 06 2c 5d 5f d8 a3 24 0a 00 .(..@.@. ,]_..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 50 18 .w...t.. ot}L..P.
0030 00 00 eb d0 00 00 ff ff ff ff ff ff ff ff ff ff ....
0040 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0050 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0060 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0070 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0080 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0090 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00a0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00b0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00c0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
00d0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
tor-project-fail
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.0
Profile: Default

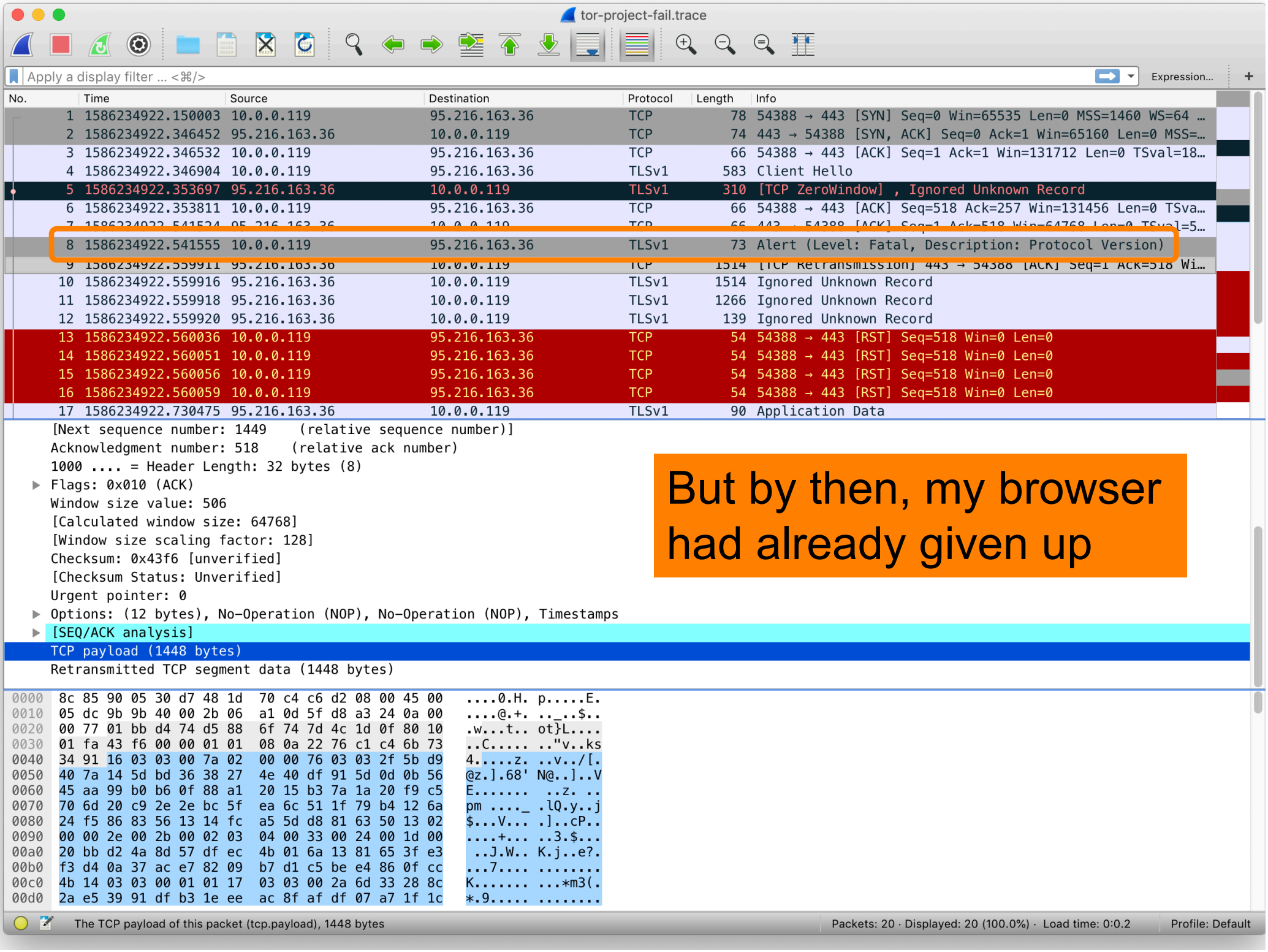

tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3 1586234922.346532 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
6 1586234922.353811 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8 1586234922.541555 10.0.0.119 95.216.163.36 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
9 1586234922.559911 95.216.163.36 10.0.0.119 TCP 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10 1586234922.559916 95.216.163.36 10.0.0.119 TLSv1 1514 Ignored Unknown Record
11 1586234922.559918 95.216.163.36 10.0.0.119 TLSv1 1266 Ignored Unknown Record
12 1586234922.559920 95.216.163.36 10.0.0.119 TLSv1 139 Ignored Unknown Record
13 1586234922.560036 10.0.0.119 95.216.163.36 TCP
14 1586234922.560051 10.0.0.119 95.216.163.36 TCP
15 1586234922.560056 10.0.0.119 95.216.163.36 TCP
16 1586234922.560059 10.0.0.119 95.216.163.36 TCP
17 1586234922.730475 95.216.163.36 10.0.0.119 TLSv1
Frame 9: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on inte
Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85
Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119
Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, L
Oho! We then see another reply with same sequence # !
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 05 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0a 00 ....@.+. .._..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 80 10 .w...t.. ot}L....
0030 01 fa 43 f6 00 00 01 01 08 0a 22 76 c1 c4 6b 73 ..C..... .."v..ks
0040 34 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5b d9 4.....z. ..v../[.
0050 40 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0b 56 @z.].68' N@..]..V
0060 45 aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f9 c5 E....... ..z. ..
0070 70 6d 20 c9 2e 2e bc 5f ea 6c 51 1f 79 b4 12 6a pm ...._ .lQ.y..j
0080 24 f5 86 83 56 13 14 fc a5 5d d8 81 63 50 13 02 $...V... .]..cP..
0090 00 00 2e 00 2b 00 02 03 04 00 33 00 24 00 1d 00 ....+... ..3.$...
00a0 20 bb d2 4a 8d 57 df ec 4b 01 6a 13 81 65 3f e3 ..J.W.. K.j..e?.
00b0 f3 d4 0a 37 ac e7 82 09 b7 d1 c5 be e4 86 0f cc ...7.... ....
00c0 4b 14 03 03 00 01 01 17 03 03 00 2a 6d 33 28 8c K....... ...*m3(.
00d0 2a e5 39 91 df b3 1e ee ac 8f af df 07 a7 1f 1c *.9..... ....
tor-project-fail
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.2
Profile: Default

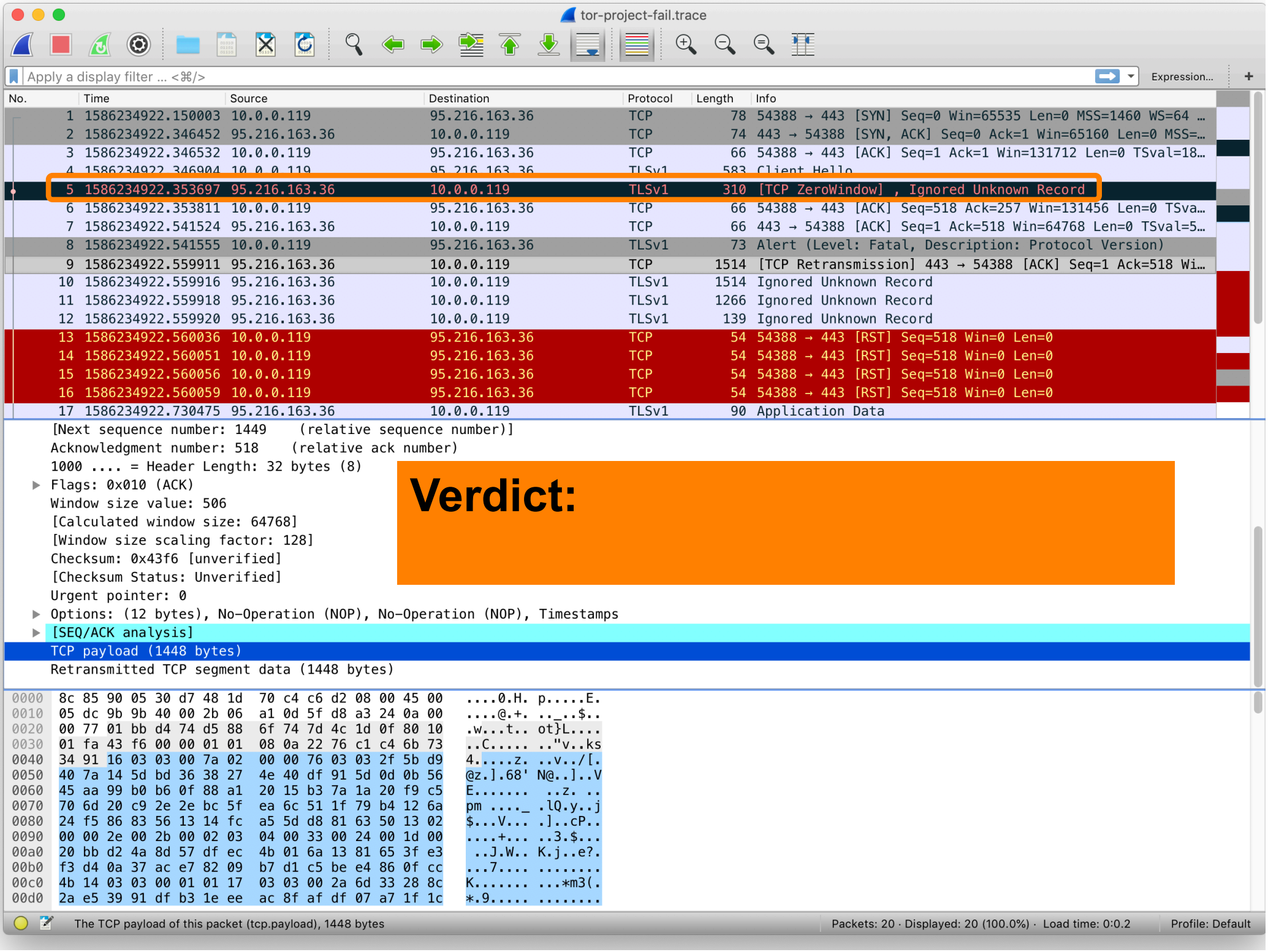

tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3 1586234922.346532 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
6 1586234922.353811 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8 1586234922.541555 10.0.0.119 95.216.163.36 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
9 1586234922.559911 95.216.163.36 10.0.0.119 TCP 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10 1586234922.559916 95.216.163.36 10.0.0.119 TLSv1 1514 Ignored Unknown Record
11 1586234922.559918 95.216.163.36 10.0.0.119 TLSv1 1266 Ignored Unknown Record
12 1586234922.559920 95.216.163.36 10.0.0.119 TLSv1 139 Ignored Unknown Record
13 1586234922.560036 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
14 1586234922.560051 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
15 1586234922.560056 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
16 1586234922.560059 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
17 1586234922.730475 95.216.163.36 10.0.0.119 TLSv1 90 Application Data
Frame 9: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0 (inbound)
Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)
Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119
Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 1448
But more data …
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 05 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0a 00 ....@.+. .._..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 80 10 .w...t.. ot}L....
0030 01 fa 43 f6 00 00 01 01 08 0a 22 76 c1 c4 6b 73 ..C..... .."v..ks
0040 34 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5b d9 4.....z. ..v../[.
0050 40 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0b 56 @z.].68' N@..]..V
0060 45 aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f9 c5 E....... ..z. ..
0070 70 6d 20 c9 2e 2e bc 5f ea 6c 51 1f 79 b4 12 6a pm ...._ .lQ.y..j
0080 24 f5 86 83 56 13 14 fc a5 5d d8 81 63 50 13 02 $...V... .]..cP..
0090 00 00 2e 00 2b 00 02 03 04 00 33 00 24 00 1d 00 ....+... ..3.$...
00a0 20 bb d2 4a 8d 57 df ec 4b 01 6a 13 81 65 3f e3 ..J.W.. K.j..e?.
00b0 f3 d4 0a 37 ac e7 82 09 b7 d1 c5 be e4 86 0f cc ...7.... ....
00c0 4b 14 03 03 00 01 01 17 03 03 00 2a 6d 33 28 8c K....... ...*m3(.
00d0 2a e5 39 91 df b3 1e ee ac 8f af df 07 a7 1f 1c *.9..... ....
tor-project-fail
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.2
Profile: Default

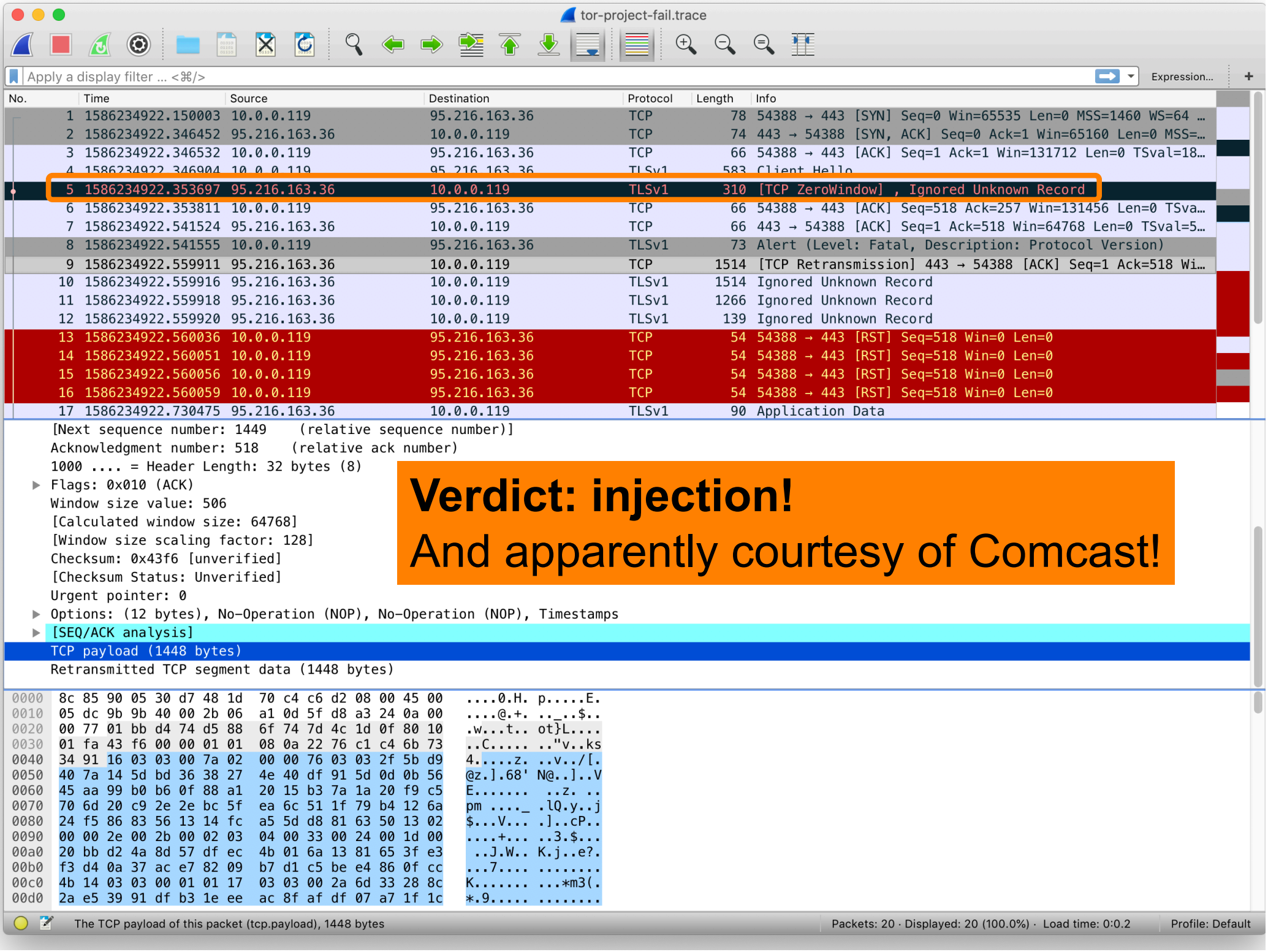

tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3 1586234922.346532 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
6 1586234922.353811 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8 1586234922.541555 10.0.0.119 95.216.163.36 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
9 1586234922.559911 95.216.163.36 10.0.0.119 TCP 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10 1586234922.559916 95.216.163.36 10.0.0.119 TLSv1 1514 Ignored Unknown Record
11 1586234922.559918 95.216.163.36 10.0.0.119 TLSv1 1266 Ignored Unknown Record
12 1586234922.559920 95.216.163.36 10.0.0.119 TLSv1 139 Ignored Unknown Record
13 1586234922.560036 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
14 1586234922.560051 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
15 1586234922.560056 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
16 1586234922.560059 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
17 1586234922.730475 95.216.163.36 10.0.0.119 TLSv1 90 Application Data
[Next sequence number: 1449 (relative sequence number)]
Acknowledgment number: 518 (relative ack number)
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window size value: 506
[Calculated window size: 64768]
[Window size scaling factor: 128]
Checksum: 0x43f6 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
TCP payload (1448 bytes)
Retransmitted TCP segment data (1448 bytes)
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 05 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0a 00 ....@.+. .._..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 80 10 .w...t.. ot}L....
0040 34 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5b d9 4.....z. ..v../[.
0050 40 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0b 56 @z.].68' N@..]..V
0060 45 aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f9 c5 E....... ..z. ..
0070 70 6d 20 c9 2e 2e bc 5f ea 6c 51 1f 79 b4 12 6a pm ...._ .lQ.y..j
0080 24 f5 86 83 56 13 14 fc a5 5d d8 81 63 50 13 02 $...V... .]..cP..
0090 00 00 2e 00 2b 00 02 03 04 00 33 00 24 00 1d 00 ....+... ..3.$...
00a0 20 bb d2 4a 8d 57 df ec 4b 01 6a 13 81 65 3f e3 ..J.W.. K.j..e?.
00b0 f3 d4 0a 37 ac e7 82 09 b7 d1 c5 be e4 86 0f cc ...7.... ....
00c0 4b 14 03 03 00 01 01 17 03 03 00 2a 6d 33 28 8c K....... ...*m3(.
00d0 2a e5 39 91 df b3 1e ee ac 8f af df 07 a7 1f 1c *.9..... ....
And it’s meaningful data
The TCP payload of this packet (tcp.payload), 1448 bytes
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.2
Profile: Default


tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3 1586234922.346532 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
6 1586234922.353811 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8 1586234922.541555 10.0.0.119 95.216.163.36 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
9 1586234922.559911 95.216.163.36 10.0.0.119 TCP 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10 1586234922.559916 95.216.163.36 10.0.0.119 TLSv1 1514 Ignored Unknown Record
11 1586234922.559918 95.216.163.36 10.0.0.119 TLSv1 1266 Ignored Unknown Record
12 1586234922.559920 95.216.163.36 10.0.0.119 TLSv1 139 Ignored Unknown Record
13 1586234922.560036 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
14 1586234922.560051 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
15 1586234922.560056 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
16 1586234922.560059 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
17 1586234922.730475 95.216.163.36 10.0.0.119 TLSv1 90 Application Data
[Next sequence number: 1449 (relative sequence number)]
Acknowledgment number: 518 (relative ack number)
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window size value: 506
[Calculated window size: 64768]
[Window size scaling factor: 128]
Checksum: 0x43f6 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
TCP payload (1448 bytes)
Retransmitted TCP segment data (1448 bytes)
Followed by additional meaningful data
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 05 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0a 00 ....@.+. .._..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 80 10 .w...t.. ot}L....
0030 01 fa 43 f6 00 00 01 01 08 0a 22 76 c1 c4 6b 73 ..C..... .."v..ks
0040 34 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5b d9 4.....z. ..v../[.
0050 40 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0b 56 @z.].68' N@..]..V
0060 45 aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f9 c5 E....... ..z. ..
0070 70 6d 20 c9 2e 2e bc 5f ea 6c 51 1f 79 b4 12 6a pm ...._ .lQ.y..j
0080 24 f5 86 83 56 13 14 fc a5 5d d8 81 63 50 13 02 $...V... .]..cP..
0090 00 00 2e 00 2b 00 02 03 04 00 33 00 24 00 1d 00 ....+... ..3.$...
00a0 20 bb d2 4a 8d 57 df ec 4b 01 6a 13 81 65 3f e3 ..J.W.. K.j..e?.
00b0 f3 d4 0a 37 ac e7 82 09 b7 d1 c5 be e4 86 0f cc ...7.... ....
00c0 4b 14 03 03 00 01 01 17 03 03 00 2a 6d 33 28 8c K....... ...*m3(.
00d0 2a e5 39 91 df b3 1e ee ac 8f af df 07 a7 1f 1c *.9..... ....
The TCP payload of this packet (tcp.payload), 1448 bytes
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.2
Profile: Default


tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
6 1586234922.353811 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
95.216.163.36 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
9 1586234922.559911 95.216.163.36 10.0.0.119 TCP 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10.0.0.119 TLSv1 1514 Ignored Unknown Record
11 1586234922.559918 95.216.163.36 10.0.0.119 TLSv1 1266 Ignored Unknown Record
12 1586234922.559920 95.216.163.36 10.0.0.119 TLSv1 139 Ignored Unknown Record
13 1586234922.560036 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
14 1586234922.560051 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
15 1586234922.560056 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
16 1586234922.560059 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
17 1586234922.730475 95.216.163.36 10.0.0.119 TLSv1 90 Application Data
[Next sequence number: 1449 (relative sequence number)]
Acknowledgment number: 518 (relative ack number)
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window size value: 506
[Calculated window size: 64768]
[Window size scaling factor: 128]
Checksum: 0x43f6 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
TCP payload (1448 bytes)
Retransmitted TCP segment data (1448 bytes)
This data started arriving ~200 msec after my browser's handshake initiation
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 05 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0a 00 ....@.+. .._..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 80 10 .w...t.. ot}L....
0030 01 fa 43 f6 00 00 01 01 08 0a 22 76 c1 c4 6b 73 ..C..... .."v..ks
0040 34 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5b d9 4.....z. ..v../[.
0050 40 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0b 56 @z.].68' N@..]..V
0060 45 aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f9 c5 E....... ..z. ..
0070 70 6d 20 c9 2e 2e bc 5f ea 6c 51 1f 79 b4 12 6a pm ...._ .lQ.y..j
0080 24 f5 86 83 56 13 14 fc a5 5d d8 81 63 50 13 02 $...V... .]..cP..
0090 00 00 2e 00 2b 00 02 03 04 00 33 00 24 00 1d 00 ....+... ..3.$...
00a0 20 bb d2 4a 8d 57 df ec 4b 01 6a 13 81 65 3f e3 ..J.W.. K.j..e?.
00b0 f3 d4 0a 37 ac e7 82 09 b7 d1 c5 be e4 86 0f cc ...7.... ....
00c0 4b 14 03 03 00 01 01 17 03 03 00 2a 6d 33 28 8c K....... ...*m3(.
00d0 2a e5 39 91 df b3 1e ee ac 8f af df 07 a7 1f 1c *.9..... ....
The TCP payload of this packet (tcp.payload), 1448 bytes
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.2
Profile: Default


tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3 1586234922.346532 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
6 1586234922.353811 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
8 1586234922.541555 10.0.0.119 95.216.163.36 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
10 1586234922.559916 95.216.163.36 10.0.0.119 TLSv1 1514 Ignored Unknown Record
11 1586234922.559918 95.216.163.36 10.0.0.119 TLSv1 1266 Ignored Unknown Record
12 1586234922.559920 95.216.163.36 10.0.0.119 TLSv1 139 Ignored Unknown Record
13 1586234922.560036 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
14 1586234922.560051 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
15 1586234922.560056 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
16 1586234922.560059 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
17 1586234922.730475 95.216.163.36 10.0.0.119 TLSv1 90 Application Data
[Next sequence number: 1449 (relative sequence number)]
Acknowledgment number: 518 (relative ack number)
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window size value: 506
[Calculated window size: 64768]
[Window size scaling factor: 128]
Checksum: 0x43f6 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
TCP payload (1448 bytes)
Retransmitted TCP segment data (1448 bytes)
But by then, my browser had already given up
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 05 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0a 00 ....@.+. .._..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 80 10 .w...t.. ot}L....
0030 01 fa 43 f6 00 00 01 01 08 0a 22 76 c1 c4 6b 73 ..C..... .."v..ks
0040 34 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5b d9 4.....z. ..v../[.
0050 40 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0b 56 @z.].68' N@..]..V
0060 45 aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f9 c5 E....... ..z. ..
0070 70 6d 20 c9 2e 2e bc 5f ea 6c 51 1f 79 b4 12 6a pm ...._ .lQ.y..j
0080 24 f5 86 83 56 13 14 fc a5 5d d8 81 63 50 13 02 $...V... .]..cP..
0090 00 00 2e 00 2b 00 02 03 04 00 33 00 24 00 1d 00 ....+... ..3.$...
00a0 20 bb d2 4a 8d 57 df ec 4b 01 6a 13 81 65 3f e3 ..J.W.. K.j..e?.
00b0 f3 d4 0a 37 ac e7 82 09 b7 d1 c5 be e4 86 0f cc ...7.... ....
00c0 4b 14 03 03 00 01 01 17 03 03 00 2a 6d 33 28 8c K....... ...*m3(.
00d0 2a e5 39 91 df b3 1e ee ac 8f af df 07 a7 1f 1c *.9..... ....
The TCP payload of this packet (tcp.payload), 1448 bytes
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.2
Profile: Default


tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3 1586234922.346532 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
6 1586234922.353811 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8 1586234922.541555 10.0.0.119 95.216.163.36 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
9 1586234922.559911 95.216.163.36 10.0.0.119 TCP 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10 1586234922.559916 95.216.163.36 10.0.0.119 TLSv1 1514 Ignored Unknown Record
11 1586234922.559918 95.216.163.36 10.0.0.119 TLSv1 1266 Ignored Unknown Record
12 1586234922.559920 95.216.163.36 10.0.0.119 TLSv1 139 Ignored Unknown Record
13 1586234922.560036 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
14 1586234922.560051 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
15 1586234922.560056 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
16 1586234922.560059 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
17 1586234922.730475 95.216.163.36 10.0.0.119 TLSv1 90 Application Data
[Next sequence number: 1449 (relative sequence number)]
Acknowledgment number: 518 (relative ack number)
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window size value: 506
[Calculated window size: 64768]
[Window size scaling factor: 128]
Checksum: 0x43f6 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
TCP payload (1448 bytes)
Retransmitted TCP segment data (1448 bytes)
Verdict:
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 05 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0a 00 ....@.+. .._..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 80 10 .w...t.. ot}L....
0030 01 fa 43 f6 00 00 01 01 08 0a 22 76 c1 c4 6b 73 ..C..... .."v..ks
0040 34 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5b d9 4.....z. ..v../[.
0050 40 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0b 56 @z.].68' N@..]..V
0060 45 aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f9 c5 E....... ..z. ..
0070 70 6d 20 c9 2e 2e bc 5f ea 6c 51 1f 79 b4 12 6a pm ...._ .lQ.y..j
0080 24 f5 86 83 56 13 14 fc a5 5d d8 81 63 50 13 02 $...V... .]..cP..
0090 00 00 2e 00 2b 00 02 03 04 00 33 00 24 00 1d 00 ....+... ..3.$...
00a0 20 bb d2 4a 8d 57 df ec 4b 01 6a 13 81 65 3f e3 ..J.W.. K.j..e?.
00b0 f3 d4 0a 37 ac e7 82 09 b7 d1 c5 be e4 86 0f cc ...7.... ....
00c0 4b 14 03 03 00 01 01 17 03 03 00 2a 6d 33 28 8c K....... ...*m3(.
00d0 2a e5 39 91 df b3 1e ee ac 8f af df 07 a7 1f 1c *.9..... ....
The TCP payload of this packet (tcp.payload), 1448 bytes
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.2
Profile: Default


tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3 1586234922.346532 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
6 1586234922.353811 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8 1586234922.541555 10.0.0.119 95.216.163.36 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
9 1586234922.559911 95.216.163.36 10.0.0.119 TCP 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10 1586234922.559916 95.216.163.36 10.0.0.119 TLSv1 1514 Ignored Unknown Record
11 1586234922.559918 95.216.163.36 10.0.0.119 TLSv1 1266 Ignored Unknown Record
12 1586234922.559920 95.216.163.36 10.0.0.119 TLSv1 139 Ignored Unknown Record
13 1586234922.560036 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
14 1586234922.560051 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
15 1586234922.560056 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
16 1586234922.560059 10.0.0.119 95.216.163.36 TCP 54 54388 → 443 [RST] Seq=518 Win=0 Len=0
17 1586234922.730475 95.216.163.36 10.0.0.119 TLSv1 90 Application Data
[Next sequence number: 1449 (relative sequence number)]
Acknowledgment number: 518 (relative ack number)
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window size value: 506
[Calculated window size: 64768]
[Window size scaling factor: 128]
Checksum: 0x43f6 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
TCP payload (1448 bytes)
Retransmitted TCP segment data (1448 bytes)
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 05 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0a 00 ....@.+. .._..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 80 10 .w...t.. ot}L....
0030 01 fa 43 f6 00 00 01 01 08 0a 22 76 c1 c4 6b 73 ..C..... .."v..ks
0040 34 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5b d9 4.....z. ..v../[.
0050 40 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0b 56 @z.].68' N@..]..V
0060 45 aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f9 c5 E....... ..z. ..
0070 70 6d 20 c9 2e 2e bc 5f ea 6c 51 1f 79 b4 12 6a pm ...._ .lQ.y..j
0080 24 f5 86 83 56 13 14 fc a5 5d d8 81 63 50 13 02 $...V... .]..cP..
0090 00 00 2e 00 2b 00 02 03 04 00 33 00 24 00 1d 00 ....+... ..3.$...
00a0 20 bb d2 4a 8d 57 df ec 4b 01 6a 13 81 65 3f e3 ..J.W.. K.j..e?.
00b0 f3 d4 0a 37 ac e7 82 09 b7 d1 c5 be e4 86 0f cc ...7.... ....
00c0 4b 14 03 03 00 01 01 17 03 03 00 2a 6d 33 28 8c K....... ...*m3(.
00d0 2a e5 39 91 df b3 1e ee ac 8f af df 07 a7 1f 1c *.9..... ....
Verdict: injection!
And apparently courtesy of Comcast!
The TCP payload of this packet (tcp.payload), 1448 bytes
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.2
Profile: Default

old.reddit.com

Comcast's XFi advanced security is autoblocking torproject.org (ERR_SSL_PROTOCOL_ERROR) : TOR

MY SUBREDDITS ▼ POPULAR ALL RANDOM USERS | ASKREDDIT WORLDNEWS FUNNY AWW PICS GAMING NEWS VIDEOS MOVIES TODAYILEARNED EXPLAINLIKEIMFIVE TIFU MILDLYINTERESTING NOTTHEONION GIFS JOKES DATAISBEAUTIFUL MORE »

Tor

COMMENTS

2

Comcast's XFi advanced security is autoblocking torproject.org (ERR_SSL_PROTOCOL_ERROR)

self.TOR

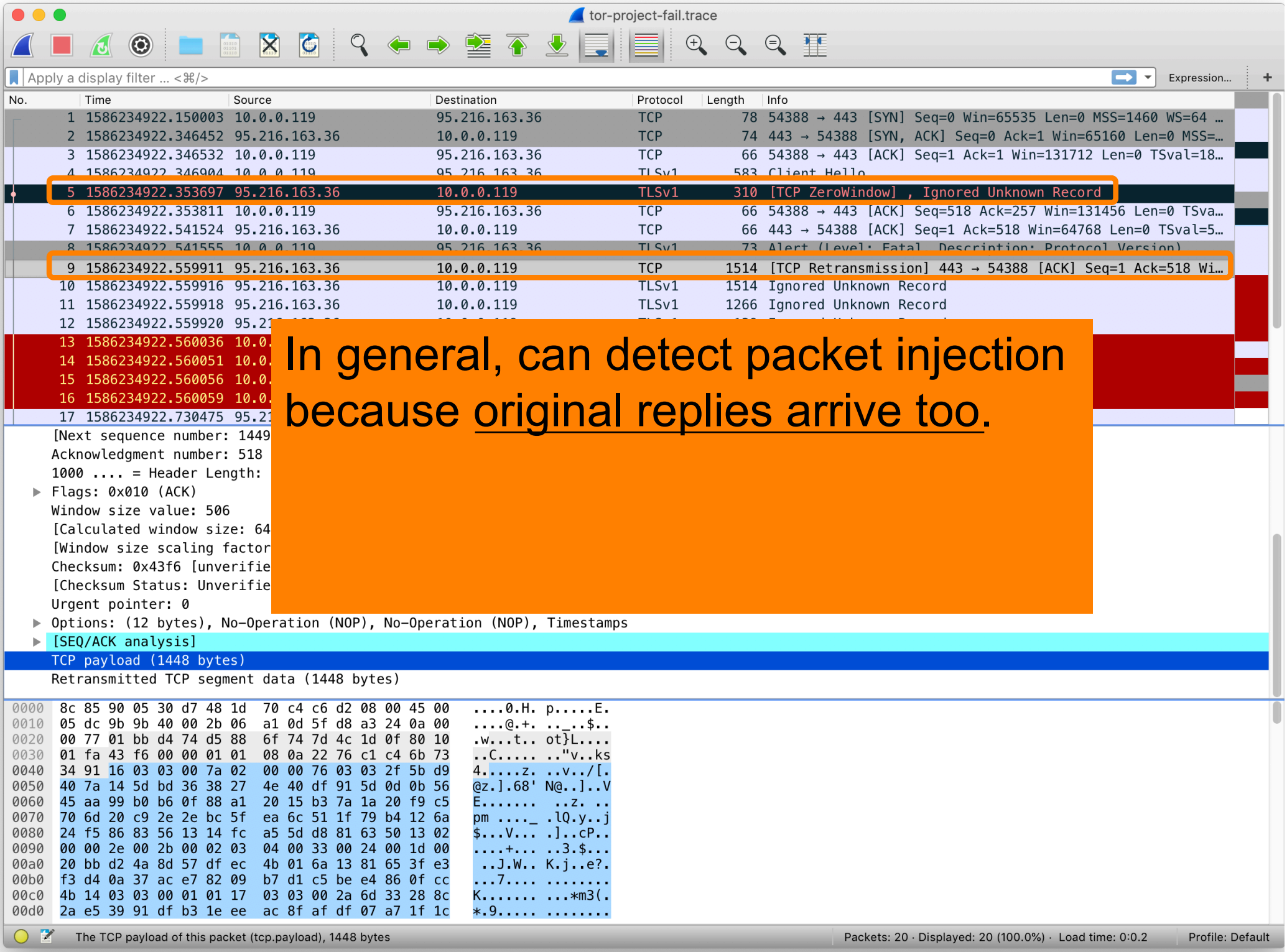
Submitted 22 days ago by MadCabbit

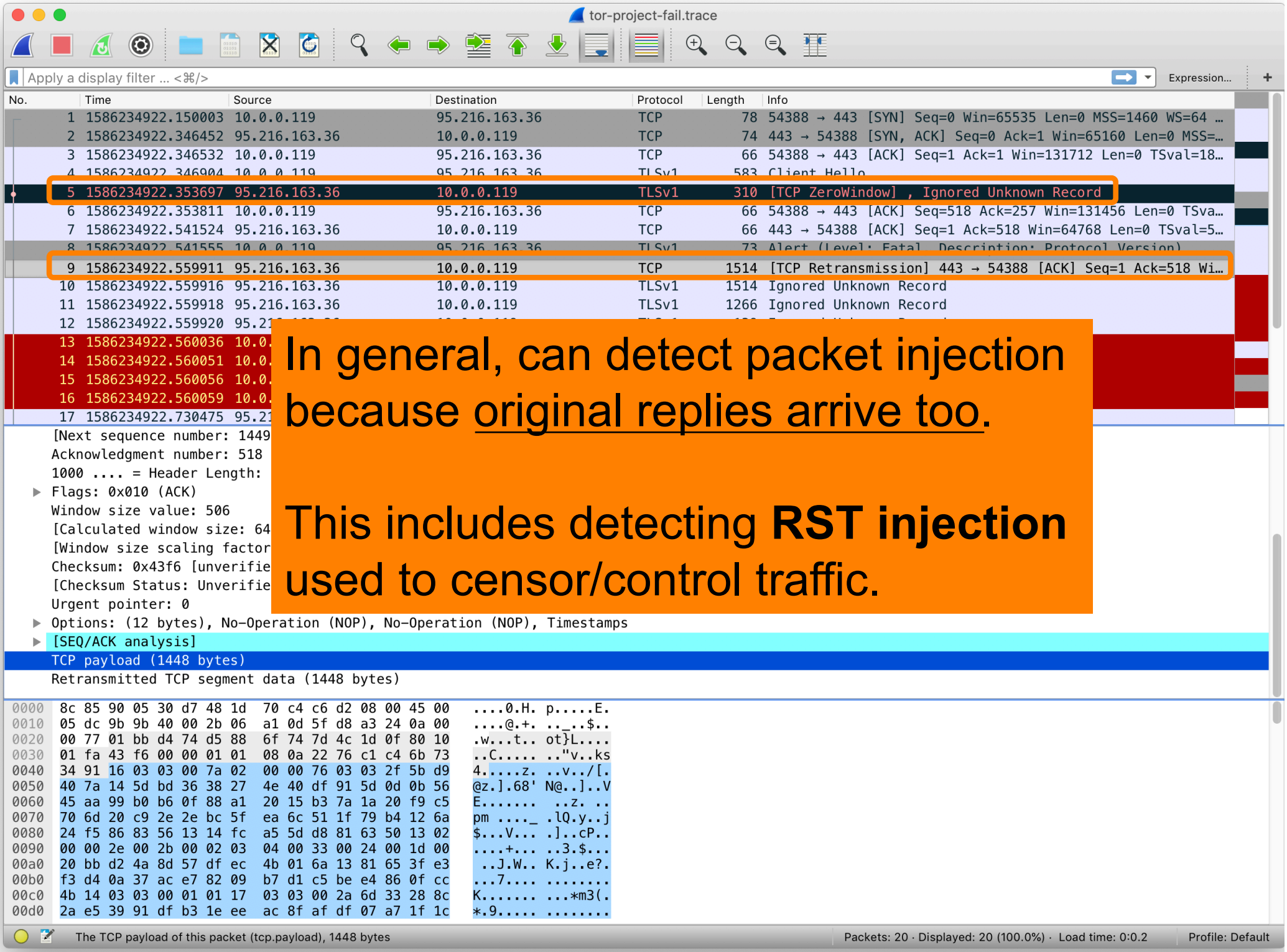
I decided to download the Tor Browser again today, but I kept getting ERR_SSL_PROTOCOL_ERROR on both my PCs, on Windows and Linux. I initially thought the site was having issues, but not seeing anyone else having this problem when googling, or in this subreddit, I eventually stumbled upon the culprit checking my networking settings, XFi Advanced Security automatically blocked it. Trying to enable it manually only works for an hour. I've put off turning this feature off despite other headaches with Comcast being so ham-handed with blocks, but this takes the cake. This feature is definitely more of a pain for advanced users than it is a benefit. I guess it shouldn't really be surprising to me, given Comcast's MO, though.

5 comments share save hide report

all 5 comments

sorted by: best▼


tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3 1586234922.346532 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
6 1586234922.353811 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8 1586234922.541555 10.0.0.119 95.216.163.36 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
9 1586234922.559911 95.216.163.36 10.0.0.119 TCP 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10 1586234922.559916 95.216.163.36 10.0.0.119 TLSv1 1514 Ignored Unknown Record
11 1586234922.559918 95.216.163.36 10.0.0.119 TLSv1 1266 Ignored Unknown Record
12 1586234922.559920 95.21
13 1586234922.560036 10.0.
14 1586234922.560051 10.0.
15 1586234922.560056 10.0.
16 1586234922.560059 10.0.
17 1586234922.730475 95.21
[Next sequence number: 1449
Acknowledgment number: 518
1000 .... = Header Length:
Flags: 0x010 (ACK)
Window size value: 506
[Calculated window size: 64
[Window size scaling factor
Checksum: 0x43f6 [unverifie
[Checksum Status: Unverifie
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
TCP payload (1448 bytes)
Retransmitted TCP segment data (1448 bytes)
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 05 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0a 00 ....@.+. .._..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 80 10 .w...t.. ot}L....
0030 01 fa 43 f6 00 00 01 01 08 0a 22 76 c1 c4 6b 73 ..C..... .."v..ks
0040 34 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5b d9 4.....z. ..v../[.
0050 40 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0b 56 @z.].68' N@..]..V
0060 45 aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f9 c5 E....... ..z. ..
0070 70 6d 20 c9 2e 2e bc 5f ea 6c 51 1f 79 b4 12 6a pm ...._ .lQ.y..j
0080 24 f5 86 83 56 13 14 fc a5 5d d8 81 63 50 13 02 $...V... .]..cP..
0090 00 00 2e 00 2b 00 02 03 04 00 33 00 24 00 1d 00 ....+... ..3.$...
00a0 20 bb d2 4a 8d 57 df ec 4b 01 6a 13 81 65 3f e3 ..J.W.. K.j..e?.
00b0 f3 d4 0a 37 ac e7 82 09 b7 d1 c5 be e4 86 0f cc ...7.... ....
00c0 4b 14 03 03 00 01 01 17 03 03 00 2a 6d 33 28 8c K....... ...*m3(.
00d0 2a e5 39 91 df b3 1e ee ac 8f af df 07 a7 1f 1c *.9..... ....
In general, can detect packet injection because original replies arrive too.
The TCP payload of this packet (tcp.payload), 1448 bytes
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.2
Profile: Default


tor-project-fail.trace
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 1586234922.150003 10.0.0.119 95.216.163.36 TCP 78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2 1586234922.346452 95.216.163.36 10.0.0.119 TCP 74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3 1586234922.346532 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922.346904 10.0.0.119 95.216.163.36 TLSv1 583 Client Hello
5 1586234922.353697 95.216.163.36 10.0.0.119 TLSv1 310 [TCP ZeroWindow] , Ignored Unknown Record
6 1586234922.353811 10.0.0.119 95.216.163.36 TCP 66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524 95.216.163.36 10.0.0.119 TCP 66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8 1586234922.541555 10.0.0.119 95.216.163.36 TLSv1 73 Alert (Level: Fatal, Description: Protocol Version)
9 1586234922.559911 95.216.163.36 10.0.0.119 TCP 1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10 1586234922.559916 95.216.163.36 10.0.0.119 TLSv1 1514 Ignored Unknown Record
11 1586234922.559918 95.216.163.36 10.0.0.119 TLSv1 1266 Ignored Unknown Record
12 1586234922.559920 95.21
13 1586234922.560036 10.0.
14 1586234922.560051 10.0.
15 1586234922.560056 10.0.
16 1586234922.560059 10.0.
17 1586234922.730475 95.21
[Next sequence number: 1449
Acknowledgment number: 518
1000 .... = Header Length:
Flags: 0x010 (ACK)
Window size value: 506
[Calculated window size: 64
[Window size scaling factor
Checksum: 0x43f6 [unverifie
[Checksum Status: Unverifie
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
TCP payload (1448 bytes)
Retransmitted TCP segment data (1448 bytes)
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 ....0.H. p.....E.
0010 05 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0a 00 ....@.+. .._..$..
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 80 10 .w...t.. ot}L....
0030 01 fa 43 f6 00 00 01 01 08 0a 22 76 c1 c4 6b 73 ..C..... .."v..ks
0040 34 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5b d9 4.....z. ..v../[.
0050 40 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0b 56 @z.].68' N@..]..V
0060 45 aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f9 c5 E....... ..z. ..
0070 70 6d 20 c9 2e 2e bc 5f ea 6c 51 1f 79 b4 12 6a pm ...._ .lQ.y..j
0080 24 f5 86 83 56 13 14 fc a5 5d d8 81 63 50 13 02 $...V... .]..cP..
0090 00 00 2e 00 2b 00 02 03 04 00 33 00 24 00 1d 00 ....+... ..3.$...
00a0 20 bb d2 4a 8d 57 df ec 4b 01 6a 13 81 65 3f e3 ..J.W.. K.j..e?.
00b0 f3 d4 0a 37 ac e7 82 09 b7 d1 c5 be e4 86 0f cc ...7.... ....
00c0 4b 14 03 03 00 01 01 17 03 03 00 2a 6d 33 28 8c K....... ...*m3(.
00d0 2a e5 39 91 df b3 1e ee ac 8f af df 07 a7 1f 1c *.9..... ....
In general, can detect packet injection because original replies arrive too.
This includes detecting RST injection used to censor/control traffic.
The TCP payload of this packet (tcp.payload), 1448 bytes
Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.2
Profile: Default

The Problem of Spam

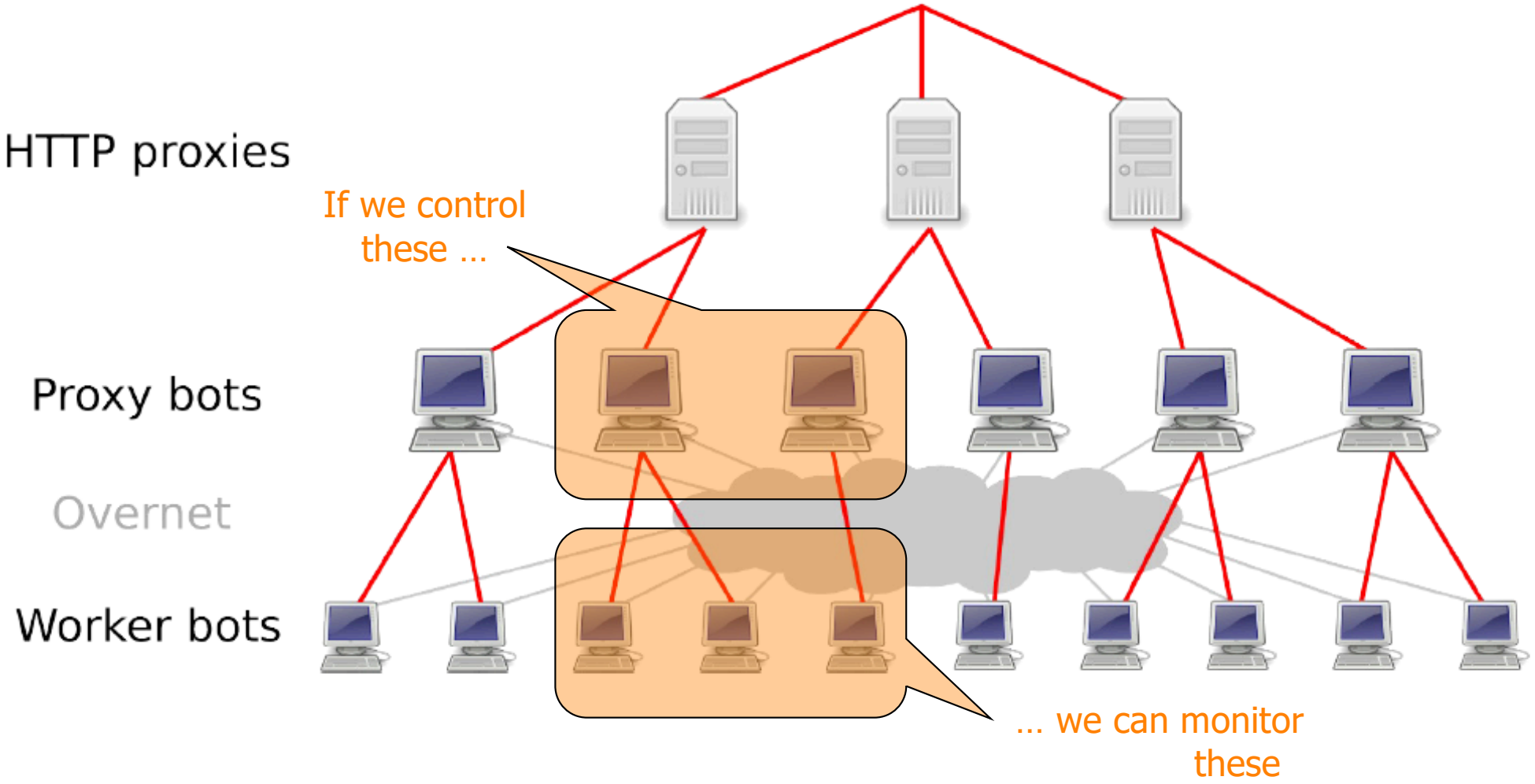
Spam: Unwanted Messages

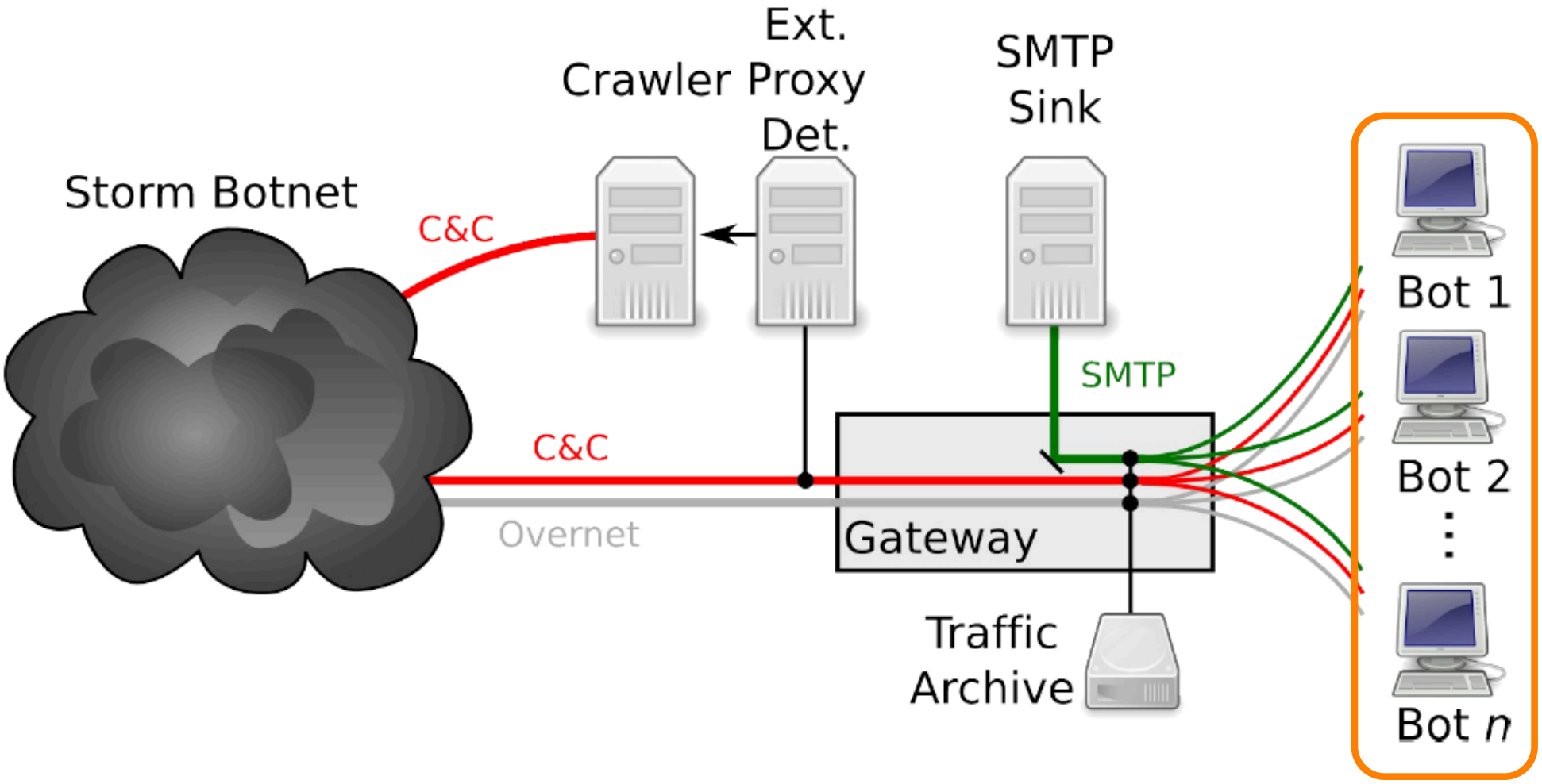
- Endemic networking problem:
  - If network is open & sending is cheap, miscreants will abuse to transmit low-value messages at **massive scale**
  - *Scale* means low value still reaps benefits

Spam: Unwanted Messages

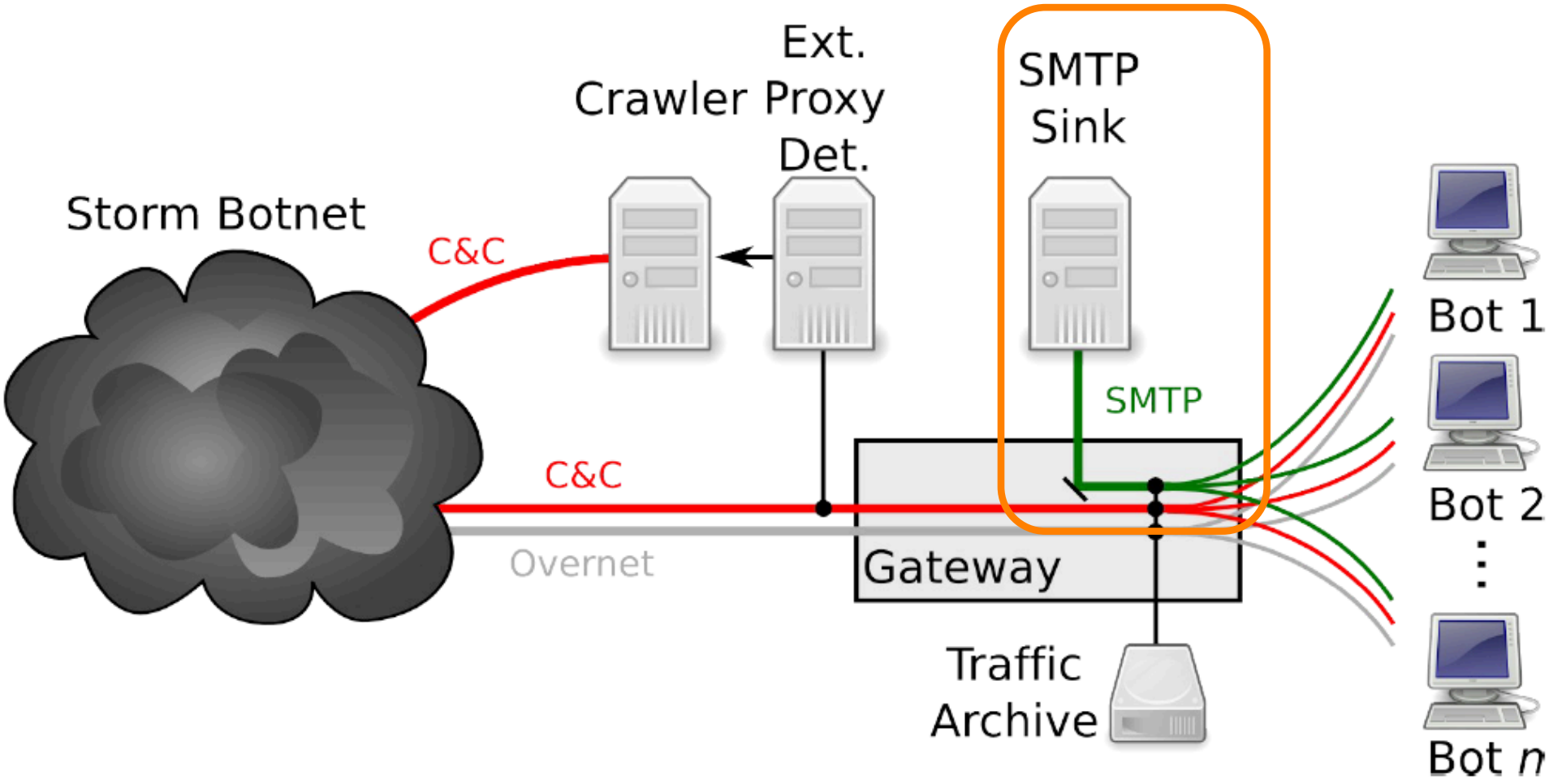
- Endemic networking problem:
  - If network is open & sending is cheap, miscreants will abuse to transmit low-value messages at **massive scale**
  - *Scale* means low value still reaps benefits
- Old as the hills
  - Telegram spam in 1864!
  - Energetic arms race
- You probably don't care …
- *… but you should:*
  - Bankrolls development of botnets (*incentivizes attacks*)
  - Gateway drug to more serious cybercrime
    - Today's bane: ransomware

Research Measurement of Spam Botmaster's Operations

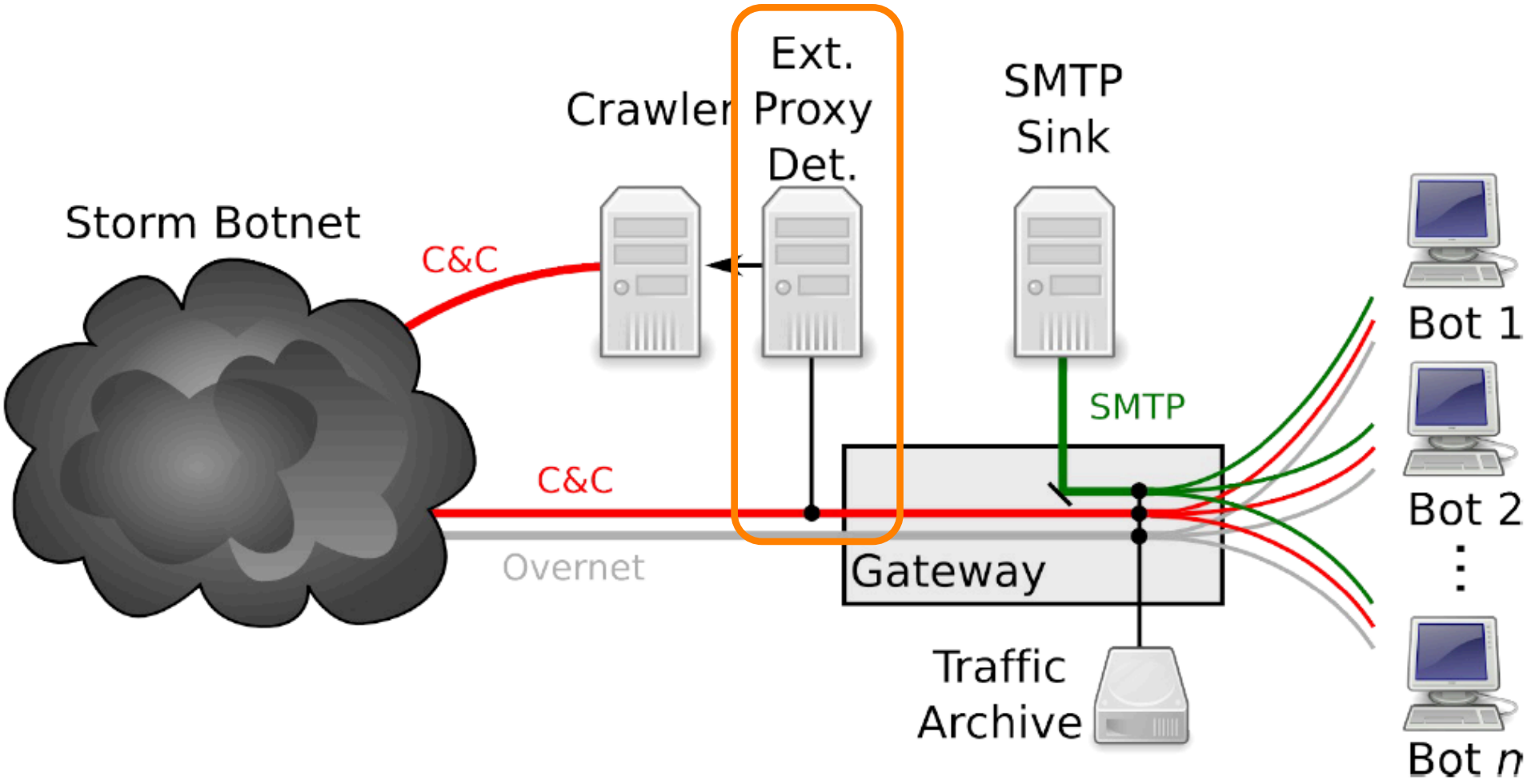




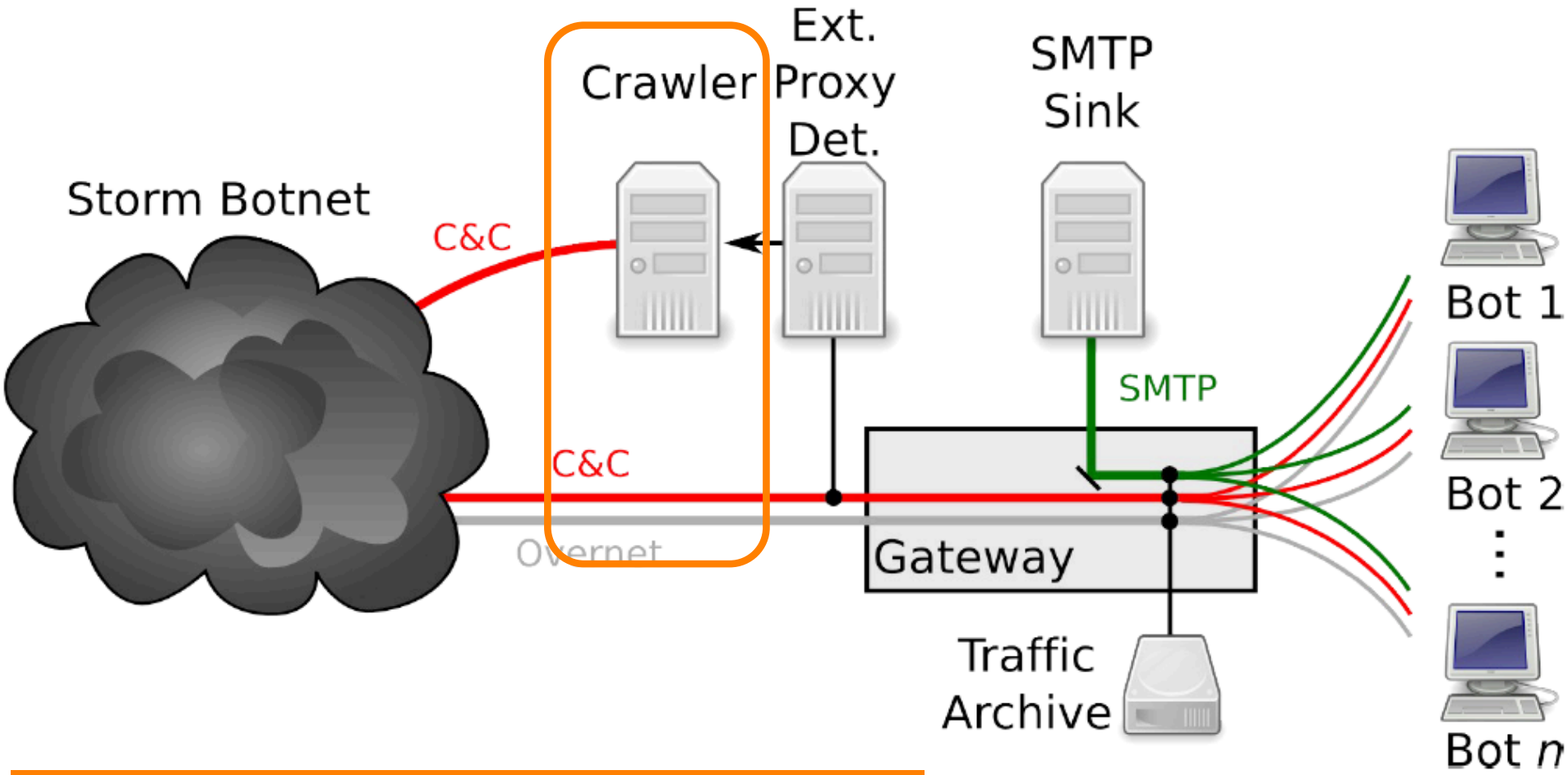
Run captive bot binaries in VMs
(repurposed worm *honeyfarm*)



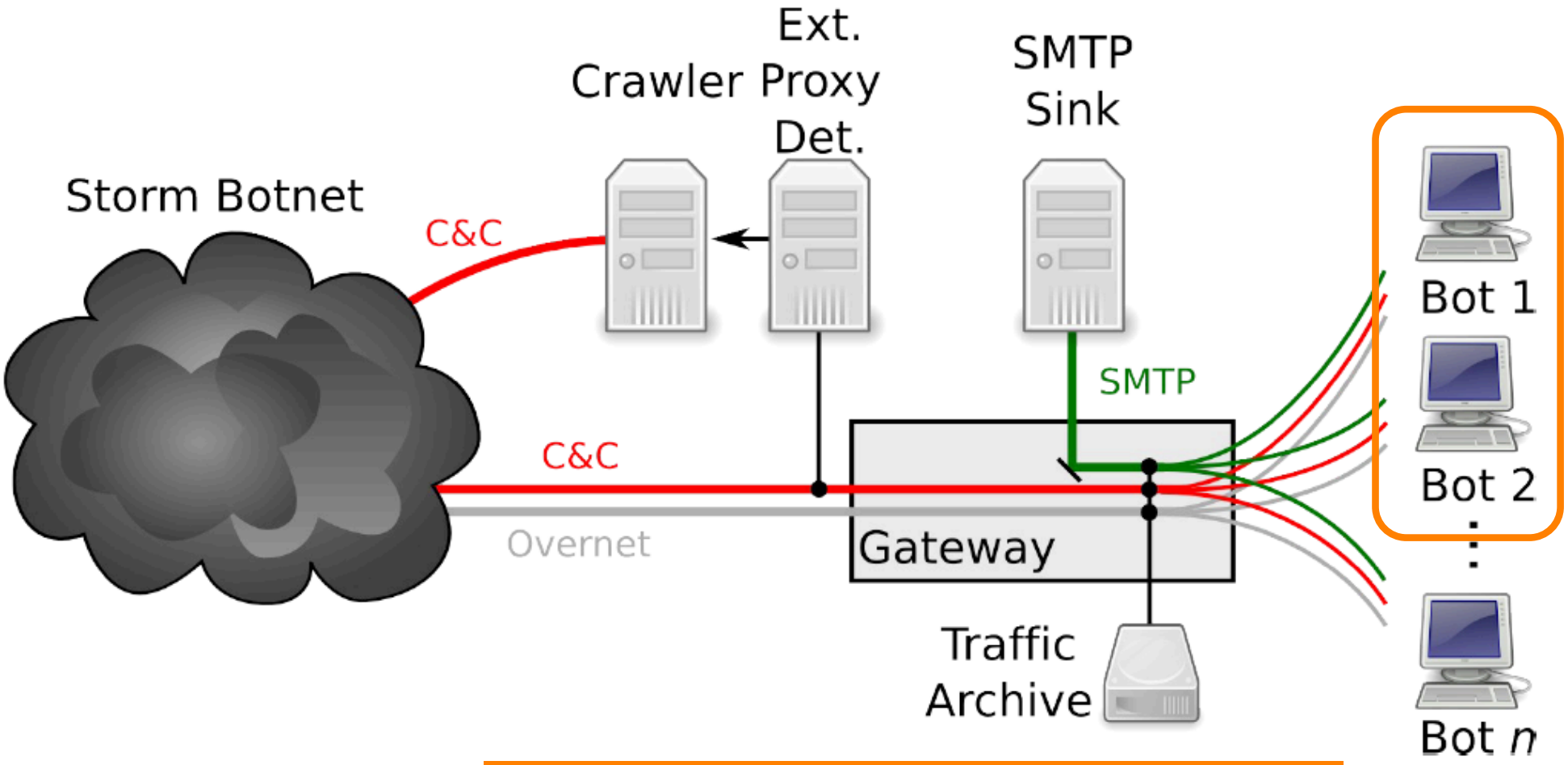
Make sure they can't send any actual spam (but think they are)



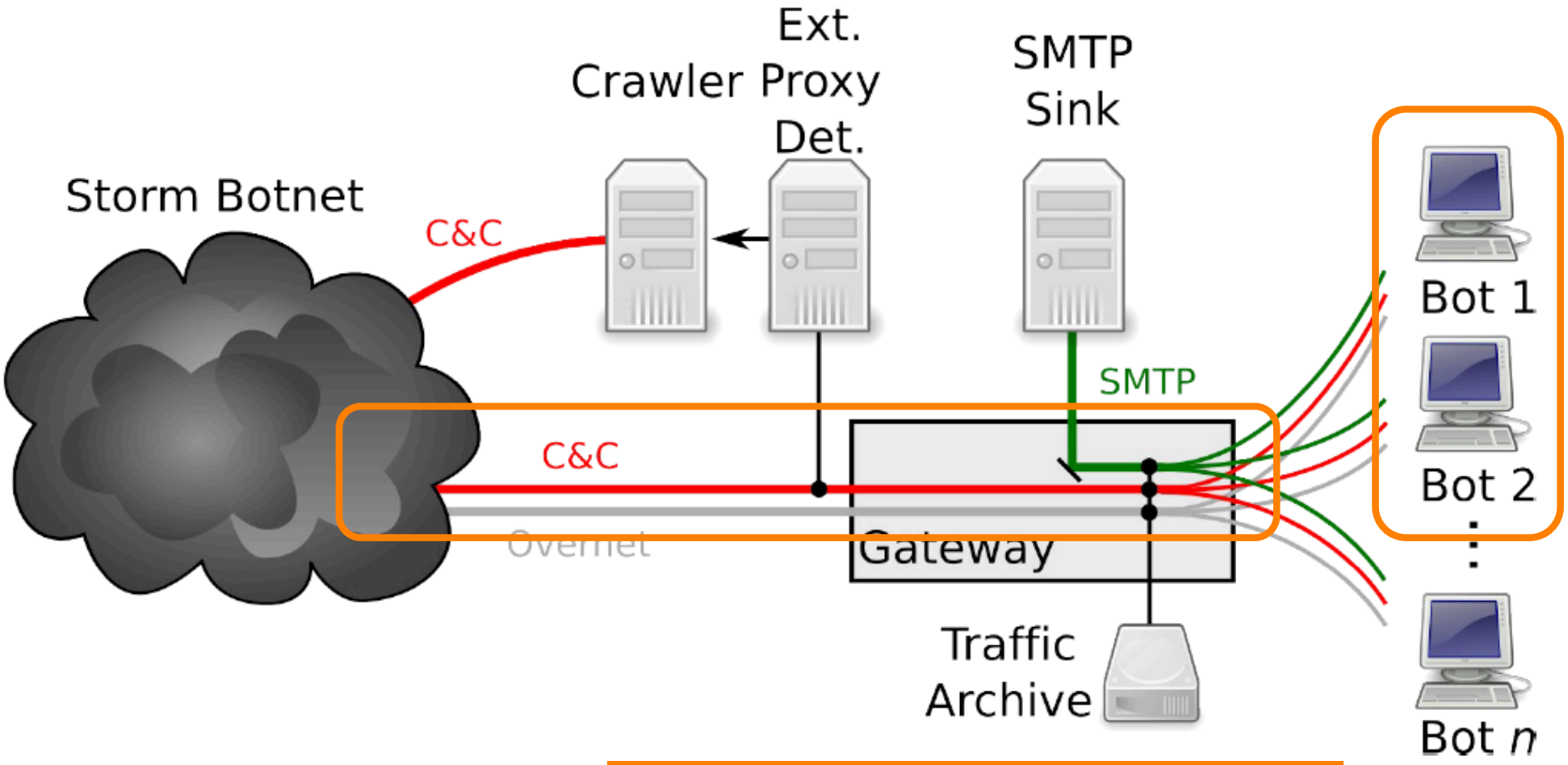
Analyze C&C traffic to identify Storm proxy bots



Crawler pretends to be a worker and relentlessly asks Storm proxies for work ("**milking**")



Also run **proxies** internally … they contact Storm's HTTP servers to directly ask for work

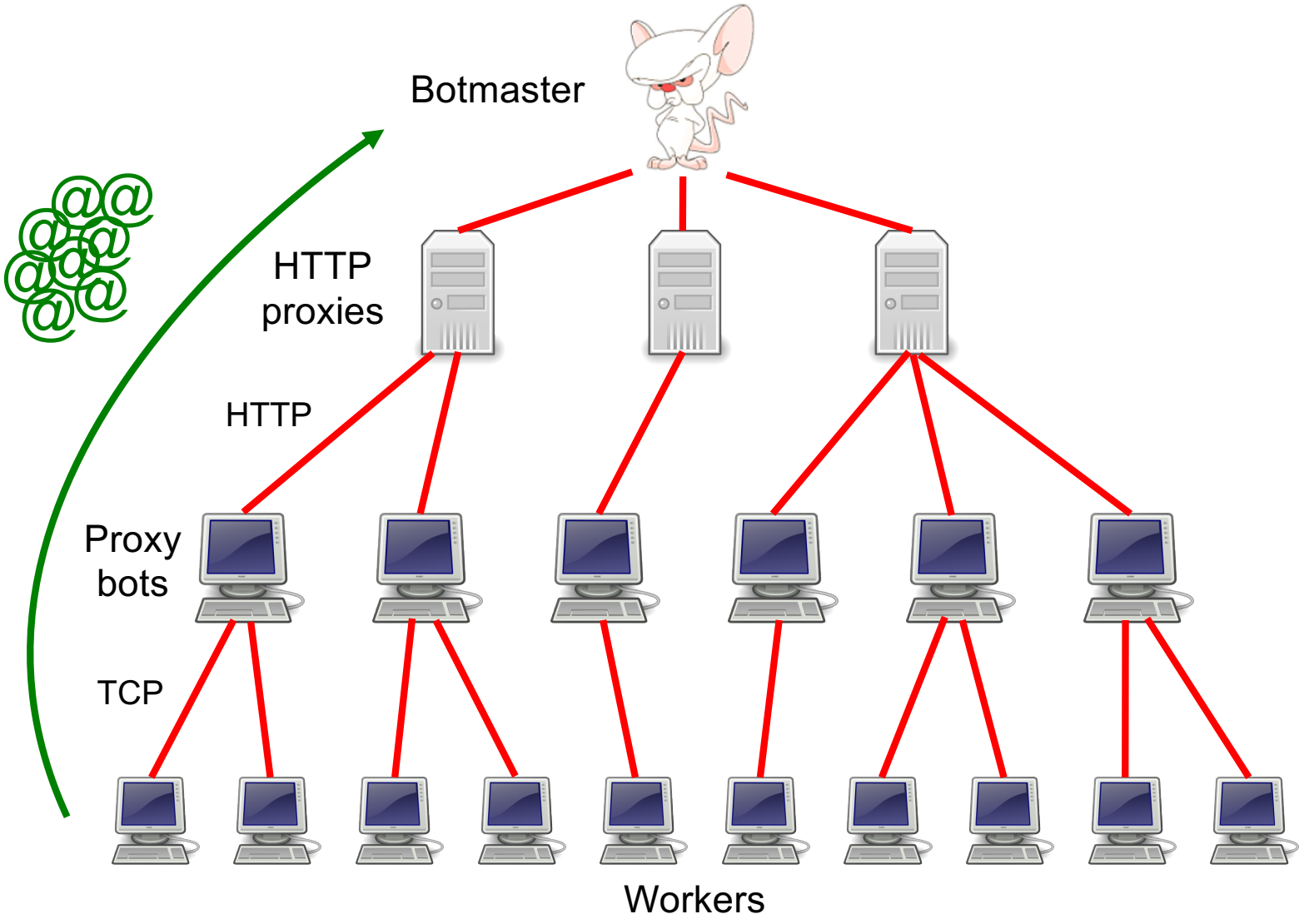


… and they **mediate C&C** for actual infected bots

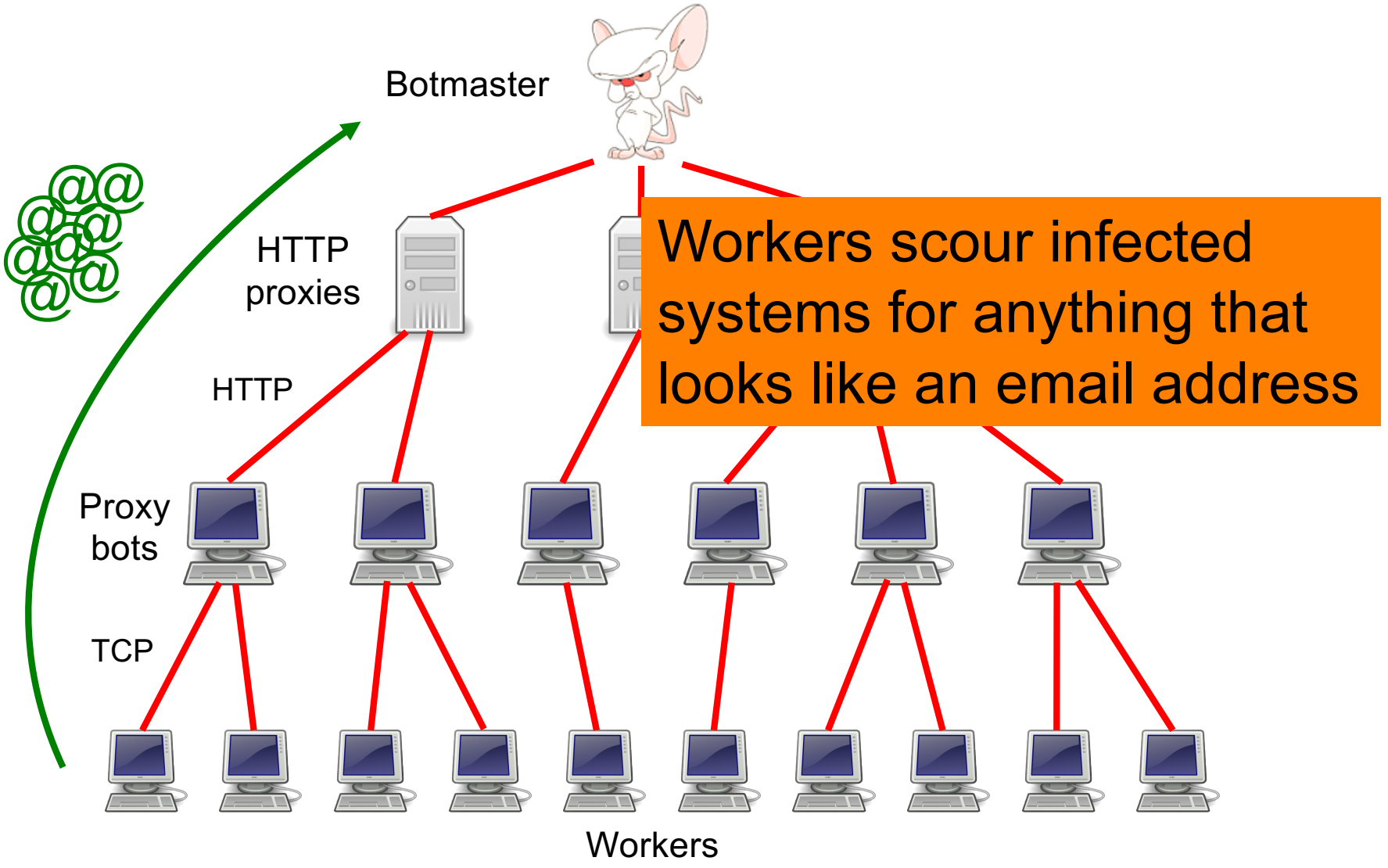
Types of Storm C&C Messages

- Activation (report from bot to botmaster)
- Email address harvests
- Spamming instructions
- Delivery reports
- DDoS instructions
- FastFlux instructions
- HTTP proxy instructions
- Sniffed passwords report
- IFRAME injection/report

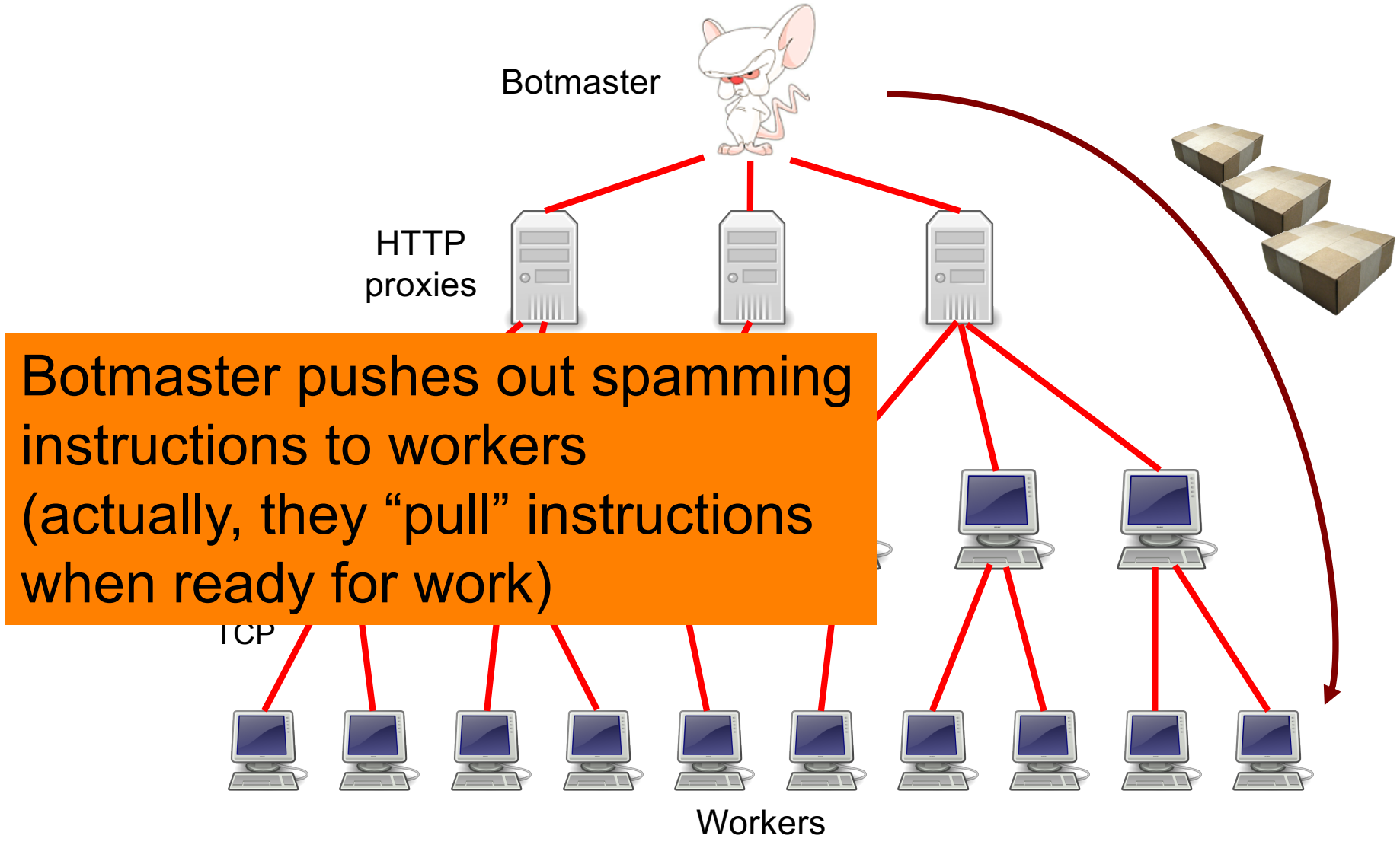
Campaign mechanics: harvest



Campaign mechanics: harvest



Campaign mechanics: spamming



MACRO	SEEN LIVE	FUNCTIONALITY
(0)	✓	Spam target email address.
(A)	✓	FQDN of sending bot, as reported to the bot as part of the preceding C&C exchange.
(B)		Creates content-boundary strings for multi-part messages.
(C*num*)	✓	Labels a field's resulting content, so it can be used elsewhere through (V); see below.
(D)	✓	Date and time, formatted per RFC 2822.
(E)		ROT-3–encodes the target email address.
(F*string*)	✓	Random value from the dictionary named *string*.[2]
(G*string*)	✓	Line-wrap *string* into 72 characters per line.
(H*string*)		Defines hidden text snippets with substitutions, for use in HTML- and plain-text parts.
(I)	✓	Random number between 1 and 255, used to generate fake IP addresses.
(J*string*)		Produces quoted-printable "=20" linewrapping.
(K)		IP address of SMTP client.
(M)	✓	6-character string compatible with Exim's message identifiers (keyed on time).
(N)		16-bit prefix of SMTP client's IP address.
(O*string*:*num*)	✓	Randomized message identifier element compatible with Microsoft SMTPSVC.
(Pnum_1[-num_2]:*string*)	✓	Random string of num_1 (up to num_2, if provided) characters taken from *string*.
(Q*string*)		Quoted-printable "=" linewrapping.
(Rnum_1-num_2)	✓	Random number between num_1 and num_2. Note, special-cased when used with (D).
(U*string*)		Randomized percent-encoding of *string*.
(V*num*)	✓	Inserts the value of the field identified by (C*num*).
(W)		Time and date as plain numbers, e.g. "20080225190434".
(X)		Previously selected member of the "names" dictionary.
(Y*num*)	✓	8-character alphanumeric string, compatible with Sendmail message identifiers.
(Z)	✓	Another Sendmail-compatible generator for message identifiers.

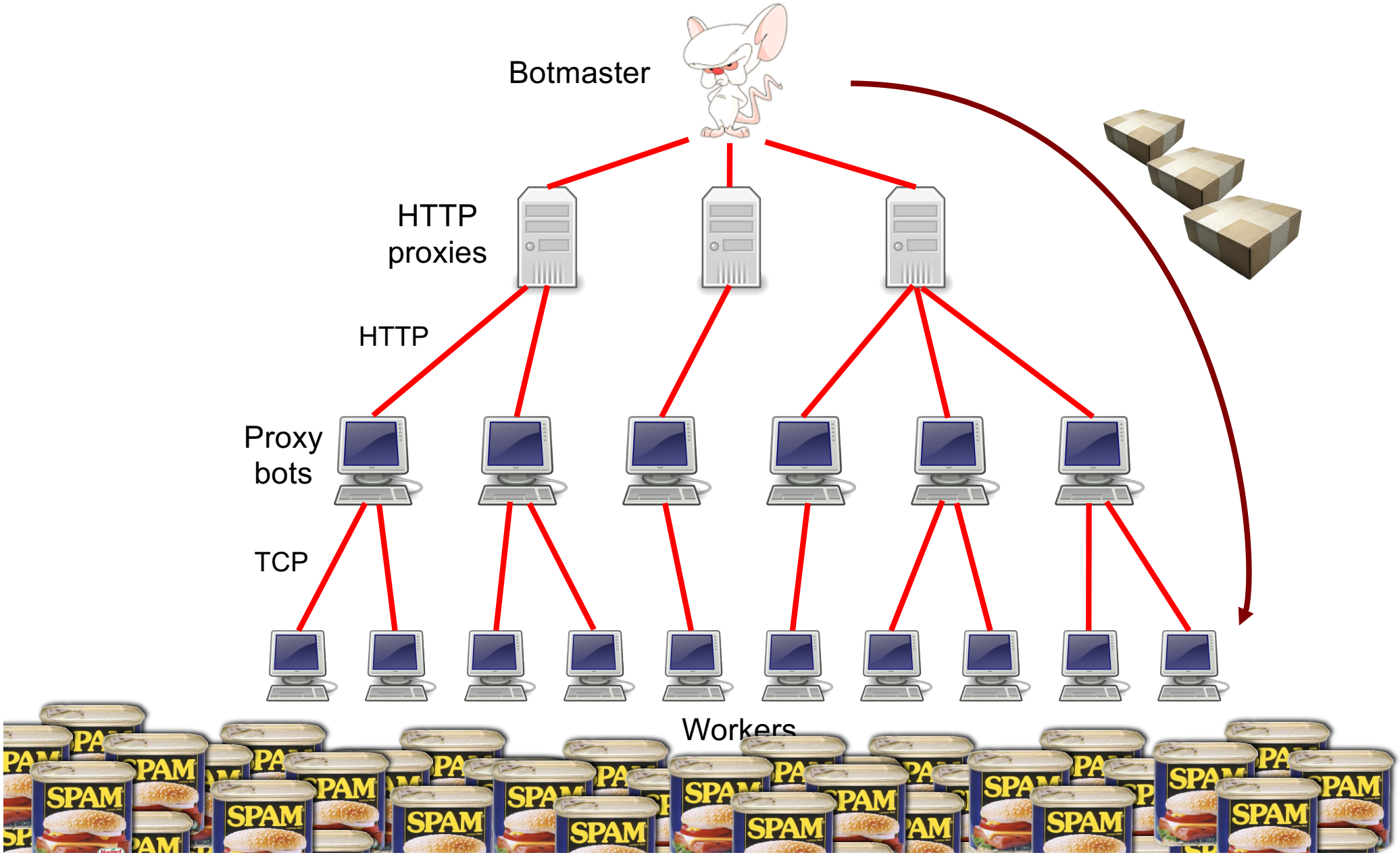
Table 2: Storm's spam-generation templating language.

```
Received: from %^C0%^P%^R2-6^%:qwertyuiopasdfghjklzxcvbnm^%.%^P%^R2-6^%:qwertyuiopasdfghjkl ▷
                                          zxcvbnm^%^% ([%^C6%^I^%.%^I^%.%^I^%.%^I^%^%]) by ▷
                                          %^A^% with Microsoft SMTPSVC(%^Fsvcver^%); %^D^%
Message-ID: <%^O%^V6^%:%^R3-50^%^%%^V0^%>
From: <%^Fnames^%@%^Fdomains^%>
To: <%^0^%>
Subject: JOB $1800/WEEK - CANADIANS WANTED!
Date: %^D-%^R30-600^%^%
```

```
Received: from auz.xwzww ([132.233.197.74]) by dsl-189-188-79-63.prod-infinitum.com.mx with ▷
                         Microsoft SMTPSVC(5.0.2195.6713); Wed, 6 Feb 2008 16:33:44 -0800
Message-ID: <002e01c86921$18919350$4ac5e984@auz.xwzww>
From: <katiera@experimentalist.org>
To: <voelker@cs.ucsd.edu>
Subject: JOB $1800/WEEK - CANADIANS WANTED!
Date: Wed, 6 Feb 2008 16:33:44 -0800
```

Figure 2: Snippet of a spam template, showing the transformation of an email header from template (top) to resulting content (bottom). The ▷-symbol indicates line continuations. Bold text corresponds to the formatting macros and their evaluation.

Campaign mechanics: spamming



CLASS	DESCRIPTION
Money mule scam	Attemps to enroll the victim in money laundering schemes
Personal ad scam	Fake dating/matchmaking invitations intended to convince victim to advance money
Job ads	Variant of money-mule scams, new "employee" is asked to forward money or goods
Self-propagation	Tricks or lures victims into executing malicious binaries[1]
Phishing	Entices victims to enter sensitive information at fake bank sites or similars
Pharmaceutical	Pointers to web sites selling Viagra, Cialis, and other "male enhancement" products
Stock scam	Tries to convince victim to buy a particular stock suppsedly about to increase in value
Other ads	Other kinds of advertising
Image spam	Image-based spam[2]
Other	Broken or empty templates, noise-only templates, etc.[3]

Table 3: Meanings of campaign classes.

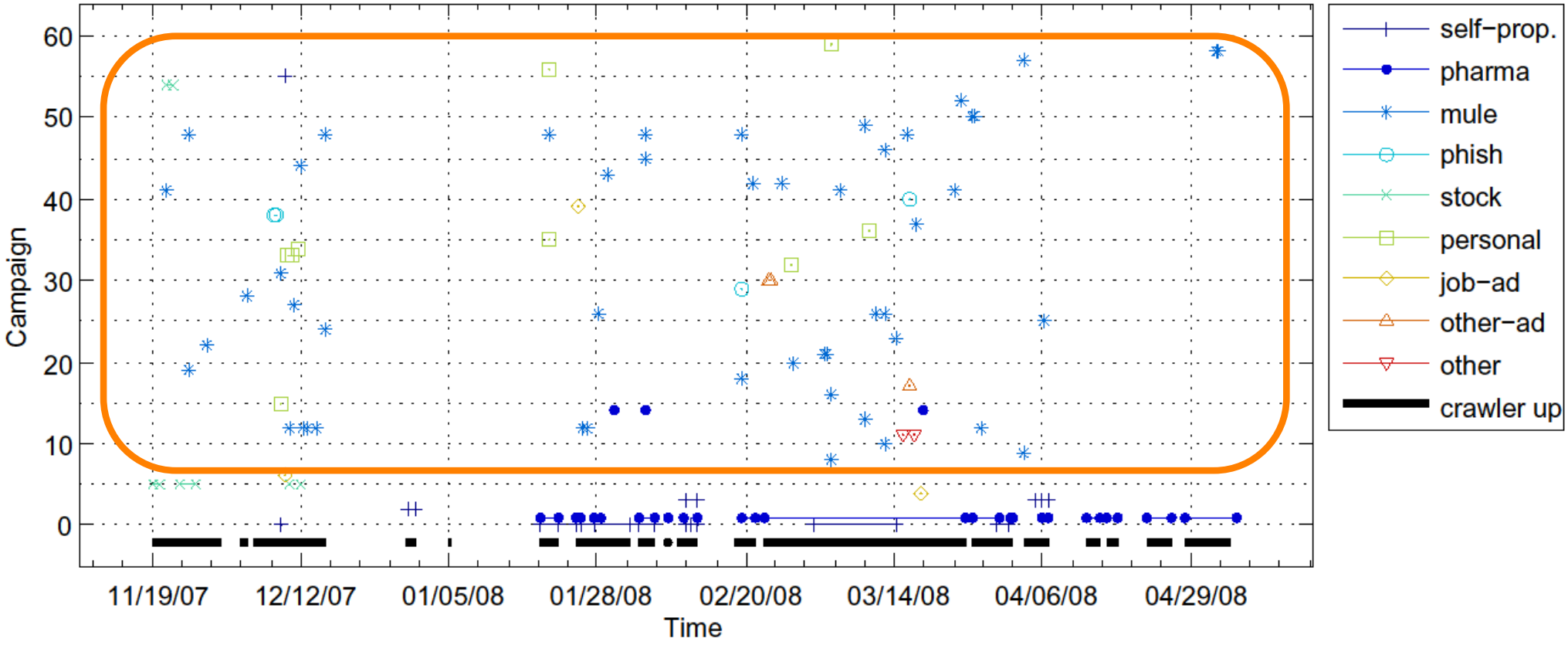


Figure 5: Classes and instances of spaming campaigns identified over time.

Storm did a wide variety of shortlived spam campaigns …

… likely for hire

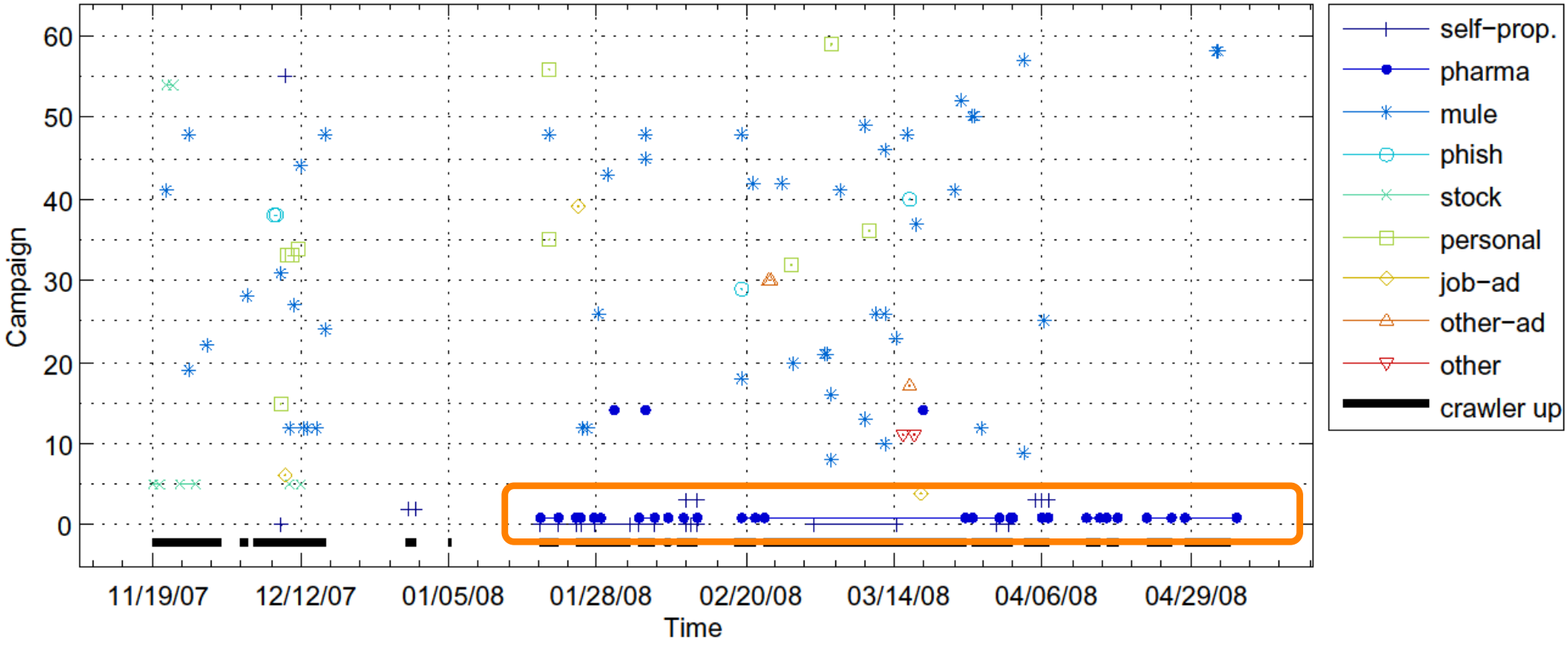


Figure 5: Classes and instances of spaming campaigns identified over time.

Plus steady pharma spam
… likely botmaster's own

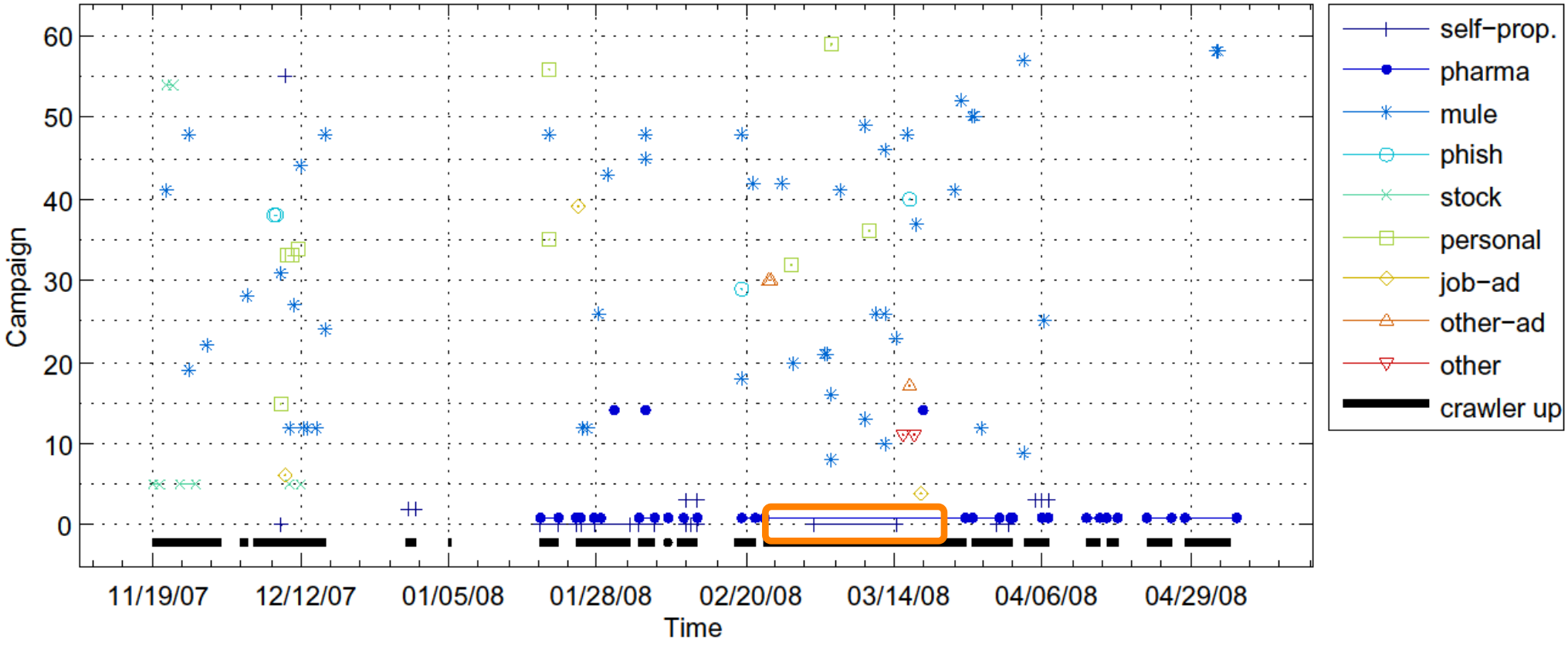
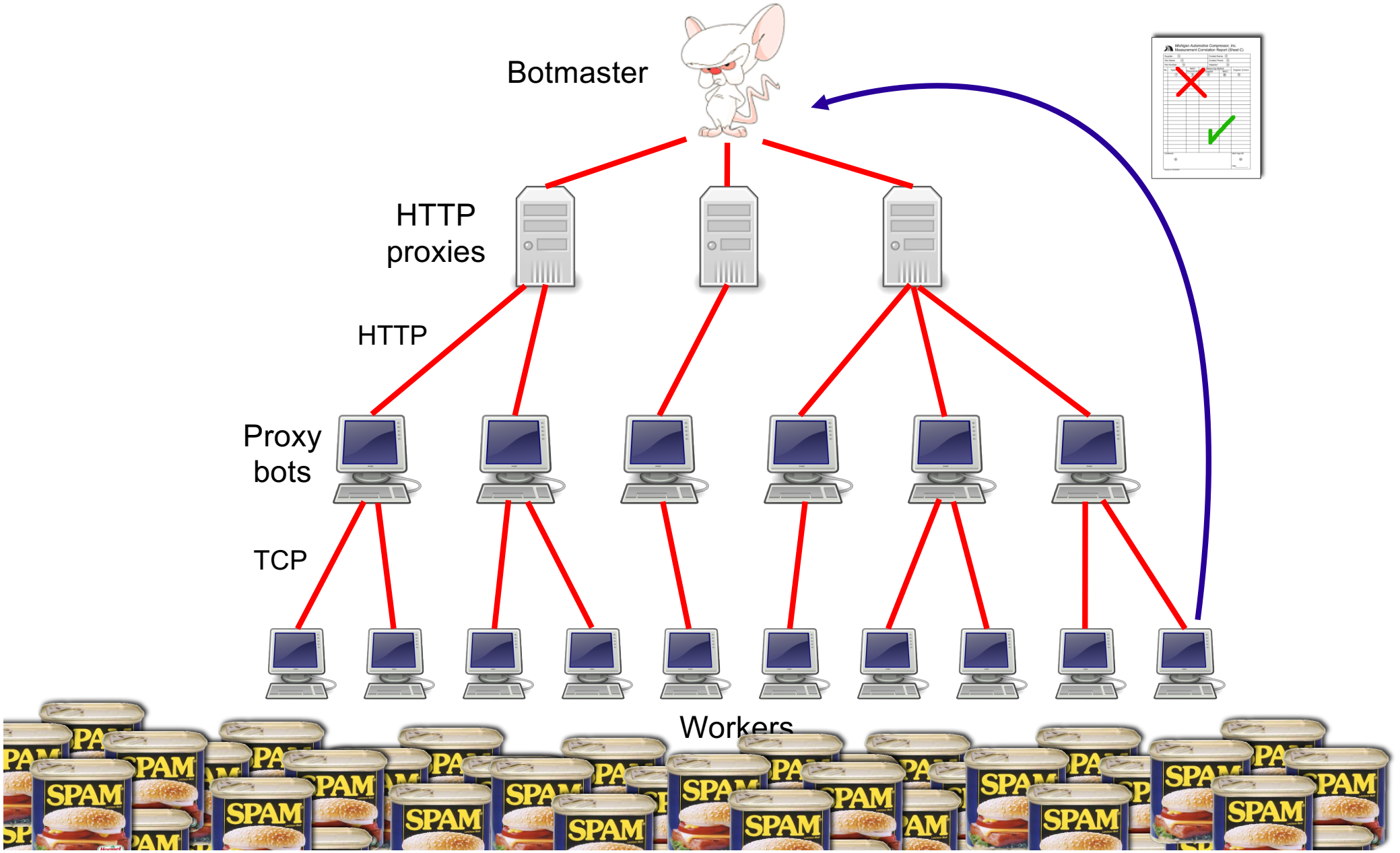


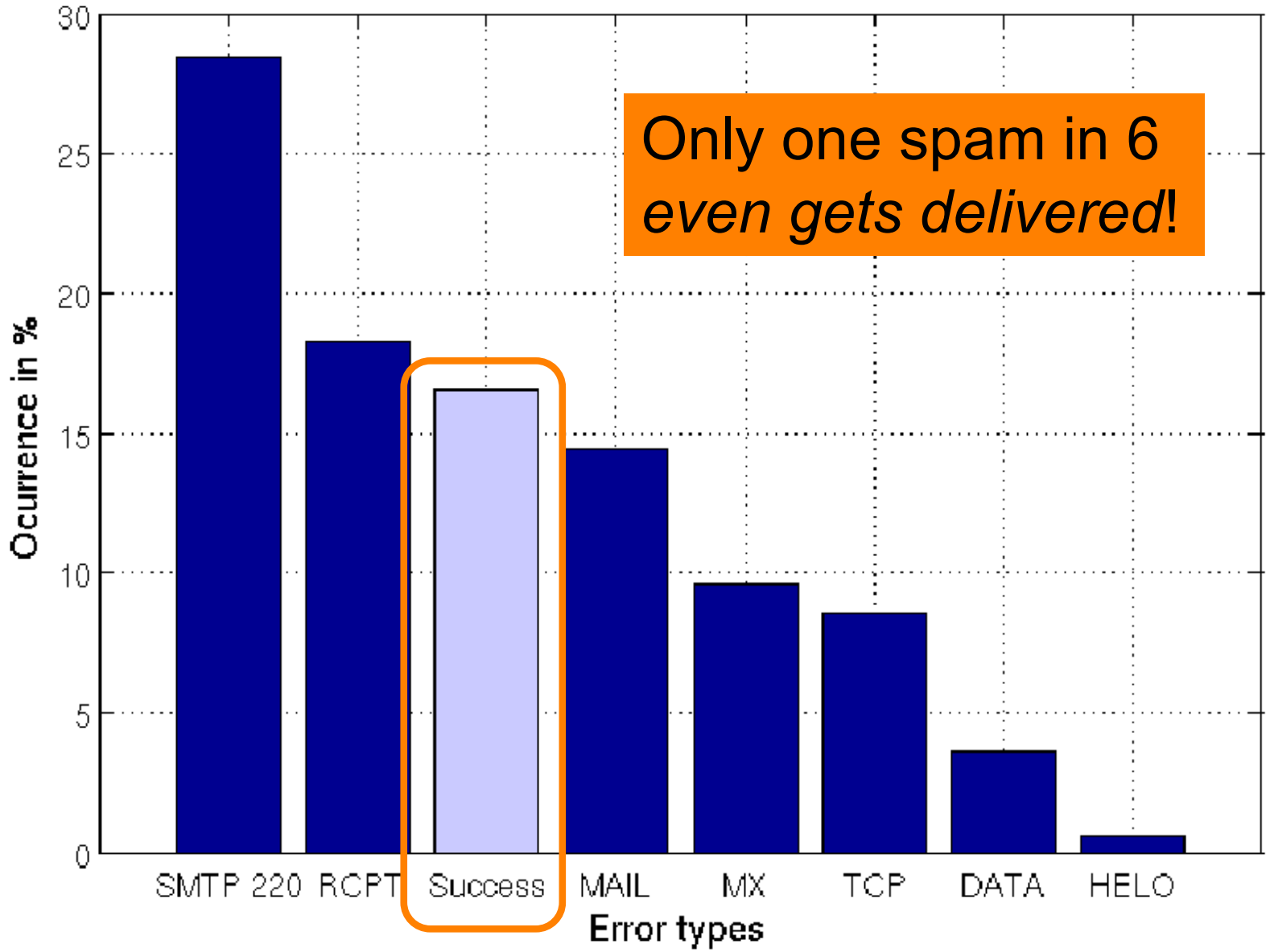
Figure 5: Classes and instances of spaming campaigns identified over time.

And occasional *stupid Postcards* spam to freshen the bot army

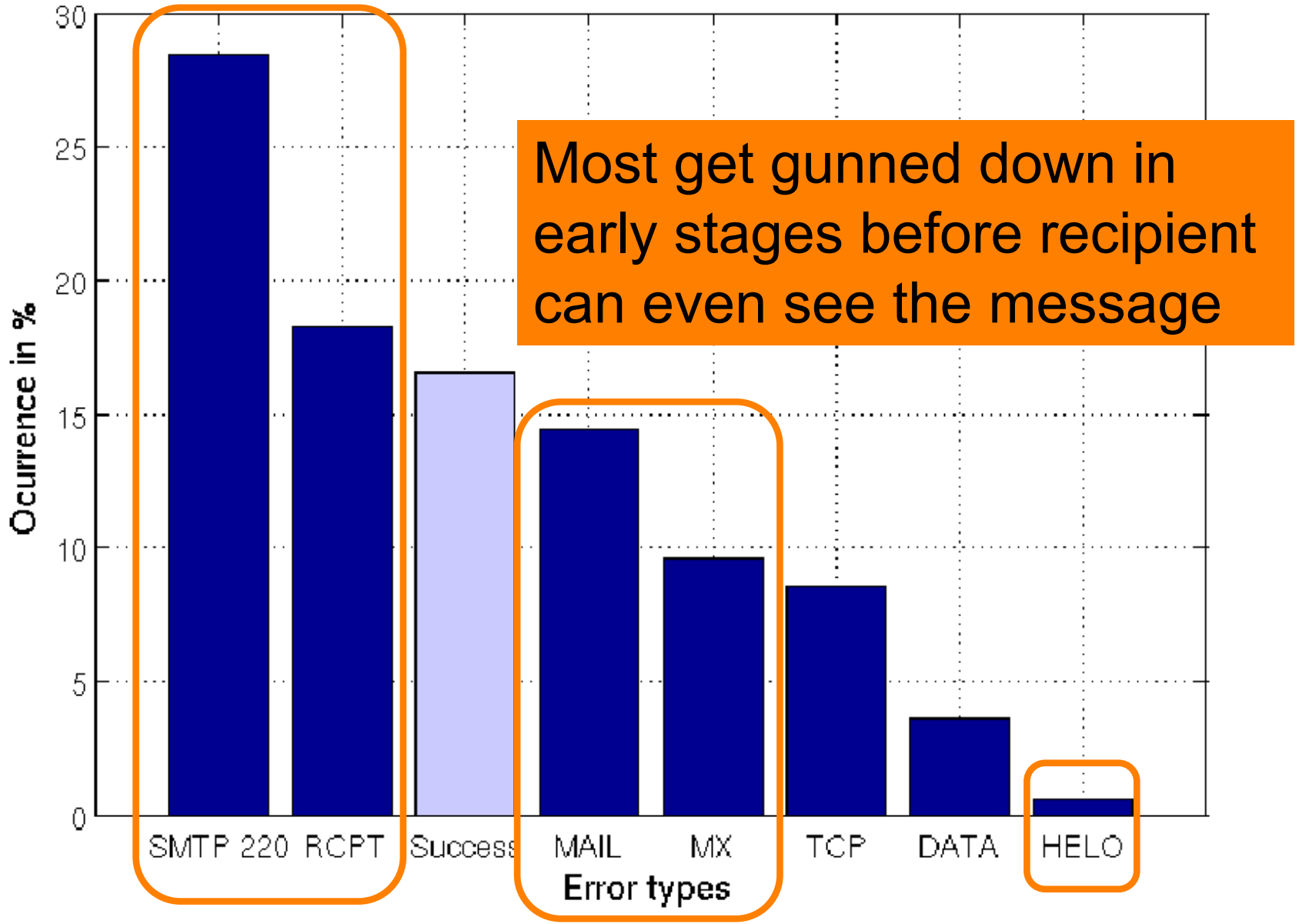
Campaign mechanics: reporting



Measurements: delivery efficacy

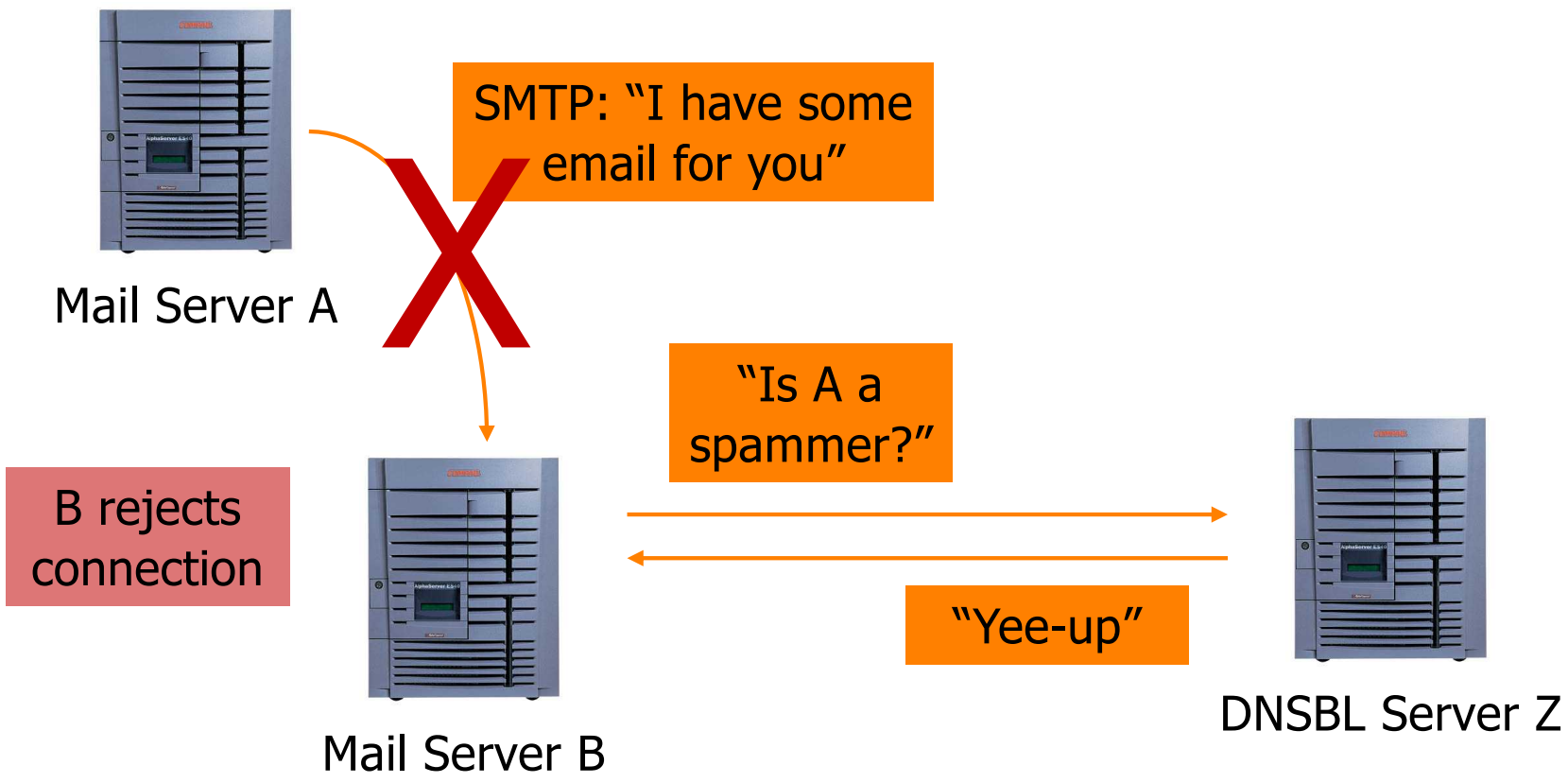


Measurements: delivery efficacy



DNS Blacklists (DNSBL)

- Spammer vulnerability: activities broadly visible
  - Defenders with large “telescopes” can view early …
  - … and distill & disseminate signatures for blocking
- Easy signature: IP address of sender
- Easy way to disseminate signatures: DNS


SMTP: "I have some email for you"
Mail Server A
"Is A a spammer?"
B rejects connection
"Yee-up"
Mail Server B
DNSBL Server Z

Mail Server A

SMTP: “I have some email for you”

“Is A a spammer?”

Mail Server B

B accepts email

“Not on my list”

DNSBL Server Z

Mail Server A

If B forwards the mail, or when B originates mail

Mail Server B

DNSBL Server Z

SMTP: "I have some email for you"

Mail Server C

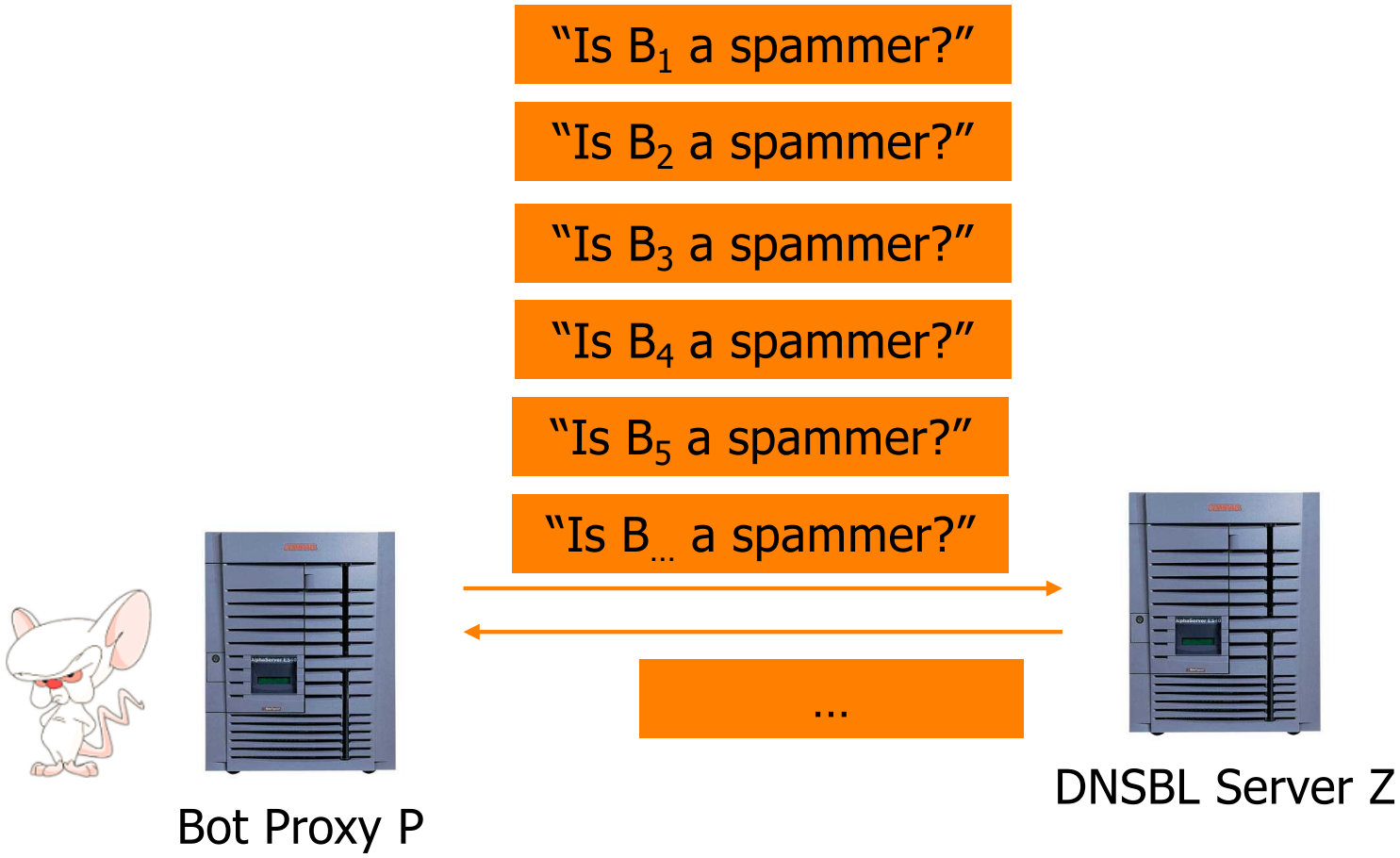
"Is B a spammer?"

...

Z will see that B both **makes a lot of lookups** *over time*, and **gets looked up** a lot *over time*

DNSBL Counter-Intelligence

- Counter-intelligence: learning about your adversary via their own attempts to gather intel
- The utility of a bot plummets if on a DNSBL
- For a spammer considering buying a set of bots, they need to determine this
  - Need to look up the bots themselves …
  - … often using an existing bot to proxy their lookup



Idea: operator of Z *seeds* analysis with list of Known Bad addresses. For any such system, *which other addresses* A_i did it look up in a burst? Add A_i to Known Bad addresses list and *recurse* ⇒ **enumerate botnet.**

Can also seed with systems that do bursts of lookups and aren't themselves looked up in non-bursts.

Counter-Intelligence, con't

- Bill M. probes spyware C&C using set of scanning hosts S_i
- C&C operators noticed some of these S_j and blacklisted them (TCP RST reply) …
- … but didn't find *all* of them (S_k)
- So: Bill scans entire Internet from S_j system *and* from S_k system
  - System replying to latter but not to former ⇒ *managed by the C&C operator*
  - Allows enumeration!

How Much $$ Do Spammers Make?

Affiliate ID: **17788**
Balance:
$0.00
Payments:
$0.00 Sent
$0.00 Hold

Stats
Creatives
Settings
Payments
Advanced
Info

Contacts

Mark 430
Skype: mark_affiliate

Vanessa 644
Skype: vanessa-affiliate

Sandra 356
Skype: sandr

Mary Ryan 608
Skype:
mary_ryan_affiliate

Liza 634
Skype: liza_affiliate

Frequently Asked Questions

Help for this Section: Eng / Rus

How do you pay?
What are your payment plans?
How do you know that this is "my" customer?
What should I do to join you?
What do you sell?
What if I don't live in the USA? May I become your affiliate?
Where can I monitor the statistics of my site?
When do you ship the orders?
Can I advertise a specific product, not the whole pharmacy?
What is the commission on the refill orders?
I need help configuring my templates what do I do?
I lost my password, what do I do?
Are you accepting call centers?

How do you pay?

We pay every week on Thursday with a 2 weeks' holdback. $50 minimum on stormpay and wires. If you require larger amounts sent at one time you can set the minimum yourself.

Payment by request is now available. Effective from 07.17.2006

Our loyal affiliates now have the chance to minimize the hold period and to get the money when they need it. Even though it will be handled individually in every case the guidelines are simple.

You should have the steady sales record for the last 3 months (that is your daily average should be at least 3 sales for the above mentioned period) and your traffic source can be easily tracked. This will not apply to the commission earned during special promotions and we won't be able to pay to PayPal earlier than scheduled. You are welcome to use Bank Wire, Epass, Egold, Webmoney and

What are your payment plans?

Our affiliate program offers 3 levels of RevShare.

You can choose to receive 30, 40 or 50% from sale. Prices of products increase with each new level of Revshare. You can set ANY price provided that it is higher than the base price (price of product at 30%).

For example, viagra 100mg x 10 pills, has the following prices:
$29.95 (30%)
$35.95 (40%)
$49.95 (50%)
- You cannot set the price lower than $29.95
- Any price between $29.95 and $35.95 will give you Revshare of 30%
- Any price between $35.95 and $49.95 will give you Revshare of 40%
- Any price higher than $49.95 will give you Revshare of 50%

To change the price enter the new figure in "Your Price" window and click on the arrow next to it. The forcast of price per pill and your commission will be shown. Click on the Save button at the buttom of the screen to enable the new prices. (If you don't click on the arrow the "Save" button won't work)

You can also change all prices by setting a needed percentage in "Value", (in the upper part of interface), or by coping the prices from another Tracking id.

Please note that some products may have only one or two levels of Revshare.

How do you know that this is "my" customer?

First, your affiliate id is clearly visible in the site's url. Our program leaves a cookie at a customer's computer to identify him at the return. And finally the customer creates an account at our site. He is sure to remember his original login name as we offer great bonuses for the returning customers.

Canadian Pharmacy

http://[redacted]/

Google

Home | Bestsellers | All products | FAQ | Contact us

$ € £

Pharma Bonus

Your cart: **$0.00** (0 items)
Proceed to Checkout >

Canadian Pharmacy

#1 Internet Online Drugstore

Products list

- **Bestsellers**
- Male Enhancement
- Men's Health
- SALES - 20% OFF
- Female Enhancement
- Weight Loss
- Gums New!
- Body-Building
- Hypnotherapy

Viagra + Cialis — 69.99 $

10 x Viagra
100 mg
10 x Cialis
20 mg

ORDER NOW

Penis Growth Pack — 179.95 $

Penis Growth Pills
1 bottle x 60caps

Penis Growth Oil
1 tube x 2oz

ORDER NOW

Viagra — 225.61 $

120 pills
100 mg
+4 Free pills

ORDER NOW

Search by name: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z S

Search:

Today's Bestsellers

Viagra

Our price
$1.21

More info | Add to cart

Cialis

Our price
$2.18

More info | Add to cart

Viagra Professional

Our price
$3.73

More info | Add to cart

Done

These folks seem trustworthy …

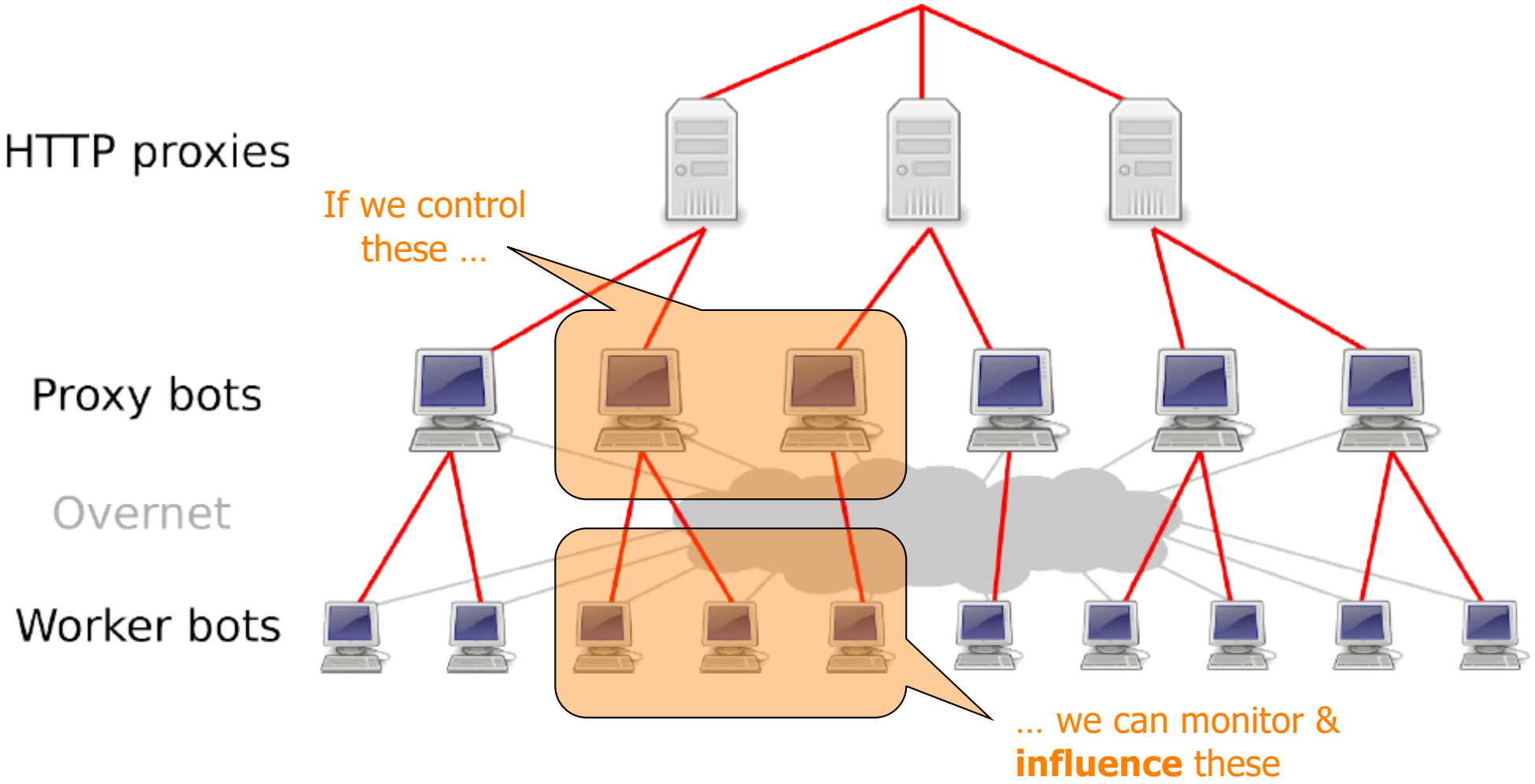
… how about these?

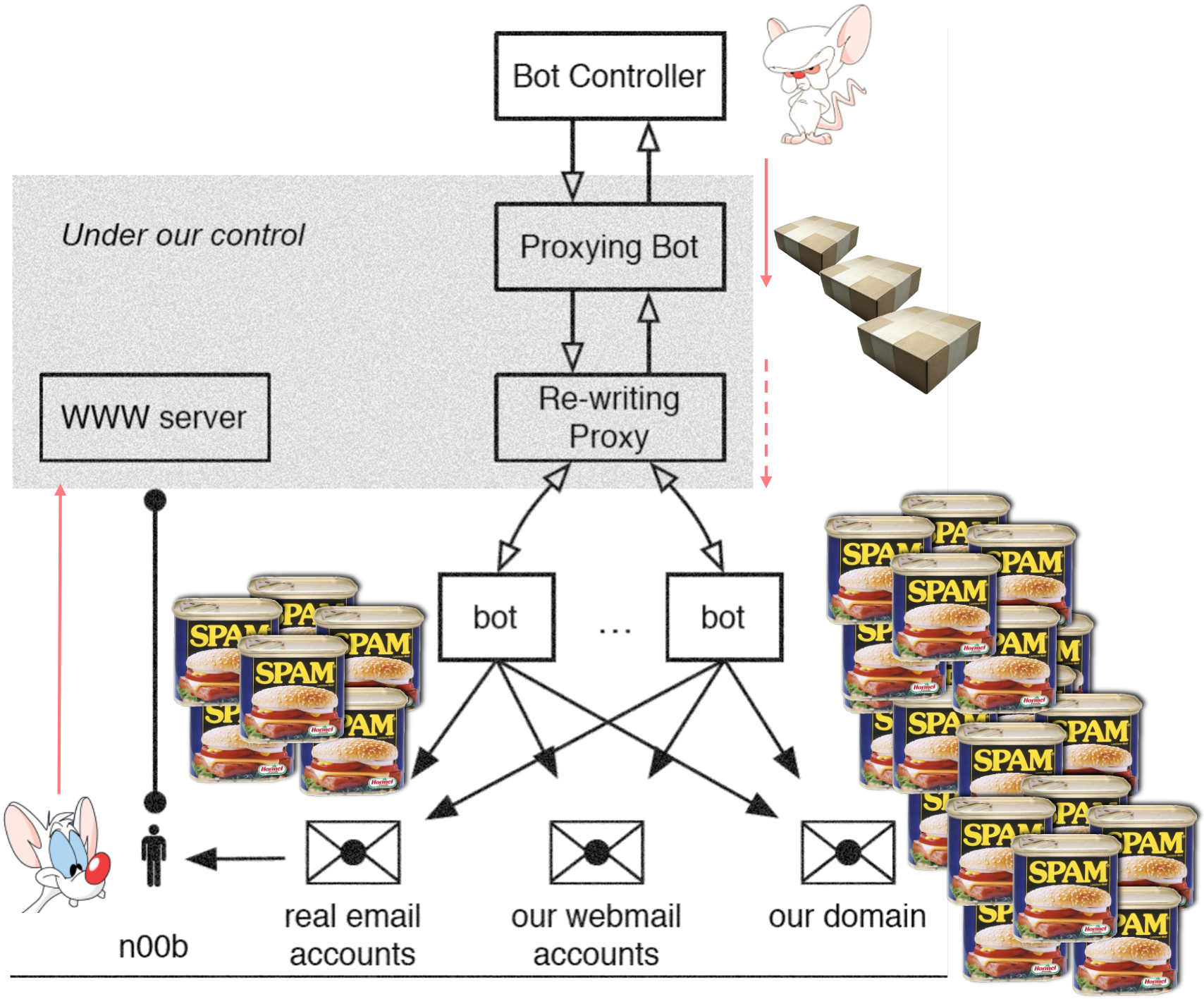
Kirill Levchenko

klevchen@cs.ucsd.edu

I am a project scientist with the Systems and Networking group in the Computer Science department at the University of California, San Diego. My current research

Research Measurement of Spam Botmaster's Operations




Bot Controller
Under our control
Proxying Bot
WWW server
Re-writing Proxy
bot
...
bot
n00b
real email accounts
our webmail accounts
our domain