

Data Exfiltration through DNS lookups and Botnet Control Structures

Nolan Berry

Cory Schwartz

Why is DNS a problem?

- Must be allowed through firewall
- Cannot block port 53 (DNS)
- Most environments don't monitor DNS requests

How does DNS data exfiltration work?

- Source sends data encoded within DNS query
- DNS query sent to authoritative server (external host)
- Destination decodes and retrieves data

DETECTION/MITIGATION

1. Block connection based on IP-reputation or Geo-location
2. Block known malicious domain names on internal DNS server
3. Traffic analysis with big-data analytics



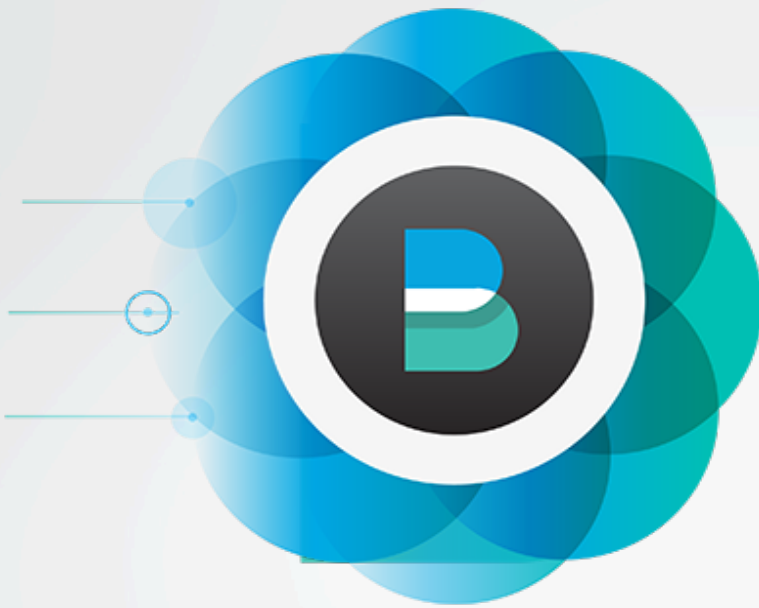
Our Exfiltration Tools

How does our tool works

- Base 64 encoding
- 200 Bytes at a time
- DNS lookup to authoritative server
- External server reassembles packets and constructs original file



Mitigation Elasticsearch + Packetbeat



beats



elastic



logstash

kibana

type:dns



client_ip: "127.0.0.1"

[Actions](#)

packetbeat*

DNS 91,405 hits

Selected Fields

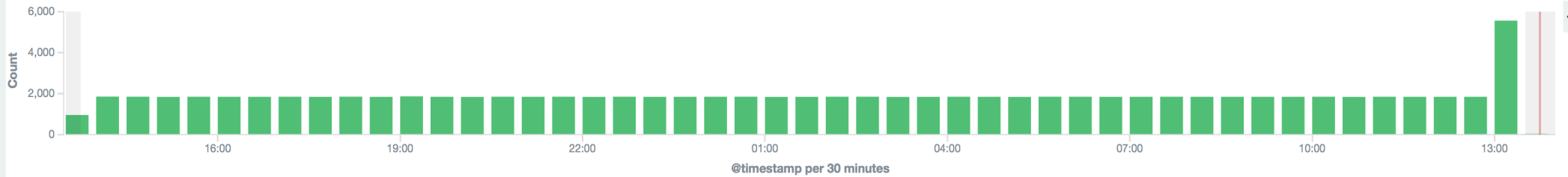
- dns.question.name
- client_ip
- method
- ip
- dns.question.type

Available Fields



Popular

- _type
- query
- server
- status
- type
- @timestamp
- _id
- _index
- _score
- beat.hostname
- beat.name
- bytes_in
- bytes_out
- client_port
- client_proc
- client_server
- count
- direction
- dns.additional
- dns.additional_count
- dns.answers
- dns.answers_count
- dns.authorities

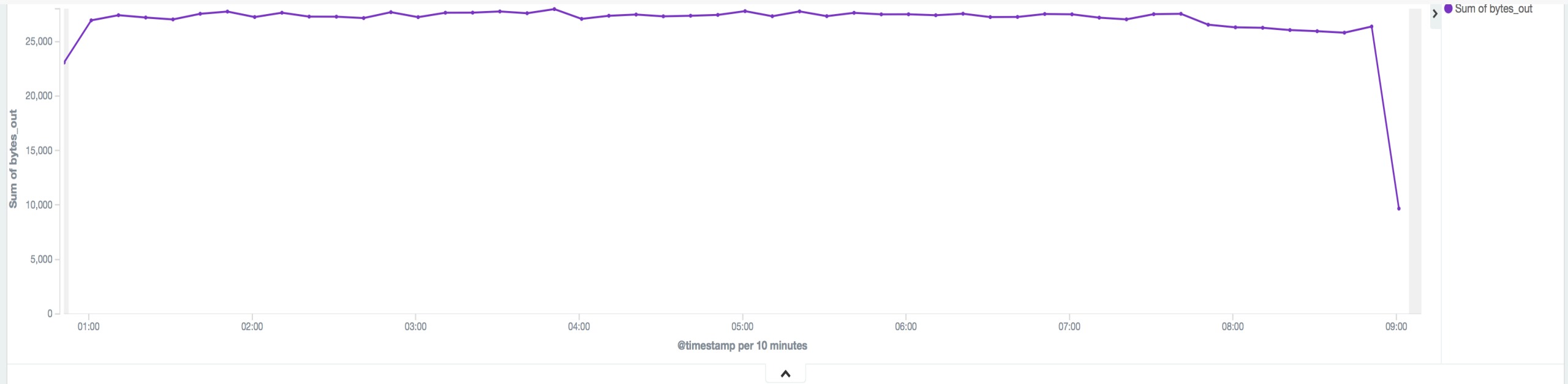


Time	client_ip	method	dns.question.type	ip	dns.question.name
▶ August 3rd 2016, 12:37:25.992	113.17.184.25	QUERY	A	23.253.76.96	1615658263.www.baidu.com
▶ August 2nd 2016, 21:31:29.815	204.42.253.2	QUERY	A	23.253.76.96	5eb40529.openresolvertest.net
▶ August 3rd 2016, 02:37:15.886	209.126.136.2	QUERY	A	23.253.76.96	www.google.com
▶ August 2nd 2016, 19:00:43.049	23.253.76.96	QUERY	A	72.3.128.241	yahoo.com
▶ August 2nd 2016, 19:00:15.415	23.253.76.96	QUERY	A	72.3.128.241	yahoo.com
▶ August 2nd 2016, 19:00:24.629	23.253.76.96	QUERY	A	72.3.128.241	yahoo.com
▶ August 2nd 2016, 19:00:31.804	23.253.76.96	QUERY	A	72.3.128.241	google.com
▶ August 2nd 2016, 19:00:35.875	23.253.76.96	QUERY	A	72.3.128.241	gmail.com
▶ August 2nd 2016, 19:00:17.450	23.253.76.96	QUERY	A	72.3.128.241	gmail.com
▶ August 2nd 2016, 19:00:08.238	23.253.76.96	QUERY	A	72.3.128.241	gmail.com
▶ August 2nd 2016, 19:00:45.085	23.253.76.96	QUERY	A	72.3.128.241	gmail.com
▶ August 2nd 2016, 19:00:14.415	23.253.76.96	QUERY	A	104.239.175.241	yahoo.com
▶ August 2nd 2016, 19:00:42.050	23.253.76.96	QUERY	A	104.239.175.241	yahoo.com
▶ August 2nd 2016, 19:00:58.697	23.253.76.96	QUERY	SRV	72.3.128.241	_monitoringagent._tcp.ord1.prod.monitoring
▶ August 2nd 2016, 19:00:58.702	23.253.76.96	QUERY	A	104.239.175.241	agent-endpoint-ord.monitoring
▶ August 2nd 2016, 19:00:56.332	23.253.76.96	QUERY	A	72.3.128.241	finance.yahoo.com
▶ August 2nd 2016, 19:01:42.401	23.253.76.96	QUERY	A	72.3.128.241	finance.yahoo.com

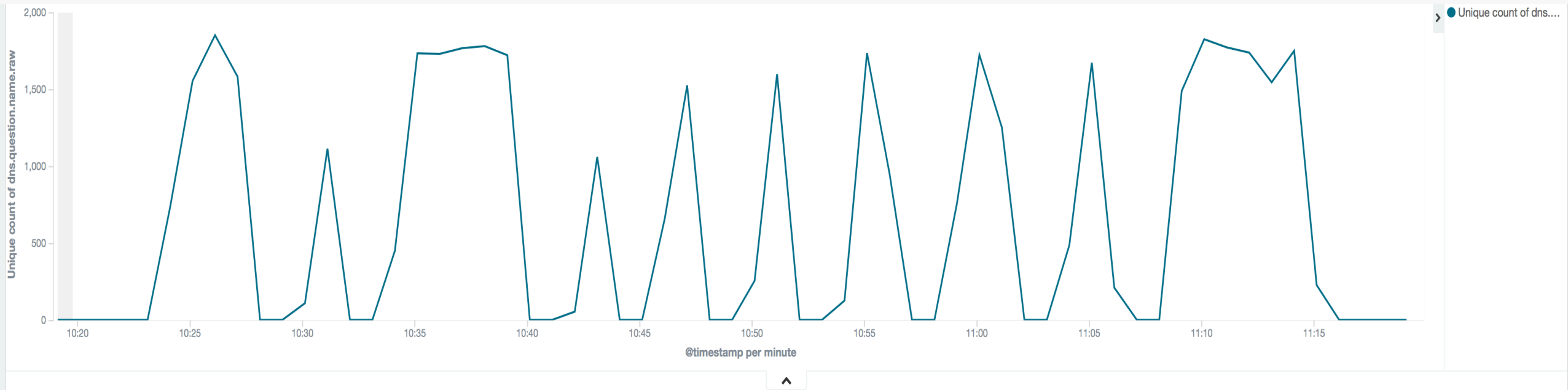
Unique FQDN by count



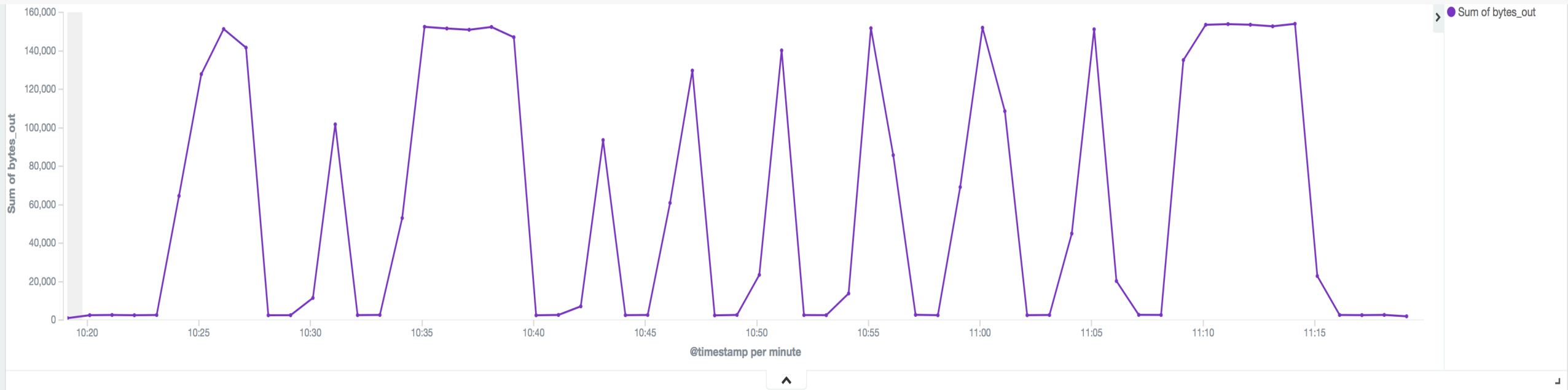
Unique FQDN in bytes

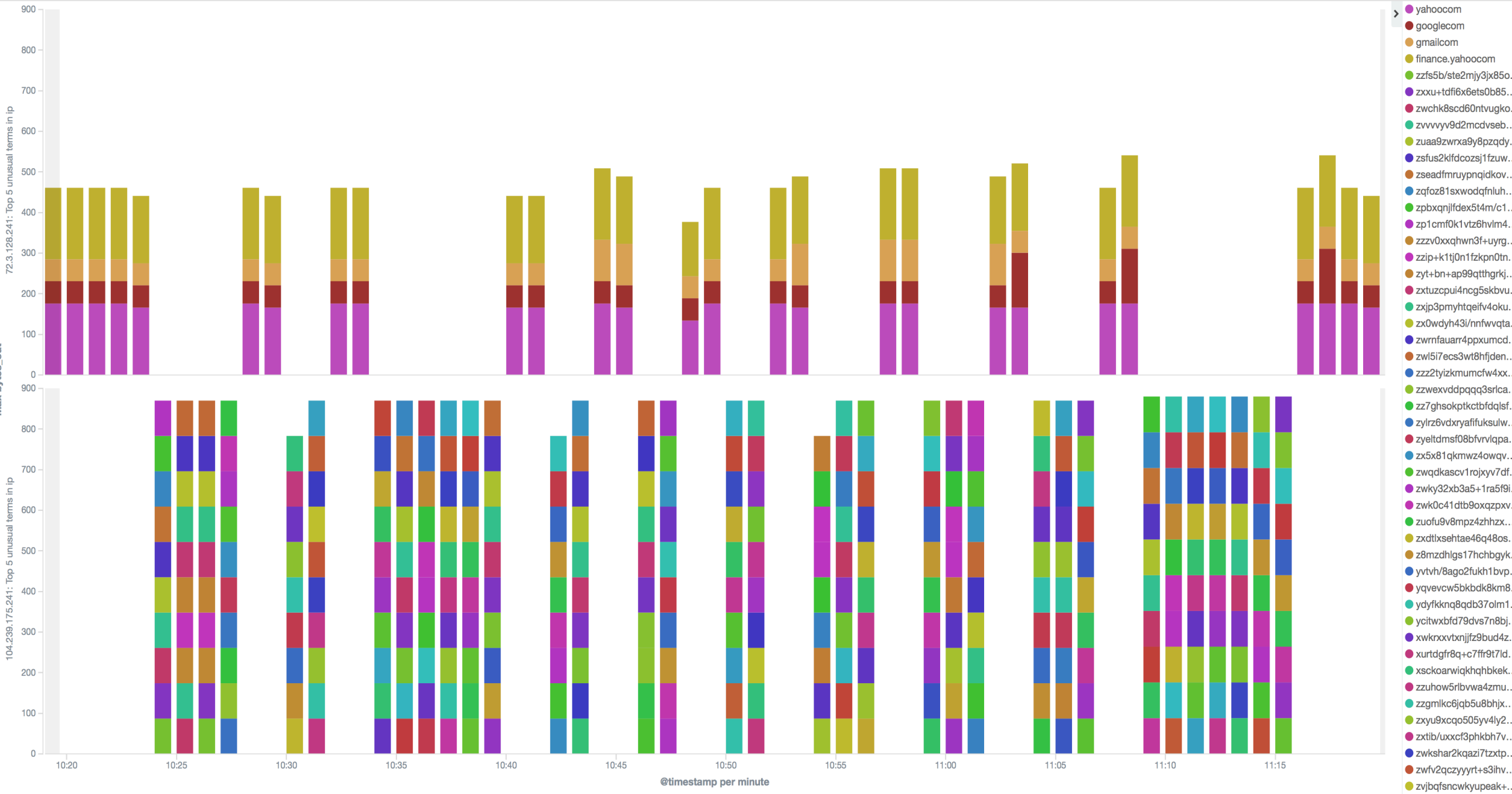


Unique FQDN by count



Unique FQDN in bytes





- yahoo.com
- google.com
- gmail.com
- finance.yahoo.com
- zzfs5b/ste2mjy3jx85o...
- zxxu+tdf6x6ets0b85...
- zwchk8scd60ntvugko...
- zvvvy9d2mcdvseb...
- zuaa9zwrxa9y8pzqdy...
- zsfus2klfdcozsj1fzuw...
- zseadfmruypnqidkov...
- zqfoz81sxwodqfnluh...
- zpbxqjifdex5t4m/c1...
- zp1cmf0k1vtz6hvim4...
- zzzv0xxqhw3f+uyrg...
- zzip+k1tj0n1fzkn0tn...
- zyt+bn+ap99qthgrkj...
- zxtuzcpu4ncg5skbv...
- zxjp3pmyhtqEIF4oku...
- zx0wdyh43i/nfwwvqta...
- zwrnfauarr4ppxumcd...
- zwl5i7ecs3wt8hfjden...
- zzz2tyizkumcfw4xx...
- zzwexvdpqq3srlica...
- zz7ghsokptkctbdfqls...
- zylrz6vdxyafikusulw...
- zyeltdmsf08bfvrvlqpa...
- zx5x81qkmwz4owqv...
- zwqdkascv1rojxy7df...
- zwky32xb3a5+1ra5f9i...
- zwk0c41dtb9oxqzpxv...
- zuofu9v8mpz4zhhzx...
- zxdtlxsehtae46q48os...
- z8mzdhlgs17hchbgyk...
- yvtvh/8ago2fukh1bvp...
- yqvevcw5bkbdk8km8...
- ydyfkknq8qd37olm1...
- ycitwxbfd79dvs7n8bj...
- xwkrxvtxnjfz9bud4z...
- xurtdgfr8q+c7ff9t7ld...
- xsckoarwiqkqhbkkek...
- zzuhow5rlbvw4zmu...
- zzgmikc6jqb5u8bhjx...
- zxyu9xcqo505yv4ly2...
- zxtib/uxxcf3phkbh7v...
- zwkshar2kqazi7tzxtp...
- zwfV2qczyyrt+s3ihv...
- zvjbfqsfncwkyupeak+...