splunk> .conf2017

Hunting the Known Unknowns

Finding Evil With SSL Traffic

Ryan Kovar | Staff Security Strategist | Splunk
Steve Brant | Senior Security Strategist | Splunk

26SEP17| Washington, DC

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

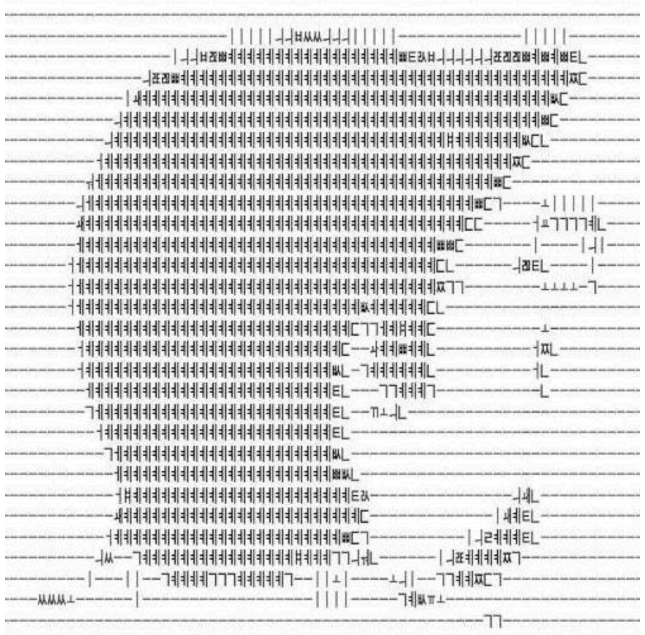
Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. I often lie. Maybe this is a lie. Wik Alsø wik Alsø alsø wik Wi nøt trei a høliday in Sweden this yër? See the løveli lakes The wøndërful telephøne system And mäni interesting furry animals The characters and incidents portrayed and the names used in this Presentation are fictitious and any similarity to the names, characters, or history of any person is entirely accidental and unintentional. Signed RICHARD M. NIXON Including the majestik møøse A Møøse once bit my Marcus… No realli! He was Karving his initials on the møøse with the sharpened end of an interspace tøøthbrush given him by Svenge – his brother-in-law – a Canadian dentist and star of many Norwegian møvies: "The Høt Hands of an Canadian Dentist", "Fillings of Passion", "The Huge Mølars of Horst Nordfink"… In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. Splunk undertakës no øbligation either to develøp the features or functionality described or to include any such feature or functionality in a future release.

whoami

Ryan Kovar: CISSP, MSc(Dist)



Staff Security Strategist

Minster of the OODAloopers

@meansec

- 17 years of cyber security experience
- Worked in US/UK Public Sector and DOD most recently in nation state hunting roles
- Enjoys clicking too fast, long walks in the woods, and data visualization
- Current role on Security Practice team focuses on incident/breach response, threat intelligence, and research
- Currently interested in automating methods to triage data collection for IR analyst review.
- Also investigating why printers are so insubordinate ಠ_ಠ

whoami

Steve Brant: CISSP

Senior Security Strategist
Minister of Truth
@trustedtech

- 23 years in the IT biz
- 8 years in Security Information and Event Management
- Novice beer snob
- Working on improving the Splunk ES out of the box experience with improved workflow and searches

I have approximate knowledge of many things.

Agenda

- Answering some **W** ’s
  - **W**hy are we doing this talk?
  - **W**hat are the known unknowns of SSL?
  - **W**hat is hunting SSL anyway?
  - **W**hat SSL data are we looking at?
  - **W**here can we get SSL wiredata from?
- Talk about the “**H**”
  - **H**ow do we can we hunt baddies in our network with SSL data?
- And now another **W**
  - **W**here can I find this info?
- Conclusion

“Hunting is creating a hypothesis about a threat or vulnerability and using the scientific method against your data to determine if the threat/vulnerability is relevant and present in your organization. Then… finding it”

- Ryan Kovar (created for this slide)

Why Did We Do This Talk?

splunk> .conf2017

SSL Hides The Threats To Your Network

Ransomware

"… Crypto-ransomware developers have switched from plaintext protocols to protected communication using TOR and SSL. "
– *Bromium **2014***

PowerShell Empire

"Using a trusted certificate and non-default Empire options will help increase your chances of getting a successful session out of a network."
*blackhillsinfosec.com, **Nov 2016***

Trickbot

"The TrickBot banking Trojan has been using legitimate SSL certificates alongside websites that closely resemble those of actual banks"
*securityweek.com, **Aug 2017***

It is everywhere

From users to malicious actors… everyone is using SSL and its only going to grow

SSL is Legitimate

This isn't something you can just "block". It is better security! For your users… and your attackers

SSL Decryption.. Works-ish?

One solution is to "MITM" SSL. This works for legitimate uses of SSL but some locations frown at MiTM. Also Adversaries KNOW you aren't looking at banking or health

SSL Hides The Threats To Your Network

Ransomware

"… Crypto-ransomware developers have switched from plaintext protocols to protected communication using TOR and SSL. "
– *Bromium **2014***

PowerShell Empire

"Using a trusted certificate and non-default Empire options will help increase your chances of getting a successful session out of a network."
*blackhillsinfosec.com, **Nov 2016***

Trickbot

"The TrickBot banking Trojan has been using legitimate SSL certificates alongside websites that closely resemble those of actual banks –
*securityweek.com, **Aug 2017***

It is everywhere

From users to malicious actors… everyone is using SSL and its only going to grow

SSL is Legitimate

This isn't something you can just "block". It is better security! For your users… and your attackers

SSL Decryption.. Works-ish?

One solution is to "MITM" SSL. This works for legitimate uses of SSL but some locations frown at MiTM. Also Adversaries KNOW you aren't looking at banking or health

SSL hides the threats to your network

Ransomware

"… crypto-ransomware developers have switched from plaintext protocols to protected communication using TOR and SSL. "
– *Bromium **2014***

PowerShell Empire

"Using a trusted certificate and non-default Empire options will help increase your chances of getting a successful session out of a network."
*blackhillsinfosec.com, **Nov 2016***

Trickbot

"The TrickBot banking Trojan has been using legitimate SSL certificates alongside websites that closely resemble those of actual banks –
*securityweek.com, **Aug 2017***

It is everywhere

From users to malicious actors… everyone is using SSL and its only going to grow

SSL is Legitimate

This isn't something you can just "block". It is better security! For your users… and your attackers

SSL Decryption.. Works-ish?

One solution is to "MITM" SSL. This works for legitimate uses of SSL but some locations frown at MiTM. Also Adversaries KNOW you aren't looking at banking or health

SSL hides the threats to your network

Ransomware

"… crypto-ransomware developers have switched from plaintext protocols to protected communication using TOR and SSL. "
– *Bromium **2014***

PowerShell Empire

"Using a trusted certificate and non-default Empire options will help increase your chances of getting a successful session out of a network."
*blackhillsinfosec.com, **Nov 2016***

Trickbot

"The TrickBot banking Trojan has been using legitimate SSL certificates alongside websites that closely resemble those of actual banks"
*securityweek.com, **Aug 2017***

It is everywhere

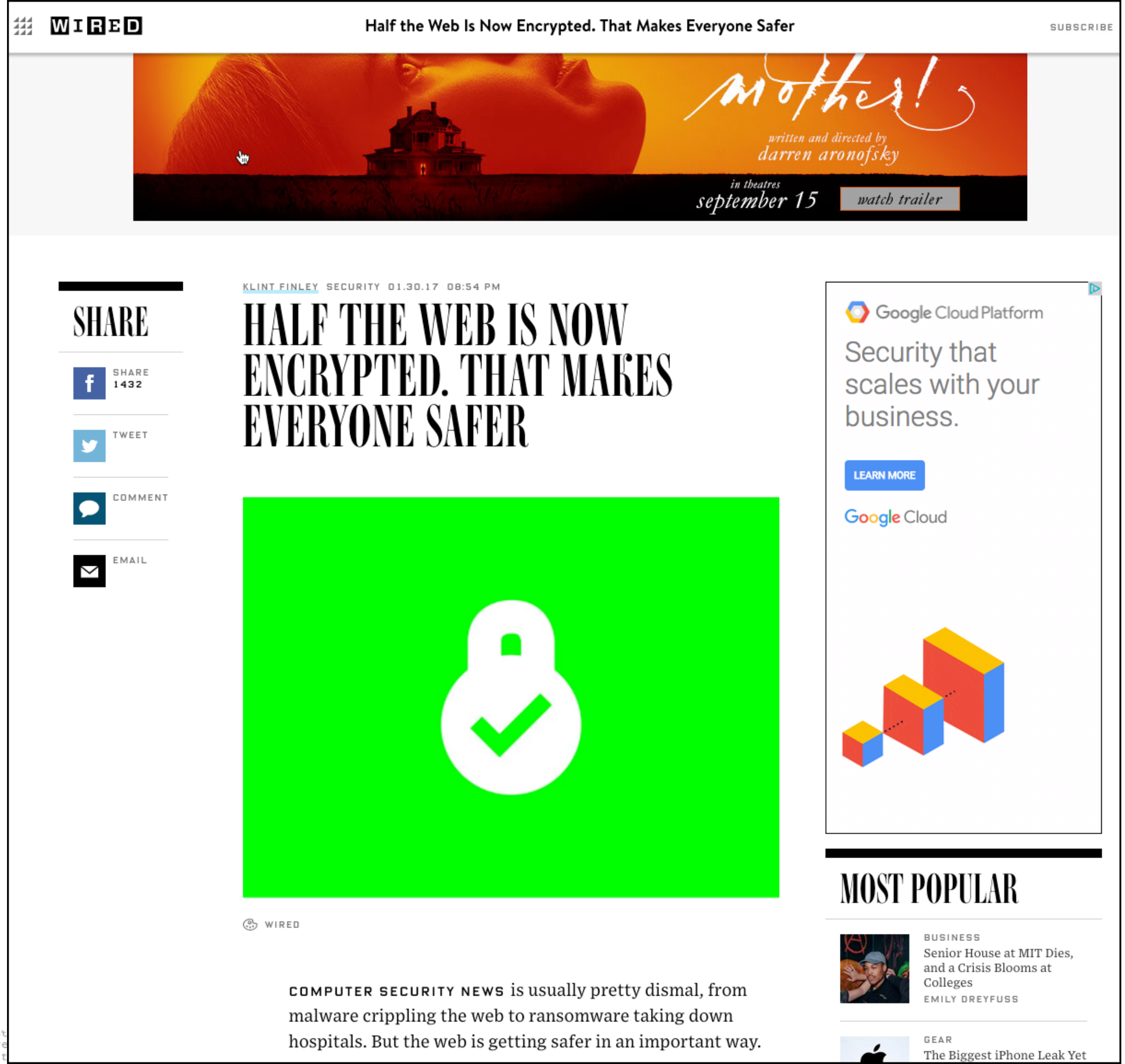
From users to malicious actors… everyone is using SSL and its only going to grow

SSL is Legitimate

This isn't something you can just "block". It is better security! For your users… and your attackers

SSL Decryption.. Works-ish?

One solution is to "MITM" SSL. This works for legitimate uses of SSL but some locations frown at MiTM. Also Adversaries KNOW you aren't looking at banking or health



Half the Web Is Now Encrypted. That Makes Everyone Safer

KLINT FINLEY SECURITY 01.30.17 08:54 PM

HALF THE WEB IS NOW ENCRYPTED. THAT MAKES EVERYONE SAFER

WIRED

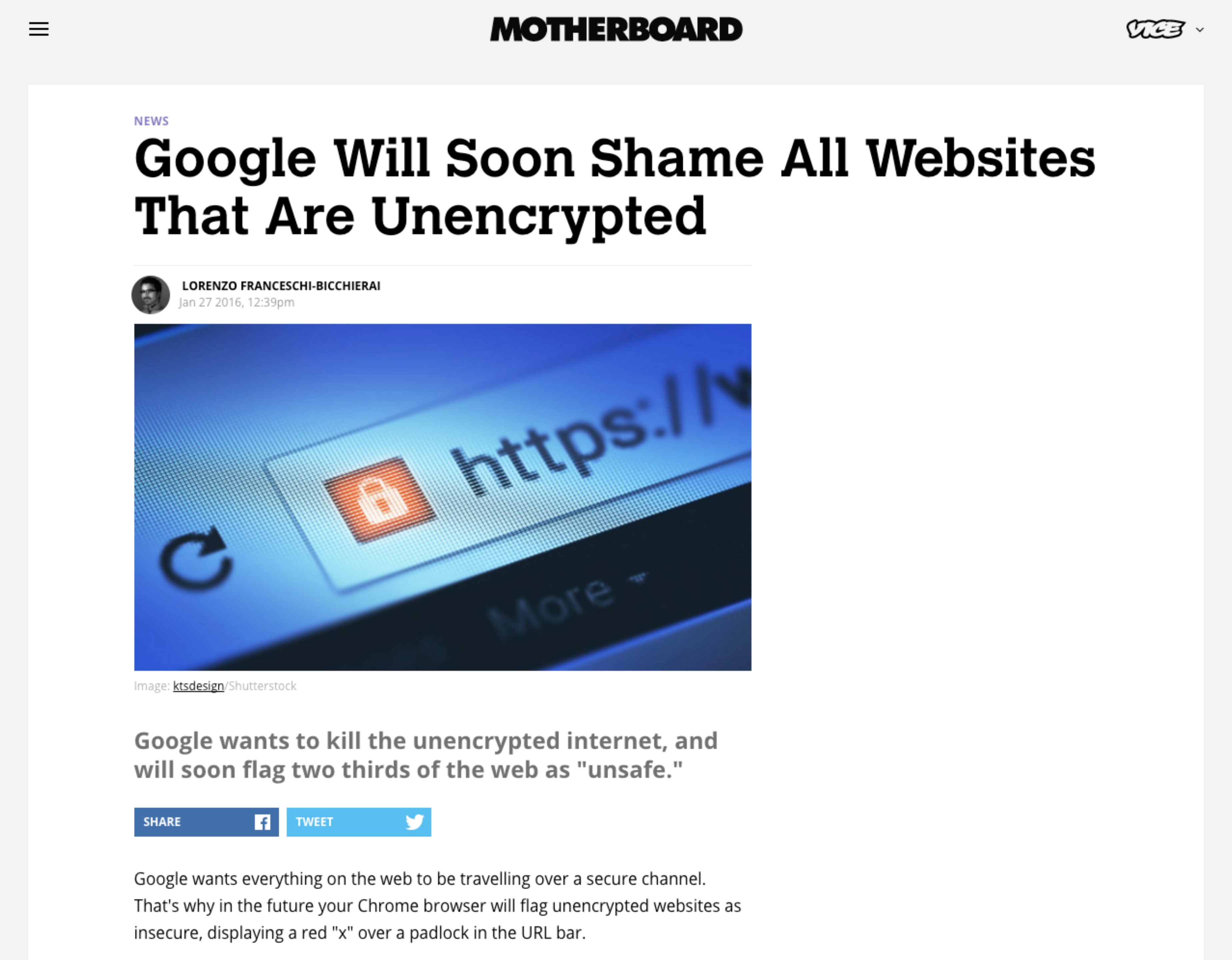
COMPUTER SECURITY NEWS is usually pretty dismal, from malware crippling the web to ransomware taking down hospitals. But the web is getting safer in an important way.

MOST POPULAR

BUSINESS
Senior House at MIT Dies, and a Crisis Blooms at Colleges
EMILY DREYFUSS

GEAR
The Biggest iPhone Leak Yet

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?cat
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.scre
" 317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?it
ows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.100
kitemId=EST-16&product_id=RP-LI-02" "O
://buttercup-shopping.com/old
do?action=purchase&it
opping.com/car
//butter
```



NEWS

Google Will Soon Shame All Websites That Are Unencrypted

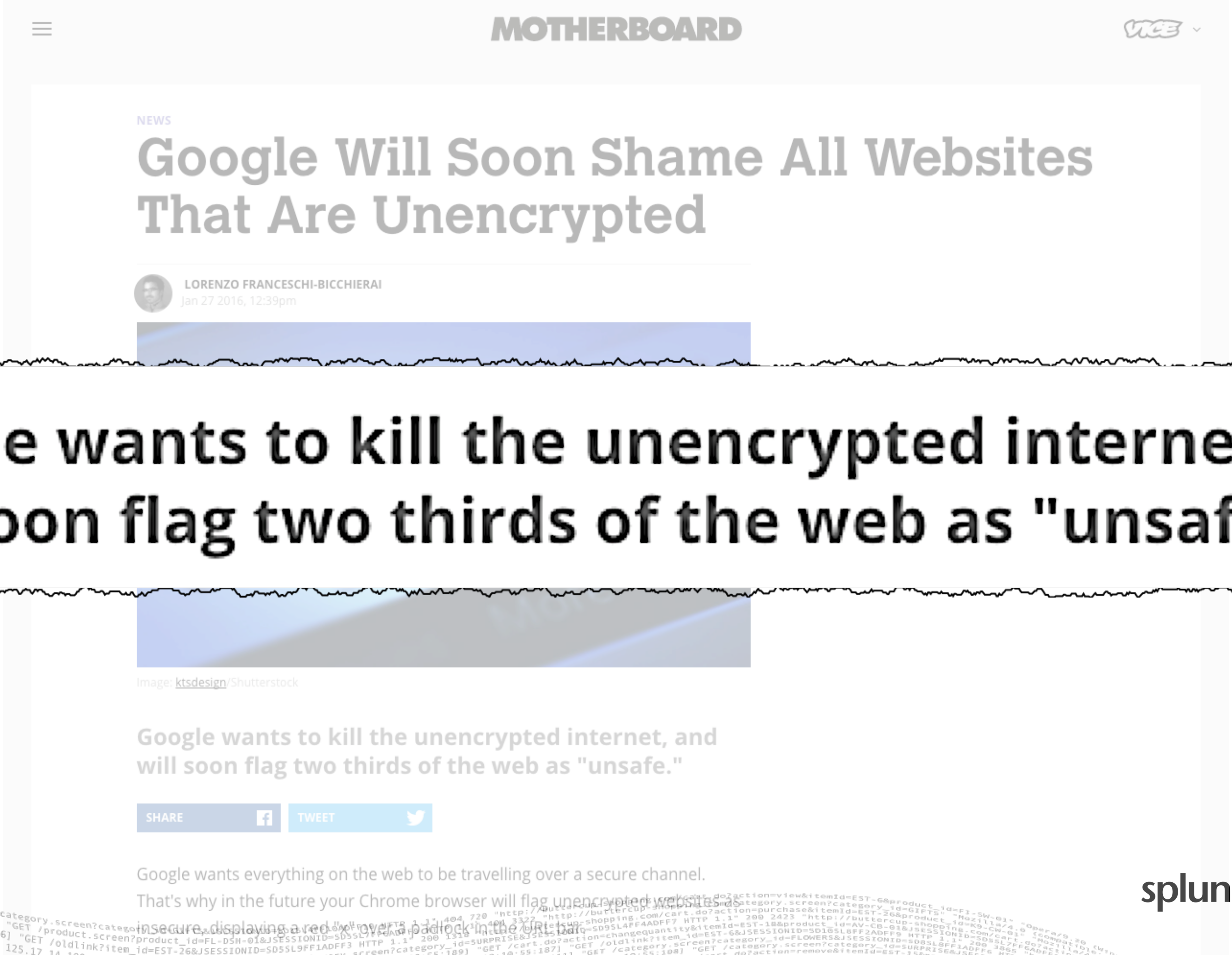
LORENZO FRANCESCHI-BICCHIERAI
Jan 27 2016, 12:39pm

Image: ktsdesign/Shutterstock

Google wants to kill the unencrypted internet, and will soon flag two thirds of the web as "unsafe."

Google wants everything on the web to be travelling over a secure channel. That's why in the future your Chrome browser will flag unencrypted websites as insecure, displaying a red "x" over a padlock in the URL bar.

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /c
128.241.220.82 - - [07/Jan 18:10:57:123]
" 317 27.160.0.0 - - [07/Jan 18:10:56:15
ows NT 5.1; SV1; .NET CLR 1.1.4322)" 468
itemId=EST-16&product_id=RP-LI-02" "O-
://buttercup-shopping.com/old
do?action=purchase&it
opping.com/car
//butter
```



NEWS

Google Will Soon Shame All Websites That Are Unencrypted

LORENZO FRANCESCHI-BICCHIERAI
Jan 27 2016, 12:39pm

Google wants to kill the unencrypted internet, and will soon flag two thirds of the web as "unsafe."

Image: ktsdesign/Shutterstock

Google wants to kill the unencrypted internet, and will soon flag two thirds of the web as "unsafe."

Google wants everything on the web to be travelling over a secure channel. That's why in the future your Chrome browser will flag unencrypted websites as insecure, displaying a red "x" over a padlock in the URL bar.

What Is Hunting Anyway?

splunk> .conf2017

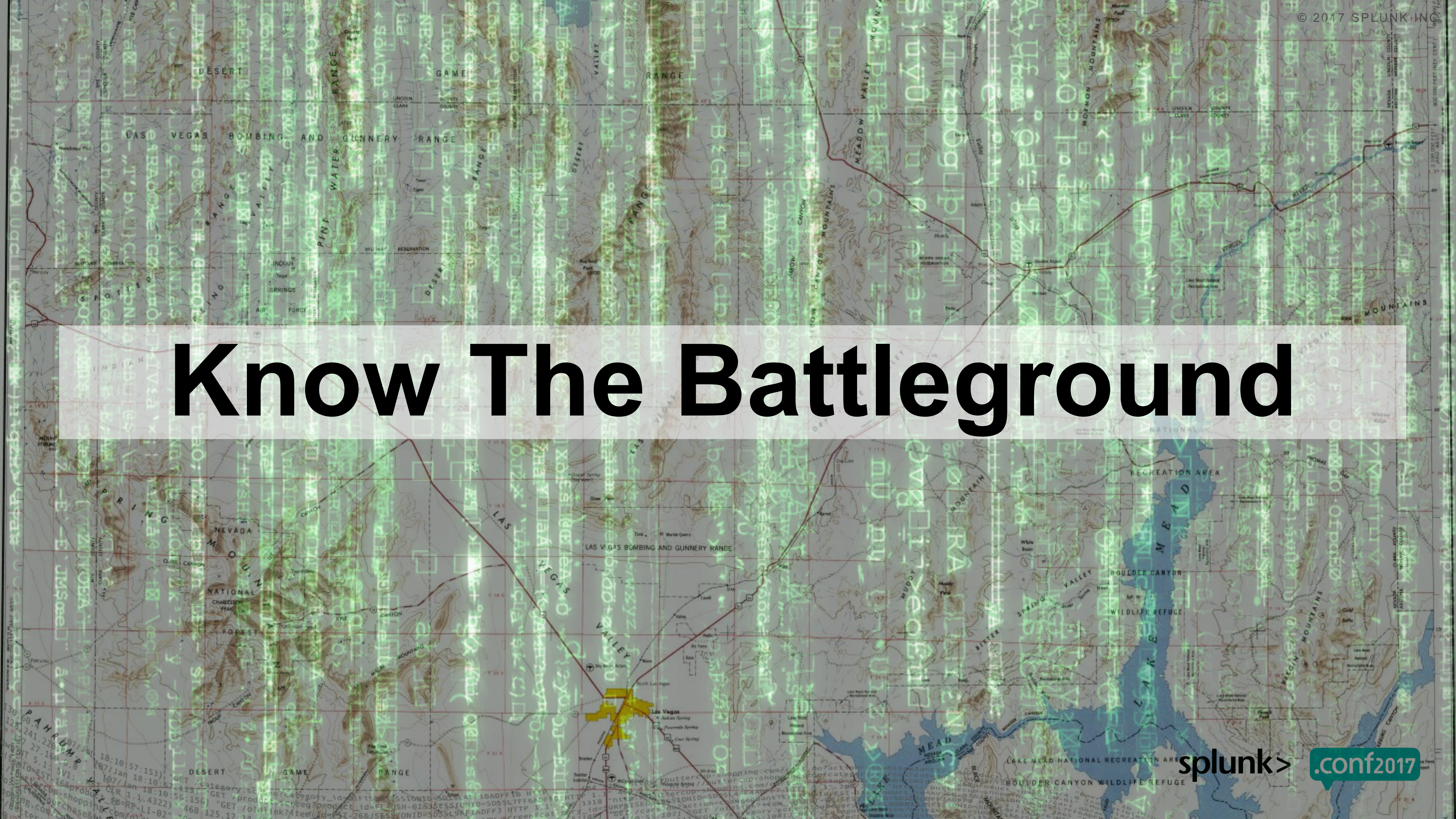
If You Are Hunting Wooly Mammoth…

...Don't Bring A 22 Caliber Bullet

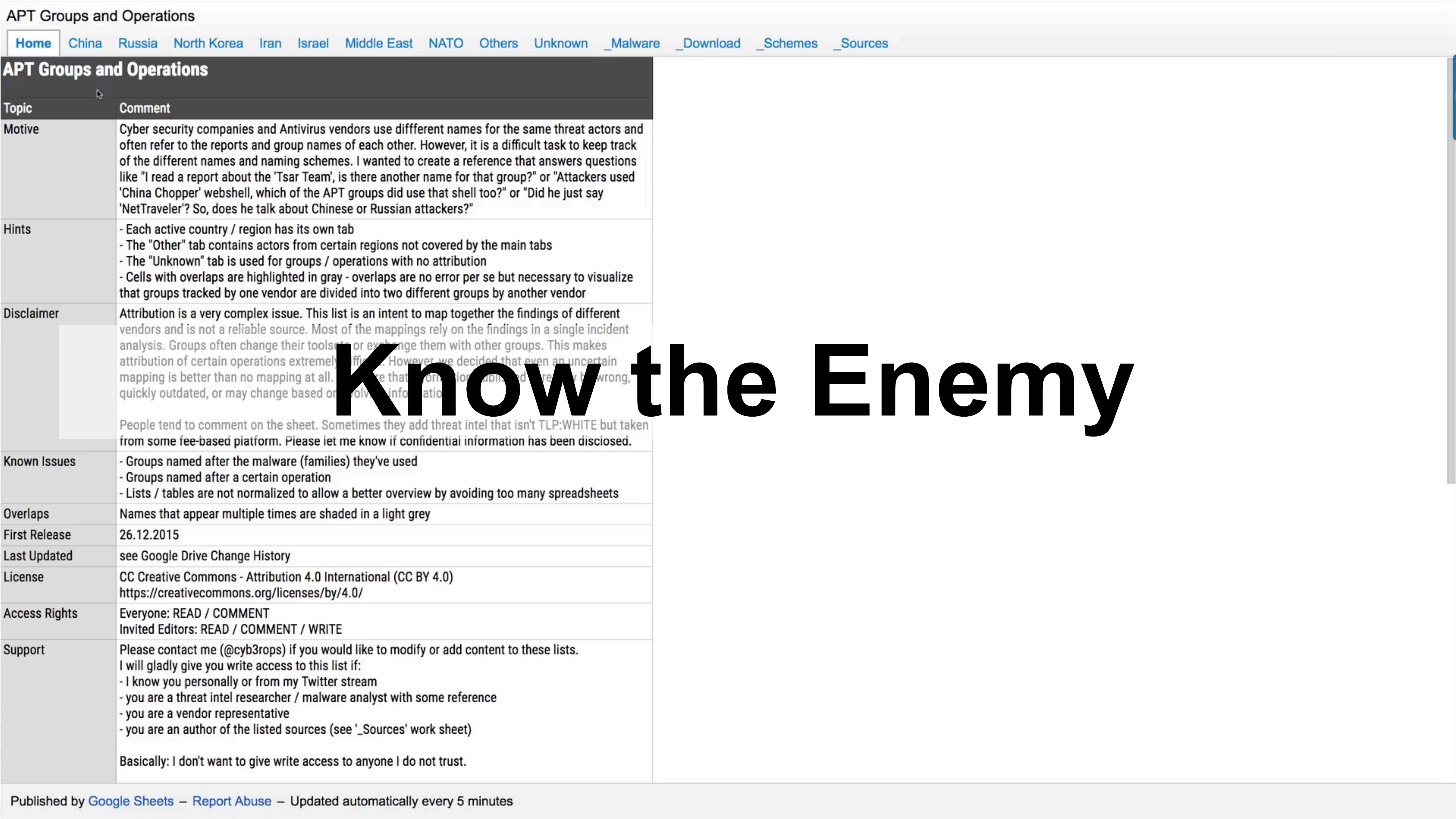
You Don’t Bring A Boat...

…When You Are Hunting Fancy Bears

Know The Battleground


LAS VEGAS BOMBING AND GUNNERY RANGE
DESERT GAME RANGE
SPRING MOUNTAINS
LAS VEGAS VALLEY
LAKE MEAD
LAKE MEAD NATIONAL RECREATION AREA
BOULDER CANYON WILDLIFE REFUGE
Las Vegas
NEVADA
NATIONAL FOREST

Know the Enemy



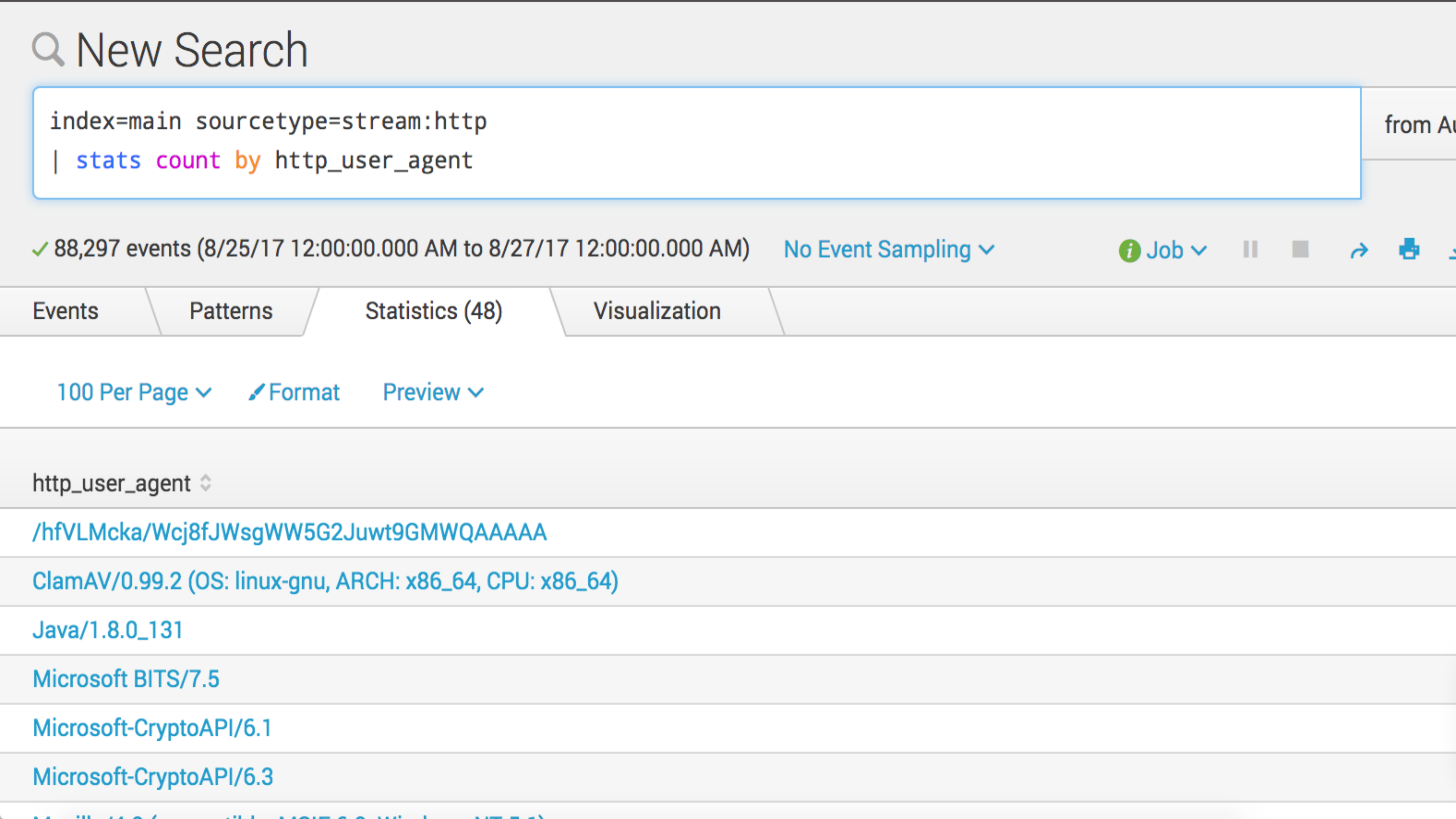
APT Groups and Operations

Topic	Comment
Motive	Cyber security companies and Antivirus vendors use diffferent names for the same threat actors and often refer to the reports and group names of each other. However, it is a difficult task to keep track of the different names and naming schemes. I wanted to create a reference that answers questions like "I read a report about the 'Tsar Team', is there another name for that group?" or "Attackers used 'China Chopper' webshell, which of the APT groups did use that shell too?" or "Did he just say 'NetTraveler'? So, does he talk about Chinese or Russian attackers?"
Hints	- Each active country / region has its own tab - The "Other" tab contains actors from certain regions not covered by the main tabs - The "Unknown" tab is used for groups / operations with no attribution - Cells with overlaps are highlighted in gray - overlaps are no error per se but necessary to visualize that groups tracked by one vendor are divided into two different groups by another vendor
Disclaimer	Attribution is a very complex issue. This list is an intent to map together the findings of different vendors and is not a reliable source. Most of the mappings rely on the findings in a single incident analysis. Groups often change their toolsets or exchange them with other groups. This makes attribution of certain operations extremely difficult. However, we decided that even an uncertain mapping is better than no mapping at all. Be aware that information published here may be wrong, quickly outdated, or may change based on evolving information. People tend to comment on the sheet. Sometimes they add threat intel that isn't TLP:WHITE but taken from some fee-based platform. Please let me know if confidential information has been disclosed.
Known Issues	- Groups named after the malware (families) they've used - Groups named after a certain operation - Lists / tables are not normalized to allow a better overview by avoiding too many spreadsheets
Overlaps	Names that appear multiple times are shaded in a light grey
First Release	26.12.2015
Last Updated	see Google Drive Change History
License	CC Creative Commons - Attribution 4.0 International (CC BY 4.0) https://creativecommons.org/licenses/by/4.0/
Access Rights	Everyone: READ / COMMENT Invited Editors: READ / COMMENT / WRITE
Support	Please contact me (@cyb3rops) if you would like to modify or add content to these lists. I will gladly give you write access to this list if: - I know you personally or from my Twitter stream - you are a threat intel researcher / malware analyst with some reference - you are a vendor representative - you are an author of the listed sources (see '_Sources' work sheet) Basically: I don't want to give write access to anyone I do not trust.

Published by Google Sheets – Report Abuse – Updated automatically every 5 minutes

What are the known unknowns of SSL?

Hunting with HTTP ☺

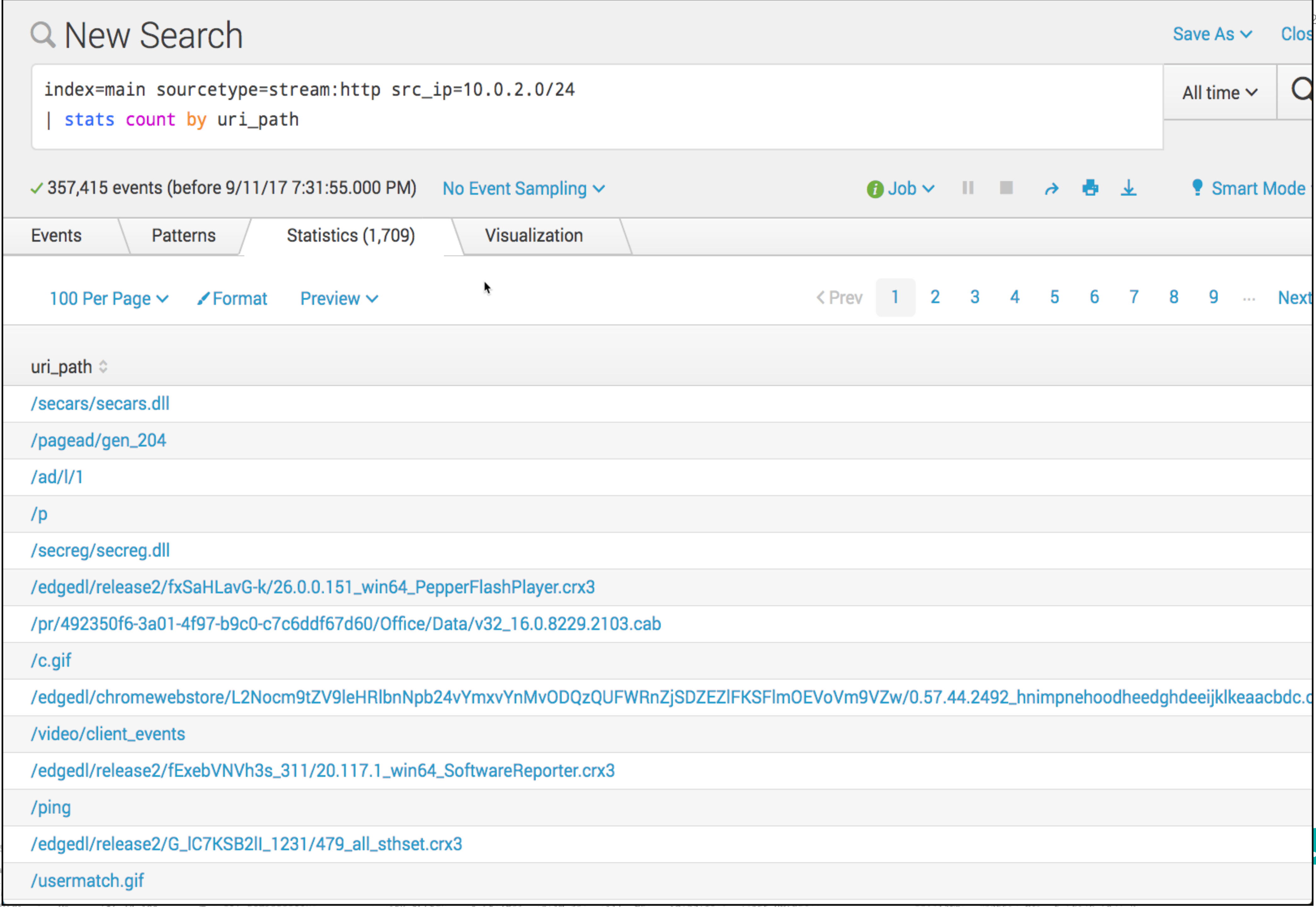


New Search

```
index=main sourcetype=stream:http
| stats count by http_user_agent
```

✓ 88,297 events (8/25/17 12:00:00.000 AM to 8/27/17 12:00:00.000 AM)

http_user_agent
/hfVLMcka/Wcj8fJWsgWW5G2Juwt9GMWQAAAAA
ClamAV/0.99.2 (OS: linux-gnu, ARCH: x86_64, CPU: x86_64)
Java/1.8.0_131
Microsoft BITS/7.5
Microsoft-CryptoAPI/6.1
Microsoft-CryptoAPI/6.3
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

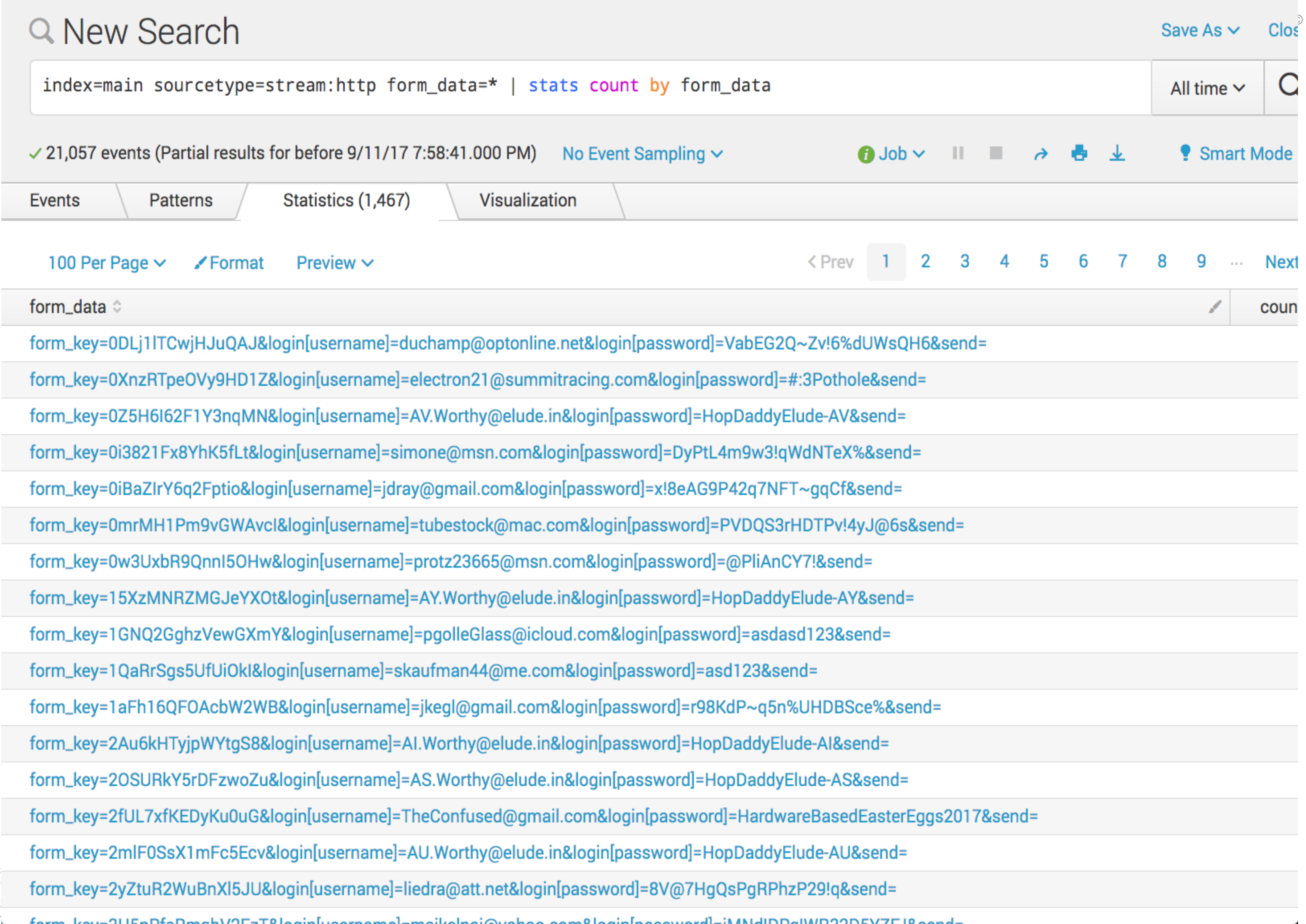


```
index=main sourcetype=stream:http src_ip=10.0.2.0/24
| stats count by uri_path
```

✓ 357,415 events (before 9/11/17 7:31:55.000 PM)

uri_path
/secars/secars.dll
/pagead/gen_204
/ad/l/1
/p
/secreg/secreg.dll
/edgedl/release2/fxSaHLavG-k/26.0.0.151_win64_PepperFlashPlayer.crx3
/pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/v32_16.0.8229.2103.cab
/c.gif
/edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnMvODQzQUFWRnZjSDZEZlFKSFlmOEVoVm9VZw/0.57.44.2492_hnimpnehoodheedghdeeijklkeaacbdc.c
/video/client_events
/edgedl/release2/fExebVNVh3s_311/20.117.1_win64_SoftwareReporter.crx3
/ping
/edgedl/release2/G_lC7KSB2lI_1231/479_all_sthset.crx3
/usermatch.gif

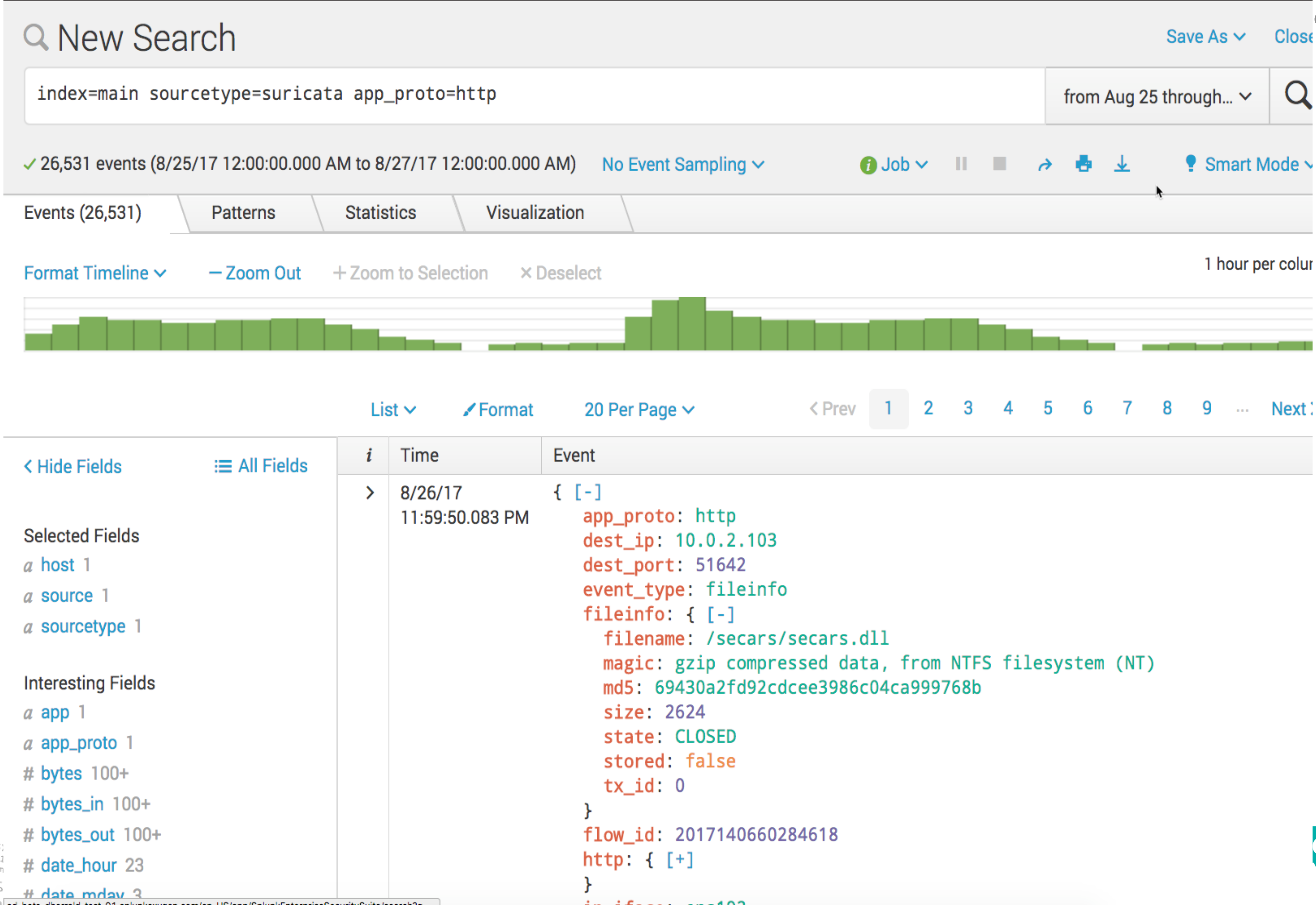
.conf2017



```
index=main sourcetype=stream:http form_data=* | stats count by form_data
```

✓ 21,057 events (Partial results for before 9/11/17 7:58:41.000 PM) No Event Sampling

form_data	coun
form_key=0DLj1lTCwjHJuQAJ&login[username]=duchamp@optonline.net&login[password]=VabEG2Q~Zv!6%dUWsQH6&send=	
form_key=0XnzRTpeOVy9HD1Z&login[username]=electron21@summitracing.com&login[password]=#:3Pothole&send=	
form_key=0Z5H6I62F1Y3nqMN&login[username]=AV.Worthy@elude.in&login[password]=HopDaddyElude-AV&send=	
form_key=0i3821Fx8YhK5fLt&login[username]=simone@msn.com&login[password]=DyPtL4m9w3!qWdNTeX%&send=	
form_key=0iBaZIrY6q2Fptio&login[username]=jdray@gmail.com&login[password]=x!8eAG9P42q7NFT~gqCf&send=	
form_key=0mrMH1Pm9vGWAvcI&login[username]=tubestock@mac.com&login[password]=PVDQS3rHDTPv!4yJ@6s&send=	
form_key=0w3UxbR9QnnI5OHw&login[username]=protz23665@msn.com&login[password]=@PliAnCY7!&send=	
form_key=15XzMNRZMGJeYXOt&login[username]=AY.Worthy@elude.in&login[password]=HopDaddyElude-AY&send=	
form_key=1GNQ2GghzVewGXmY&login[username]=pgolleGlass@icloud.com&login[password]=asdasd123&send=	
form_key=1QaRrSgs5UfUiOkI&login[username]=skaufman44@me.com&login[password]=asd123&send=	
form_key=1aFh16QFOAcbW2WB&login[username]=jkegl@gmail.com&login[password]=r98KdP~q5n%UHDBSce%&send=	
form_key=2Au6kHTyjpWYtgS8&login[username]=AI.Worthy@elude.in&login[password]=HopDaddyElude-AI&send=	
form_key=2OSURkY5rDFzwoZu&login[username]=AS.Worthy@elude.in&login[password]=HopDaddyElude-AS&send=	
form_key=2fUL7xfKEDyKu0uG&login[username]=TheConfused@gmail.com&login[password]=HardwareBasedEasterEggs2017&send=	
form_key=2mlF0SsX1mFc5Ecv&login[username]=AU.Worthy@elude.in&login[password]=HopDaddyElude-AU&send=	
form_key=2yZtuR2WuBnXl5JU&login[username]=liedra@att.net&login[password]=8V@7HgQsPgRPhzP29!q&send=	



```
index=main sourcetype=suricata app_proto=http
```

✓ 26,531 events (8/25/17 12:00:00.000 AM to 8/27/17 12:00:00.000 AM)

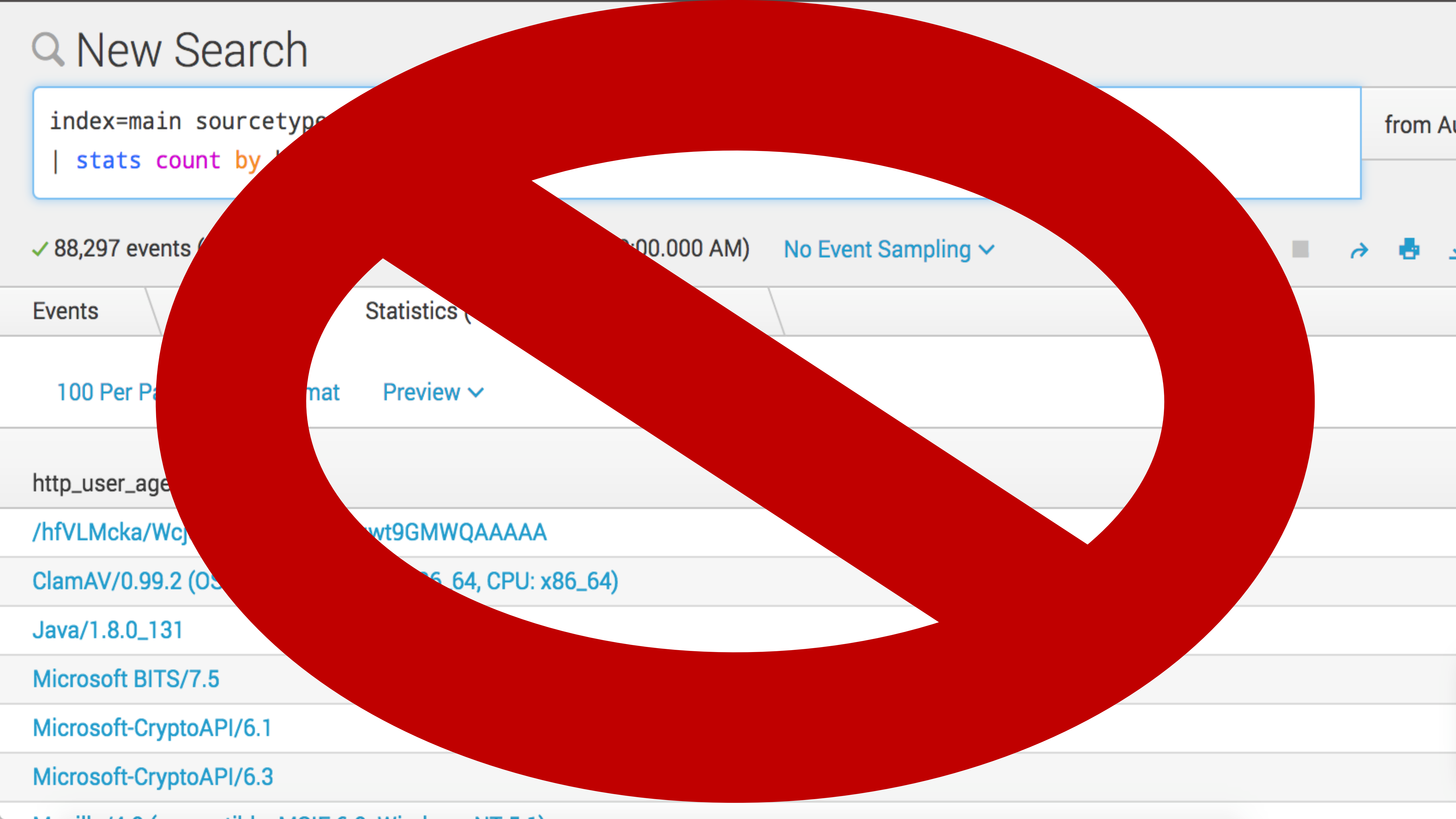
Selected Fields
- a host 1
- a source 1
- a sourcetype 1

Interesting Fields
- a app 1
- a app_proto 1
- # bytes 100+
- # bytes_in 100+
- # bytes_out 100+
- # date_hour 23
- # date_mday 3

> 8/26/17 11:59:50.083 PM

```
{ [-]
   app_proto: http
   dest_ip: 10.0.2.103
   dest_port: 51642
   event_type: fileinfo
   fileinfo: { [-]
     filename: /secars/secars.dll
     magic: gzip compressed data, from NTFS filesystem (NT)
     md5: 69430a2fd92cdcee3986c04ca999768b
     size: 2624
     state: CLOSED
     stored: false
     tx_id: 0
   }
   flow_id: 2017140660284618
   http: { [+]
   }
```

Hunting with SSL ☹



```
index=main sourcetyp
| stats count by
```

http_user_age

/hfVLMcka/Wcj wt9GMWQAAAAA

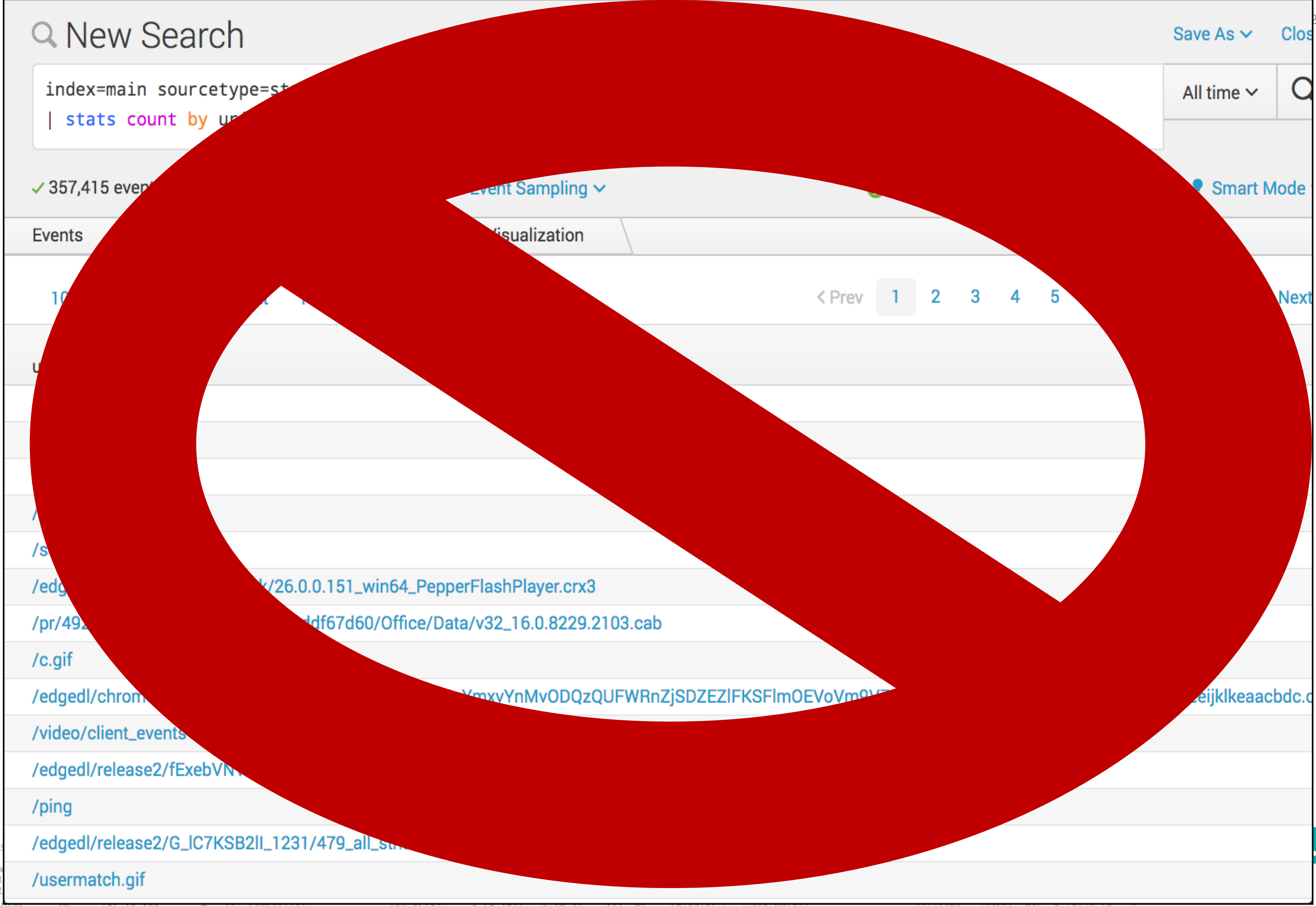
ClamAV/0.99.2 (OS 6_64, CPU: x86_64)

Java/1.8.0_131

Microsoft BITS/7.5

Microsoft-CryptoAPI/6.1

Microsoft-CryptoAPI/6.3



New Search

```
index=main sourcetype=st
| stats count by ur
```

✓ 357,415 even

/

/s

/edg k/26.0.0.151_win64_PepperFlashPlayer.crx3

/pr/492 ldf67d60/Office/Data/v32_16.0.8229.2103.cab

/c.gif

/edgedl/chrom YmxyYnMvODQzQUFWRnZjSDZEZlFKSFlmOEVoVm9V eijklkeaacbdc.c

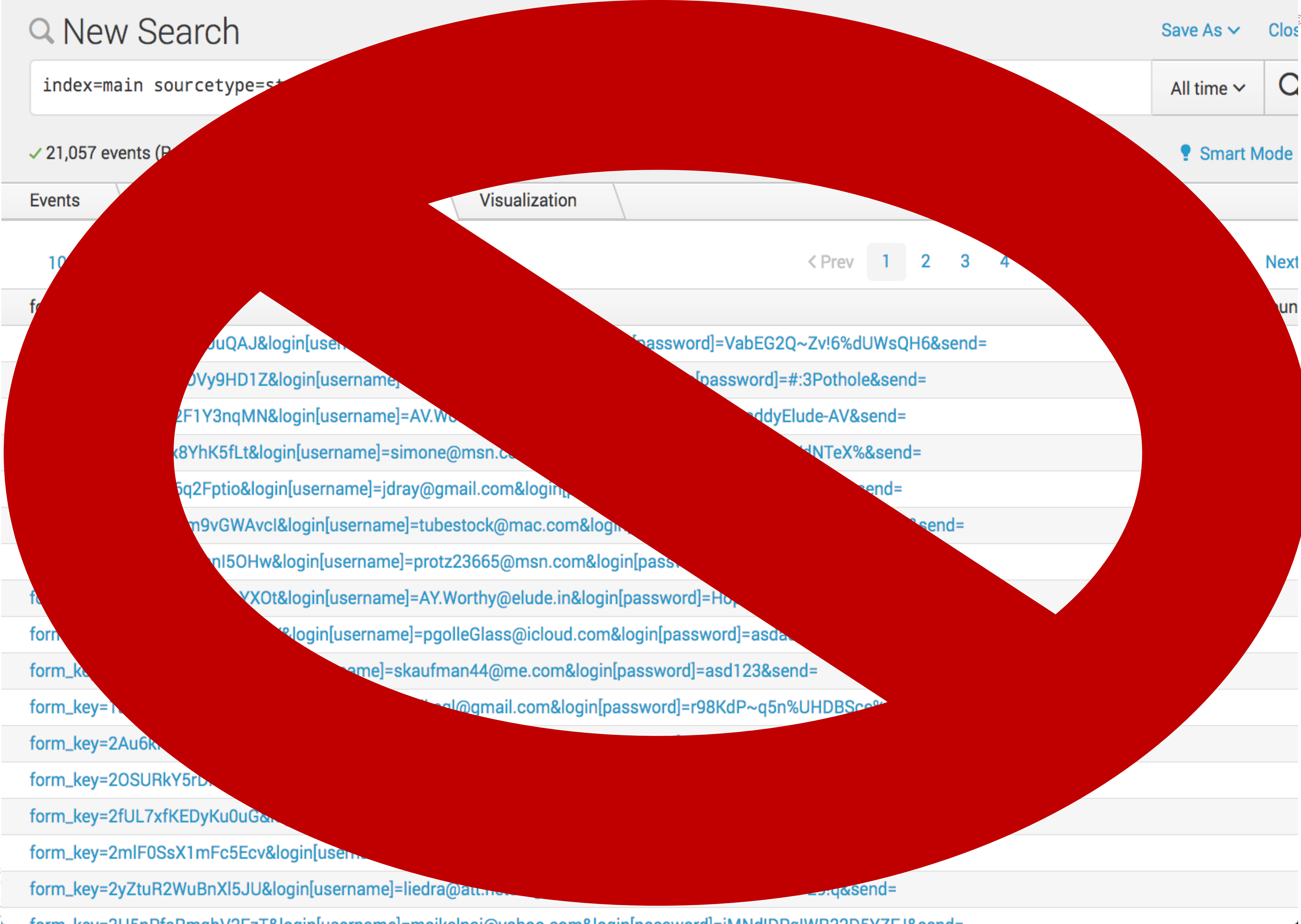
/video/client_events

/edgedl/release2/fExebVN

/ping

/edgedl/release2/G_lC7KSB2lI_1231/479_all_st

/usermatch.gif

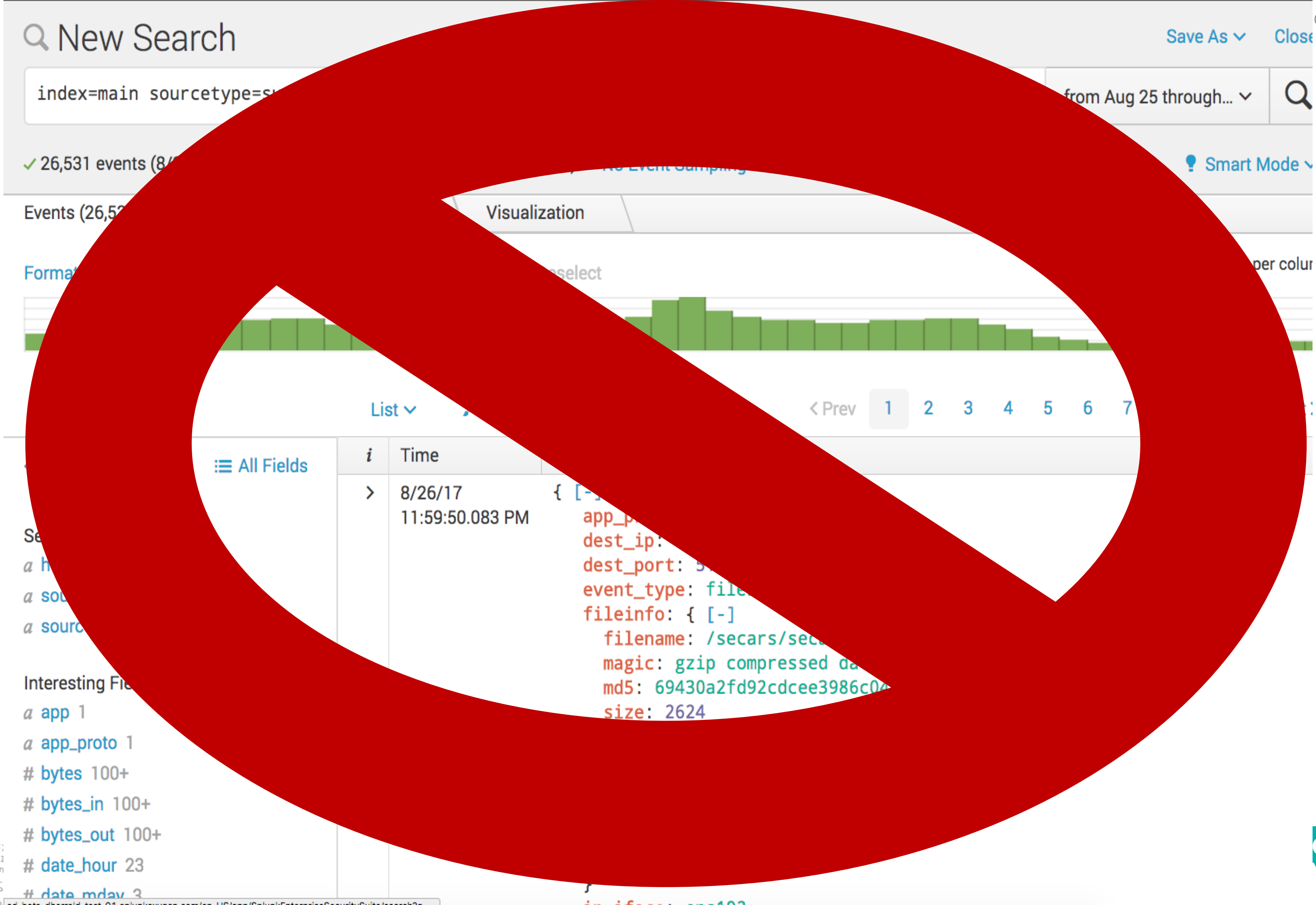


```
index=main sourcetype=s
```

✓ 21,057 events (R

```
uQAJ&login[use                    [password]=VabEG2Q~Zv!6%dUWsQH6&send=
DVy9HD1Z&login[username]                    [password]=#:3Pothole&send=
2F1Y3nqMN&login[username]=AV.W                    ddyElude-AV&send=
k8YhK5fLt&login[username]=simone@msn.c                    dNTeX%&send=
6q2Fptio&login[username]=jdray@gmail.com&login[                    end=
m9vGWAvcI&login[username]=tubestock@mac.com&logi                    send=
nI5OHw&login[username]=protz23665@msn.com&login[pass
f      YXOt&login[username]=AY.Worthy@elude.in&login[password]=Ho
forr      &login[username]=pgolleGlass@icloud.com&login[password]=asda
form_ke      ame]=skaufman44@me.com&login[password]=asd123&send=
form_key=1      gl@gmail.com&login[password]=r98KdP~q5n%UHDBSc
form_key=2Au6k
form_key=2OSURkY5rD
form_key=2fUL7xfKEDyKu0uG&
form_key=2mlF0SsX1mFc5Ecv&login[use
form_key=2yZtuR2WuBnXl5JU&login[username]=liedra@att.n      .q&send=
form_key=2U5nRfeRmghV2FzT&login[username]=maikelnai@yahoo.com&login[password]=iMNdIDRqlWR22D5YZFJ&send=
```

.conf2017



index=main sourcetype=s

✓ 26,531 events (8/

No Event Sampling

Events (26,5

8/26/17 11:59:50.083 PM

```
{ [-]
   app_p
   dest_ip:
   dest_port: 5
   event_type: file
   fileinfo: { [-]
     filename: /secars/sec
     magic: gzip compressed da
     md5: 69430a2fd92cdcee3986c04
     size: 2624
   }
   in_iface: ens192
```

Se
- a h
- a sou
- a sourc

Interesting Fi
- a app 1
- a app_proto 1
- # bytes 100+
- # bytes_in 100+
- # bytes_out 100+
- # date_hour 23
- # date_mday 3

conf2017

Reducing the view

Can simplify and bring the unknown to the surface

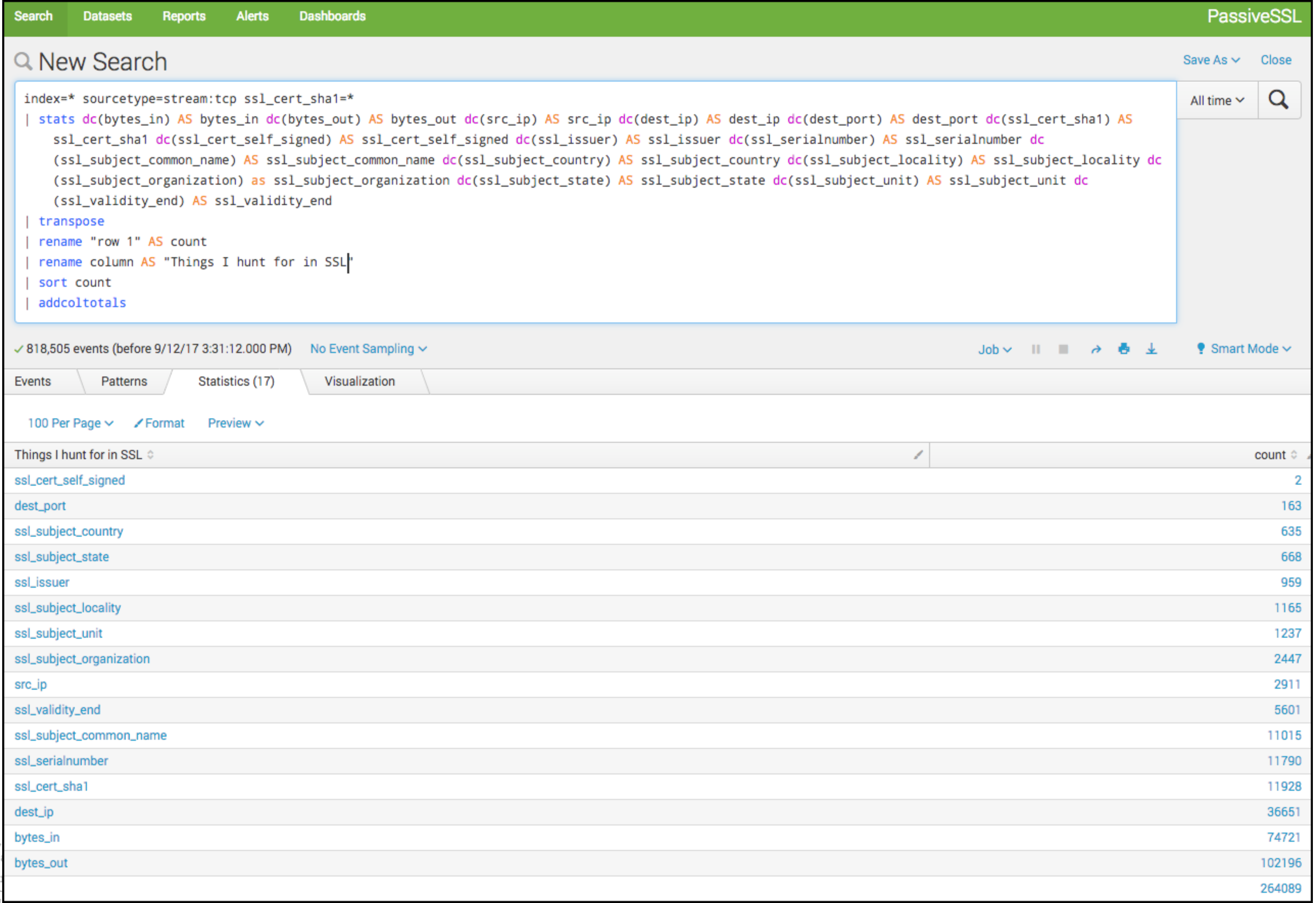
.conf2017

Huh? Less is more?

HTTP fields of interest	SSL fields of interest
http_method	ssl_cert_self_signed
http_comment	dest_port
dest_port	ssl_subject_country
http_content_type	ssl_subject_state
src_ip	ssl_issuer
bytes_in	ssl_subject_locality
site	ssl_subject_unit
http_referrer	ssl_subject_organization
http_user_agent	src_ip
dest_ip	ssl_validity_end
http_content_length	ssl_subject_common_name
bytes_out	ssl_serialnumber
uri	ssl_cert_sha1
request	dest_ip
dest_headers	bytes_in
uri_path	bytes_out
src_headers	
uri_query	
form_data	

"I can **eyeball** the results when there are only a few hundred results"

Ben "Bubbles" Withnell



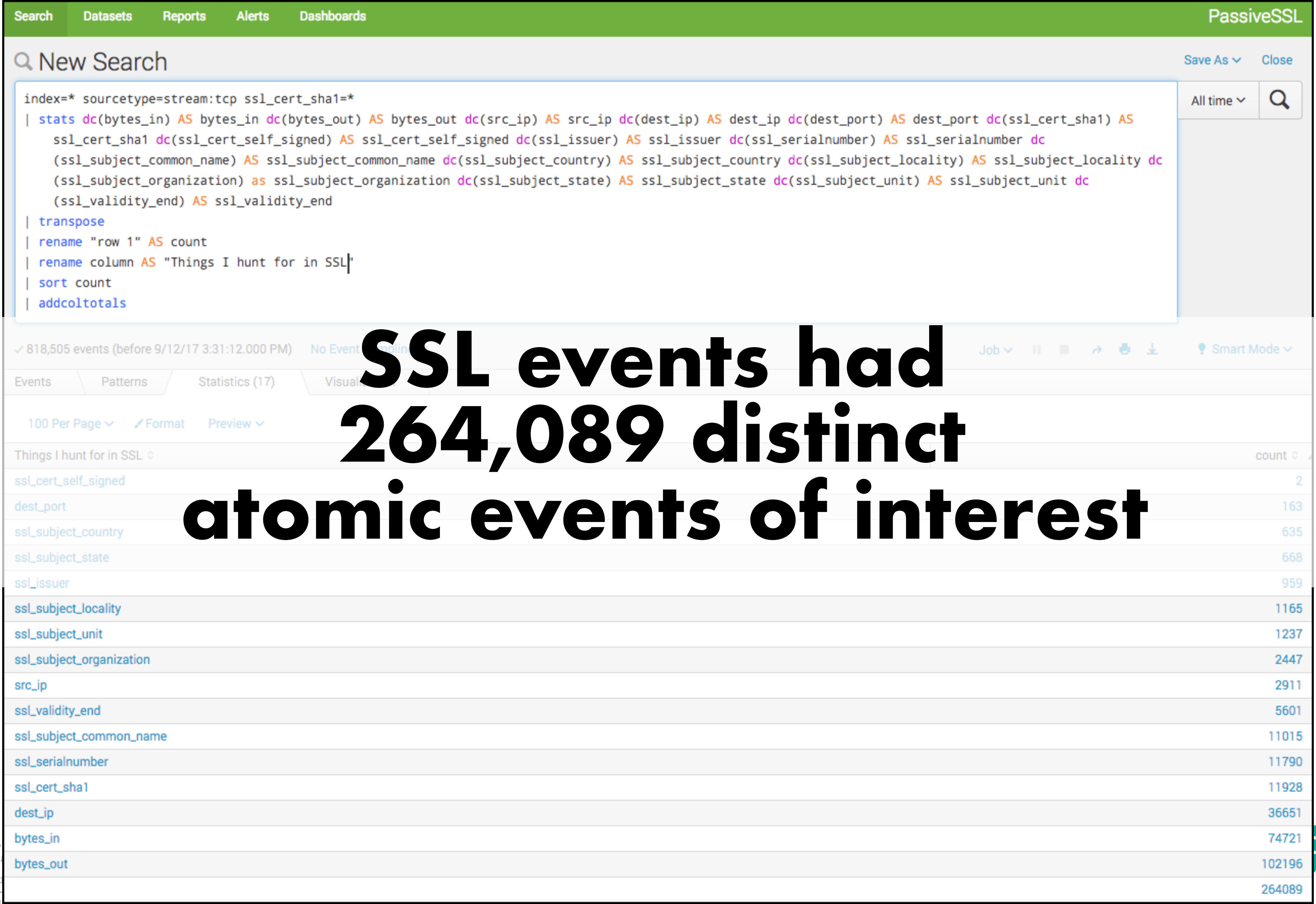
New Search

```
index=* sourcetype=stream:tcp ssl_cert_sha1=*
| stats dc(bytes_in) AS bytes_in dc(bytes_out) AS bytes_out dc(src_ip) AS src_ip dc(dest_ip) AS dest_ip dc(dest_port) AS dest_port dc(ssl_cert_sha1) AS
    ssl_cert_sha1 dc(ssl_cert_self_signed) AS ssl_cert_self_signed dc(ssl_issuer) AS ssl_issuer dc(ssl_serialnumber) AS ssl_serialnumber dc
    (ssl_subject_common_name) AS ssl_subject_common_name dc(ssl_subject_country) AS ssl_subject_country dc(ssl_subject_locality) AS ssl_subject_locality dc
    (ssl_subject_organization) as ssl_subject_organization dc(ssl_subject_state) AS ssl_subject_state dc(ssl_subject_unit) AS ssl_subject_unit dc
    (ssl_validity_end) AS ssl_validity_end
| transpose
| rename "row 1" AS count
| rename column AS "Things I hunt for in SSL"
| sort count
| addcoltotals
```

✓ 818,505 events (before 9/12/17 3:31:12.000 PM) No Event Sampling

Things I hunt for in SSL	count
ssl_cert_self_signed	2
dest_port	163
ssl_subject_country	635
ssl_subject_state	668
ssl_issuer	959
ssl_subject_locality	1165
ssl_subject_unit	1237
ssl_subject_organization	2447
src_ip	2911
ssl_validity_end	5601
ssl_subject_common_name	11015
ssl_serialnumber	11790
ssl_cert_sha1	11928
dest_ip	36651
bytes_in	74721
bytes_out	102196
	264089

SSL events had 264,089 distinct atomic events of interest

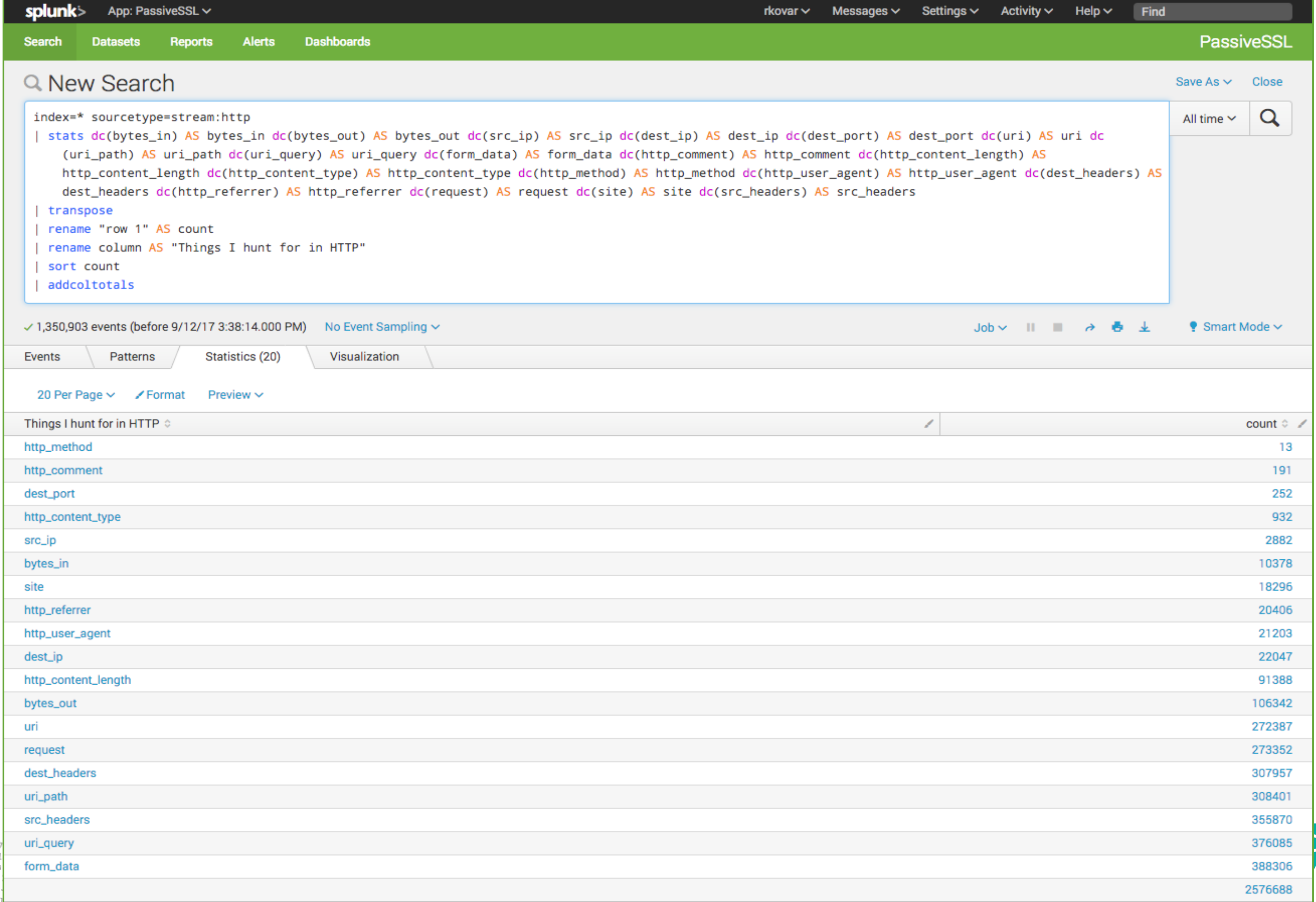


```
index=* sourcetype=stream:tcp ssl_cert_sha1=*
| stats dc(bytes_in) AS bytes_in dc(bytes_out) AS bytes_out dc(src_ip) AS src_ip dc(dest_ip) AS dest_ip dc(dest_port) AS dest_port dc(ssl_cert_sha1) AS
    ssl_cert_sha1 dc(ssl_cert_self_signed) AS ssl_cert_self_signed dc(ssl_issuer) AS ssl_issuer dc(ssl_serialnumber) AS ssl_serialnumber dc
    (ssl_subject_common_name) AS ssl_subject_common_name dc(ssl_subject_country) AS ssl_subject_country dc(ssl_subject_locality) AS ssl_subject_locality dc
    (ssl_subject_organization) as ssl_subject_organization dc(ssl_subject_state) AS ssl_subject_state dc(ssl_subject_unit) AS ssl_subject_unit dc
    (ssl_validity_end) AS ssl_validity_end
| transpose
| rename "row 1" AS count
| rename column AS "Things I hunt for in SSL"
| sort count
| addcoltotals
```

✓ 818,505 events (before 9/12/17 3:31:12.000 PM) No Event

Things I hunt for in SSL	count
ssl_cert_self_signed	2
dest_port	163
ssl_subject_country	635
ssl_subject_state	668
ssl_issuer	959
ssl_subject_locality	1165
ssl_subject_unit	1237
ssl_subject_organization	2447
src_ip	2911
ssl_validity_end	5601
ssl_subject_common_name	11015
ssl_serialnumber	11790
ssl_cert_sha1	11928
dest_ip	36651
bytes_in	74721
bytes_out	102196
	264089

conf2017

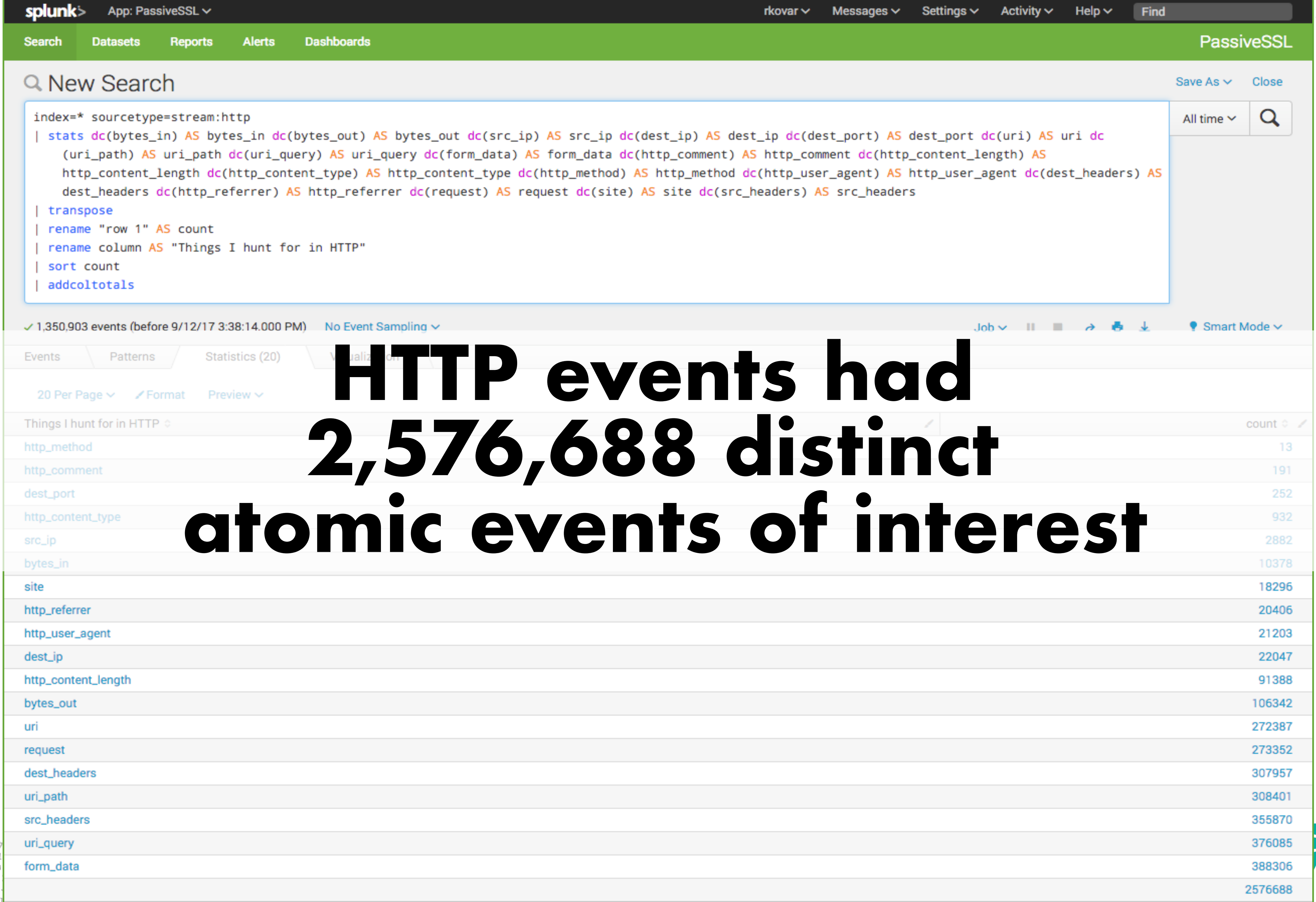


```
index=* sourcetype=stream:http
| stats dc(bytes_in) AS bytes_in dc(bytes_out) AS bytes_out dc(src_ip) AS src_ip dc(dest_ip) AS dest_ip dc(dest_port) AS dest_port dc(uri) AS uri dc
   (uri_path) AS uri_path dc(uri_query) AS uri_query dc(form_data) AS form_data dc(http_comment) AS http_comment dc(http_content_length) AS
   http_content_length dc(http_content_type) AS http_content_type dc(http_method) AS http_method dc(http_user_agent) AS http_user_agent dc(dest_headers) AS
   dest_headers dc(http_referrer) AS http_referrer dc(request) AS request dc(site) AS site dc(src_headers) AS src_headers
| transpose
| rename "row 1" AS count
| rename column AS "Things I hunt for in HTTP"
| sort count
| addcoltotals
```

✓ 1,350,903 events (before 9/12/17 3:38:14.000 PM) No Event Sampling

Things I hunt for in HTTP	count
http_method	13
http_comment	191
dest_port	252
http_content_type	932
src_ip	2882
bytes_in	10378
site	18296
http_referrer	20406
http_user_agent	21203
dest_ip	22047
http_content_length	91388
bytes_out	106342
uri	272387
request	273352
dest_headers	307957
uri_path	308401
src_headers	355870
uri_query	376085
form_data	388306
	2576688

conf2017



```
index=* sourcetype=stream:http
| stats dc(bytes_in) AS bytes_in dc(bytes_out) AS bytes_out dc(src_ip) AS src_ip dc(dest_ip) AS dest_ip dc(dest_port) AS dest_port dc(uri) AS uri dc
    (uri_path) AS uri_path dc(uri_query) AS uri_query dc(form_data) AS form_data dc(http_comment) AS http_comment dc(http_content_length) AS
    http_content_length dc(http_content_type) AS http_content_type dc(http_method) AS http_method dc(http_user_agent) AS http_user_agent dc(dest_headers) AS
    dest_headers dc(http_referrer) AS http_referrer dc(request) AS request dc(site) AS site dc(src_headers) AS src_headers
| transpose
| rename "row 1" AS count
| rename column AS "Things I hunt for in HTTP"
| sort count
| addcoltotals
```

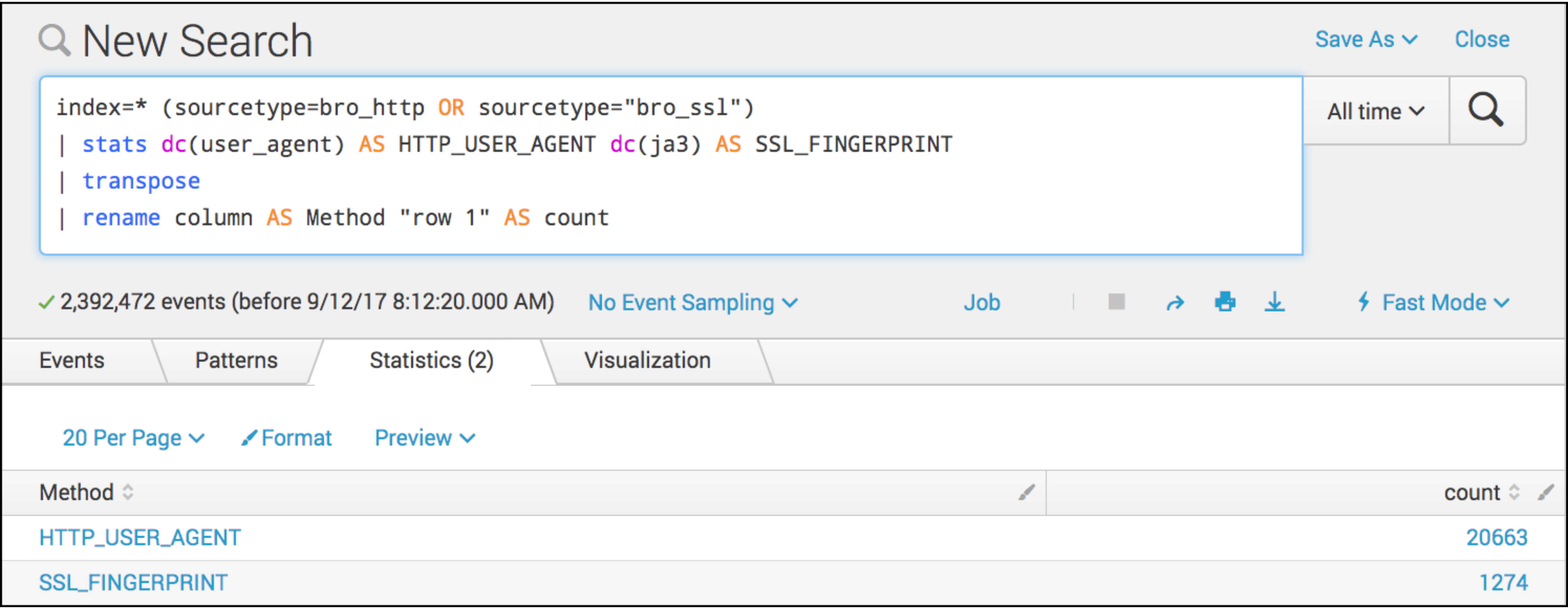
✓ 1,350,903 events (before 9/12/17 3:38:14.000 PM) No Event Sampling

Things I hunt for in HTTP	count
http_method	13
http_comment	191
dest_port	252
http_content_type	932
src_ip	2882
bytes_in	10378
site	18296
http_referrer	20406
http_user_agent	21203
dest_ip	22047
http_content_length	91388
bytes_out	106342
uri	272387
request	273352
dest_headers	307957
uri_path	308401
src_headers	355870
uri_query	376085
form_data	388306
	2576688

HTTP events had 2,576,688 distinct atomic events of interest

conf2017

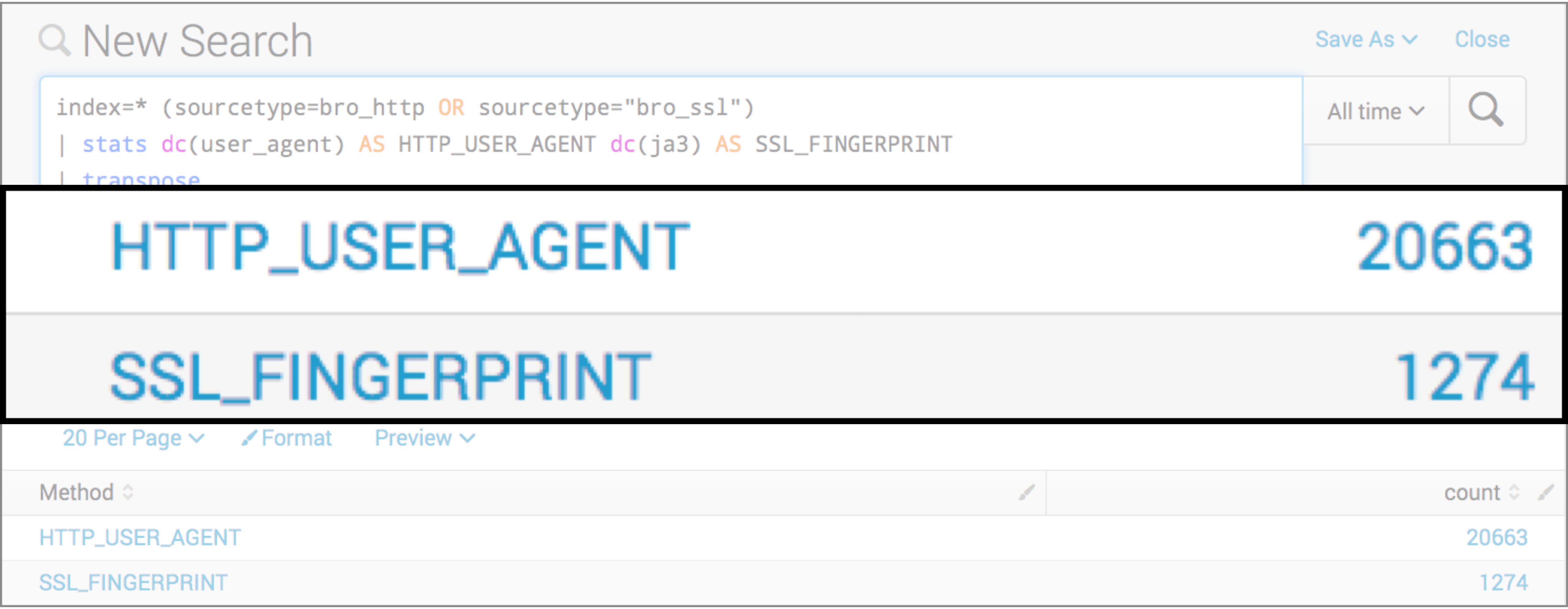
90%
OFF



```
index=* (sourcetype=bro_http OR sourcetype="bro_ssl")
| stats dc(user_agent) AS HTTP_USER_AGENT dc(ja3) AS SSL_FINGERPRINT
| transpose
| rename column AS Method "row 1" AS count
```

✓ 2,392,472 events (before 9/12/17 8:12:20.000 AM)

Method	count
HTTP_USER_AGENT	20663
SSL_FINGERPRINT	1274



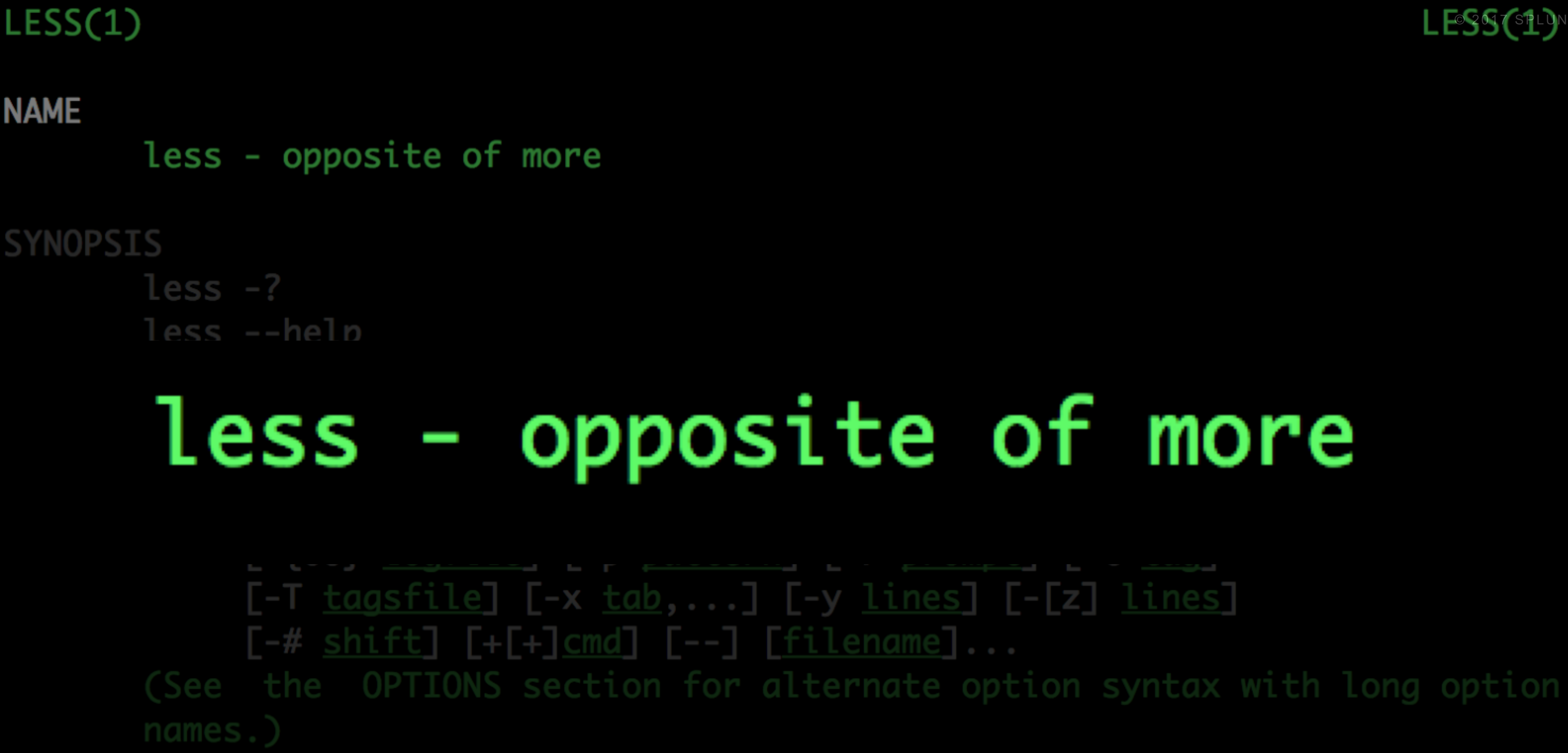
```
index=* (sourcetype=bro_http OR sourcetype="bro_ssl")
| stats dc(user_agent) AS HTTP_USER_AGENT dc(ja3) AS SSL_FINGERPRINT
| transpose
```

HTTP_USER_AGENT 20663

SSL_FINGERPRINT 1274

Method	count
HTTP_USER_AGENT	20663
SSL_FINGERPRINT	1274

94%

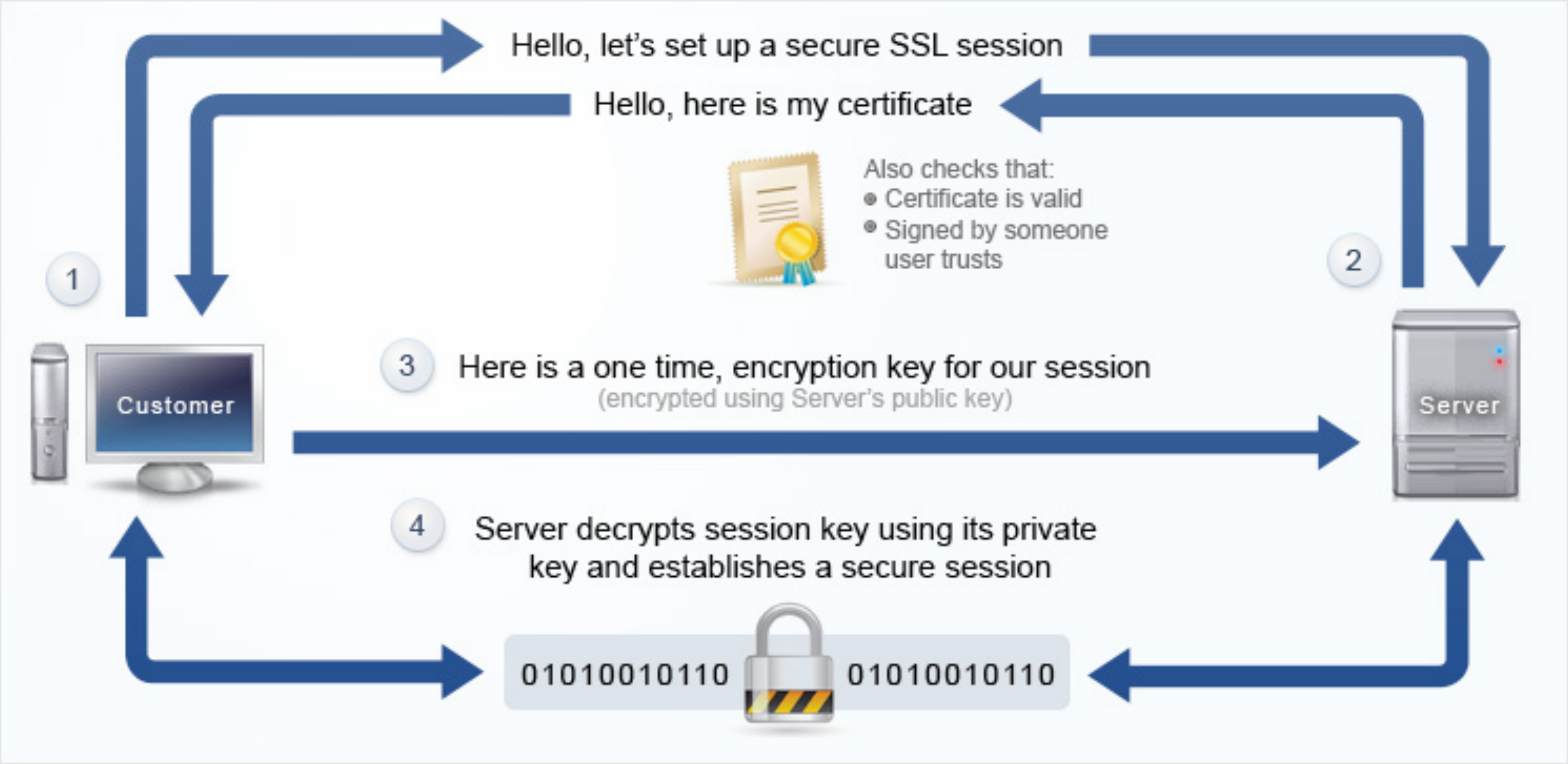


```
LESS(1)                                                         LESS(1)

NAME
       less - opposite of more

SYNOPSIS
       less -?
       less --help

          [-T tagsfile] [-x tab,...] [-y lines] [-[z] lines]
          [-# shift] [+[+]cmd] [--] [filename]...
       (See  the  OPTIONS section for alternate option syntax with long option
       names.)
```

less - opposite of more

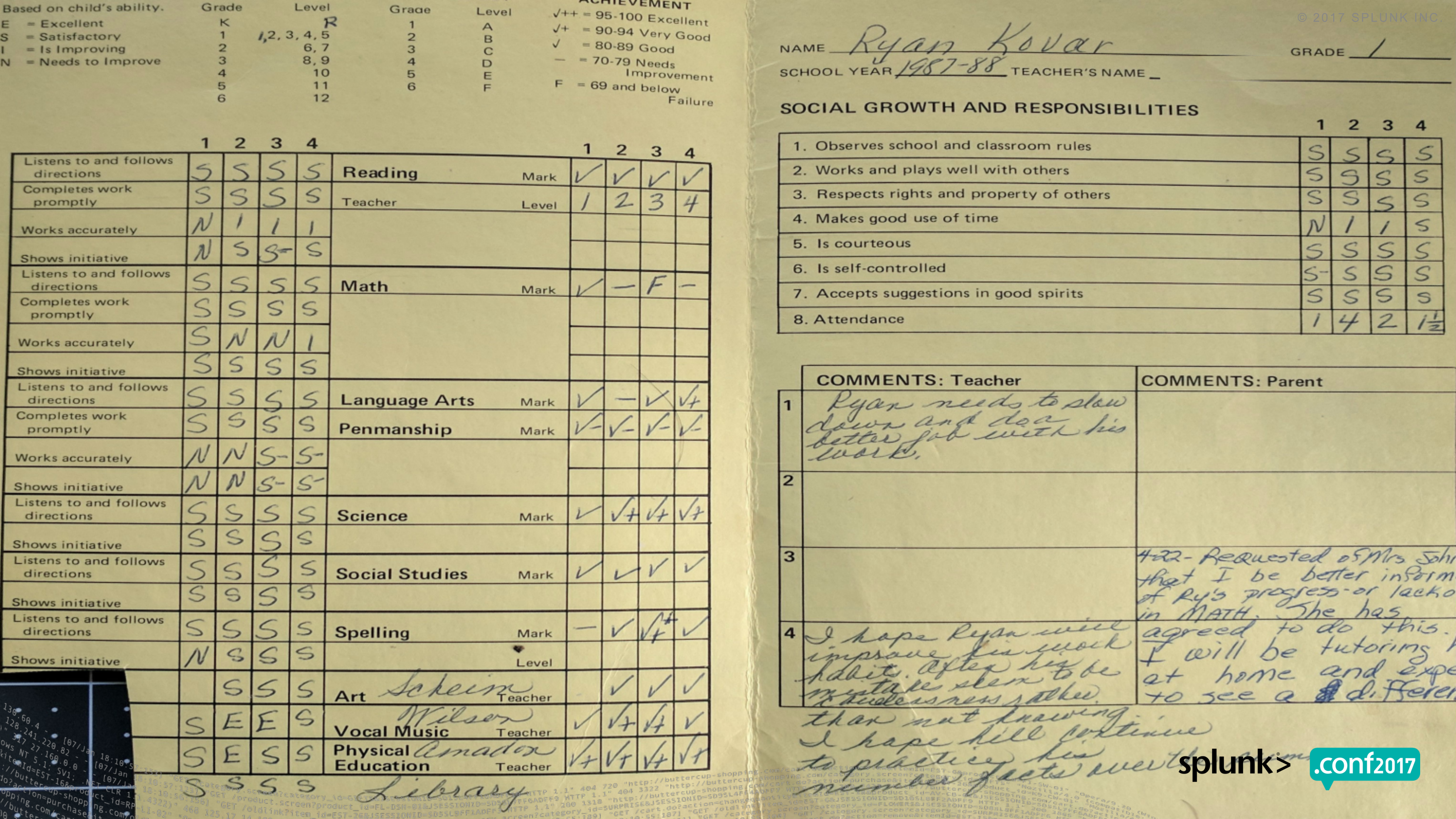
What SSL data are we looking at?

So… Quick refresher on SSL



1
Hello, let's set up a secure SSL session
Hello, here is my certificate
Also checks that:
● Certificate is valid
● Signed by someone user trusts
2
Customer
Server
3
Here is a one time, encryption key for our session
(encrypted using Server's public key)
4
Server decrypts session key using its private key and establishes a secure session
01010010110
01010010110

Lets look under the SSL hood



Based on child's ability.
E = Excellent
S = Satisfactory
I = Is Improving
N = Needs to Improve

Grade	Level	Grade	Level
K	R	1	A
1	1, 2, 3, 4, 5	2	B
2	6, 7	3	C
3	8, 9	4	D
4	10	5	E
5	11	6	F
6	12		

ACHIEVEMENT
✓++ = 95-100 Excellent
✓+ = 90-94 Very Good
✓ = 80-89 Good
— = 70-79 Needs Improvement
F = 69 and below Failure

	1	2	3	4			1	2	3	4
Listens to and follows directions	S	S	S	S	Reading	Mark	✓	✓	✓	✓
Completes work promptly	S	S	S	S	Teacher	Level	1	2	3	4
Works accurately	N	I	I	I						
Shows initiative	N	S	S-	S						
Listens to and follows directions	S	S	S	S	Math	Mark	✓	—	F	—
Completes work promptly	S	S	S	S						
Works accurately	S	N	N	I						
Shows initiative	S	S	S	S						
Listens to and follows directions	S	S	S	S	Language Arts	Mark	✓	—	✓	✓+
Completes work promptly	S	S	S	S	Penmanship	Mark	✓-	✓-	✓-	✓-
Works accurately	N	N	S-	S-						
Shows initiative	N	N	S-	S-						
Listens to and follows directions	S	S	S	S	Science	Mark	✓	✓+	✓+	✓+
Shows initiative	S	S	S	S						
Listens to and follows directions	S	S	S	S	Social Studies	Mark	✓	✓	✓	✓
Shows initiative	S	S	S	S						
Listens to and follows directions	S	S	S	S	Spelling	Mark	—	✓	✓+	✓
Shows initiative	N	S	S	S		Level				
		S	S	S	Art Scheim Teacher			✓	✓	✓
	S	E	E	S	Vocal Music Wilson Teacher		✓	✓+	✓+	✓
	S	E	S	S	Physical Education Amadon Teacher		✓+	✓+	✓+	✓+
	S	S	S	S	Library					

NAME Ryan Kovar GRADE 1

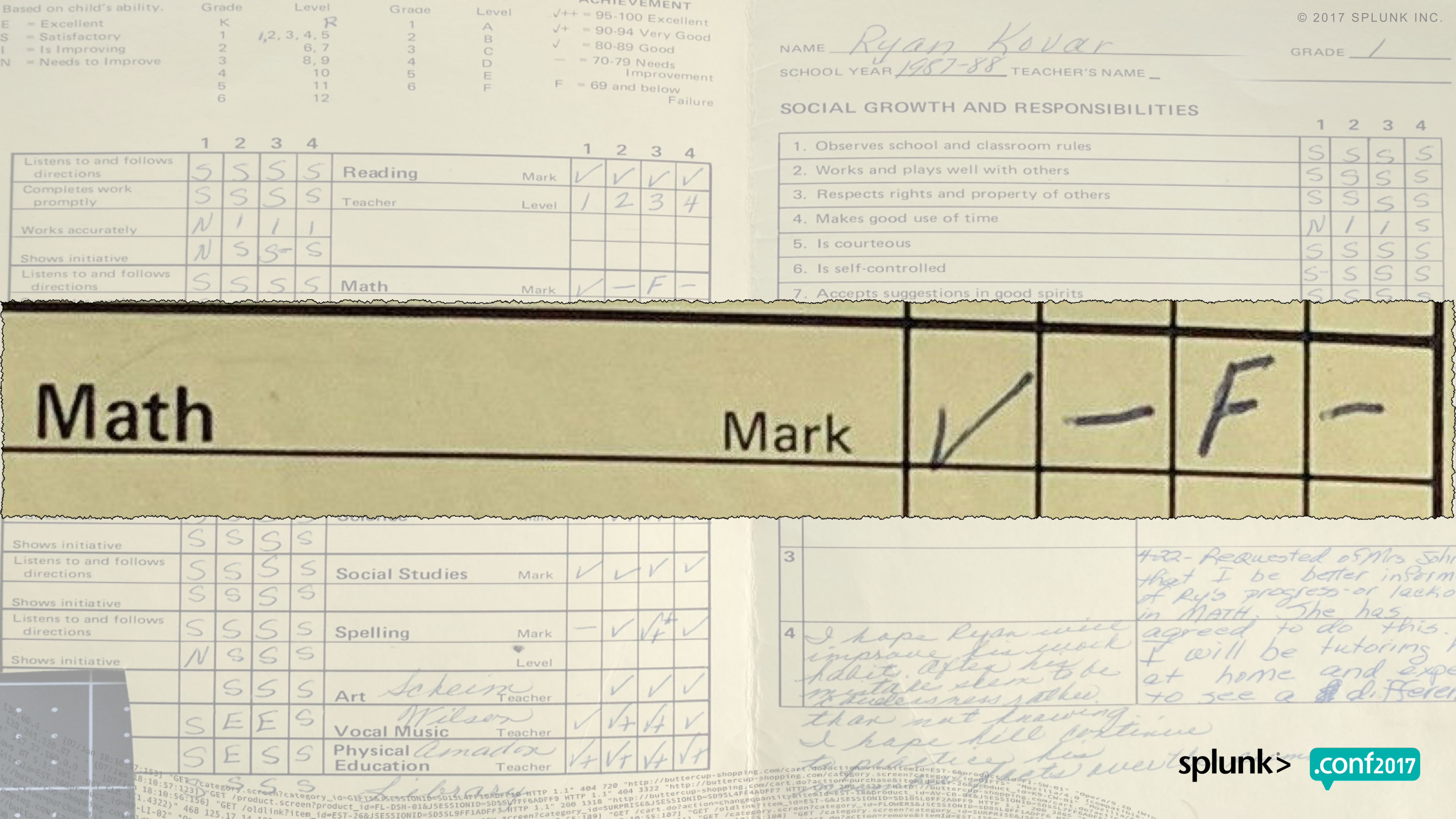
SCHOOL YEAR 1987-88 TEACHER'S NAME

SOCIAL GROWTH AND RESPONSIBILITIES

	1	2	3	4
1. Observes school and classroom rules	S	S	S	S
2. Works and plays well with others	S	S	S	S
3. Respects rights and property of others	S	S	S	S
4. Makes good use of time	N	I	I	S
5. Is courteous	S	S	S	S
6. Is self-controlled	S-	S	S	S
7. Accepts suggestions in good spirits	S	S	S	S
8. Attendance	1	4	2	1½

	COMMENTS: Teacher	COMMENTS: Parent
1	Ryan needs to slow down and do a better job with his work.	
2		
3		4-22- Requested of Mrs Johr that I be better inform of Ry's progress-or lack o in MATH. She has
4	I hope Ryan will improve his work habits. After his mistakes seem to be carelessness rather	agreed to do this. I will be tutoring h at home and expe to see a differen

than not knowing. I hope he'll continue to practice his number facts over the



Based on child's ability.
E = Excellent
S = Satisfactory
I = Is Improving
N = Needs to Improve

Grade	Level
K	R
1	1, 2, 3, 4, 5
2	6, 7
3	8, 9
4	10
5	11
6	12

Grade	Level
1	A
2	B
3	C
4	D
5	E
6	F

ACHIEVEMENT
√++ = 95-100 Excellent
√+ = 90-94 Very Good
√ = 80-89 Good
— = 70-79 Needs Improvement
F = 69 and below Failure

NAME Ryan Kovar GRADE 1
SCHOOL YEAR 1987-88 TEACHER'S NAME

SOCIAL GROWTH AND RESPONSIBILITIES

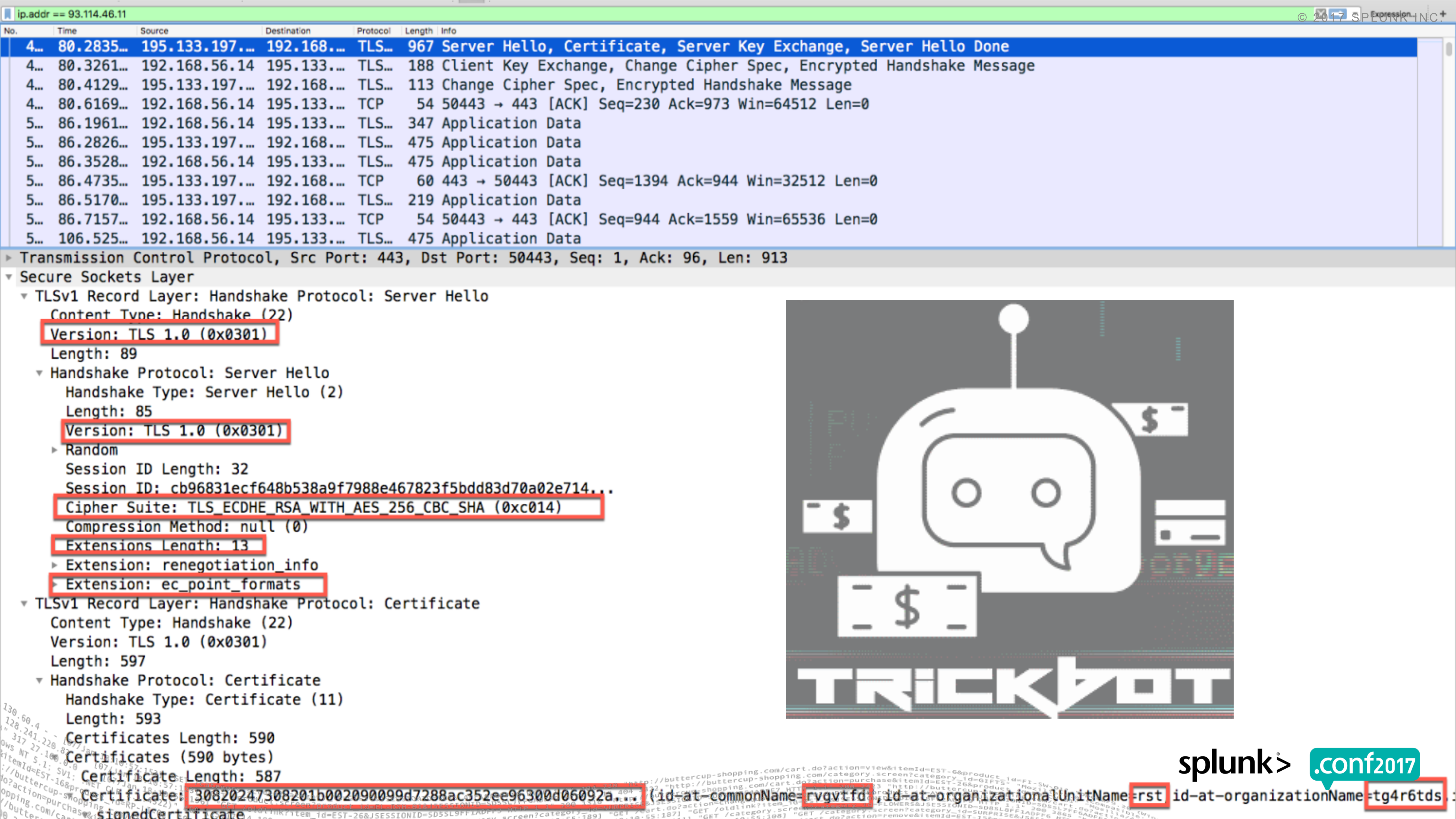
	1	2	3	4
1. Observes school and classroom rules	S	S	S	S
2. Works and plays well with others	S	S	S	S
3. Respects rights and property of others	S	S	S	S
4. Makes good use of time	N	I	I	S
5. Is courteous	S	S	S	S
6. Is self-controlled	S-	S	S	S
7. Accepts suggestions in good spirits	S	S	S	S

	1	2	3	4			1	2	3	4
Listens to and follows directions	S	S	S	S	Reading	Mark	√	√	√	√
Completes work promptly	S	S	S	S	Teacher	Level	1	2	3	4
Works accurately	N	I	I	I						
Shows initiative	N	S	S-	S						
Listens to and follows directions	S	S	S	S	Math	Mark	√	—	F	—

Math	Mark	√	—	F	—

Shows initiative	S	S	S	S						
Listens to and follows directions	S	S	S	S	Social Studies	Mark	√	√	√	√
Shows initiative	S	S	S	S						
Listens to and follows directions	S	S	S	S	Spelling	Mark	—	√	√+	√
Shows initiative	N	S	S	S		Level				
		S	S	S	Art Schein	Teacher		√	√	√
	S	E	E	S	Vocal Music Wilson	Teacher	√	√+	√+	√
	S	E	S	S	Physical Education Amador	Teacher	√+	√+	√+	√+
		S	S	S	Library					

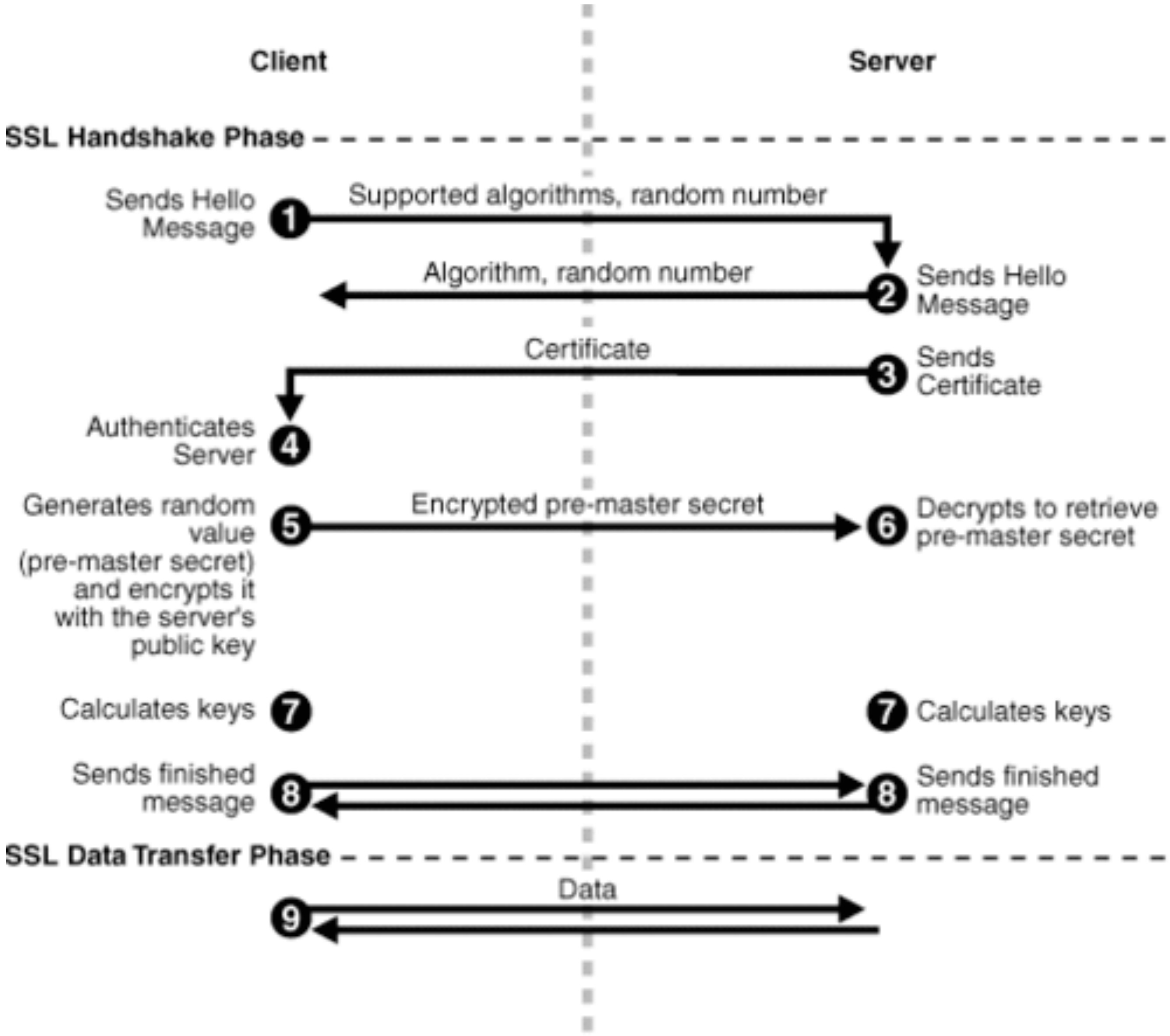
3		4-22- Requested of Mrs Sohn that I be better inform of Ry's progress - or lack of in MATH. She has agreed to do this. I will be tutoring h at home and expe to see a difference
4	I hope Ryan will improve his work habits. After his mistakes seem to be carelessness rather than not knowing. I hope he'll continue to practice his facts over the summer.	



```
No.  Time       Source          Destination  Protocol Length Info
4…   80.2835…   195.133.197.…   192.168.…    TLS…     967 Server Hello, Certificate, Server Key Exchange, Server Hello Done
4…   80.3261…   192.168.56.14   195.133.…    TLS…     188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
4…   80.4129…   195.133.197.…   192.168.…    TLS…     113 Change Cipher Spec, Encrypted Handshake Message
4…   80.6169…   192.168.56.14   195.133.…    TCP       54 50443 → 443 [ACK] Seq=230 Ack=973 Win=64512 Len=0
5…   86.1961…   192.168.56.14   195.133.…    TLS…     347 Application Data
5…   86.2826…   195.133.197.…   192.168.…    TLS…     475 Application Data
5…   86.3528…   192.168.56.14   195.133.…    TLS…     475 Application Data
5…   86.4735…   195.133.197.…   192.168.…    TCP       60 443 → 50443 [ACK] Seq=1394 Ack=944 Win=32512 Len=0
5…   86.5170…   195.133.197.…   192.168.…    TLS…     219 Application Data
5…   86.7157…   192.168.56.14   195.133.…    TCP       54 50443 → 443 [ACK] Seq=944 Ack=1559 Win=65536 Len=0
5…   106.525…   192.168.56.14   195.133.…    TLS…     475 Application Data
```

```
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 50443, Seq: 1, Ack: 96, Len: 913
▾ Secure Sockets Layer
  ▾ TLSv1 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 89
    ▾ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 85
        Version: TLS 1.0 (0x0301)
      ▸ Random
        Session ID Length: 32
        Session ID: cb96831ecf648b538a9f7988e467823f5bdd83d70a02e714...
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
        Compression Method: null (0)
        Extensions Length: 13
      ▸ Extension: renegotiation_info
      ▸ Extension: ec_point_formats
  ▾ TLSv1 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 597
    ▾ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 593
        Certificates Length: 590
        Certificates (590 bytes)
          Certificate Length: 587
          Certificate: 3082024730820 1b002090099d7288ac352ee96300d06092a... (id-at-commonName=rvgvtfd,id-at-organizationalUnitName=rst id-at-organizationName=tg4r6tds
          signedCertificate
```

SSL Handshakes



Client

Server

SSL Handshake Phase

1 Sends Hello Message — Supported algorithms, random number →

2 Sends Hello Message — ← Algorithm, random number

3 Sends Certificate — ← Certificate

4 Authenticates Server

5 Generates random value (pre-master secret) and encrypts it with the server's public key — Encrypted pre-master secret →

6 Decrypts to retrieve pre-master secret

7 Calculates keys

7 Calculates keys

8 Sends finished message ⇄ 8 Sends finished message

SSL Data Transfer Phase

9 Data ⇄

Everything after that... is secret

Certificate of Achievement

awarded to

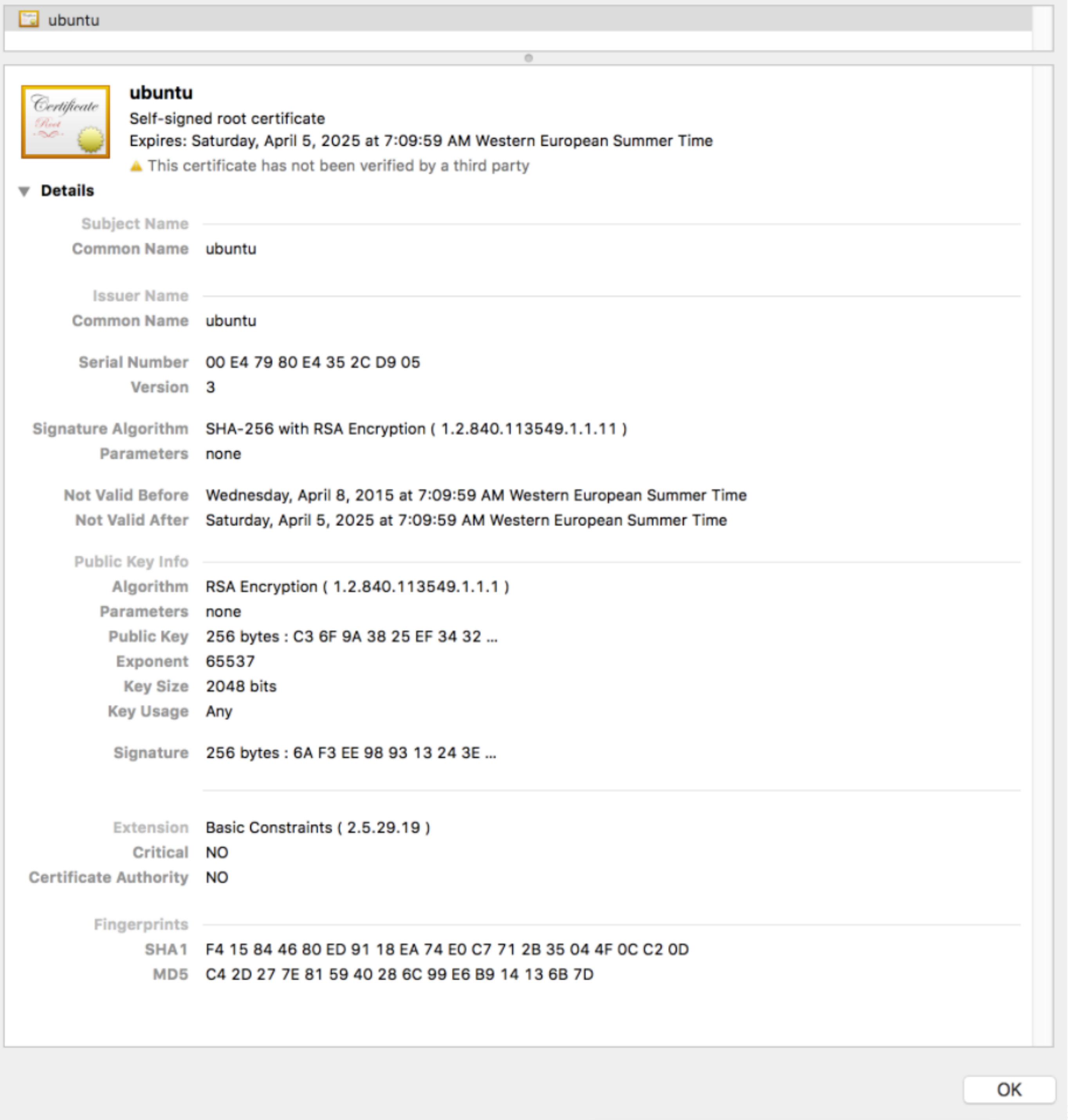
This presentation for Awesome

26SEP2017

date

Ryan Kovar

Signature



ubuntu

Self-signed root certificate

Expires: Saturday, April 5, 2025 at 7:09:59 AM Western European Summer Time

⚠ This certificate has not been verified by a third party

▼ **Details**

Subject Name
Common Name ubuntu

Issuer Name
Common Name ubuntu

Serial Number 00 E4 79 80 E4 35 2C D9 05
Version 3

Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters none

Not Valid Before Wednesday, April 8, 2015 at 7:09:59 AM Western European Summer Time
Not Valid After Saturday, April 5, 2025 at 7:09:59 AM Western European Summer Time

Public Key Info
Algorithm RSA Encryption (1.2.840.113549.1.1.1)
Parameters none
Public Key 256 bytes : C3 6F 9A 38 25 EF 34 32 ...
Exponent 65537
Key Size 2048 bits
Key Usage Any

Signature 256 bytes : 6A F3 EE 98 93 13 24 3E ...

Extension Basic Constraints (2.5.29.19)
Critical NO
Certificate Authority NO

Fingerprints
SHA1 F4 15 84 46 80 ED 91 18 EA 74 E0 C7 71 2B 35 04 4F 0C C2 0D
MD5 C4 2D 27 7E 81 59 40 28 6C 99 E6 B9 14 13 6B 7D

Where do we get all this tasty SSL data from?

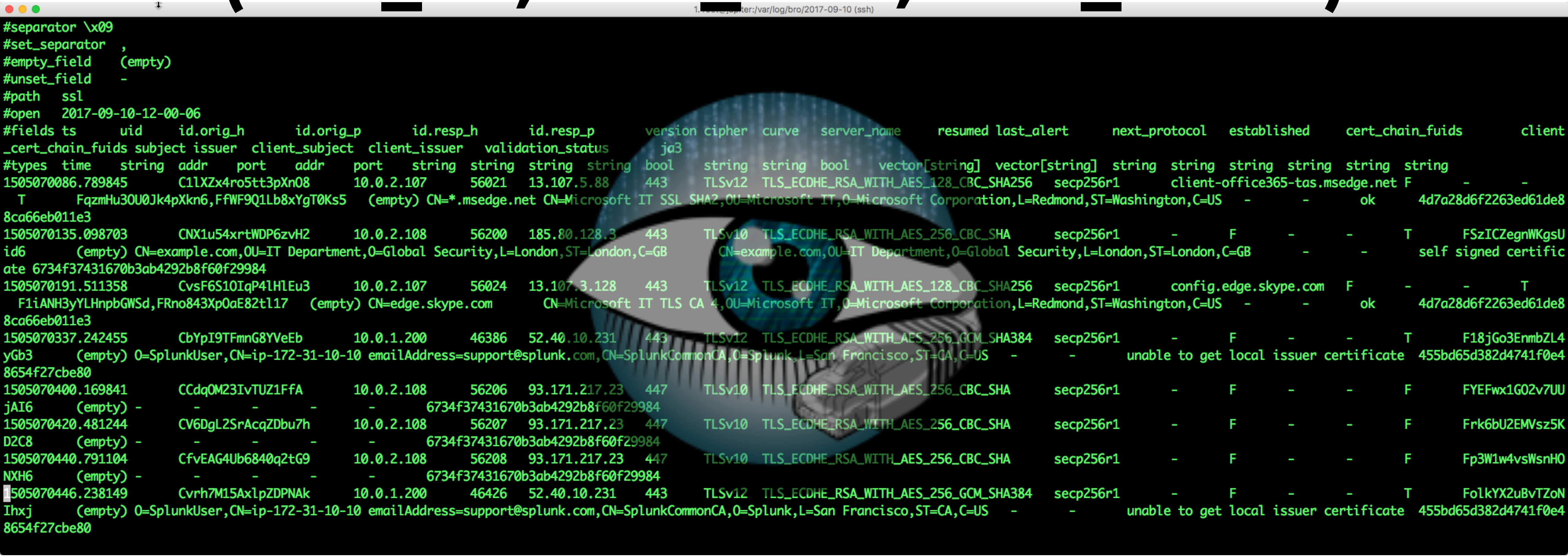
The Three Biggies in Splunklandia

Bro

Stream

Suricata

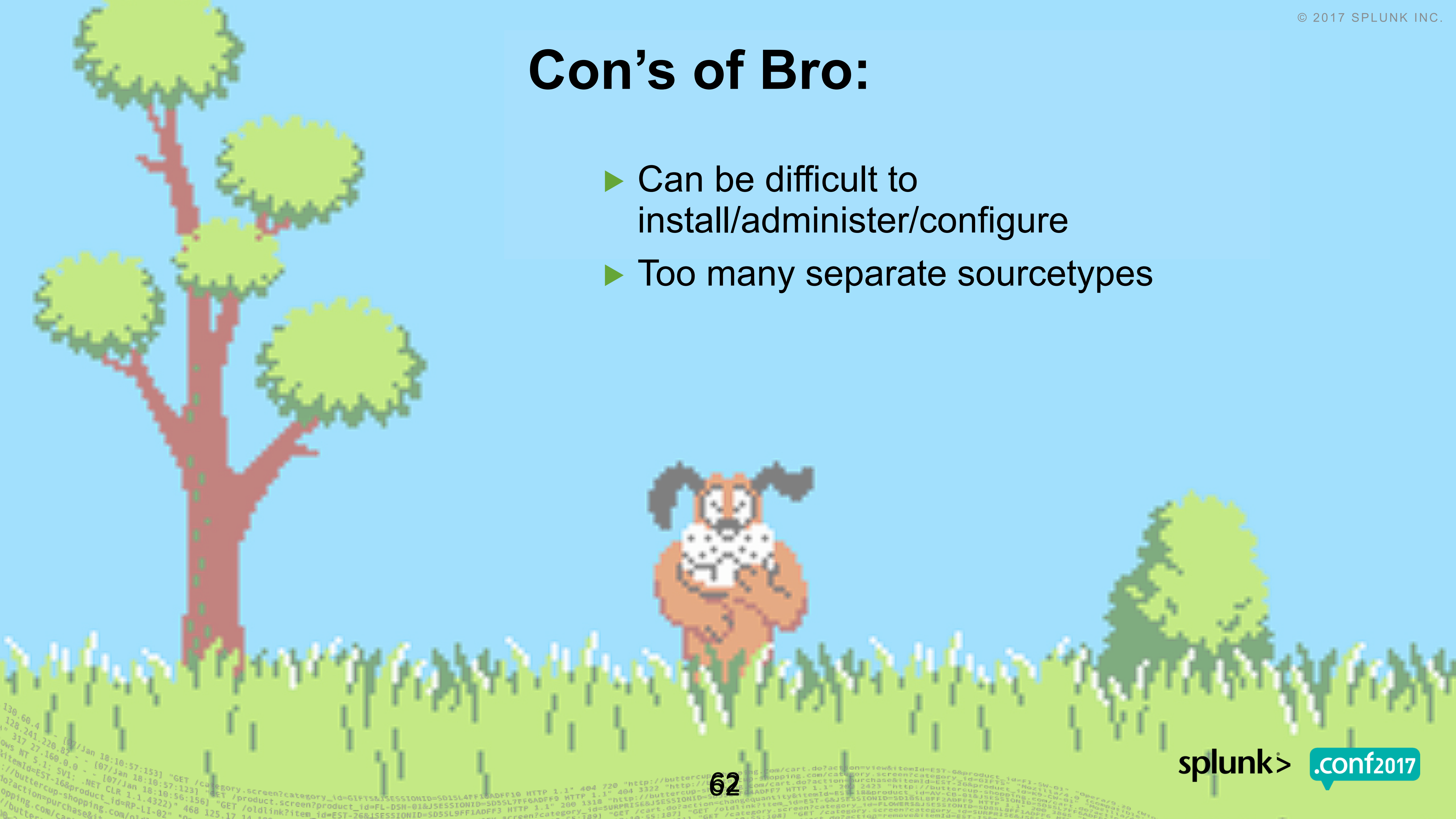
Bro SSL Logs
(bro_ssl, bro_files, bro_x509)



```
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   ssl
#open   2017-09-10-12-00-06
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       version cipher  curve   server_name     resumed last_alert      next_protocol   established     cert_chain_fuids        client
_cert_chain_fuids subject issuer  client_subject  client_issuer   validation_status       ja3
#types  time    string  addr    port    addr    port    string  string  string  string  bool    string  string  bool    vector[string]  vector[string]  string  string  string  string  string  string
1505070086.789845       C1lXZx4ro5tt3pXn08      10.0.2.107      56021   13.107.5.88     443     TLSv12  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256   secp256r1       client-office365-tas.msedge.net F       -       -
  T       FqzmHu3OU0Jk4pXkn6,FfWF9Q1Lb8xYgT0Ks5   (empty) CN=*.msedge.net CN=Microsoft IT SSL SHA2,OU=Microsoft IT,O=Microsoft Corporation,L=Redmond,ST=Washington,C=US   -       -       ok      4d7a28d6f2263ed61de8
8ca66eb011e3
1505070135.098703       CNX1u54xrtWDP6zvH2      10.0.2.108      56200   185.80.128.3    443     TLSv10  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA      secp256r1       -       F       -       -       T       FSzICZegnWKgsU
id6     (empty) CN=example.com,OU=IT Department,O=Global Security,L=London,ST=London,C=GB       CN=example.com,OU=IT Department,O=Global Security,L=London,ST=London,C=GB       -       -       self signed certific
ate 6734f37431670b3ab4292b8f60f29984
1505070191.511358       CvsF6S1OIqP4lHlEu3      10.0.2.107      56024   13.107.3.128    443     TLSv12  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256   secp256r1       config.edge.skype.com   F       -       -       T
  F1iANH3yYLHnpbGWSd,FRno843XpOaE82tl17   (empty) CN=edge.skype.com       CN=Microsoft IT TLS CA 4,OU=Microsoft IT,O=Microsoft Corporation,L=Redmond,ST=Washington,C=US   -       -       ok      4d7a28d6f2263ed61de8
8ca66eb011e3
1505070337.242455       CbYpI9TFmnG8YVeEb       10.0.1.200      46386   52.40.10.231    443     TLSv12  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384   secp256r1       -       F       -       -       T       F18jGo3EnmbZL4
yGb3    (empty) O=SplunkUser,CN=ip-172-31-10-10 emailAddress=support@splunk.com,CN=SplunkCommonCA,O=Splunk,L=San Francisco,ST=CA,C=US   -       -       unable to get local issuer certificate  455bd65d382d4741f0e4
8654f27cbe80
1505070400.169841       CCdqOM23IvTUZ1FfA       10.0.2.108      56206   93.171.217.23   447     TLSv10  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA      secp256r1       -       F       -       -       F       FYEFwx1GO2v7UU
jAI6    (empty) -       -       -       -       -       6734f37431670b3ab4292b8f60f29984
1505070420.481244       CV6DgL2SrAcqZDbu7h      10.0.2.108      56207   93.171.217.23   447     TLSv10  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA      secp256r1       -       F       -       -       F       Frk6bU2EMVsz5K
D2C8    (empty) -       -       -       -       -       6734f37431670b3ab4292b8f60f29984
1505070440.791104       CfvEAG4Ub6840q2tG9      10.0.2.108      56208   93.171.217.23   447     TLSv10  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA      secp256r1       -       F       -       -       F       Fp3W1w4vsWsnHO
NXH6    (empty) -       -       -       -       -       6734f37431670b3ab4292b8f60f29984
1505070446.238149       Cvrh7M15AxlpZDPNAk      10.0.1.200      46426   52.40.10.231    443     TLSv12  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384   secp256r1       -       F       -       -       T       FolkYX2uBvTZoN
Ihxj    (empty) O=SplunkUser,CN=ip-172-31-10-10 emailAddress=support@splunk.com,CN=SplunkCommonCA,O=Splunk,L=San Francisco,ST=CA,C=US   -       -       unable to get local issuer certificate  455bd65d382d4741f0e4
8654f27cbe80
```

Pro’s of Bro:

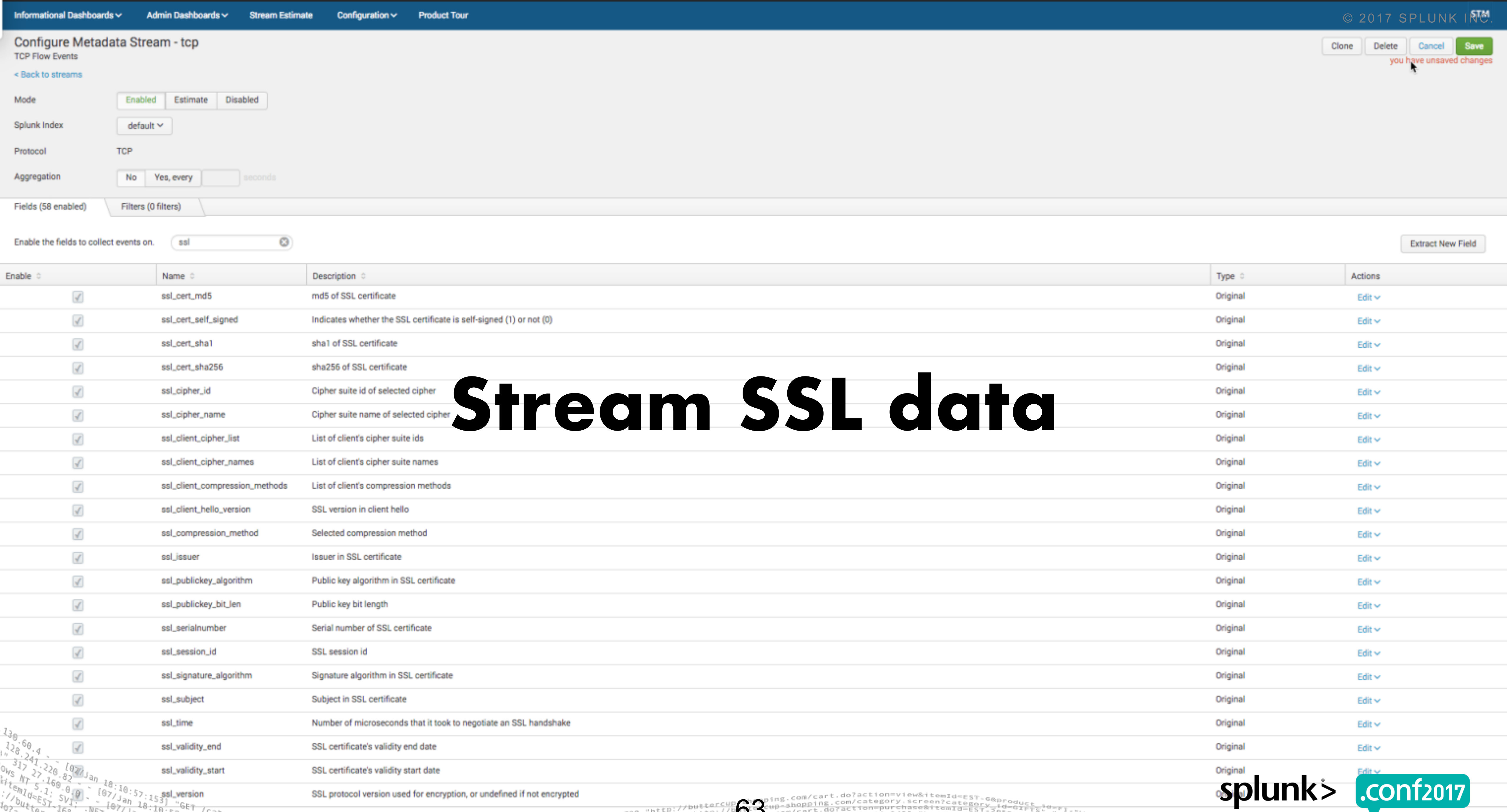
- High Adoption by Security Community
- Allows you to easily add new detections
- Very high fidelity of ALL SSL traffic
- Adding Fun SSL detection Scripts



Con’s of Bro:

- Can be difficult to install/administer/configure
- Too many separate sourcetypes

Stream SSL data



Configure Metadata Stream - tcp

TCP Flow Events

Mode: Enabled | Estimate | Disabled

Splunk Index: default

Protocol: TCP

Aggregation: No | Yes, every [ ] seconds

Fields (58 enabled) | Filters (0 filters)

Enable the fields to collect events on. ssl

Enable	Name	Description	Type	Actions
☑	ssl_cert_md5	md5 of SSL certificate	Original	Edit
☑	ssl_cert_self_signed	Indicates whether the SSL certificate is self-signed (1) or not (0)	Original	Edit
☑	ssl_cert_sha1	sha1 of SSL certificate	Original	Edit
☑	ssl_cert_sha256	sha256 of SSL certificate	Original	Edit
☑	ssl_cipher_id	Cipher suite id of selected cipher	Original	Edit
☑	ssl_cipher_name	Cipher suite name of selected cipher	Original	Edit
☑	ssl_client_cipher_list	List of client's cipher suite ids	Original	Edit
☑	ssl_client_cipher_names	List of client's cipher suite names	Original	Edit
☑	ssl_client_compression_methods	List of client's compression methods	Original	Edit
☑	ssl_client_hello_version	SSL version in client hello	Original	Edit
☑	ssl_compression_method	Selected compression method	Original	Edit
☑	ssl_issuer	Issuer in SSL certificate	Original	Edit
☑	ssl_publickey_algorithm	Public key algorithm in SSL certificate	Original	Edit
☑	ssl_publickey_bit_len	Public key bit length	Original	Edit
☑	ssl_serialnumber	Serial number of SSL certificate	Original	Edit
☑	ssl_session_id	SSL session id	Original	Edit
☑	ssl_signature_algorithm	Signature algorithm in SSL certificate	Original	Edit
☑	ssl_subject	Subject in SSL certificate	Original	Edit
☑	ssl_time	Number of microseconds that it took to negotiate an SSL handshake	Original	Edit
☑	ssl_validity_end	SSL certificate's validity end date	Original	Edit
☑	ssl_validity_start	SSL certificate's validity start date	Original	Edit
☑	ssl_version	SSL protocol version used for encryption, or undefined if not encrypted	O	

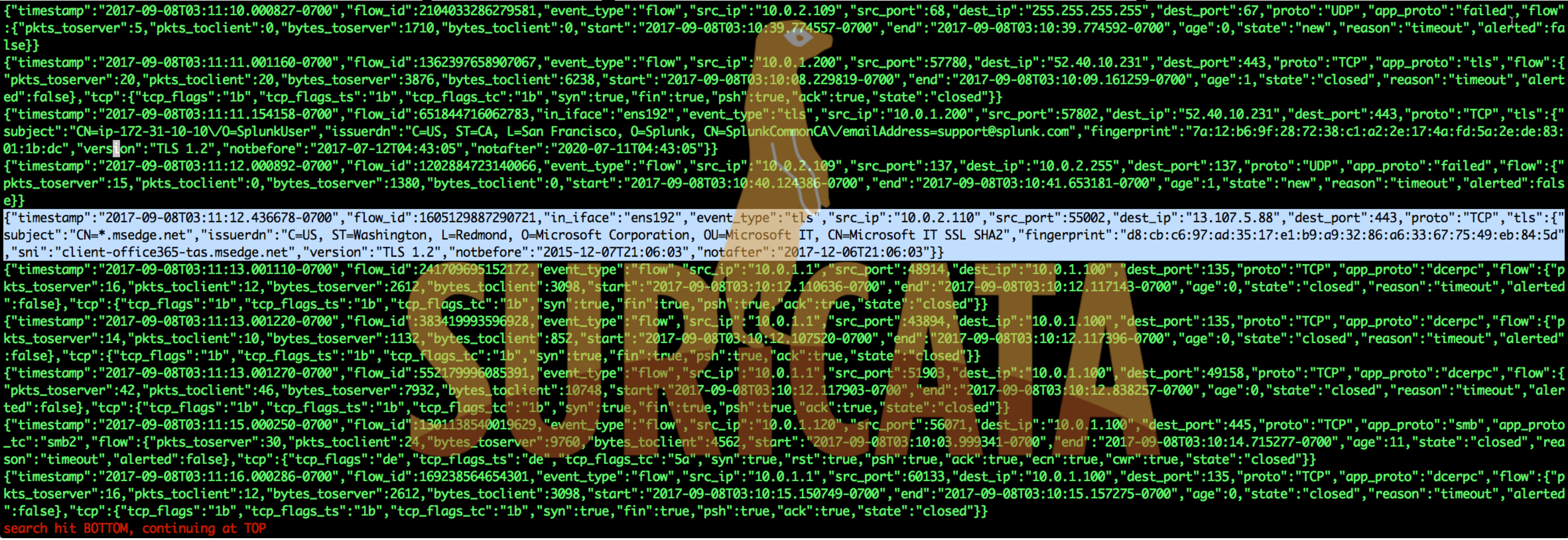
Pro's of Stream:

- Splunk Supported
- Easy to install
- Only one source type to look at!

Con’s of Stream:

- Doesn’t show hostnames in SSL certificate
- Doesn’t show all of the interesting handshake fields

Suricata Logs (eve.json and certs)



```
{"timestamp":"2017-09-08T03:11:10.000827-0700","flow_id":2104033286279581,"event_type":"flow","src_ip":"10.0.2.109","src_port":68,"dest_ip":"255.255.255.255","dest_port":67,"proto":"UDP","app_proto":"failed","flow"
:{"pkts_toserver":5,"pkts_toclient":0,"bytes_toserver":1710,"bytes_toclient":0,"start":"2017-09-08T03:10:39.774557-0700","end":"2017-09-08T03:10:39.774592-0700","age":0,"state":"new","reason":"timeout","alerted":fa
lse}}
{"timestamp":"2017-09-08T03:11:11.001160-0700","flow_id":1362397658907067,"event_type":"flow","src_ip":"10.0.1.200","src_port":57780,"dest_ip":"52.40.10.231","dest_port":443,"proto":"TCP","app_proto":"tls","flow":{
"pkts_toserver":20,"pkts_toclient":20,"bytes_toserver":3876,"bytes_toclient":6238,"start":"2017-09-08T03:10:08.229819-0700","end":"2017-09-08T03:10:09.161259-0700","age":1,"state":"closed","reason":"timeout","alert
ed":false},"tcp":{"tcp_flags":"1b","tcp_flags_ts":"1b","tcp_flags_tc":"1b","syn":true,"fin":true,"psh":true,"ack":true,"state":"closed"}}
{"timestamp":"2017-09-08T03:11:11.154158-0700","flow_id":651844716062783,"in_iface":"ens192","event_type":"tls","src_ip":"10.0.1.200","src_port":57802,"dest_ip":"52.40.10.231","dest_port":443,"proto":"TCP","tls":{"
subject":"CN=ip-172-31-10-10\/O=SplunkUser","issuerdn":"C=US, ST=CA, L=San Francisco, O=Splunk, CN=SplunkCommonCA\/emailAddress=support@splunk.com","fingerprint":"7a:12:b6:9f:28:72:38:c1:a2:2e:17:4a:fd:5a:2e:de:83:
01:1b:dc","version":"TLS 1.2","notbefore":"2017-07-12T04:43:05","notafter":"2020-07-11T04:43:05"}}
{"timestamp":"2017-09-08T03:11:12.000892-0700","flow_id":1202884723140066,"event_type":"flow","src_ip":"10.0.2.109","src_port":137,"dest_ip":"10.0.2.255","dest_port":137,"proto":"UDP","app_proto":"failed","flow":{"
pkts_toserver":15,"pkts_toclient":0,"bytes_toserver":1380,"bytes_toclient":0,"start":"2017-09-08T03:10:40.124386-0700","end":"2017-09-08T03:10:41.653181-0700","age":1,"state":"new","reason":"timeout","alerted":fals
e}}
{"timestamp":"2017-09-08T03:11:12.436678-0700","flow_id":1605129887290721,"in_iface":"ens192","event_type":"tls","src_ip":"10.0.2.110","src_port":55002,"dest_ip":"13.107.5.88","dest_port":443,"proto":"TCP","tls":{"
subject":"CN=*.msedge.net","issuerdn":"C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, OU=Microsoft IT, CN=Microsoft IT SSL SHA2","fingerprint":"d8:cb:c6:97:ad:35:17:e1:b9:a9:32:86:a6:33:67:75:49:eb:84:5d"
,"sni":"client-office365-tas.msedge.net","version":"TLS 1.2","notbefore":"2015-12-07T21:06:03","notafter":"2017-12-06T21:06:03"}}
{"timestamp":"2017-09-08T03:11:13.001110-0700","flow_id":241709695152172,"event_type":"flow","src_ip":"10.0.1.1","src_port":48914,"dest_ip":"10.0.1.100","dest_port":135,"proto":"TCP","app_proto":"dcerpc","flow":{"p
kts_toserver":16,"pkts_toclient":12,"bytes_toserver":2612,"bytes_toclient":3098,"start":"2017-09-08T03:10:12.110636-0700","end":"2017-09-08T03:10:12.117143-0700","age":0,"state":"closed","reason":"timeout","alerted
":false},"tcp":{"tcp_flags":"1b","tcp_flags_ts":"1b","tcp_flags_tc":"1b","syn":true,"fin":true,"psh":true,"ack":true,"state":"closed"}}
{"timestamp":"2017-09-08T03:11:13.001220-0700","flow_id":383419993596928,"event_type":"flow","src_ip":"10.0.1.1","src_port":43894,"dest_ip":"10.0.1.100","dest_port":135,"proto":"TCP","app_proto":"dcerpc","flow":{"p
kts_toserver":14,"pkts_toclient":10,"bytes_toserver":1132,"bytes_toclient":852,"start":"2017-09-08T03:10:12.107520-0700","end":"2017-09-08T03:10:12.117396-0700","age":0,"state":"closed","reason":"timeout","alerted"
:false},"tcp":{"tcp_flags":"1b","tcp_flags_ts":"1b","tcp_flags_tc":"1b","syn":true,"fin":true,"psh":true,"ack":true,"state":"closed"}}
{"timestamp":"2017-09-08T03:11:13.001270-0700","flow_id":552179996085391,"event_type":"flow","src_ip":"10.0.1.1","src_port":51903,"dest_ip":"10.0.1.100","dest_port":49158,"proto":"TCP","app_proto":"dcerpc","flow":{
"pkts_toserver":42,"pkts_toclient":46,"bytes_toserver":7932,"bytes_toclient":10748,"start":"2017-09-08T03:10:12.117903-0700","end":"2017-09-08T03:10:12.838257-0700","age":0,"state":"closed","reason":"timeout","aler
ted":false},"tcp":{"tcp_flags":"1b","tcp_flags_ts":"1b","tcp_flags_tc":"1b","syn":true,"fin":true,"psh":true,"ack":true,"state":"closed"}}
{"timestamp":"2017-09-08T03:11:15.000250-0700","flow_id":1301138540019629,"event_type":"flow","src_ip":"10.0.1.120","src_port":56071,"dest_ip":"10.0.1.100","dest_port":445,"proto":"TCP","app_proto":"smb","app_proto
_tc":"smb2","flow":{"pkts_toserver":30,"pkts_toclient":24,"bytes_toserver":9760,"bytes_toclient":4562,"start":"2017-09-08T03:10:03.999341-0700","end":"2017-09-08T03:10:14.715277-0700","age":11,"state":"closed","rea
son":"timeout","alerted":false},"tcp":{"tcp_flags":"de","tcp_flags_ts":"de","tcp_flags_tc":"5a","syn":true,"rst":true,"psh":true,"ack":true,"ecn":true,"cwr":true,"state":"closed"}}
{"timestamp":"2017-09-08T03:11:16.000286-0700","flow_id":169238564654301,"event_type":"flow","src_ip":"10.0.1.1","src_port":60133,"dest_ip":"10.0.1.100","dest_port":135,"proto":"TCP","app_proto":"dcerpc","flow":{"p
kts_toserver":16,"pkts_toclient":12,"bytes_toserver":2612,"bytes_toclient":3098,"start":"2017-09-08T03:10:15.150749-0700","end":"2017-09-08T03:10:15.157275-0700","age":0,"state":"closed","reason":"timeout","alerted
":false},"tcp":{"tcp_flags":"1b","tcp_flags_ts":"1b","tcp_flags_tc":"1b","syn":true,"fin":true,"psh":true,"ack":true,"state":"closed"}}
search hit BOTTOM, continuing at TOP
```

Pro’s of Suricata:

- Very easy to configure
- Low volume
- Extensively used by the security Community

Con’s of Suricata:

- Less Fidelity
- Harder to customize

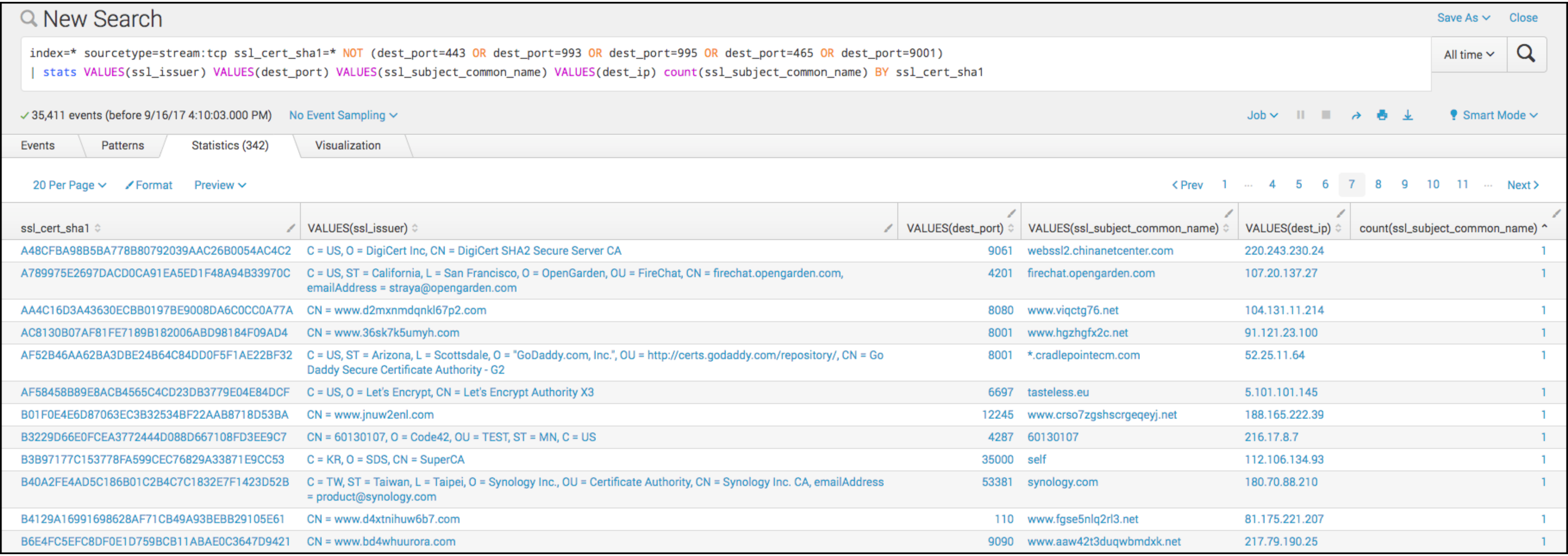
How do we hunt the baddies!

Finding shared unusual SSL activity on unusual ports

- Detection

```
sourcetype=stream:tcp ssl_cert_sha1=* NOT (dest_port=443 OR
dest_port=993 OR dest_port=995 OR dest_port=465 OR
dest_port=9001)
| stats VALUES(ssl_issuer) VALUES(dest_port)
VALUES(ssl_subject_common_name) VALUES(dest_ip)
count(ssl_subject_common_name) BY ssl_cert_sha1
```

Finding Shared Unusual SSL Activity On Unusual Ports

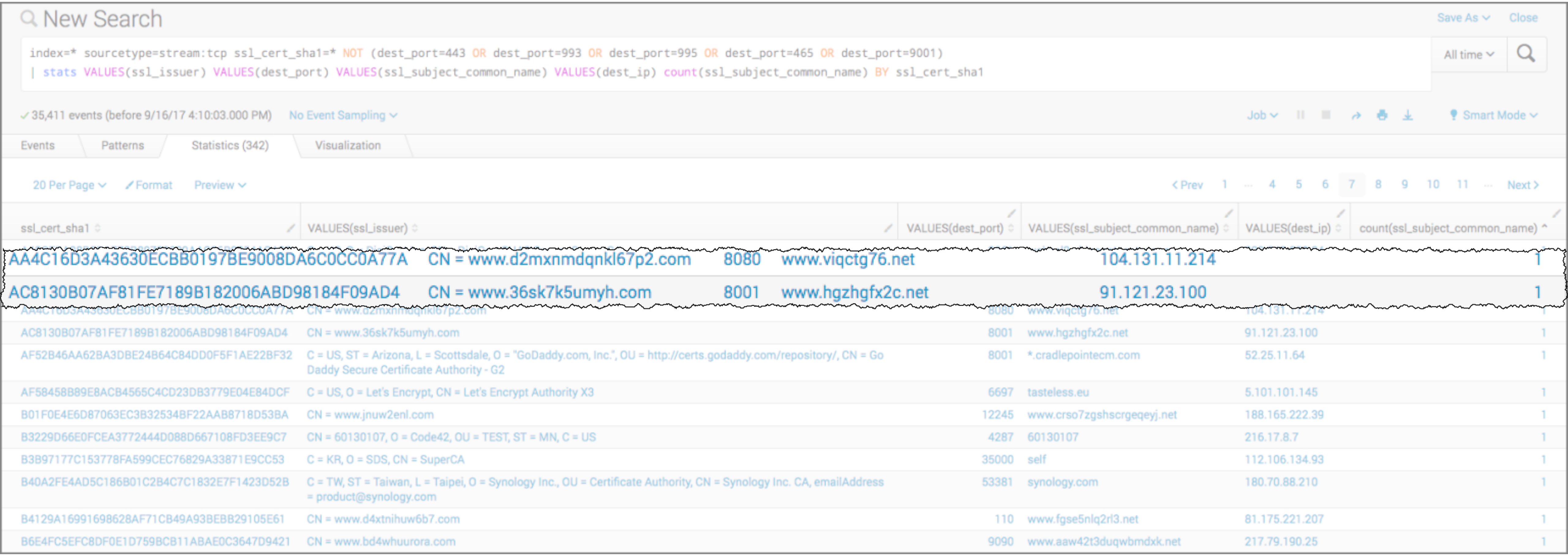


```
index=* sourcetype=stream:tcp ssl_cert_sha1=* NOT (dest_port=443 OR dest_port=993 OR dest_port=995 OR dest_port=465 OR dest_port=9001)
| stats VALUES(ssl_issuer) VALUES(dest_port) VALUES(ssl_subject_common_name) VALUES(dest_ip) count(ssl_subject_common_name) BY ssl_cert_sha1
```

✓ 35,411 events (before 9/16/17 4:10:03.000 PM)

ssl_cert_sha1	VALUES(ssl_issuer)	VALUES(dest_port)	VALUES(ssl_subject_common_name)	VALUES(dest_ip)	count(ssl_subject_common_name)
A48CFBA98B5BA778B80792039AAC26B0054AC4C2	C = US, O = DigiCert Inc, CN = DigiCert SHA2 Secure Server CA	9061	webssl2.chinanetcenter.com	220.243.230.24	1
A789975E2697DACD0CA91EA5ED1F48A94B33970C	C = US, ST = California, L = San Francisco, O = OpenGarden, OU = FireChat, CN = firechat.opengarden.com, emailAddress = straya@opengarden.com	4201	firechat.opengarden.com	107.20.137.27	1
AA4C16D3A43630ECBB0197BE9008DA6C0CC0A77A	CN = www.d2mxnmdqnkl67p2.com	8080	www.viqctg76.net	104.131.11.214	1
AC8130B07AF81FE7189B182006ABD98184F09AD4	CN = www.36sk7k5umyh.com	8001	www.hgzhgfx2c.net	91.121.23.100	1
AF52B46AA62BA3DBE24B64C84DD0F5F1AE22BF32	C = US, ST = Arizona, L = Scottsdale, O = "GoDaddy.com, Inc.", OU = http://certs.godaddy.com/repository/, CN = Go Daddy Secure Certificate Authority - G2	8001	*.cradlepointecm.com	52.25.11.64	1
AF58458B89E8ACB4565C4CD23DB3779E04E84DCF	C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3	6697	tasteless.eu	5.101.101.145	1
B01F0E4E6D87063EC3B32534BF22AAB8718D53BA	CN = www.jnuw2enl.com	12245	www.crso7zgshscrgeqeyj.net	188.165.222.39	1
B3229D66E0FCEA3772444D088D667108FD3EE9C7	CN = 60130107, O = Code42, OU = TEST, ST = MN, C = US	4287	60130107	216.17.8.7	1
B3B97177C153778FA599CEC76829A33871E9CC53	C = KR, O = SDS, CN = SuperCA	35000	self	112.106.134.93	1
B40A2FE4AD5C186B01C2B4C7C1832E7F1423D52B	C = TW, ST = Taiwan, L = Taipei, O = Synology Inc., OU = Certificate Authority, CN = Synology Inc. CA, emailAddress = product@synology.com	53381	synology.com	180.70.88.210	1
B4129A16991698628AF71CB49A93BEBB29105E61	CN = www.d4xtnihuw6b7.com	110	www.fgse5nlq2rl3.net	81.175.221.207	1
B6E4FC5EFC8DF0E1D759BCB11ABAE0C3647D9421	CN = www.bd4whuurora.com	9090	www.aaw42t3duqwbmdxk.net	217.79.190.25	1

Finding Shared Unusual SSL Activity On Unusual Ports



```
index=* sourcetype=stream:tcp ssl_cert_sha1=* NOT (dest_port=443 OR dest_port=993 OR dest_port=995 OR dest_port=465 OR dest_port=9001)
| stats VALUES(ssl_issuer) VALUES(dest_port) VALUES(ssl_subject_common_name) VALUES(dest_ip) count(ssl_subject_common_name) BY ssl_cert_sha1
```

✓ 35,411 events (before 9/16/17 4:10:03.000 PM) No Event Sampling

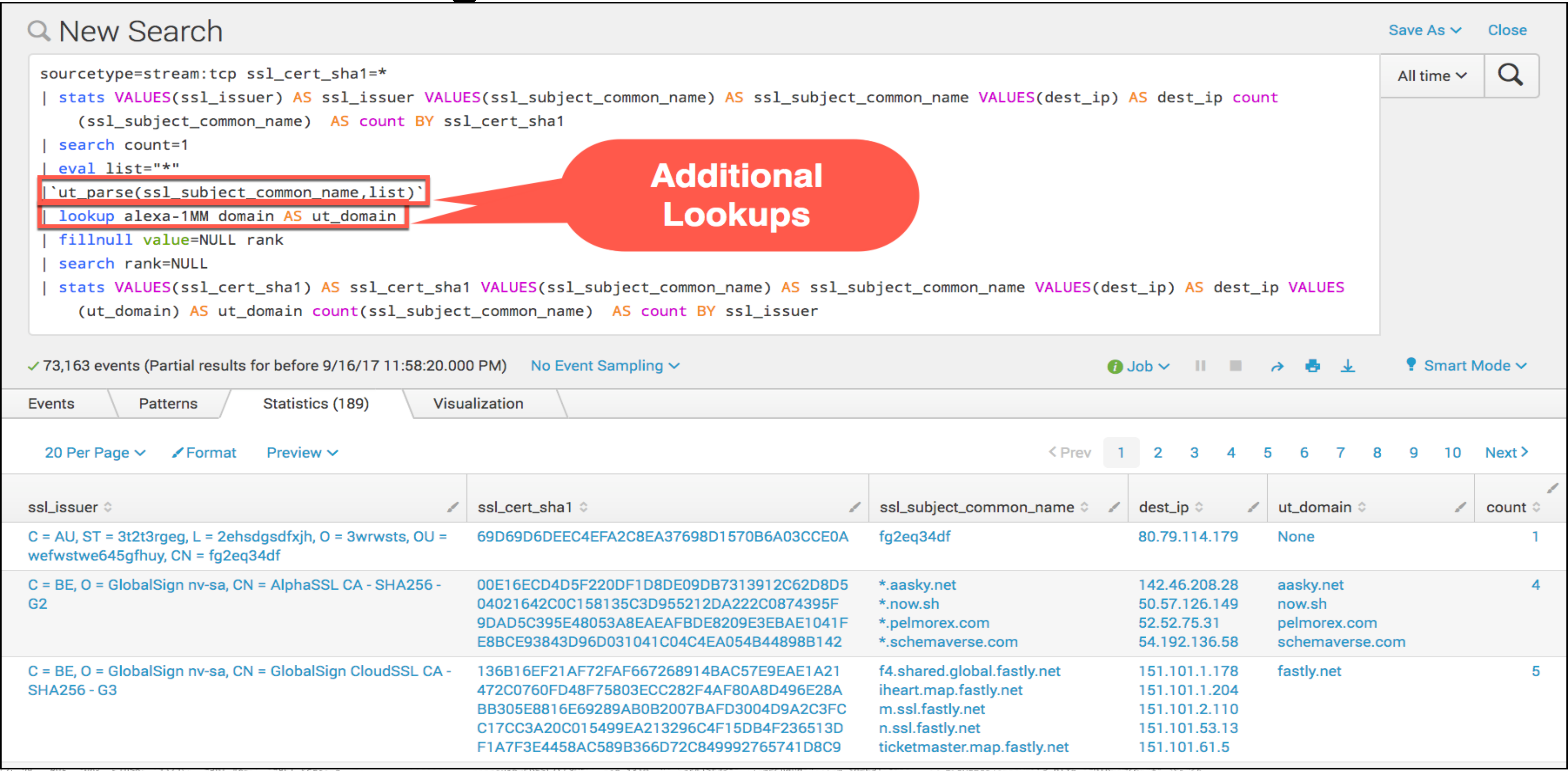
ssl_cert_sha1	VALUES(ssl_issuer)	VALUES(dest_port)	VALUES(ssl_subject_common_name)	VALUES(dest_ip)	count(ssl_subject_common_name)
AA4C16D3A43630ECBB0197BE9008DA6C0CC0A77A	CN = www.d2mxnmdqnkl67p2.com	8080	www.viqctg76.net	104.131.11.214	1
AC8130B07AF81FE7189B182006ABD98184F09AD4	CN = www.36sk7k5umyh.com	8001	www.hgzhgfx2c.net	91.121.23.100	1
AA4C16D3A43630ECBB0197BE9008DA6C0CC0A77A	CN = www.d2mxnmdqnkl67p2.com	8080	www.viqctg76.net	104.131.11.214	1
AC8130B07AF81FE7189B182006ABD98184F09AD4	CN = www.36sk7k5umyh.com	8001	www.hgzhgfx2c.net	91.121.23.100	1
AF52B46AA62BA3DBE24B64C84DD0F5F1AE22BF32	C = US, ST = Arizona, L = Scottsdale, O = "GoDaddy.com, Inc.", OU = http://certs.godaddy.com/repository/, CN = Go Daddy Secure Certificate Authority - G2	8001	*.cradlepointecm.com	52.25.11.64	1
AF58458B89E8ACB4565C4CD23DB3779E04E84DCF	C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3	6697	tasteless.eu	5.101.101.145	1
B01F0E4E6D87063EC3B32534BF22AAB8718D53BA	CN = www.jnuw2enl.com	12245	www.crso7zgshscrgeqeyj.net	188.165.222.39	1
B3229D66E0FCEA3772444D088D667108FD3EE9C7	CN = 60130107, O = Code42, OU = TEST, ST = MN, C = US	4287	60130107	216.17.8.7	1
B3B97177C153778FA599CEC76829A33871E9CC53	C = KR, O = SDS, CN = SuperCA	35000	self	112.106.134.93	1
B40A2FE4AD5C186B01C2B4C7C1832E7F1423D52B	C = TW, ST = Taiwan, L = Taipei, O = Synology Inc., OU = Certificate Authority, CN = Synology Inc. CA, emailAddress = product@synology.com	53381	synology.com	180.70.88.210	1
B4129A16991698628AF71CB49A93BEBB29105E61	CN = www.d4xtnihuw6b7.com	110	www.fgse5nlq2rl3.net	81.175.221.207	1
B6E4FC5EFC8DF0E1D759BCB11ABAE0C3647D9421	CN = www.bd4whuurora.com	9090	www.aaw42t3duqwbmdxk.net	217.79.190.25	1

Finding Weird SSL Certificate Values

- Detection

```
sourcetype=stream:tcp ssl_cert_sha1=*
| stats VALUES(ssl_issuer) AS ssl_issuer VALUES(ssl_subject_common_name) AS
ssl_subject_common_name VALUES(dest_ip) AS dest_ip
count(ssl_subject_common_name)  AS count BY ssl_cert_sha1
| search count=1
| eval list="*”
|`ut_parse(ssl_subject_common_name,list)`
| lookup alexa-1MM domain AS ut_domain
| fillnull value=NULL rank
| search rank=NULL
| stats VALUES(ssl_cert_sha1) VALUES(ssl_subject_common_name) AS
ssl_subject_common_name VALUES(dest_ip) AS dest_ip values(ut_domain) AS
ut_domain count(ssl_subject_common_name)  AS count BY ssl_issuer
```

Finding Weird SSL Certificate Values



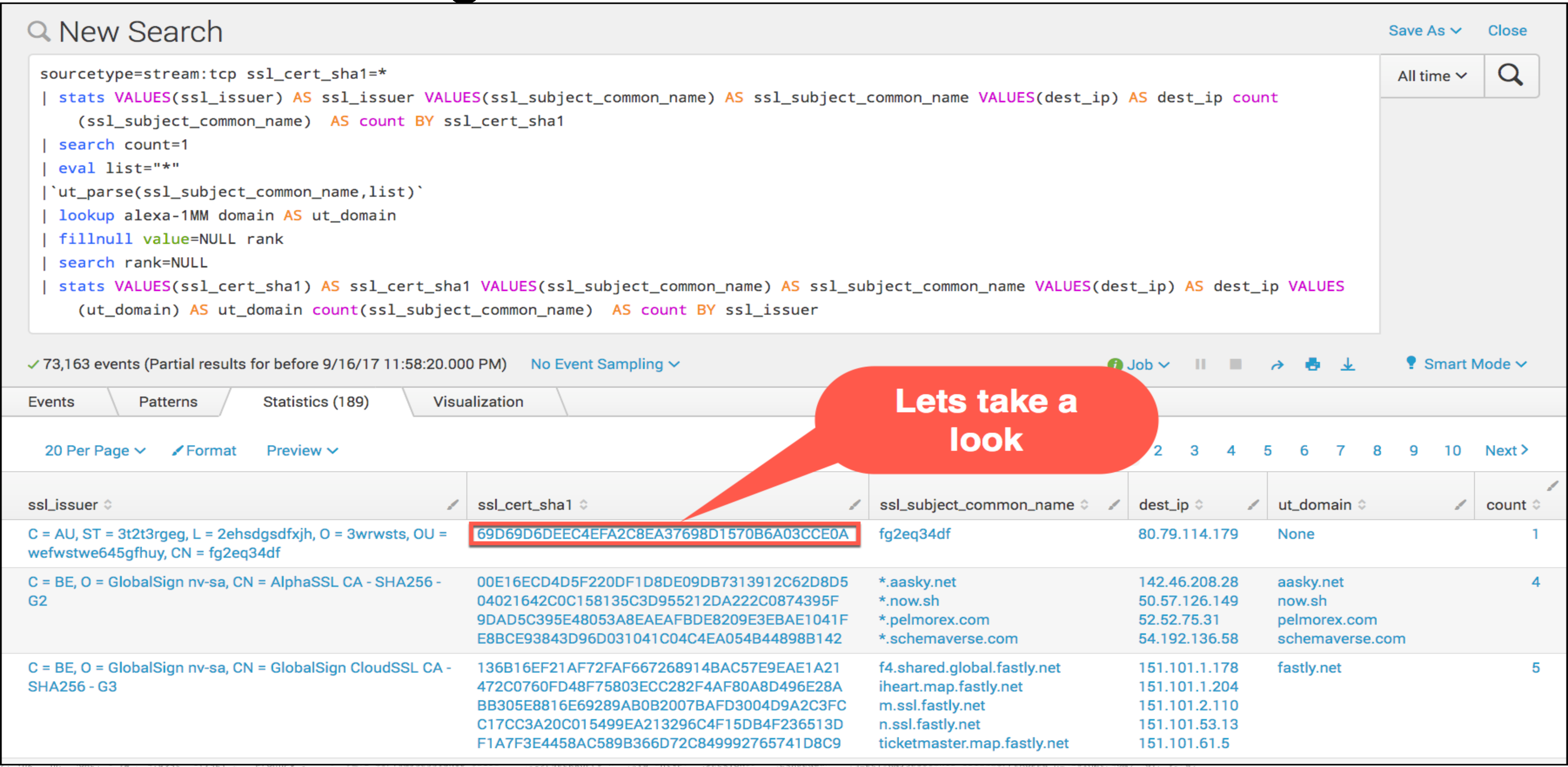
```
sourcetype=stream:tcp ssl_cert_sha1=*
| stats VALUES(ssl_issuer) AS ssl_issuer VALUES(ssl_subject_common_name) AS ssl_subject_common_name VALUES(dest_ip) AS dest_ip count
    (ssl_subject_common_name)  AS count BY ssl_cert_sha1
| search count=1
| eval list="*"
| `ut_parse(ssl_subject_common_name,list)`
| lookup alexa-1MM domain AS ut_domain
| fillnull value=NULL rank
| search rank=NULL
| stats VALUES(ssl_cert_sha1) AS ssl_cert_sha1 VALUES(ssl_subject_common_name) AS ssl_subject_common_name VALUES(dest_ip) AS dest_ip VALUES
    (ut_domain) AS ut_domain count(ssl_subject_common_name)  AS count BY ssl_issuer
```

Additional Lookups

✓ 73,163 events (Partial results for before 9/16/17 11:58:20.000 PM)

ssl_issuer	ssl_cert_sha1	ssl_subject_common_name	dest_ip	ut_domain	count
C = AU, ST = 3t2t3rgeg, L = 2ehsdgsdfxjh, O = 3wrwsts, OU = wefwstwe645gfhuy, CN = fg2eq34df	69D69D6DEEC4EFA2C8EA37698D1570B6A03CCE0A	fg2eq34df	80.79.114.179	None	1
C = BE, O = GlobalSign nv-sa, CN = AlphaSSL CA - SHA256 - G2	00E16ECD4D5F220DF1D8DE09DB7313912C62D8D5 04021642C0C158135C3D955212DA222C0874395F 9DAD5C395E48053A8EAEAFBDE8209E3EBAE1041F E8BCE93843D96D031041C04C4EA054B44898B142	*.aasky.net *.now.sh *.pelmorex.com *.schemaverse.com	142.46.208.28 50.57.126.149 52.52.75.31 54.192.136.58	aasky.net now.sh pelmorex.com schemaverse.com	4
C = BE, O = GlobalSign nv-sa, CN = GlobalSign CloudSSL CA - SHA256 - G3	136B16EF21AF72FAF667268914BAC57E9EAE1A21 472C0760FD48F75803ECC282F4AF80A8D496E28A BB305E8816E69289AB0B2007BAFD3004D9A2C3FC C17CC3A20C015499EA213296C4F15DB4F236513D F1A7F3E4458AC589B366D72C849992765741D8C9	f4.shared.global.fastly.net iheart.map.fastly.net m.ssl.fastly.net n.ssl.fastly.net ticketmaster.map.fastly.net	151.101.1.178 151.101.1.204 151.101.2.110 151.101.53.13 151.101.61.5	fastly.net	5

Finding Weird SSL Certificate Values



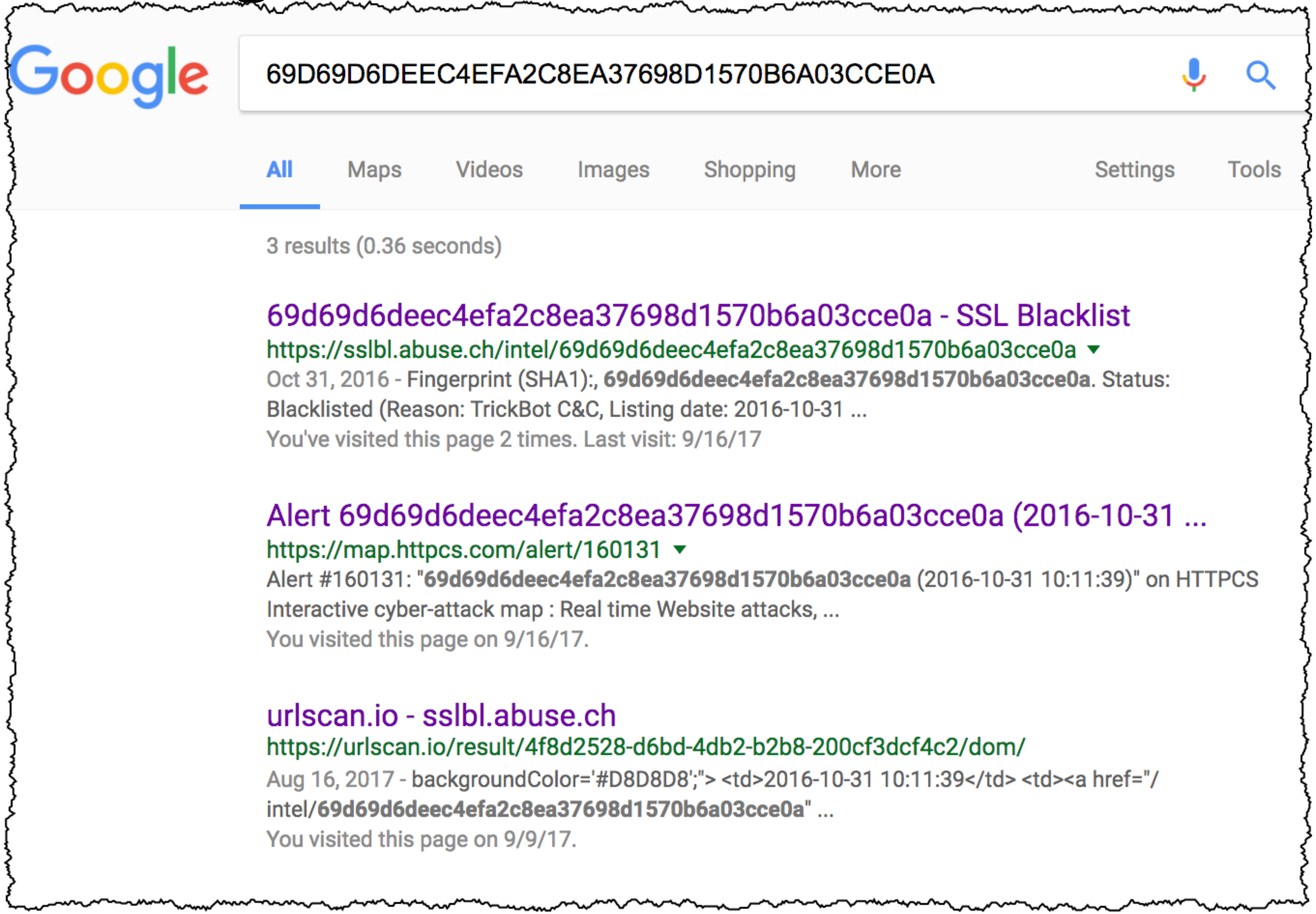
```
sourcetype=stream:tcp ssl_cert_sha1=*
| stats VALUES(ssl_issuer) AS ssl_issuer VALUES(ssl_subject_common_name) AS ssl_subject_common_name VALUES(dest_ip) AS dest_ip count
    (ssl_subject_common_name)  AS count BY ssl_cert_sha1
| search count=1
| eval list="*"
|`ut_parse(ssl_subject_common_name,list)`
| lookup alexa-1MM domain AS ut_domain
| fillnull value=NULL rank
| search rank=NULL
| stats VALUES(ssl_cert_sha1) AS ssl_cert_sha1 VALUES(ssl_subject_common_name) AS ssl_subject_common_name VALUES(dest_ip) AS dest_ip VALUES
    (ut_domain) AS ut_domain count(ssl_subject_common_name)  AS count BY ssl_issuer
```

✓ 73,163 events (Partial results for before 9/16/17 11:58:20.000 PM) No Event Sampling

Lets take a look

ssl_issuer	ssl_cert_sha1	ssl_subject_common_name	dest_ip	ut_domain	count
C = AU, ST = 3t2t3rgeg, L = 2ehsdgsdfxjh, O = 3wrwsts, OU = wefwstwe645gfhuy, CN = fg2eq34df	69D69D6DEEC4EFA2C8EA37698D1570B6A03CCE0A	fg2eq34df	80.79.114.179	None	1
C = BE, O = GlobalSign nv-sa, CN = AlphaSSL CA - SHA256 - G2	00E16ECD4D5F220DF1D8DE09DB7313912C62D8D5 04021642C0C158135C3D955212DA222C0874395F 9DAD5C395E48053A8EAEAFBDE8209E3EBAE1041F E8BCE93843D96D031041C04C4EA054B44898B142	*.aasky.net *.now.sh *.pelmorex.com *.schemaverse.com	142.46.208.28 50.57.126.149 52.52.75.31 54.192.136.58	aasky.net now.sh pelmorex.com schemaverse.com	4
C = BE, O = GlobalSign nv-sa, CN = GlobalSign CloudSSL CA - SHA256 - G3	136B16EF21AF72FAF667268914BAC57E9EAE1A21 472C0760FD48F75803ECC282F4AF80A8D496E28A BB305E8816E69289AB0B2007BAFD3004D9A2C3FC C17CC3A20C015499EA213296C4F15DB4F236513D F1A7F3E4458AC589B366D72C849992765741D8C9	f4.shared.global.fastly.net iheart.map.fastly.net m.ssl.fastly.net n.ssl.fastly.net ticketmaster.map.fastly.net	151.101.1.178 151.101.1.204 151.101.2.110 151.101.53.13 151.101.61.5	fastly.net	5

Finding Weird SSL Certificate Values



69D69D6DEEC4EFA2C8EA37698D1570B6A03CCE0A

3 results (0.36 seconds)

69d69d6deec4efa2c8ea37698d1570b6a03cce0a - SSL Blacklist
https://sslbl.abuse.ch/intel/69d69d6deec4efa2c8ea37698d1570b6a03cce0a
Oct 31, 2016 - Fingerprint (SHA1):, **69d69d6deec4efa2c8ea37698d1570b6a03cce0a**. Status: Blacklisted (Reason: TrickBot C&C, Listing date: 2016-10-31 ...
You've visited this page 2 times. Last visit: 9/16/17

Alert 69d69d6deec4efa2c8ea37698d1570b6a03cce0a (2016-10-31 ...
https://map.httpcs.com/alert/160131
Alert #160131: "**69d69d6deec4efa2c8ea37698d1570b6a03cce0a** (2016-10-31 10:11:39)" on HTTPCS Interactive cyber-attack map : Real time Website attacks, ...
You visited this page on 9/16/17.

urlscan.io - sslbl.abuse.ch
https://urlscan.io/result/4f8d2528-d6bd-4db2-b2b8-200cf3dcf4c2/dom/
Aug 16, 2017 - backgroundColor='#D8D8D8';"> <td>2016-10-31 10:11:39</td> <td><a href="/intel/**69d69d6deec4efa2c8ea37698d1570b6a03cce0a**" ...
You visited this page on 9/9/17.

SSL Certificates

ssl_issuer

ssl_cert_sh1

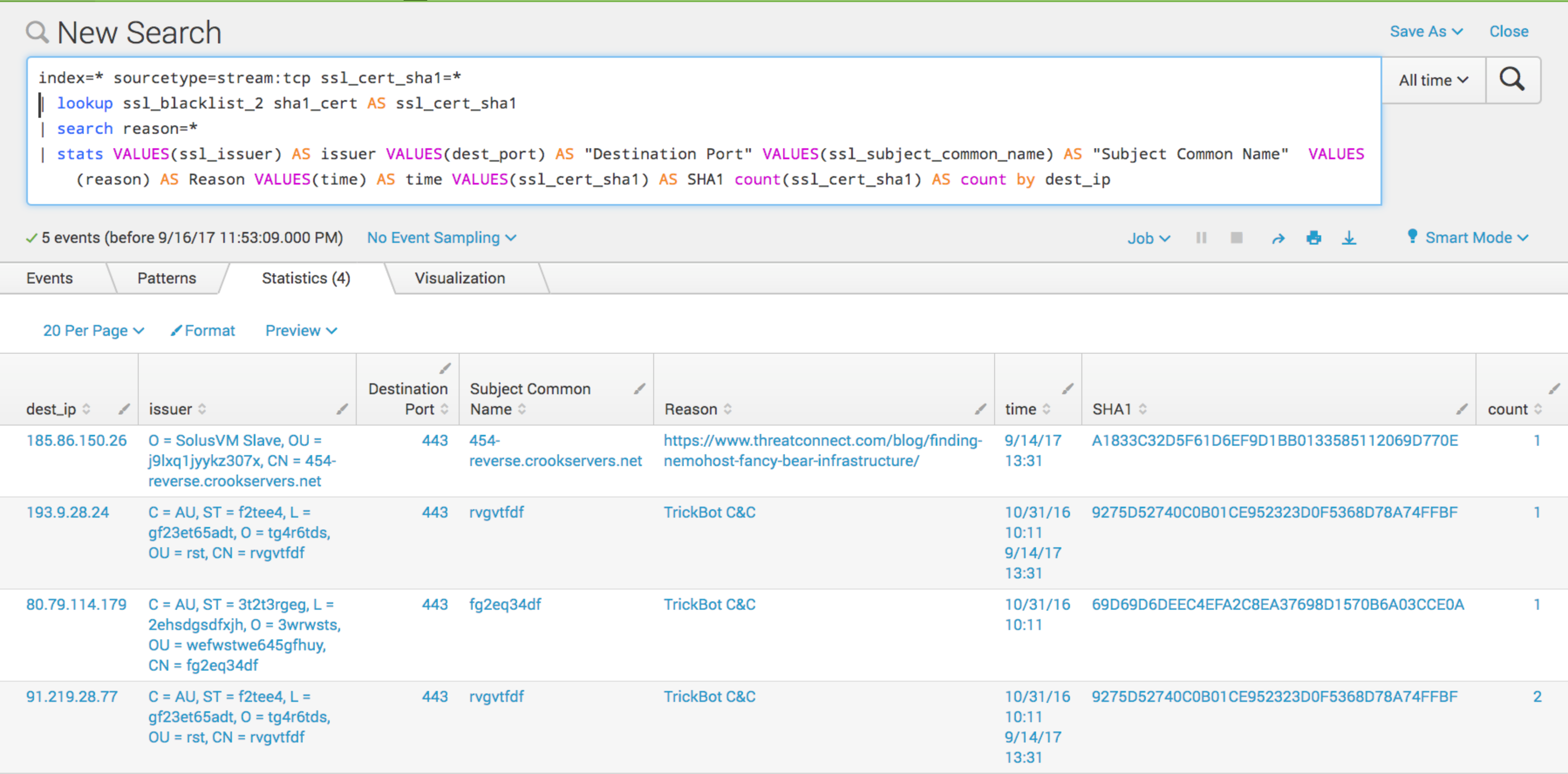
ssl_subject_org

Finding SSL Certificates On A Black List

- Detection

```
index=* sourcetype=stream:tcp ssl_cert_sha1=*
| lookup ssl_block_list sha1_cert AS ssl_cert_sha1
| search reason=*
| stats VALUES(ssl_issuer) AS issuer VALUES(dest_port) AS "Destination
Port" VALUES(ssl_subject_common_name) AS "Subject Common Name"
VALUES(reason) AS Reason  VALUES(ssl_cert_sha1) AS SHA1
count(ssl_cert_sha1) AS count by dest_ip
```

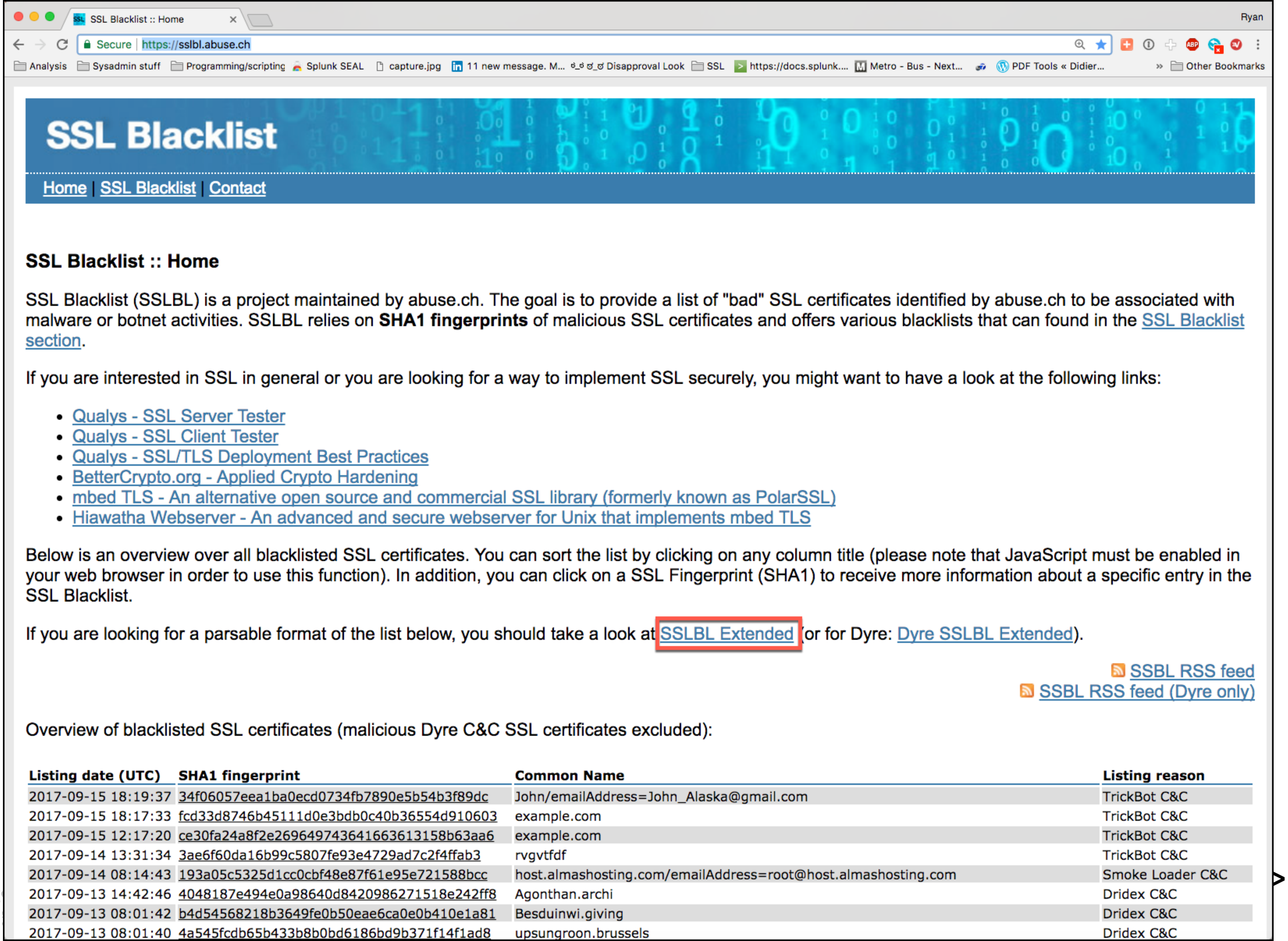
Finding SSL Certificates On A Black List



```
index=* sourcetype=stream:tcp ssl_cert_sha1=*
| lookup ssl_blacklist_2 sha1_cert AS ssl_cert_sha1
| search reason=*
| stats VALUES(ssl_issuer) AS issuer VALUES(dest_port) AS "Destination Port" VALUES(ssl_subject_common_name) AS "Subject Common Name"  VALUES
   (reason) AS Reason VALUES(time) AS time VALUES(ssl_cert_sha1) AS SHA1 count(ssl_cert_sha1) AS count by dest_ip
```

✓ 5 events (before 9/16/17 11:53:09.000 PM)

dest_ip	issuer	Destination Port	Subject Common Name	Reason	time	SHA1	count
185.86.150.26	O = SolusVM Slave, OU = j9lxq1jyykz307x, CN = 454-reverse.crookservers.net	443	454-reverse.crookservers.net	https://www.threatconnect.com/blog/finding-nemohost-fancy-bear-infrastructure/	9/14/17 13:31	A1833C32D5F61D6EF9D1BB0133585112069D770E	1
193.9.28.24	C = AU, ST = f2tee4, L = gf23et65adt, O = tg4r6tds, OU = rst, CN = rvgvtfdf	443	rvgvtfdf	TrickBot C&C	10/31/16 10:11 9/14/17 13:31	9275D52740C0B01CE952323D0F5368D78A74FFBF	1
80.79.114.179	C = AU, ST = 3t2t3rgeg, L = 2ehsdgsdfxjh, O = 3wrwsts, OU = wefwstwe645gfhuy, CN = fg2eq34df	443	fg2eq34df	TrickBot C&C	10/31/16 10:11	69D69D6DEEC4EFA2C8EA37698D1570B6A03CCE0A	1
91.219.28.77	C = AU, ST = f2tee4, L = gf23et65adt, O = tg4r6tds, OU = rst, CN = rvgvtfdf	443	rvgvtfdf	TrickBot C&C	10/31/16 10:11 9/14/17 13:31	9275D52740C0B01CE952323D0F5368D78A74FFBF	2



SSL Blacklist

Home | SSL Blacklist | Contact

SSL Blacklist :: Home

SSL Blacklist (SSLBL) is a project maintained by abuse.ch. The goal is to provide a list of "bad" SSL certificates identified by abuse.ch to be associated with malware or botnet activities. SSLBL relies on **SHA1 fingerprints** of malicious SSL certificates and offers various blacklists that can found in the SSL Blacklist section.

If you are interested in SSL in general or you are looking for a way to implement SSL securely, you might want to have a look at the following links:

- Qualys - SSL Server Tester
- Qualys - SSL Client Tester
- Qualys - SSL/TLS Deployment Best Practices
- BetterCrypto.org - Applied Crypto Hardening
- mbed TLS - An alternative open source and commercial SSL library (formerly known as PolarSSL)
- Hiawatha Webserver - An advanced and secure webserver for Unix that implements mbed TLS

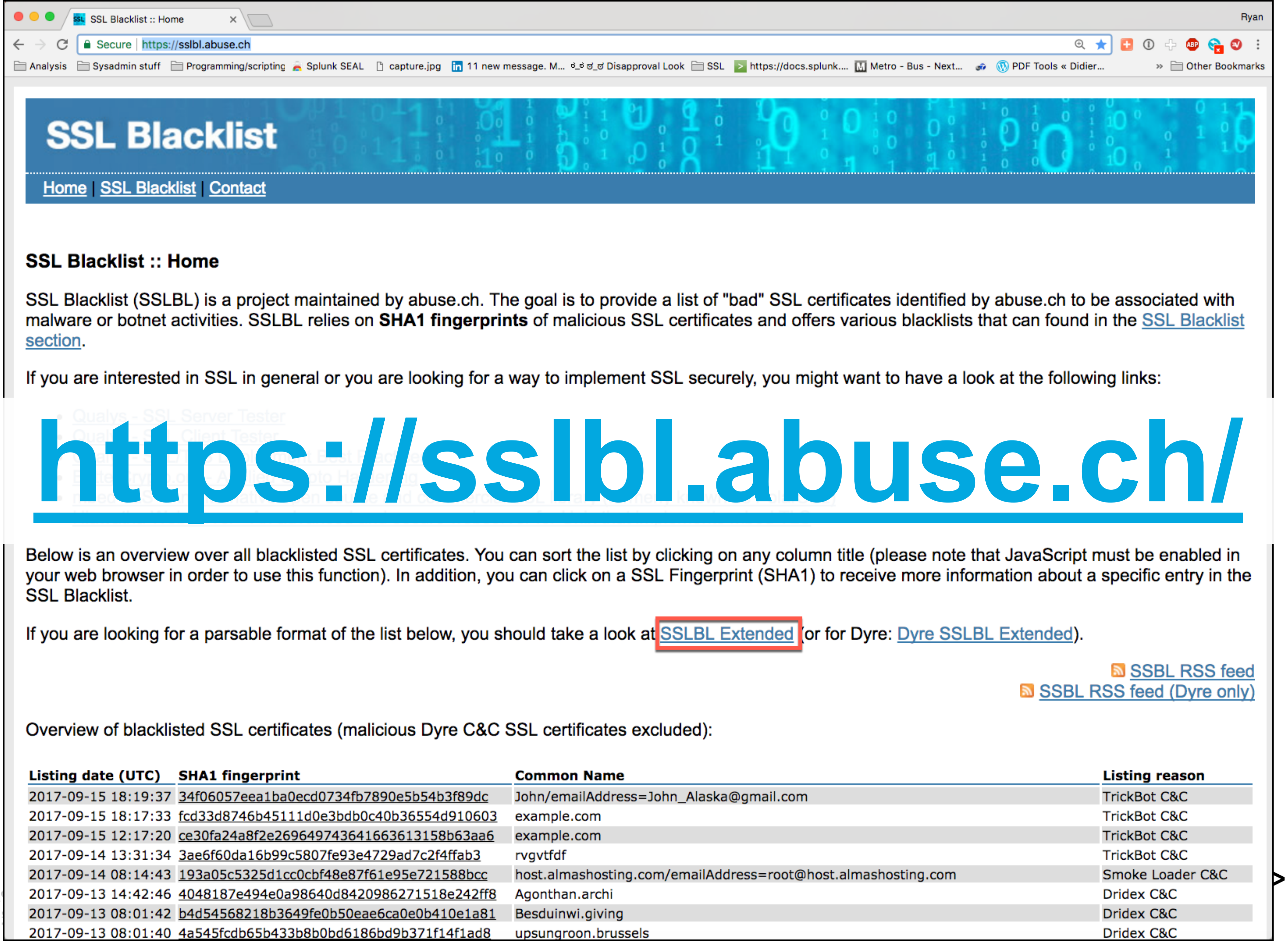
Below is an overview over all blacklisted SSL certificates. You can sort the list by clicking on any column title (please note that JavaScript must be enabled in your web browser in order to use this function). In addition, you can click on a SSL Fingerprint (SHA1) to receive more information about a specific entry in the SSL Blacklist.

If you are looking for a parsable format of the list below, you should take a look at SSLBL Extended (or for Dyre: Dyre SSLBL Extended).

SSBL RSS feed
SSBL RSS feed (Dyre only)

Overview of blacklisted SSL certificates (malicious Dyre C&C SSL certificates excluded):

Listing date (UTC)	SHA1 fingerprint	Common Name	Listing reason
2017-09-15 18:19:37	34f06057eea1ba0ecd0734fb7890e5b54b3f89dc	John/emailAddress=John_Alaska@gmail.com	TrickBot C&C
2017-09-15 18:17:33	fcd33d8746b45111d0e3bdb0c40b36554d910603	example.com	TrickBot C&C
2017-09-15 12:17:20	ce30fa24a8f2e269649743641663613158b63aa6	example.com	TrickBot C&C
2017-09-14 13:31:34	3ae6f60da16b99c5807fe93e4729ad7c2f4ffab3	rvgvtfdf	TrickBot C&C
2017-09-14 08:14:43	193a05c5325d1cc0cbf48e87f61e95e721588bcc	host.almashosting.com/emailAddress=root@host.almashosting.com	Smoke Loader C&C
2017-09-13 14:42:46	4048187e494e0a98640d8420986271518e242ff8	Agonthan.archi	Dridex C&C
2017-09-13 08:01:42	b4d54568218b3649fe0b50eae6ca0e0b410e1a81	Besduinwi.giving	Dridex C&C
2017-09-13 08:01:40	4a545fcdb65b433b8b0bd6186bd9b371f14f1ad8	upsungroon.brussels	Dridex C&C



SSL Blacklist

Home | SSL Blacklist | Contact

SSL Blacklist :: Home

SSL Blacklist (SSLBL) is a project maintained by abuse.ch. The goal is to provide a list of "bad" SSL certificates identified by abuse.ch to be associated with malware or botnet activities. SSLBL relies on **SHA1 fingerprints** of malicious SSL certificates and offers various blacklists that can found in the SSL Blacklist section.

If you are interested in SSL in general or you are looking for a way to implement SSL securely, you might want to have a look at the following links:

https://sslbl.abuse.ch/

Below is an overview over all blacklisted SSL certificates. You can sort the list by clicking on any column title (please note that JavaScript must be enabled in your web browser in order to use this function). In addition, you can click on a SSL Fingerprint (SHA1) to receive more information about a specific entry in the SSL Blacklist.

If you are looking for a parsable format of the list below, you should take a look at SSLBL Extended (or for Dyre: Dyre SSLBL Extended).

SSBL RSS feed
SSBL RSS feed (Dyre only)

Overview of blacklisted SSL certificates (malicious Dyre C&C SSL certificates excluded):

Listing date (UTC)	SHA1 fingerprint	Common Name	Listing reason
2017-09-15 18:19:37	34f06057eea1ba0ecd0734fb7890e5b54b3f89dc	John/emailAddress=John_Alaska@gmail.com	TrickBot C&C
2017-09-15 18:17:33	fcd33d8746b45111d0e3bdb0c40b36554d910603	example.com	TrickBot C&C
2017-09-15 12:17:20	ce30fa24a8f2e269649743641663613158b63aa6	example.com	TrickBot C&C
2017-09-14 13:31:34	3ae6f60da16b99c5807fe93e4729ad7c2f4ffab3	rvgvtfdf	TrickBot C&C
2017-09-14 08:14:43	193a05c5325d1cc0cbf48e87f61e95e721588bcc	host.almashosting.com/emailAddress=root@host.almashosting.com	Smoke Loader C&C
2017-09-13 14:42:46	4048187e494e0a98640d8420986271518e242ff8	Agonthan.archi	Dridex C&C
2017-09-13 08:01:42	b4d54568218b3649fe0b50eae6ca0e0b410e1a81	Besduinwi.giving	Dridex C&C
2017-09-13 08:01:40	4a545fcdb65b433b8b0bd6186bd9b371f14f1ad8	upsungroon.brussels	Dridex C&C

Credit Card
1234 5678 9012 3456
1234
08/13 VALID DATES 08/17
RRENT NAME
Card

Mark Parsons
“Lord of SSL Pivoting”

@markpars0ns

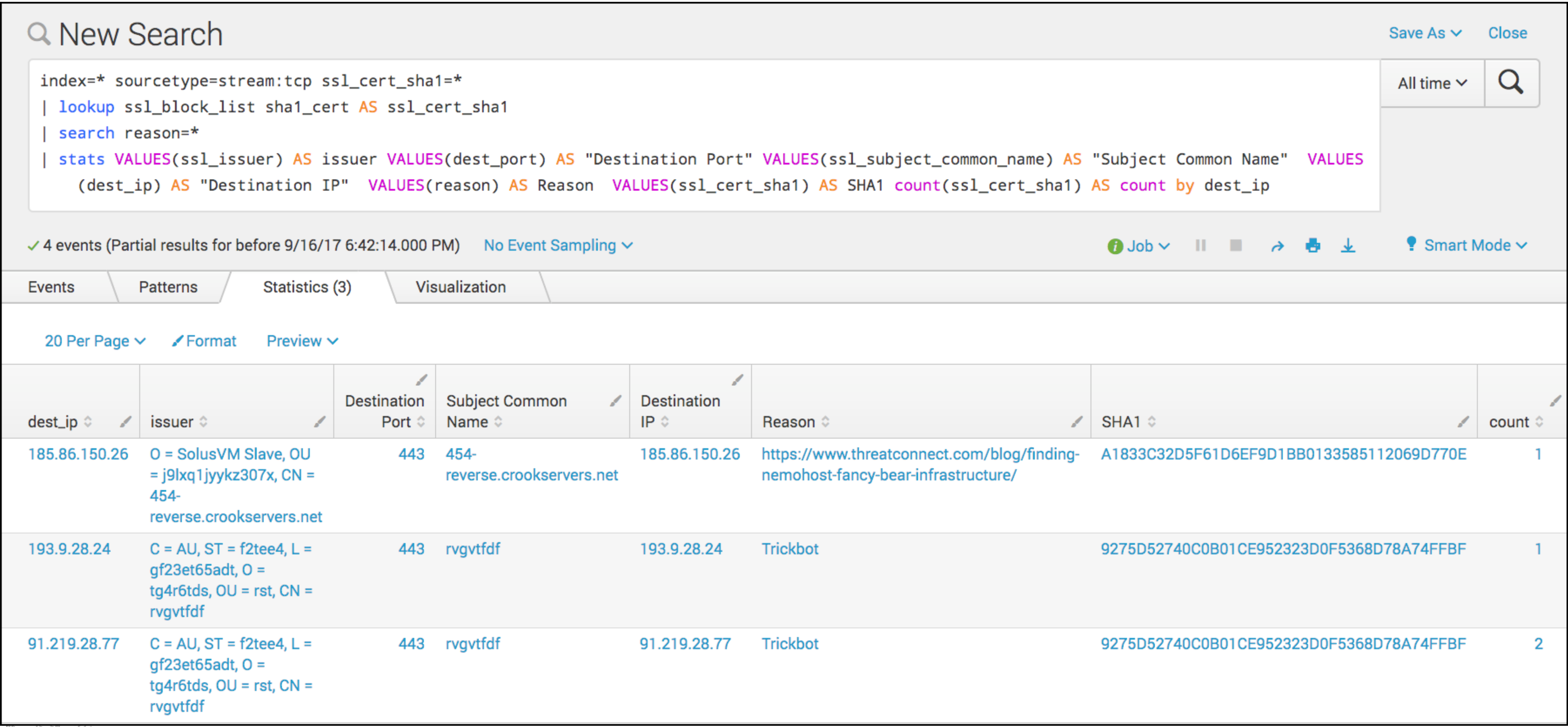
- https://t.co/amyR9pU8o4
- https://medium.com/@mark.parsons/hunting-a-tls-certificate-series-post-1-6ad7adfebe44
- https://mpars0ns.github.io/bsidescharm-2016slides/
- https://mpars0ns.github.io/archc0n-2016-tls-slides/#/

Pivoting On SSL Certificates With Censys.Io

- **Hunting**

```
workflow_action.conf
[censys]
#requires user to already be logged in
display_location = both
fields = ssl_cert_sha1, ssl_cert_md5,
ssl_cert_sha256,ssl_issuer,ssl_serialnumber
label = Censys.io cert: ($@field_value$)
link.method = get
link.uri = http://censys.io/ipv4?q=$@field_value$
link.target = blank
type = link
```

Pivoting On SSL Certificates With Censys.Io

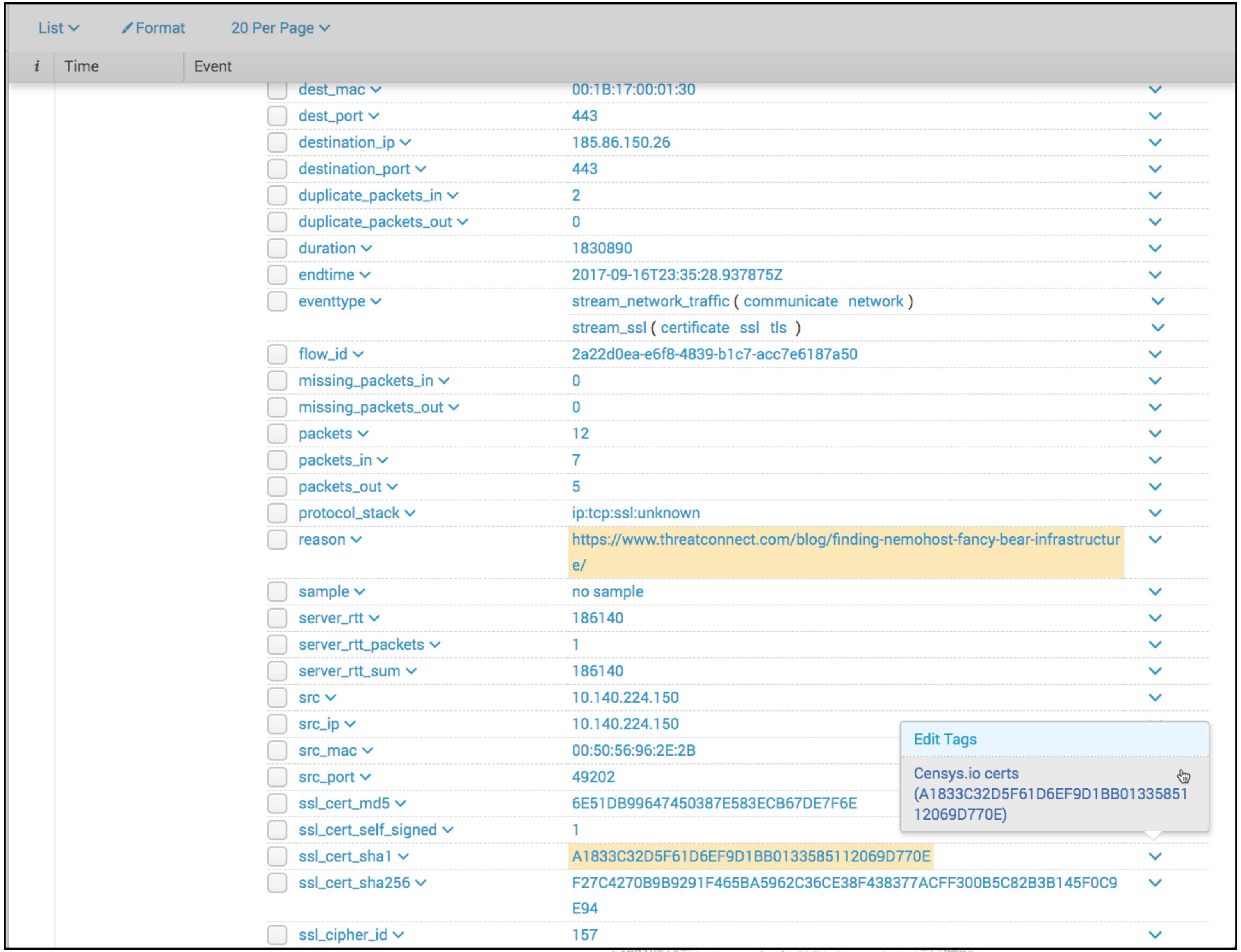


```
index=* sourcetype=stream:tcp ssl_cert_sha1=*
| lookup ssl_block_list sha1_cert AS ssl_cert_sha1
| search reason=*
| stats VALUES(ssl_issuer) AS issuer VALUES(dest_port) AS "Destination Port" VALUES(ssl_subject_common_name) AS "Subject Common Name"  VALUES
   (dest_ip) AS "Destination IP"  VALUES(reason) AS Reason  VALUES(ssl_cert_sha1) AS SHA1 count(ssl_cert_sha1) AS count by dest_ip
```

✓ 4 events (Partial results for before 9/16/17 6:42:14.000 PM)

dest_ip	issuer	Destination Port	Subject Common Name	Destination IP	Reason	SHA1	count
185.86.150.26	O = SolusVM Slave, OU = j9lxq1jyykz307x, CN = 454-reverse.crookservers.net	443	454-reverse.crookservers.net	185.86.150.26	https://www.threatconnect.com/blog/finding-nemohost-fancy-bear-infrastructure/	A1833C32D5F61D6EF9D1BB0133585112069D770E	1
193.9.28.24	C = AU, ST = f2tee4, L = gf23et65adt, O = tg4r6tds, OU = rst, CN = rvgvtfdf	443	rvgvtfdf	193.9.28.24	Trickbot	9275D52740C0B01CE952323D0F5368D78A74FFBF	1
91.219.28.77	C = AU, ST = f2tee4, L = gf23et65adt, O = tg4r6tds, OU = rst, CN = rvgvtfdf	443	rvgvtfdf	91.219.28.77	Trickbot	9275D52740C0B01CE952323D0F5368D78A74FFBF	2

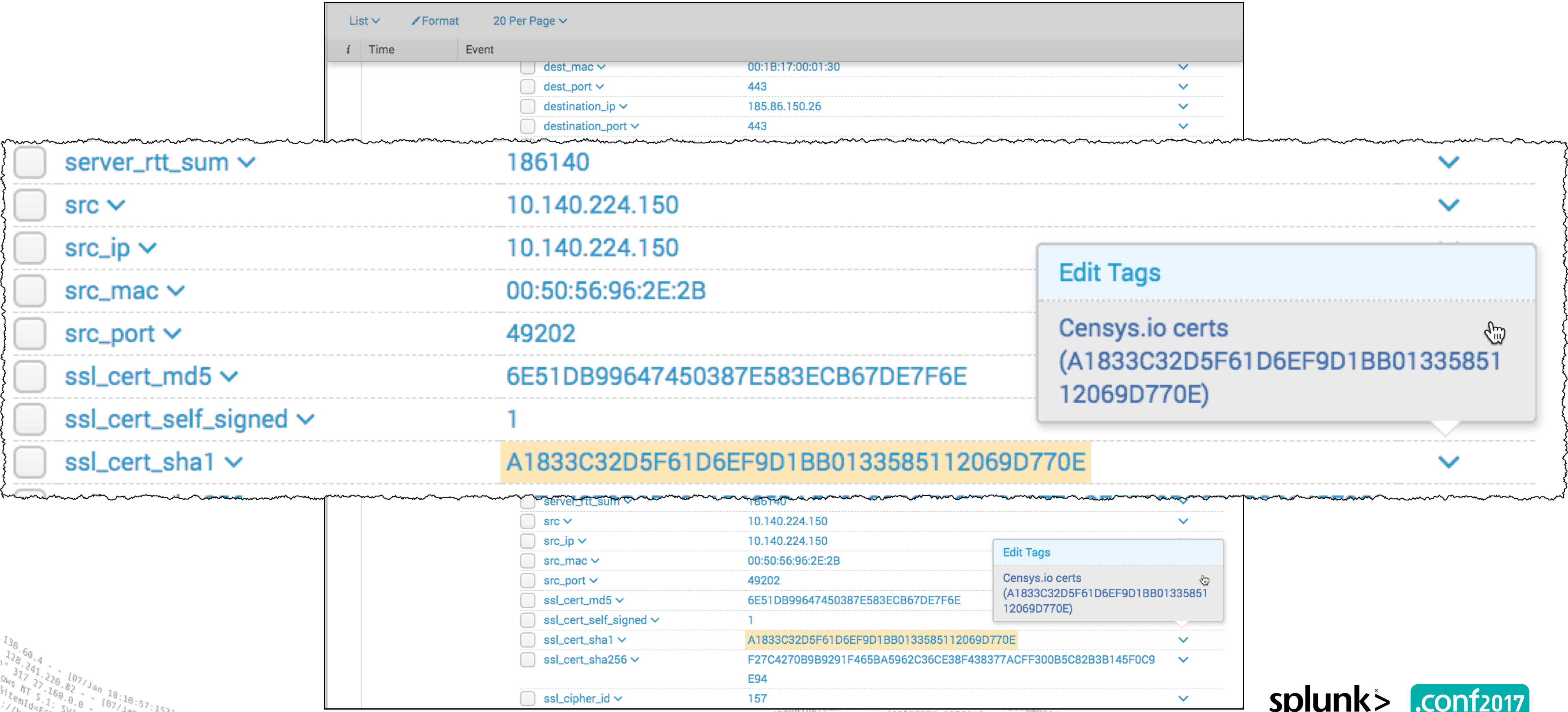
Pivoting On SSL Certificates With Censys.Io



□ dest_mac	00:1B:17:00:01:30
□ dest_port	443
□ destination_ip	185.86.150.26
□ destination_port	443
□ duplicate_packets_in	2
□ duplicate_packets_out	0
□ duration	1830890
□ endtime	2017-09-16T23:35:28.937875Z
□ eventtype	stream_network_traffic (communicate network) stream_ssl (certificate ssl tls)
□ flow_id	2a22d0ea-e6f8-4839-b1c7-acc7e6187a50
□ missing_packets_in	0
□ missing_packets_out	0
□ packets	12
□ packets_in	7
□ packets_out	5
□ protocol_stack	ip:tcp:ssl:unknown
□ reason	https://www.threatconnect.com/blog/finding-nemohost-fancy-bear-infrastructure/
□ sample	no sample
□ server_rtt	186140
□ server_rtt_packets	1
□ server_rtt_sum	186140
□ src	10.140.224.150
□ src_ip	10.140.224.150
□ src_mac	00:50:56:96:2E:2B
□ src_port	49202
□ ssl_cert_md5	6E51DB99647450387E583ECB67DE7F6E
□ ssl_cert_self_signed	1
□ ssl_cert_sha1	A1833C32D5F61D6EF9D1BB0133585112069D770E
□ ssl_cert_sha256	F27C4270B9B9291F465BA5962C36CE38F438377ACFF300B5C82B3B145F0C9E94
□ ssl_cipher_id	157

Censys.io certs (A1833C32D5F61D6EF9D1BB0133585112069D770E)

Pivoting On SSL Certificates With Censys.Io



dest_mac	00:1B:17:00:01:30
dest_port	443
destination_ip	185.86.150.26
destination_port	443
server_rtt_sum	186140
src	10.140.224.150
src_ip	10.140.224.150
src_mac	00:50:56:96:2E:2B
src_port	49202
ssl_cert_md5	6E51DB99647450387E583ECB67DE7F6E
ssl_cert_self_signed	1
ssl_cert_sha1	A1833C32D5F61D6EF9D1BB0133585112069D770E
ssl_cert_sha256	F27C4270B9B9291F465BA5962C36CE38F438377ACFF300B5C82B3B145F0C9E94
ssl_cipher_id	157

Edit Tags

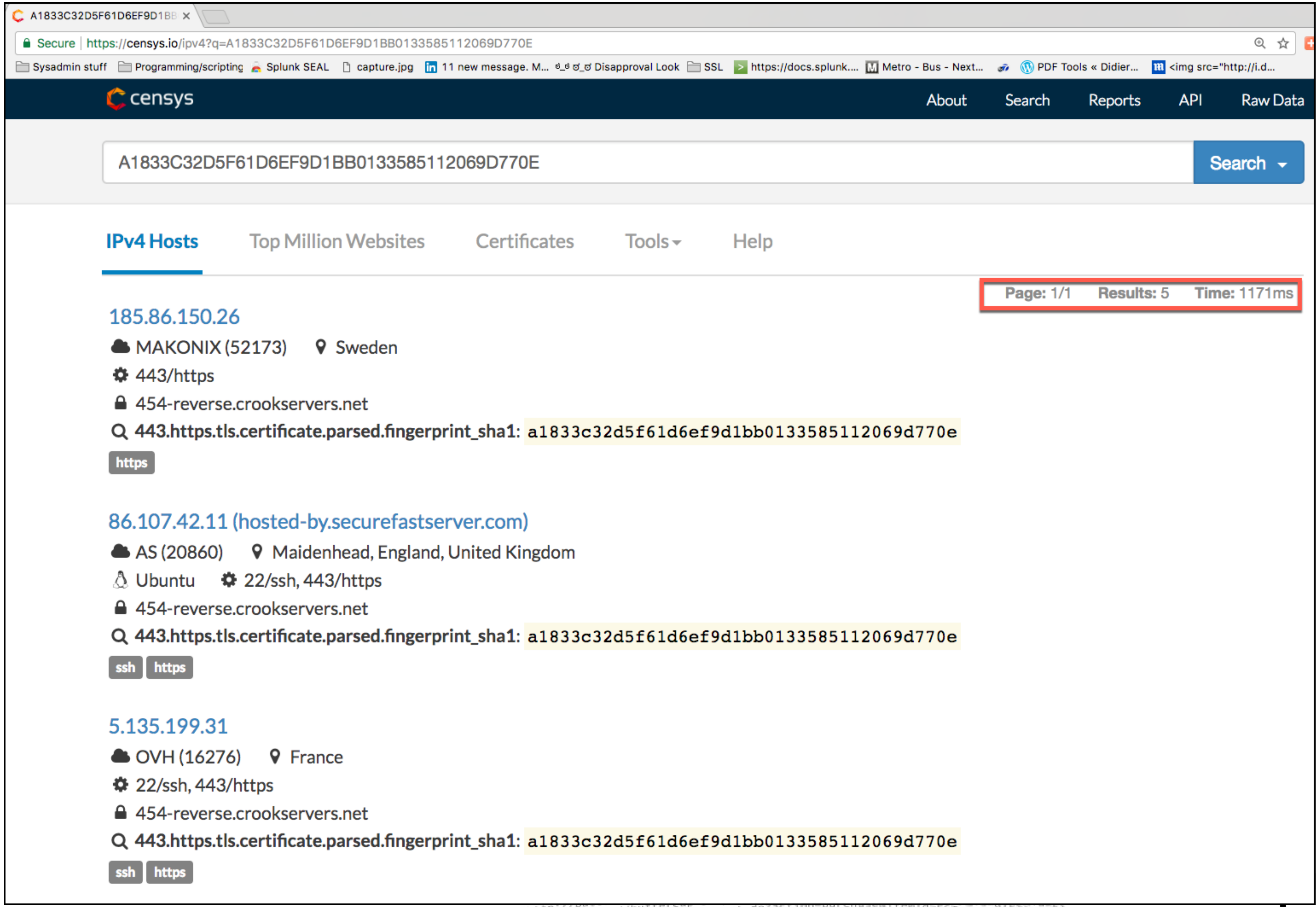
Censys.io certs (A1833C32D5F61D6EF9D1BB0133585112069D770E)

server_rtt_sum	186140
src	10.140.224.150
src_ip	10.140.224.150
src_mac	00:50:56:96:2E:2B
src_port	49202
ssl_cert_md5	6E51DB99647450387E583ECB67DE7F6E
ssl_cert_self_signed	1
ssl_cert_sha1	A1833C32D5F61D6EF9D1BB0133585112069D770E

Edit Tags

Censys.io certs (A1833C32D5F61D6EF9D1BB0133585112069D770E)

Pivoting On SSL Certificates With Censys.Io



Page: 1/1 **Results:** 5 **Time:** 1171ms

185.86.150.26
MAKONIX (52173) Sweden
443/https
454-reverse.crookservers.net
443.https.tls.certificate.parsed.fingerprint_sha1: `a1833c32d5f61d6ef9d1bb0133585112069d770e`
https

86.107.42.11 (hosted-by.securefastserver.com)
AS (20860) Maidenhead, England, United Kingdom
Ubuntu 22/ssh, 443/https
454-reverse.crookservers.net
443.https.tls.certificate.parsed.fingerprint_sha1: `a1833c32d5f61d6ef9d1bb0133585112069d770e`
ssh https

5.135.199.31
OVH (16276) France
22/ssh, 443/https
454-reverse.crookservers.net
443.https.tls.certificate.parsed.fingerprint_sha1: `a1833c32d5f61d6ef9d1bb0133585112069d770e`
ssh https

HUNTING THREAT ACTORS WITH TLS CERTIFICATES

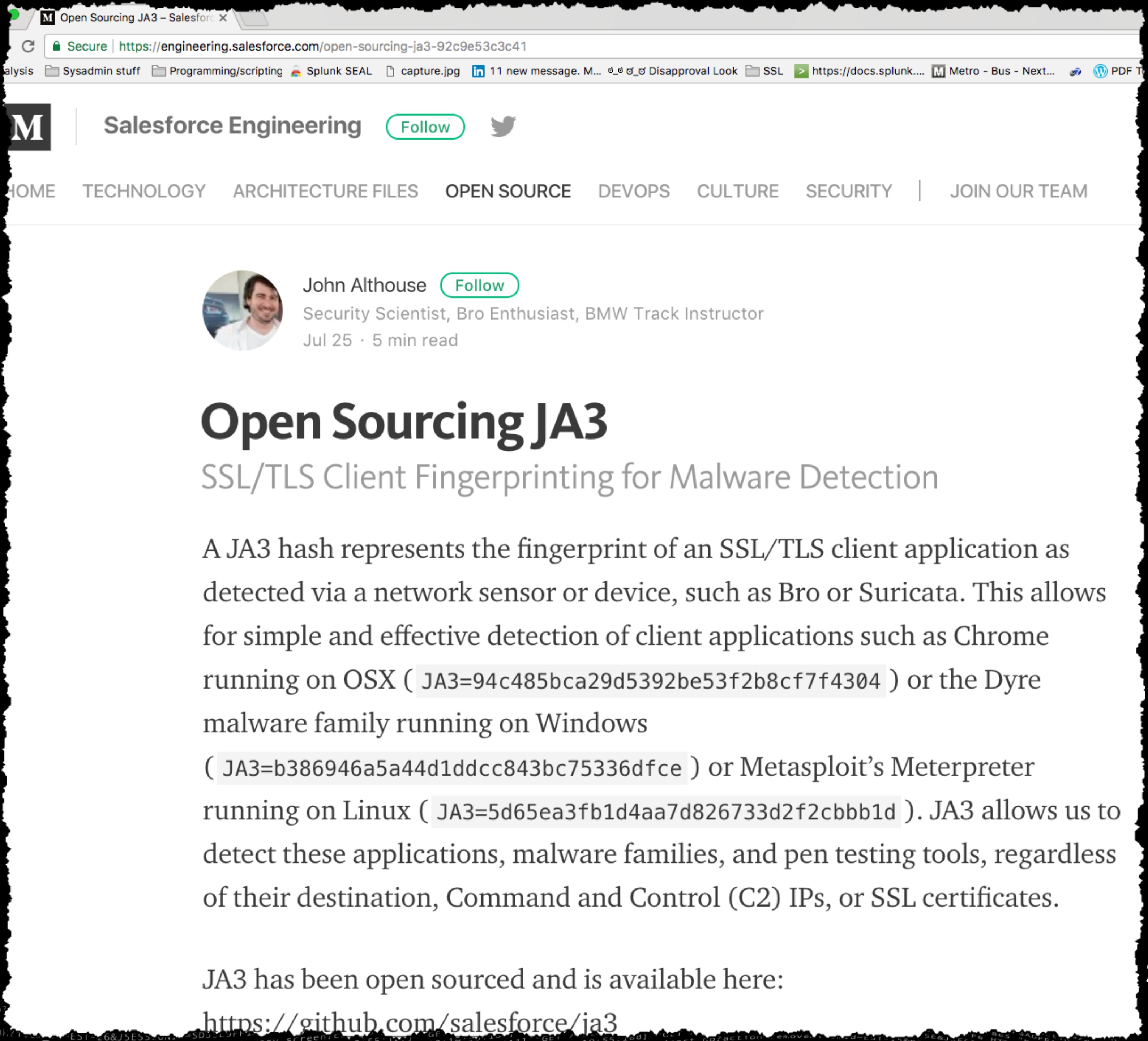
USING OPEN SOURCE DATA TO DEFEND NETWORKS

Mark Parsons / @markpars0ns / mark at accessviolation.org

JA3

SSLVersion,Ciphers,Extensions,EllipticCurves,EllipticCurvePointFormats

SSL Handshakes



John Althouse Follow
Security Scientist, Bro Enthusiast, BMW Track Instructor
Jul 25 · 5 min read

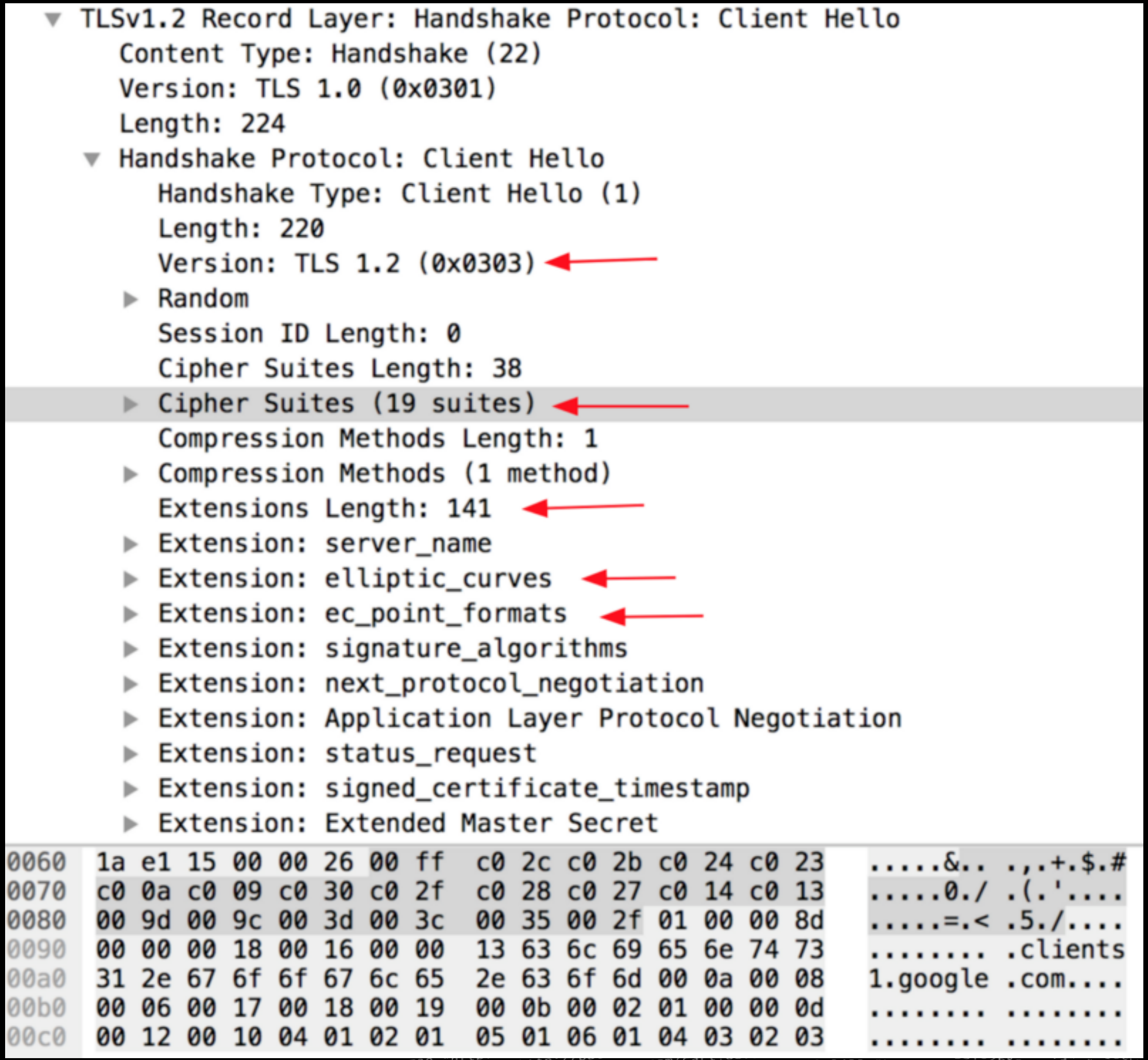
Open Sourcing JA3

SSL/TLS Client Fingerprinting for Malware Detection

A JA3 hash represents the fingerprint of an SSL/TLS client application as detected via a network sensor or device, such as Bro or Suricata. This allows for simple and effective detection of client applications such as Chrome running on OSX (`JA3=94c485bca29d5392be53f2b8cf7f4304`) or the Dyre malware family running on Windows (`JA3=b386946a5a44d1ddcc843bc75336dfce`) or Metasploit's Meterpreter running on Linux (`JA3=5d65ea3fb1d4aa7d826733d2f2cbbb1d`). JA3 allows us to detect these applications, malware families, and pen testing tools, regardless of their destination, Command and Control (C2) IPs, or SSL certificates.

JA3 has been open sourced and is available here: https://github.com/salesforce/ja3

SSLVersion, Ciphers, Extensions, EllipticCurves, EllipticCurve PointFormats



```
▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 224
  ▼ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 220
      Version: TLS 1.2 (0x0303)
    ▶ Random
      Session ID Length: 0
      Cipher Suites Length: 38
    ▶ Cipher Suites (19 suites)
      Compression Methods Length: 1
    ▶ Compression Methods (1 method)
      Extensions Length: 141
    ▶ Extension: server_name
    ▶ Extension: elliptic_curves
    ▶ Extension: ec_point_formats
    ▶ Extension: signature_algorithms
    ▶ Extension: next_protocol_negotiation
    ▶ Extension: Application Layer Protocol Negotiation
    ▶ Extension: status_request
    ▶ Extension: signed_certificate_timestamp
    ▶ Extension: Extended Master Secret
0060  1a e1 15 00 00 26 00 ff  c0 2c c0 2b c0 24 c0 23   .....&.. .,.+.$.#
0070  c0 0a c0 09 c0 30 c0 2f  c0 28 c0 27 c0 14 c0 13   .....0./ .(.'....
0080  00 9d 00 9c 00 3d 00 3c  00 35 00 2f 01 00 00 8d   .....=.< .5./....
0090  00 00 00 18 00 16 00 00  13 63 6c 69 65 6e 74 73   ........ .clients
00a0  31 2e 67 6f 6f 67 6c 65  2e 63 6f 6d 00 0a 00 08   1.google .com....
00b0  00 06 00 17 00 18 00 19  00 0b 00 02 01 00 00 0d   ........ ........
00c0  00 12 00 10 04 01 02 01  05 01 06 01 04 03 02 03   ........ ........
```

OK. Why do I care?

SSL cert hash doesn’t matter

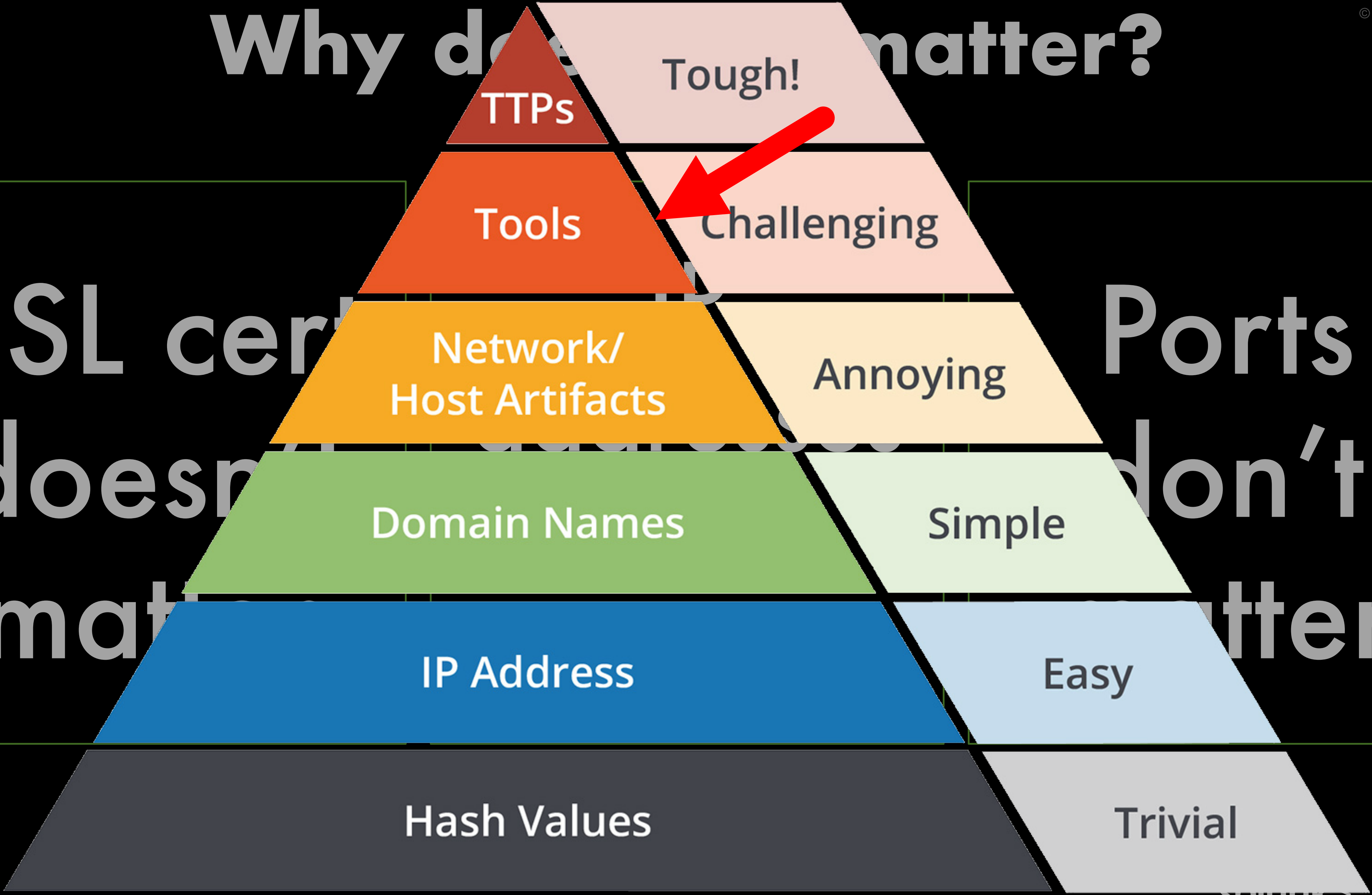
IP addresses don’t matter

Ports don’t matter

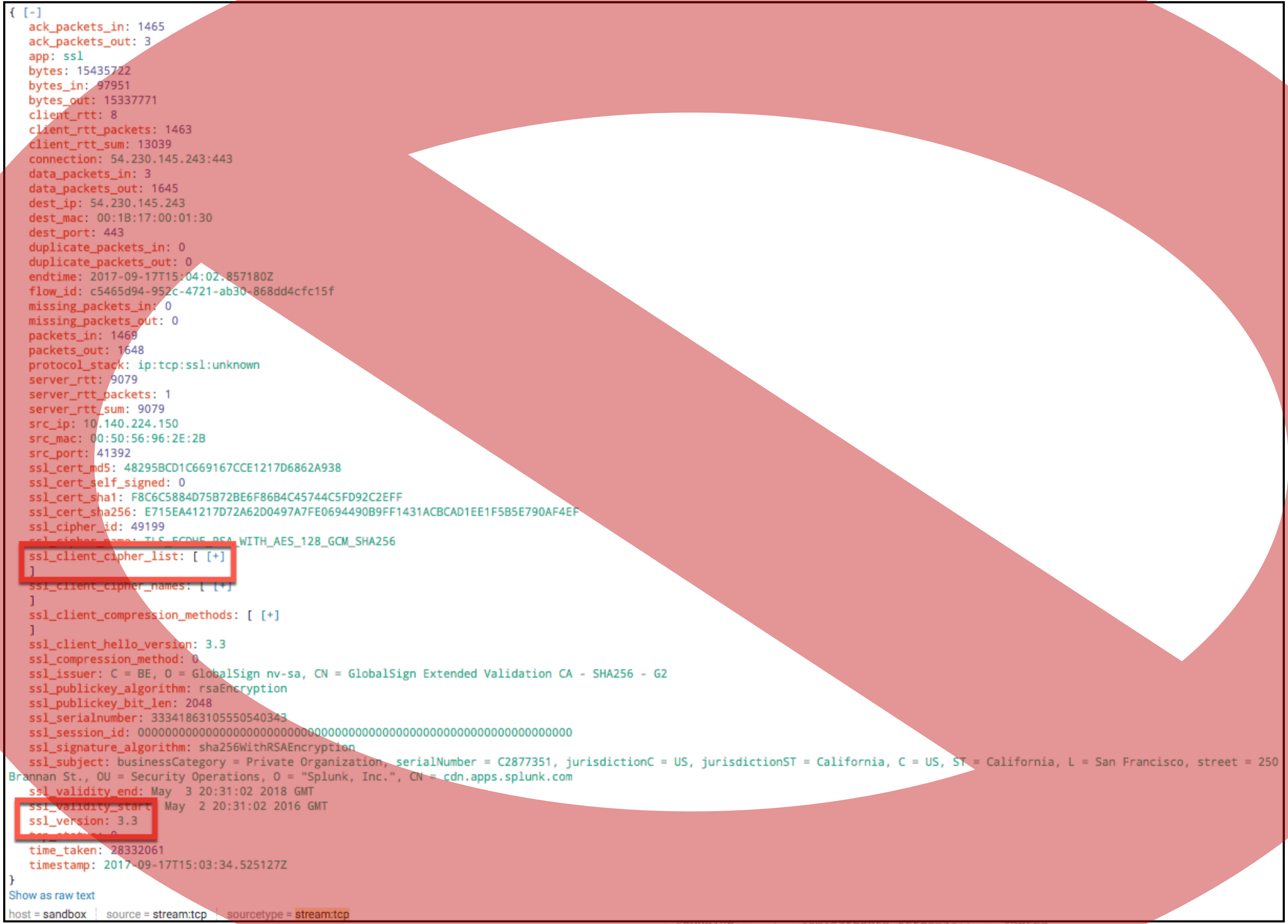
Why d matter?

SSL cer
does
ma

Ports
don't
tter



Stream doesn’t support… yet ☹

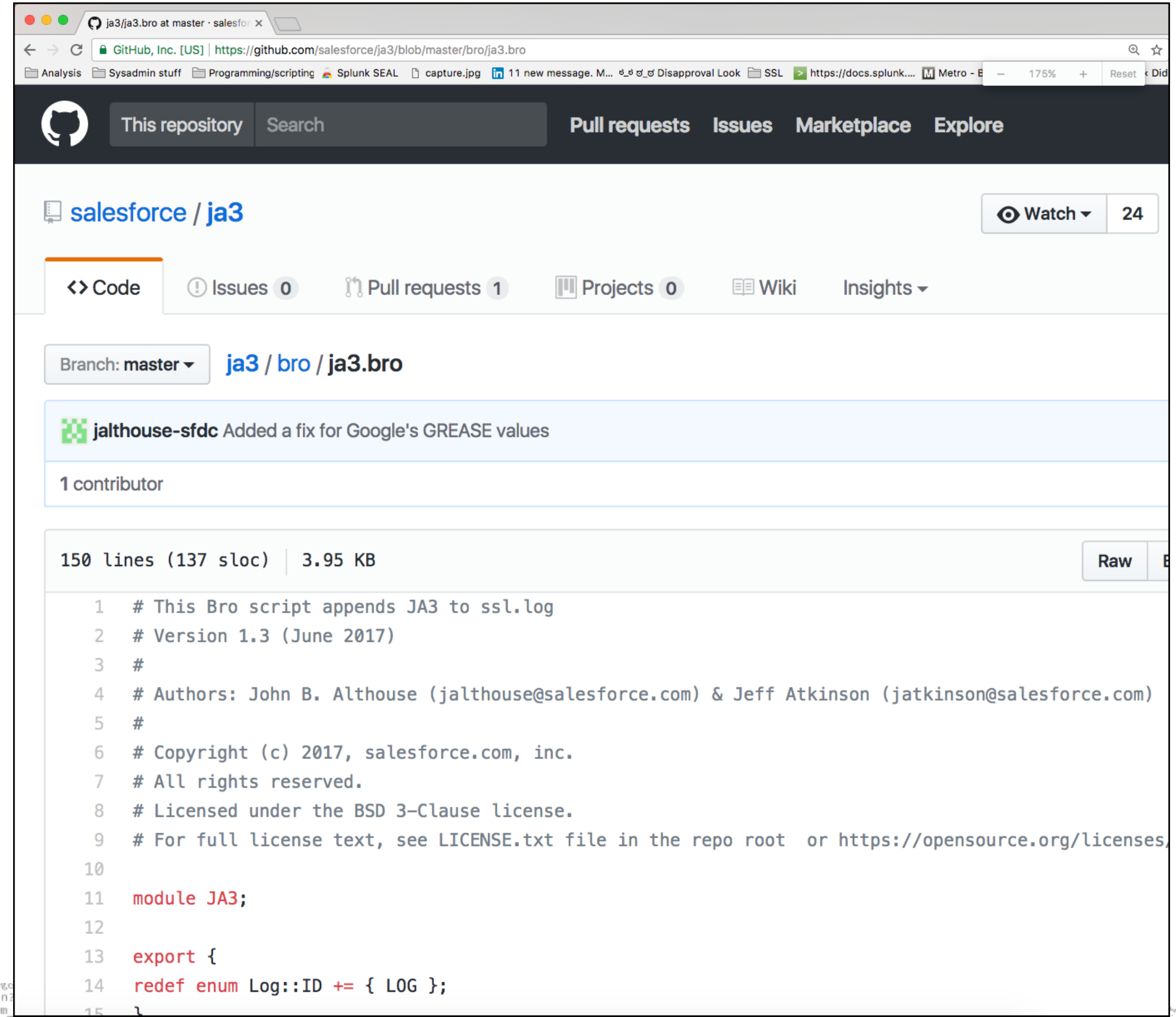


```
{ [-]
   ack_packets_in: 1465
   ack_packets_out: 3
   app: ssl
   bytes: 15435722
   bytes_in: 97951
   bytes_out: 15337771
   client_rtt: 8
   client_rtt_packets: 1463
   client_rtt_sum: 13039
   connection: 54.230.145.243:443
   data_packets_in: 3
   data_packets_out: 1645
   dest_ip: 54.230.145.243
   dest_mac: 00:1B:17:00:01:30
   dest_port: 443
   duplicate_packets_in: 0
   duplicate_packets_out: 0
   endtime: 2017-09-17T15:04:02.857180Z
   flow_id: c5465d94-952c-4721-ab30-868dd4cfc15f
   missing_packets_in: 0
   missing_packets_out: 0
   packets_in: 1469
   packets_out: 1648
   protocol_stack: ip:tcp:ssl:unknown
   server_rtt: 9079
   server_rtt_packets: 1
   server_rtt_sum: 9079
   src_ip: 10.140.224.150
   src_mac: 00:50:56:96:2E:2B
   src_port: 41392
   ssl_cert_md5: 48295BCD1C669167CCE1217D6862A938
   ssl_cert_self_signed: 0
   ssl_cert_sha1: F8C6C5884D75B72BE6F86B4C45744C5FD92C2EFF
   ssl_cert_sha256: E715EA41217D72A62D0497A7FE0694490B9FF1431ACBCAD1EE1F5B5E790AF4EF
   ssl_cipher_id: 49199
   ssl_cipher_name: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
   ssl_client_cipher_list: [ [+]
   ]
   ssl_client_cipher_names: [ [+]
   ]
   ssl_client_compression_methods: [ [+]
   ]
   ssl_client_hello_version: 3.3
   ssl_compression_method: 0
   ssl_issuer: C = BE, O = GlobalSign nv-sa, CN = GlobalSign Extended Validation CA - SHA256 - G2
   ssl_publickey_algorithm: rsaEncryption
   ssl_publickey_bit_len: 2048
   ssl_serialnumber: 33341863105550540343
   ssl_session_id: 0000000000000000000000000000000000000000000000000000000000000000
   ssl_signature_algorithm: sha256WithRSAEncryption
   ssl_subject: businessCategory = Private Organization, serialNumber = C2877351, jurisdictionC = US, jurisdictionST = California, C = US, ST = California, L = San Francisco, street = 250
Brannan St., OU = Security Operations, O = "Splunk, Inc.", CN = cdn.apps.splunk.com
   ssl_validity_end: May  3 20:31:02 2018 GMT
   ssl_validity_start: May  2 20:31:02 2016 GMT
   ssl_version: 3.3
   tcp_status: 0
   time_taken: 28332061
   timestamp: 2017-09-17T15:03:34.525127Z
}
```

Show as raw text

host = sandbox | source = stream:tcp | sourcetype = stream:tcp

But Bro Does ☺



salesforce / ja3

ja3 / bro / ja3.bro

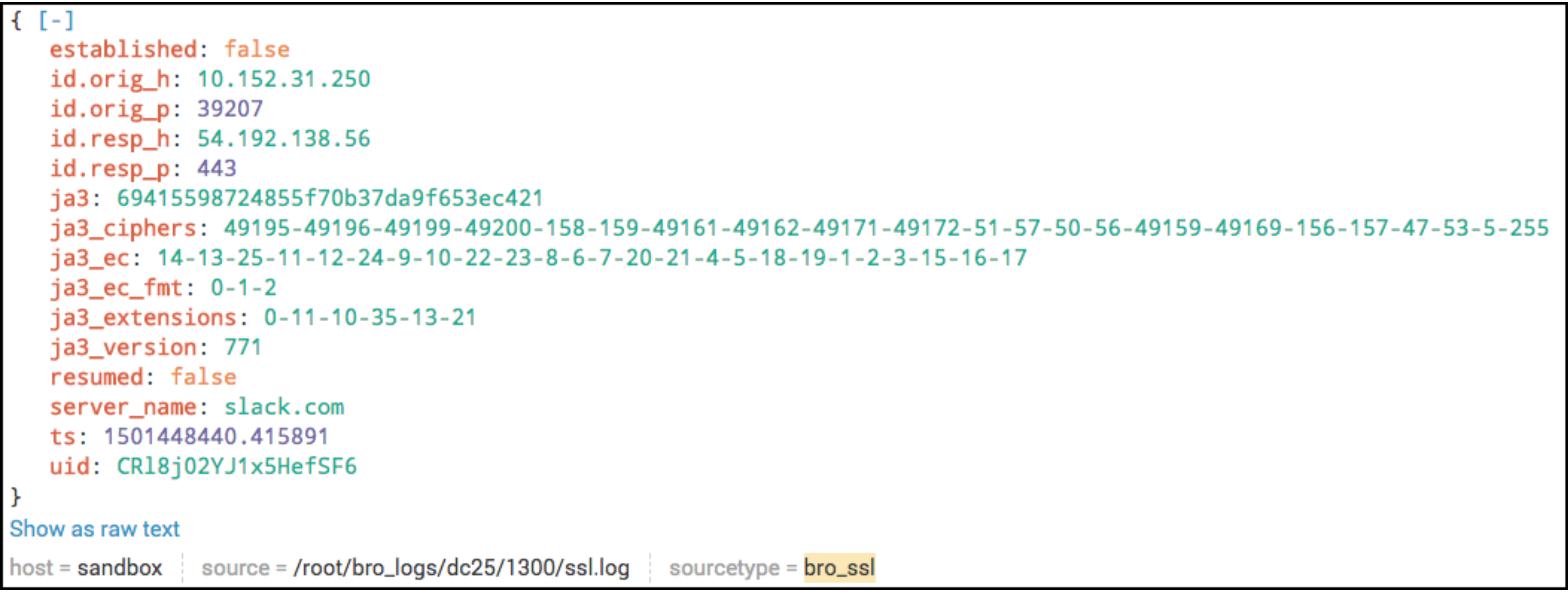
jalthouse-sfdc Added a fix for Google's GREASE values

1 contributor

150 lines (137 sloc) | 3.95 KB

```
# This Bro script appends JA3 to ssl.log
# Version 1.3 (June 2017)
#
# Authors: John B. Althouse (jalthouse@salesforce.com) & Jeff Atkinson (jatkinson@salesforce.com)
#
# Copyright (c) 2017, salesforce.com, inc.
# All rights reserved.
# Licensed under the BSD 3-Clause license.
# For full license text, see LICENSE.txt file in the repo root  or https://opensource.org/licenses/

module JA3;

export {
redef enum Log::ID += { LOG };
}
```

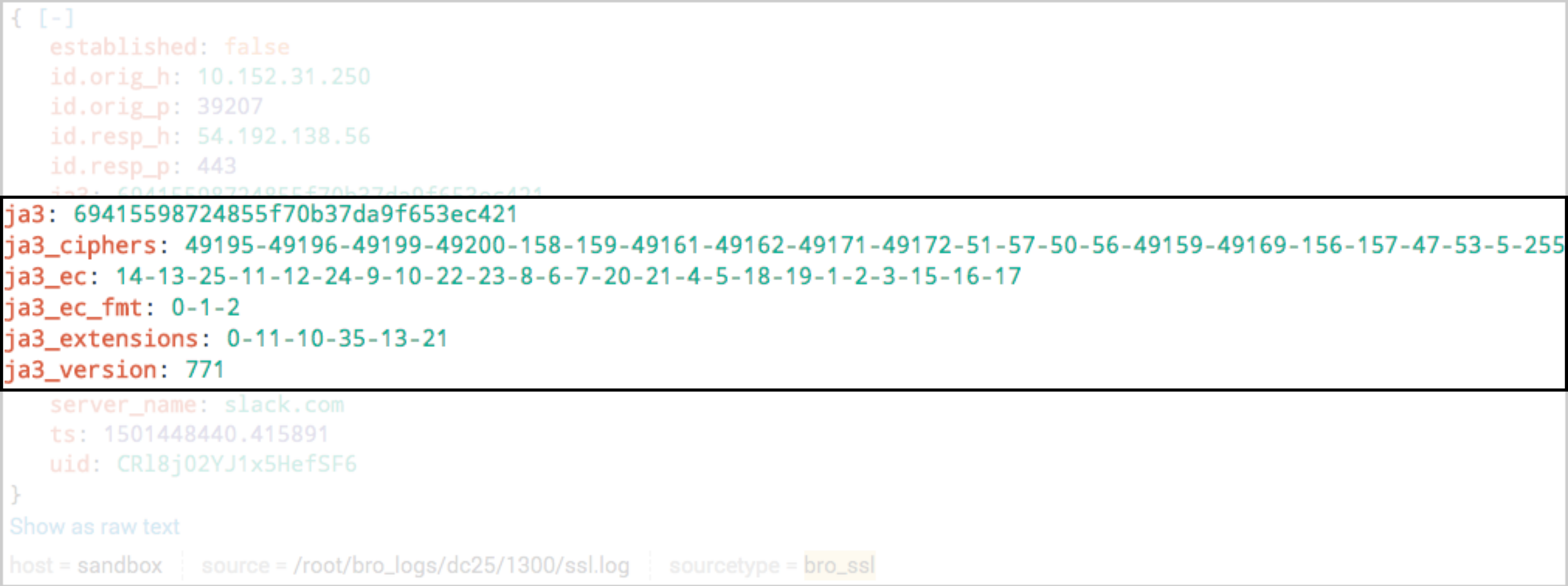
But Bro Does ☺



```
{ [-]
   established: false
   id.orig_h: 10.152.31.250
   id.orig_p: 39207
   id.resp_h: 54.192.138.56
   id.resp_p: 443
   ja3: 69415598724855f70b37da9f653ec421
   ja3_ciphers: 49195-49196-49199-49200-158-159-49161-49162-49171-49172-51-57-50-56-49159-49169-156-157-47-53-5-255
   ja3_ec: 14-13-25-11-12-24-9-10-22-23-8-6-7-20-21-4-5-18-19-1-2-3-15-16-17
   ja3_ec_fmt: 0-1-2
   ja3_extensions: 0-11-10-35-13-21
   ja3_version: 771
   resumed: false
   server_name: slack.com
   ts: 1501448440.415891
   uid: CRl8j02YJ1x5HefSF6
}
```

host = sandbox | source = /root/bro_logs/dc25/1300/ssl.log | sourcetype = bro_ssl

But Bro Does ☺



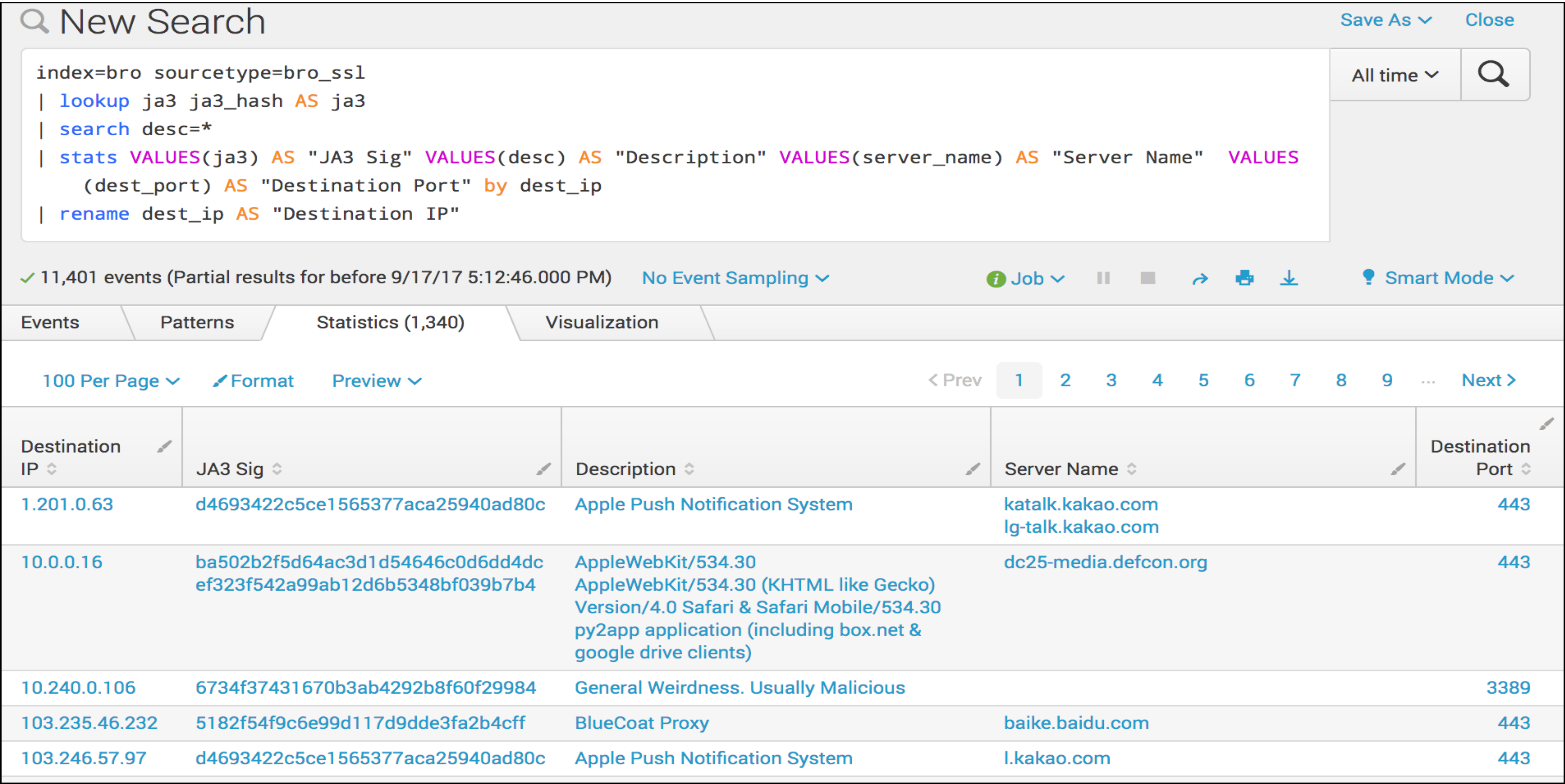
```
{ [-]
   established: false
   id.orig_h: 10.152.31.250
   id.orig_p: 39207
   id.resp_h: 54.192.138.56
   id.resp_p: 443
ja3: 694155598724855f70b37da9f653ec421
ja3_ciphers: 49195-49196-49199-49200-158-159-49161-49162-49171-49172-51-57-50-56-49159-49169-156-157-47-53-5-255
ja3_ec: 14-13-25-11-12-24-9-10-22-23-8-6-7-20-21-4-5-18-19-1-2-3-15-16-17
ja3_ec_fmt: 0-1-2
ja3_extensions: 0-11-10-35-13-21
ja3_version: 771
   server_name: slack.com
   ts: 1501448440.415891
   uid: CRl8j02YJ1x5HefSF6
}
Show as raw text
host = sandbox   source = /root/bro_logs/dc25/1300/ssl.log   sourcetype = bro_ssl
```

Using JA3 TLS Fingerprint Lookup

- **Hunting**

```
index=bro sourcetype=bro_ssl
| lookup ja3 ja3_hash AS ja3
| search desc=*
| stats VALUES(ja3) AS "JA3 Sig"
VALUES(desc) AS "Description"
VALUES(server_name) AS "Server Name"
VALUES(src_ip) AS “Source IP”
VALUES(dest_port) AS "Destination Port" by
dest_ip| rename dest_ip AS "Destination IP"
```

Using JA3 TLS Fingerprint Lookup

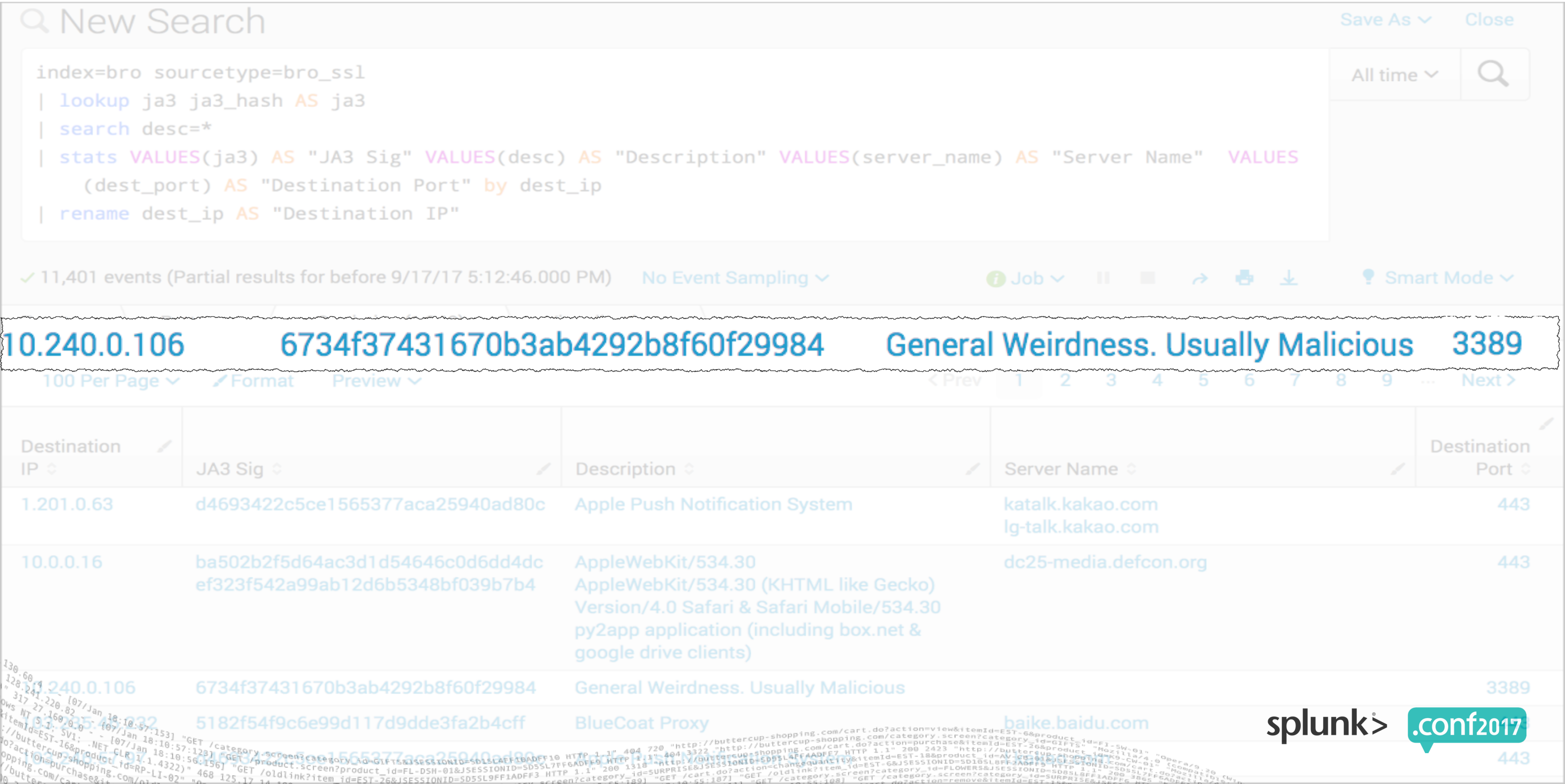


```
index=bro sourcetype=bro_ssl
| lookup ja3 ja3_hash AS ja3
| search desc=*
| stats VALUES(ja3) AS "JA3 Sig" VALUES(desc) AS "Description" VALUES(server_name) AS "Server Name"  VALUES
    (dest_port) AS "Destination Port" by dest_ip
| rename dest_ip AS "Destination IP"
```

✓ 11,401 events (Partial results for before 9/17/17 5:12:46.000 PM)

Destination IP	JA3 Sig	Description	Server Name	Destination Port
1.201.0.63	d4693422c5ce1565377aca25940ad80c	Apple Push Notification System	katalk.kakao.com lg-talk.kakao.com	443
10.0.0.16	ba502b2f5d64ac3d1d54646c0d6dd4dc ef323f542a99ab12d6b5348bf039b7b4	AppleWebKit/534.30 AppleWebKit/534.30 (KHTML like Gecko) Version/4.0 Safari & Safari Mobile/534.30 py2app application (including box.net & google drive clients)	dc25-media.defcon.org	443
10.240.0.106	6734f37431670b3ab4292b8f60f29984	General Weirdness. Usually Malicious		3389
103.235.46.232	5182f54f9c6e99d117d9dde3fa2b4cff	BlueCoat Proxy	baike.baidu.com	443
103.246.57.97	d4693422c5ce1565377aca25940ad80c	Apple Push Notification System	l.kakao.com	443

Using JA3 TLS fingerprint Lookup



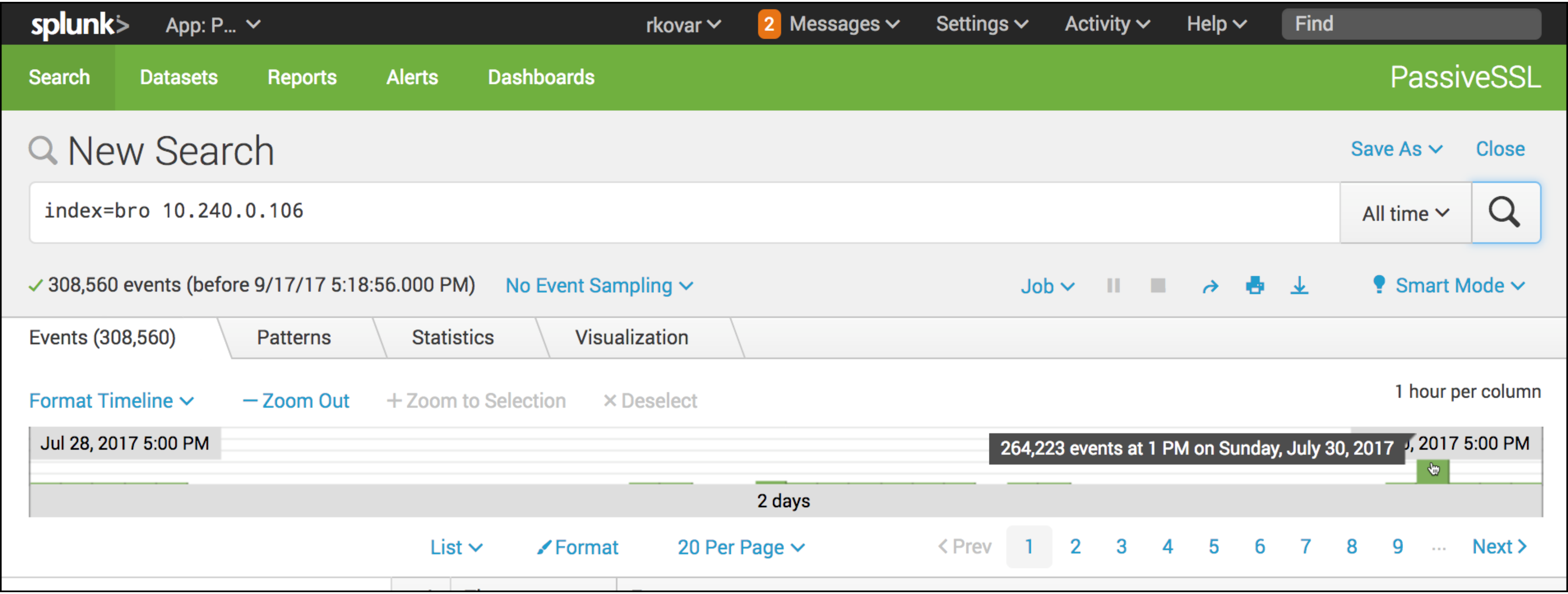
```
index=bro sourcetype=bro_ssl
| lookup ja3 ja3_hash AS ja3
| search desc=*
| stats VALUES(ja3) AS "JA3 Sig" VALUES(desc) AS "Description" VALUES(server_name) AS "Server Name"  VALUES
    (dest_port) AS "Destination Port" by dest_ip
| rename dest_ip AS "Destination IP"
```

✓ 11,401 events (Partial results for before 9/17/17 5:12:46.000 PM)

10.240.0.106 6734f37431670b3ab4292b8f60f29984 General Weirdness. Usually Malicious 3389

Destination IP	JA3 Sig	Description	Server Name	Destination Port
1.201.0.63	d4693422c5ce1565377aca25940ad80c	Apple Push Notification System	katalk.kakao.com lg-talk.kakao.com	443
10.0.0.16	ba502b2f5d64ac3d1d54646c0d6dd4dc ef323f542a99ab12d6b5348bf039b7b4	AppleWebKit/534.30 AppleWebKit/534.30 (KHTML like Gecko) Version/4.0 Safari & Safari Mobile/534.30 py2app application (including box.net & google drive clients)	dc25-media.defcon.org	443
[illegible].240.0.106	6734f37431670b3ab4292b8f60f29984	General Weirdness. Usually Malicious		3389
[illegible]	5182f54f9c6e99d117d9dde3fa2b4cff	BlueCoat Proxy	baike.baidu.com	[illegible]
[illegible]	[illegible]1565377aca25940ad80c	[illegible]	[illegible]	443

Using JA3 TLS Fingerprint Lookup



New Search

```
index=bro 10.240.0.106
```

All time

✓ 308,560 events (before 9/17/17 5:18:56.000 PM)

No Event Sampling

Events (308,560)

1 hour per column

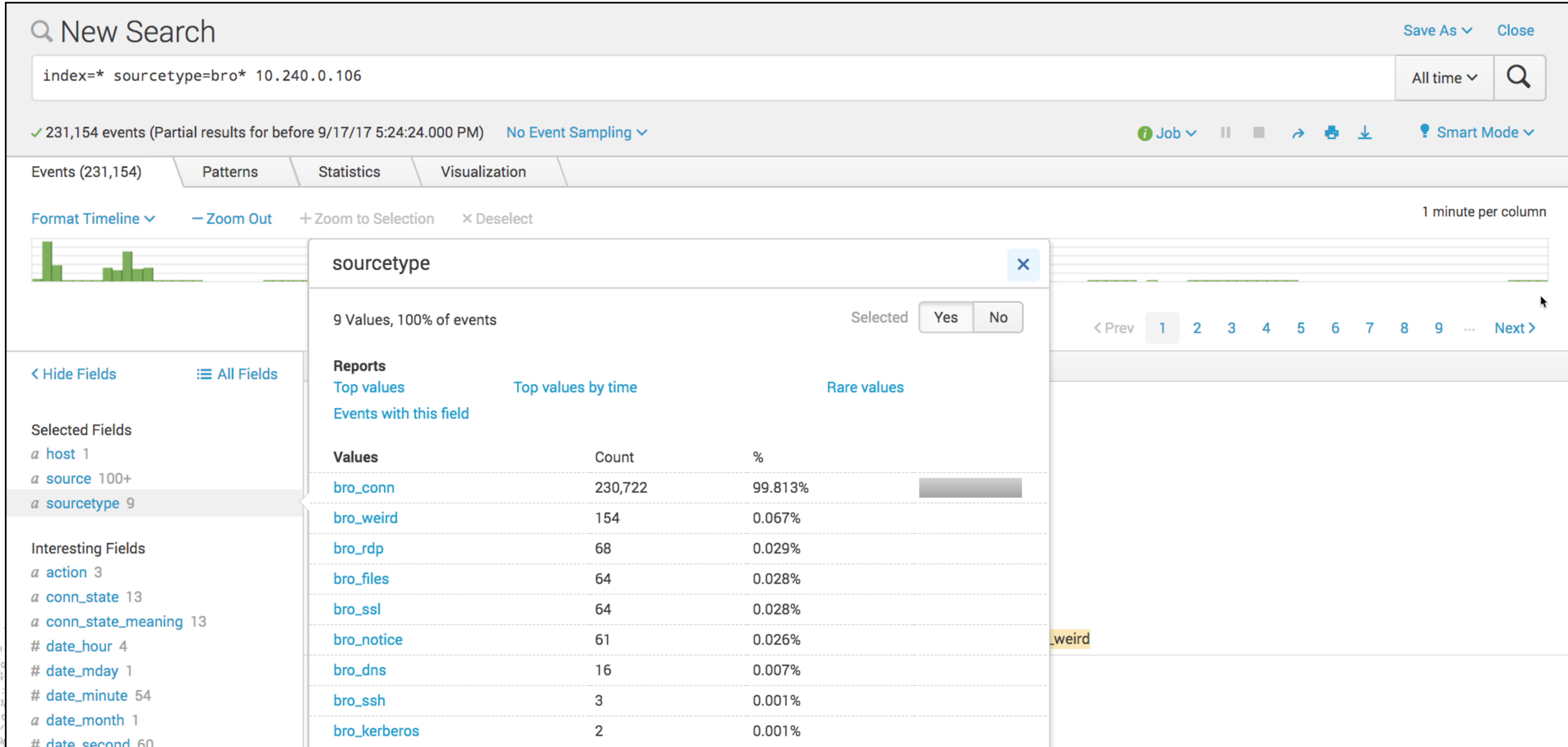
Jul 28, 2017 5:00 PM

264,223 events at 1 PM on Sunday, July 30, 2017

, 2017 5:00 PM

2 days

Using JA3 TLS Fingerprint Lookup



```
index=* sourcetype=bro* 10.240.0.106
```

✓ 231,154 events (Partial results for before 9/17/17 5:24:24.000 PM)

Selected Fields

a host	1
a source	100+
a sourcetype	9

Interesting Fields

a action	3
a conn_state	13
a conn_state_meaning	13
# date_hour	4
# date_mday	1
# date_minute	54
a date_month	1
# date_second	60

sourcetype ✕

9 Values, 100% of events

Selected Yes No

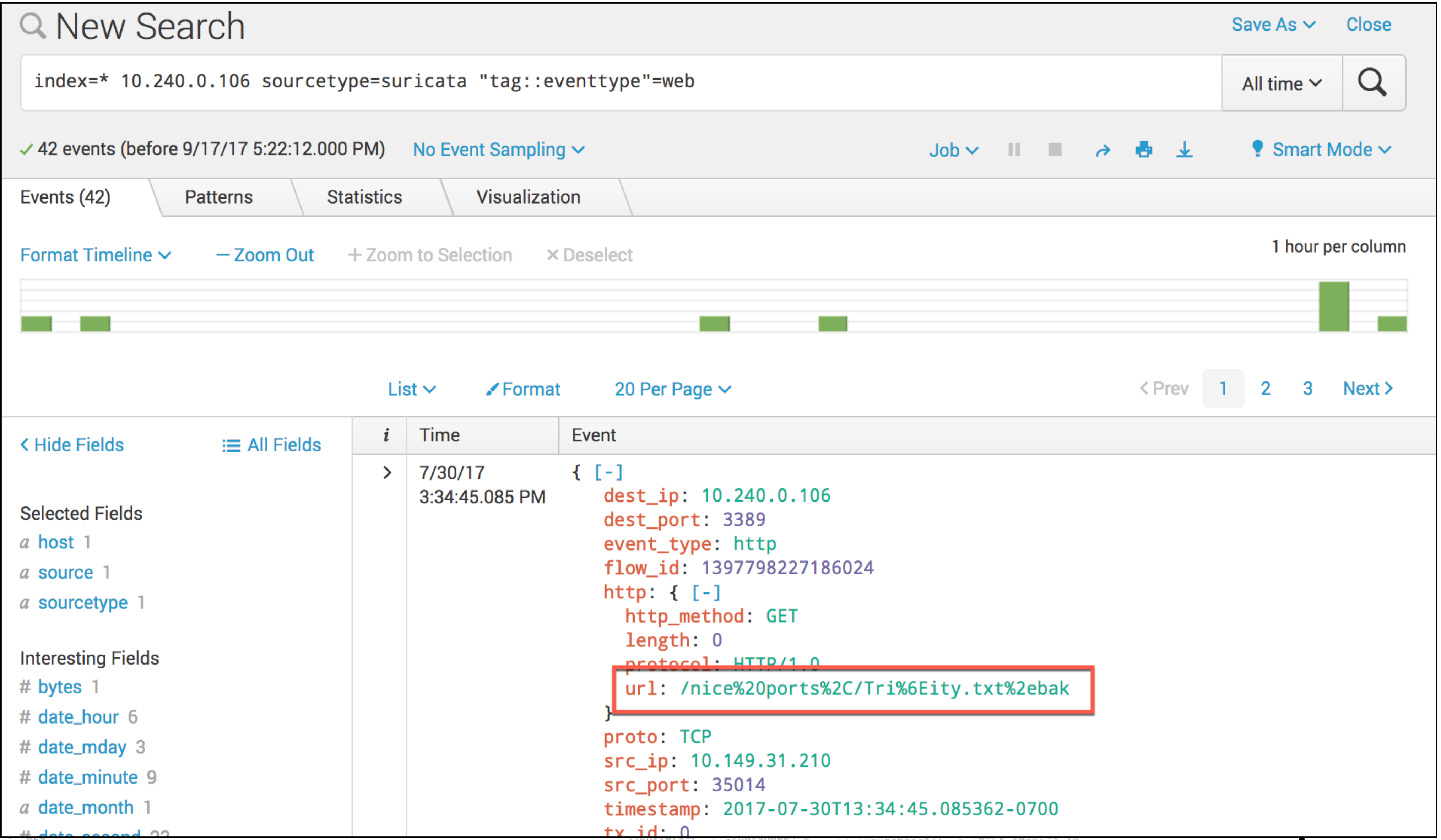
Reports

Top values　Top values by time　Rare values

Events with this field

Values	Count	%
bro_conn	230,722	99.813%
bro_weird	154	0.067%
bro_rdp	68	0.029%
bro_files	64	0.028%
bro_ssl	64	0.028%
bro_notice	61	0.026%
bro_dns	16	0.007%
bro_ssh	3	0.001%
bro_kerberos	2	0.001%

Using JA3 TLS Fingerprint Lookup



```
index=* 10.240.0.106 sourcetype=suricata "tag::eventtype"=web
```

✓ 42 events (before 9/17/17 5:22:12.000 PM) No Event Sampling

Selected Fields

- a host 1
- a source 1
- a sourcetype 1

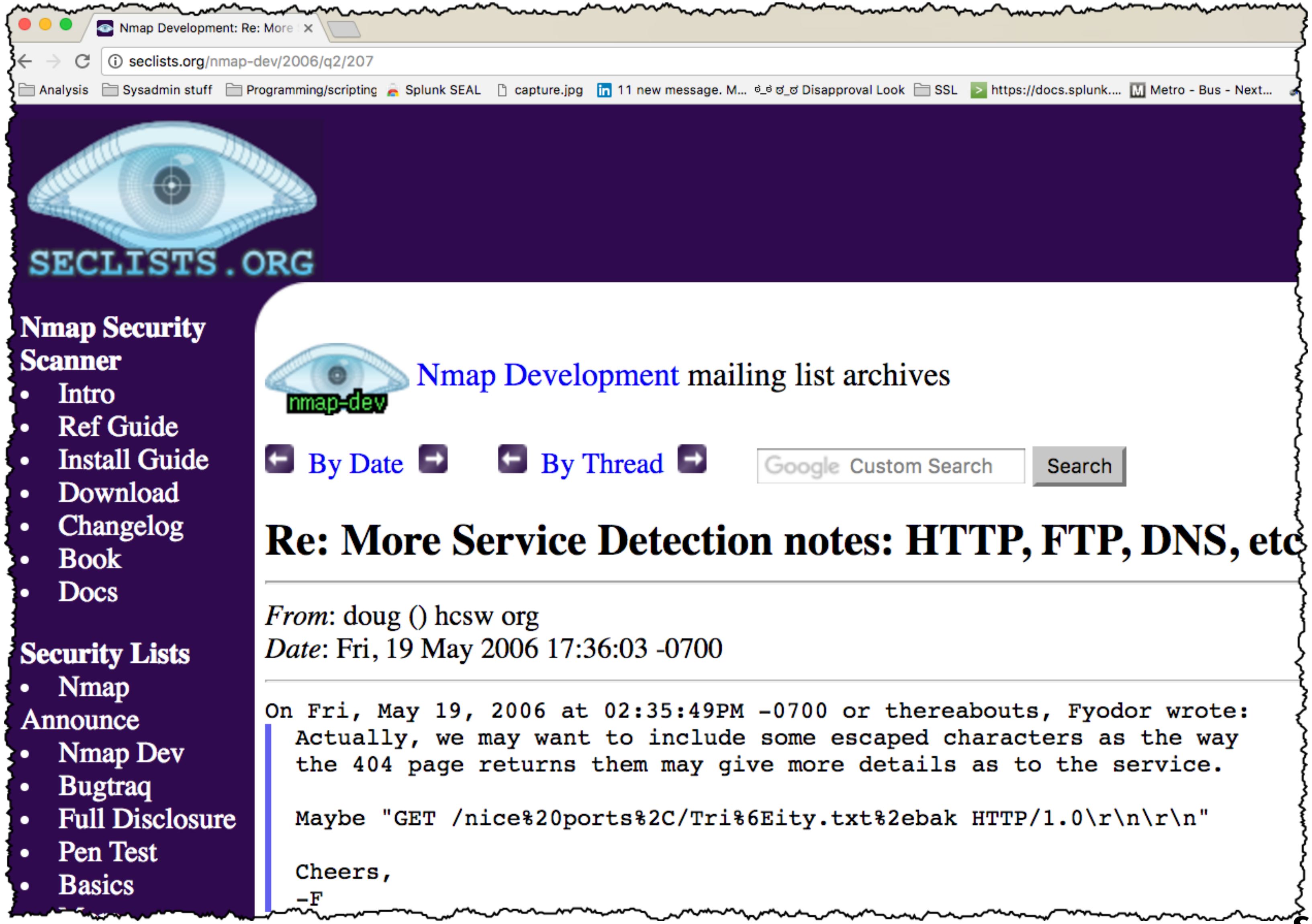
Interesting Fields

- # bytes 1
- # date_hour 6
- # date_mday 3
- # date_minute 9
- a date_month 1
- # date_second 22

7/30/17 3:34:45.085 PM

```
{ [-]
   dest_ip: 10.240.0.106
   dest_port: 3389
   event_type: http
   flow_id: 1397798227186024
   http: { [-]
     http_method: GET
     length: 0
     protocol: HTTP/1.0
     url: /nice%20ports%2C/Tri%6Eity.txt%2ebak
   }
   proto: TCP
   src_ip: 10.149.31.210
   src_port: 35014
   timestamp: 2017-07-30T13:34:45.085362-0700
   tx_id: 0
```

Using JA3 TLS Fingerprint Lookup



Nmap Security Scanner

- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

Security Lists

- Nmap Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics

Nmap Development mailing list archives

By Date By Thread

Google Custom Search | Search

Re: More Service Detection notes: HTTP, FTP, DNS, etc

From: doug () hcsw org
Date: Fri, 19 May 2006 17:36:03 -0700

```
On Fri, May 19, 2006 at 02:35:49PM -0700 or thereabouts, Fyodor wrote:
 Actually, we may want to include some escaped characters as the way
 the 404 page returns them may give more details as to the service.

 Maybe "GET /nice%20ports%2C/Tri%6Eity.txt%2ebak HTTP/1.0\r\n\r\n"

 Cheers,
 -F
```

BONUS ROUND

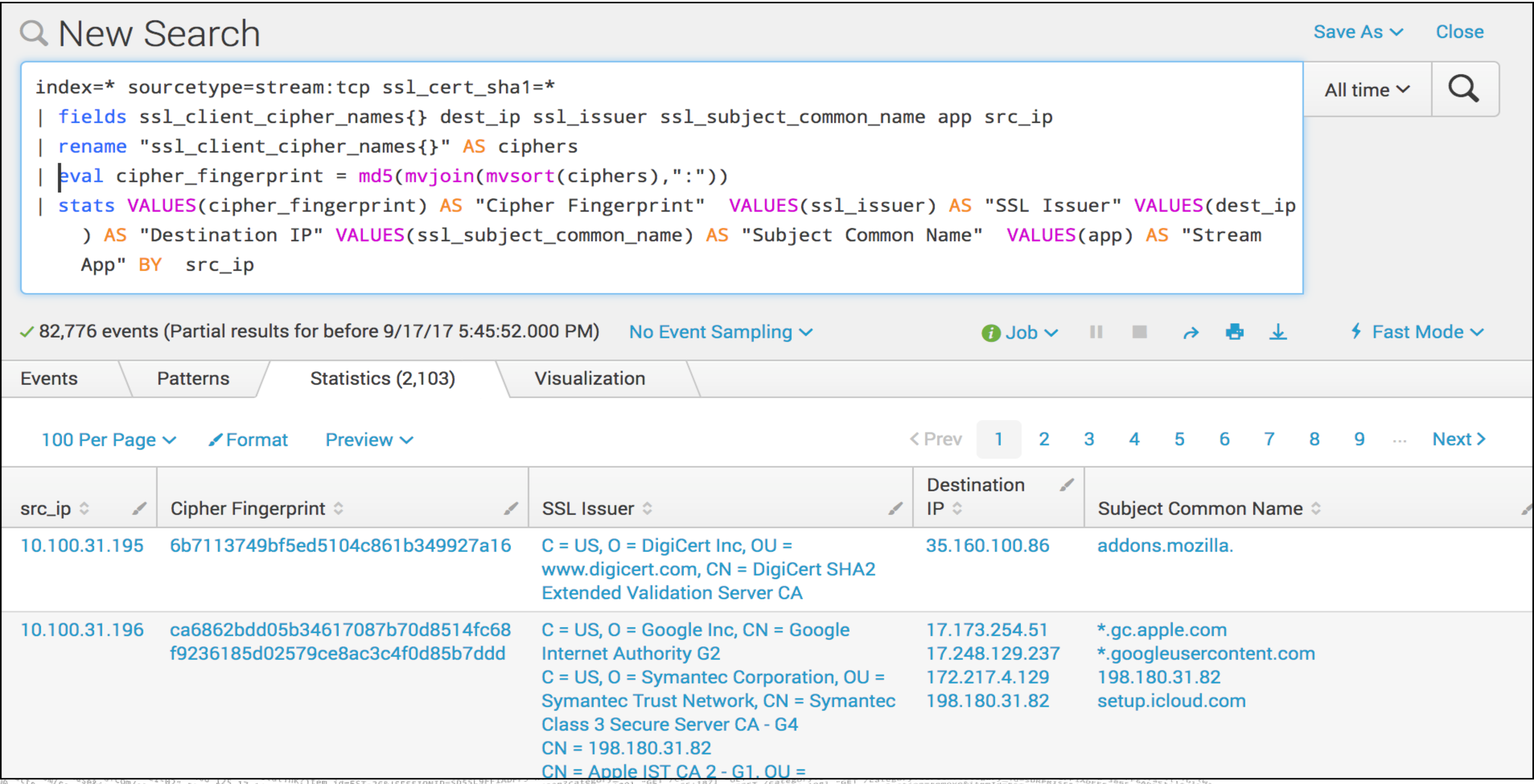
Stream Cipher fingerprint

- Hunting

```
index=* sourcetype=stream:tcp ssl_cert_sha1=*
| fields ssl_client_cipher_names{} dest_ip ssl_issuer
ssl_subject_common_name app src_ip
| rename "ssl_client_cipher_names{}" AS ciphers|eval
cipher_fingerprint = md5(mvjoin(mvsort(ciphers),":"))
| stats count(cipher_fingerprint) values(ssl_issuer)
values(dest_ip)  values(ssl_subject_common_name)
values(app) BY  src_ip
```

Special thanks to
@alacercogitatus
(Kyle Smith) for help

Stream Cipher Fingerprint



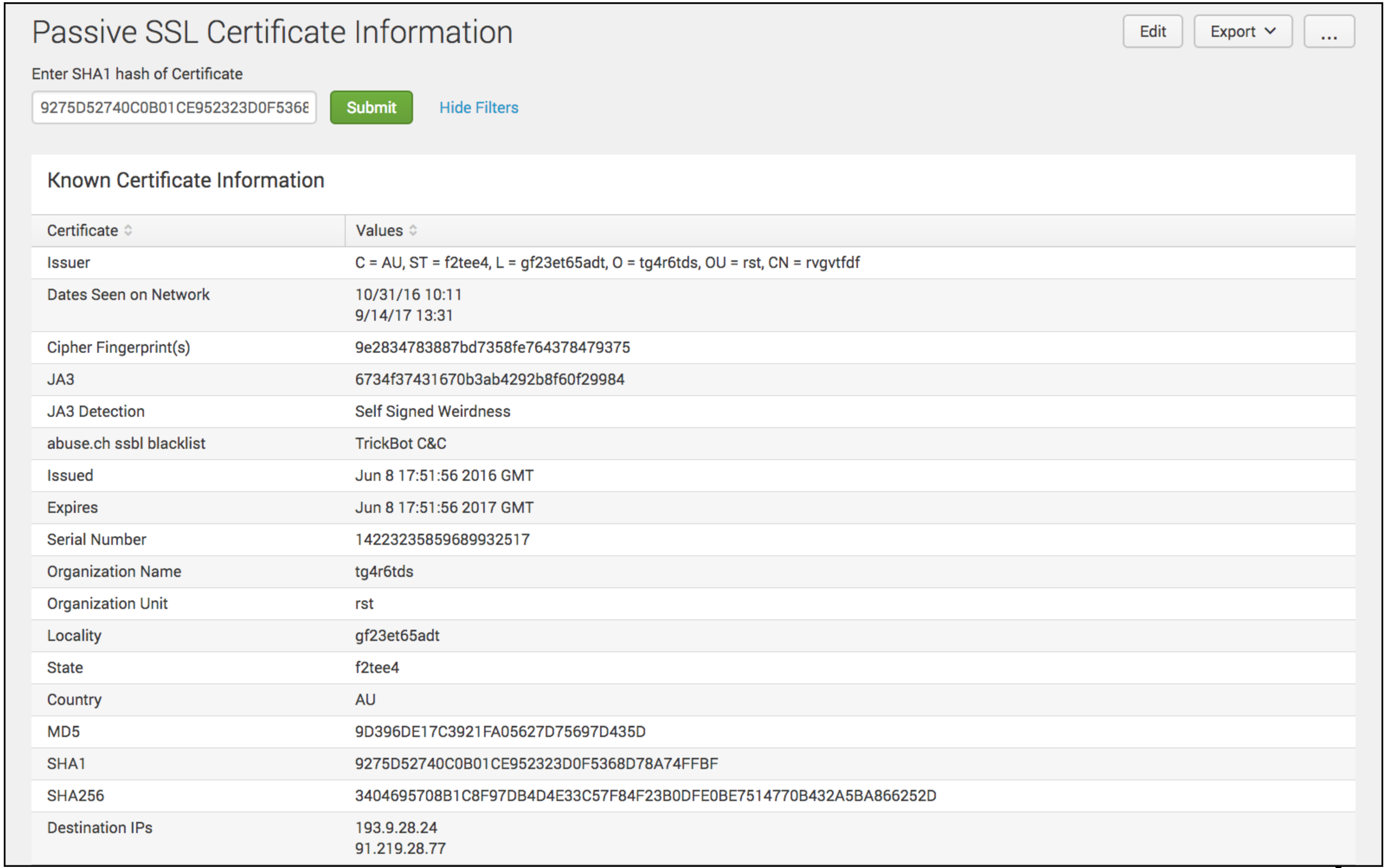
```
index=* sourcetype=stream:tcp ssl_cert_sha1=*
| fields ssl_client_cipher_names{} dest_ip ssl_issuer ssl_subject_common_name app src_ip
| rename "ssl_client_cipher_names{}" AS ciphers
| eval cipher_fingerprint = md5(mvjoin(mvsort(ciphers),":"))
| stats VALUES(cipher_fingerprint) AS "Cipher Fingerprint"  VALUES(ssl_issuer) AS "SSL Issuer" VALUES(dest_ip
   ) AS "Destination IP" VALUES(ssl_subject_common_name) AS "Subject Common Name"  VALUES(app) AS "Stream
   App" BY  src_ip
```

✓ 82,776 events (Partial results for before 9/17/17 5:45:52.000 PM)

src_ip	Cipher Fingerprint	SSL Issuer	Destination IP	Subject Common Name
10.100.31.195	6b7113749bf5ed5104c861b349927a16	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert SHA2 Extended Validation Server CA	35.160.100.86	addons.mozilla.

10.100.31.196	ca6862bdd05b34617087b70d8514fc68
	f9236185d02579ce8ac3c4f0d85b7ddd
		C = US, O = Google Inc, CN = Google Internet Authority G2
		C = US, O = Symantec Corporation, OU = Symantec Trust Network, CN = Symantec Class 3 Secure Server CA - G4
		CN = 198.180.31.82
		CN = Apple IST CA 2 - G1, OU =
			17.173.254.51
			17.248.129.237
			172.217.4.129
			198.180.31.82
				*.gc.apple.com
				*.googleusercontent.com
				198.180.31.82
				setup.icloud.com

Passive SSL App



Passive SSL Certificate Information

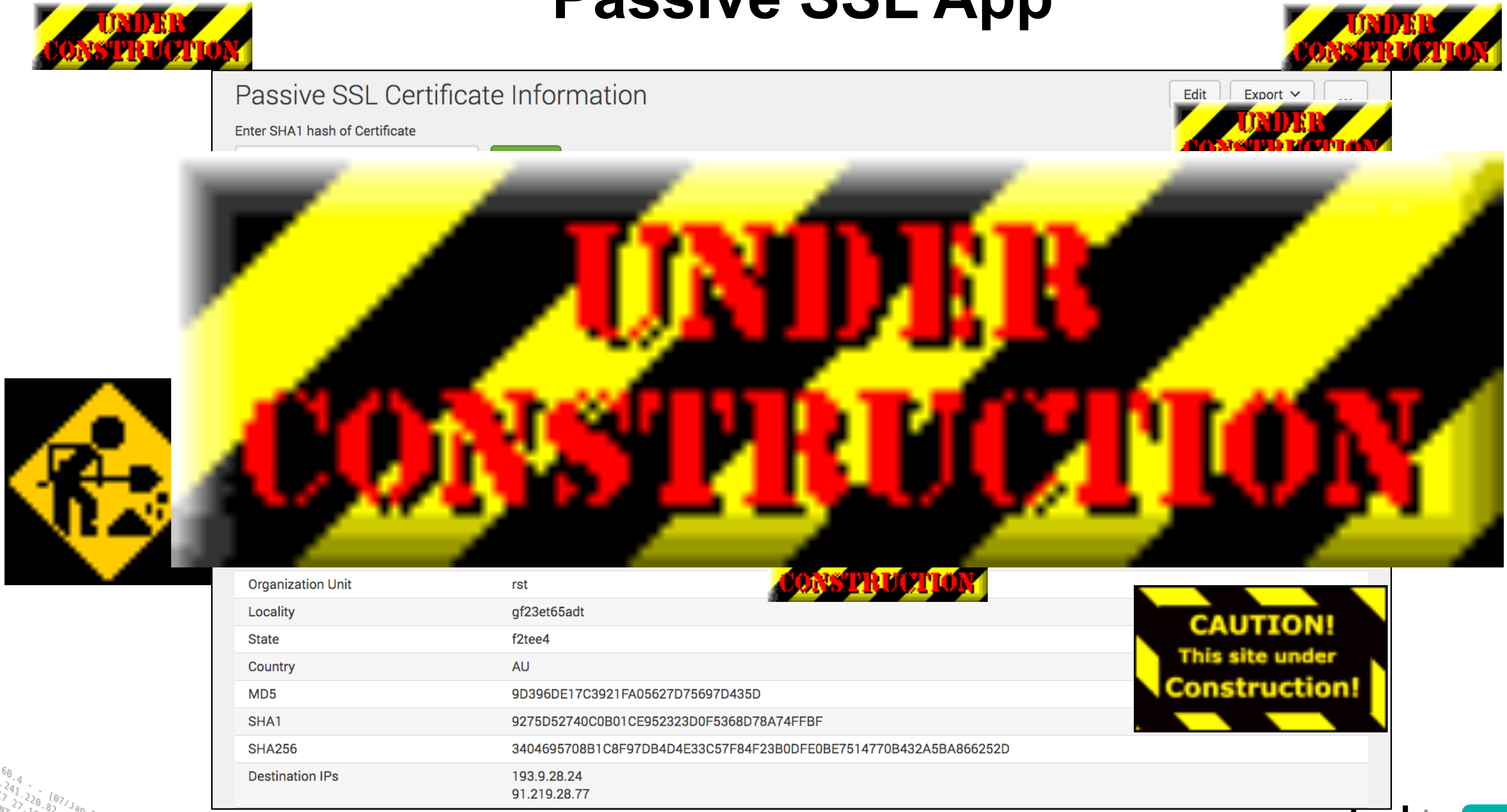
Enter SHA1 hash of Certificate

9275D52740C0B01CE952323D0F5368

Known Certificate Information

Certificate	Values
Issuer	C = AU, ST = f2tee4, L = gf23et65adt, O = tg4r6tds, OU = rst, CN = rvgvtfdf
Dates Seen on Network	10/31/16 10:11 9/14/17 13:31
Cipher Fingerprint(s)	9e2834783887bd7358fe764378479375
JA3	6734f37431670b3ab4292b8f60f29984
JA3 Detection	Self Signed Weirdness
abuse.ch ssbl blacklist	TrickBot C&C
Issued	Jun 8 17:51:56 2016 GMT
Expires	Jun 8 17:51:56 2017 GMT
Serial Number	14223235859689932517
Organization Name	tg4r6tds
Organization Unit	rst
Locality	gf23et65adt
State	f2tee4
Country	AU
MD5	9D396DE17C3921FA05627D75697D435D
SHA1	9275D52740C0B01CE952323D0F5368D78A74FFBF
SHA256	3404695708B1C8F97DB4D4E33C57F84F23B0DFE0BE7514770B432A5BA866252D
Destination IPs	193.9.28.24 91.219.28.77

Passive SSL App



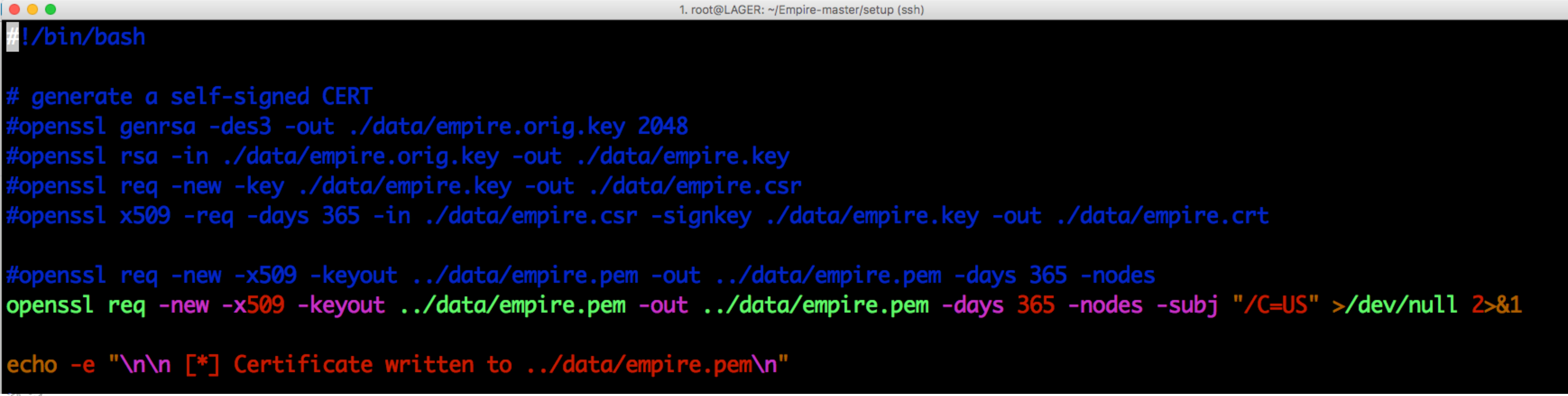
Passive SSL Certificate Information

Enter SHA1 hash of Certificate

Organization Unit	rst
Locality	gf23et65adt
State	f2tee4
Country	AU
MD5	9D396DE17C3921FA05627D75697D435D
SHA1	9275D52740C0B01CE952323D0F5368D78A74FFBF
SHA256	3404695708B1C8F97DB4D4E33C57F84F23B0DFE0BE7514770B432A5BA866252D
Destination IPs	193.9.28.24 91.219.28.77

Conclusion

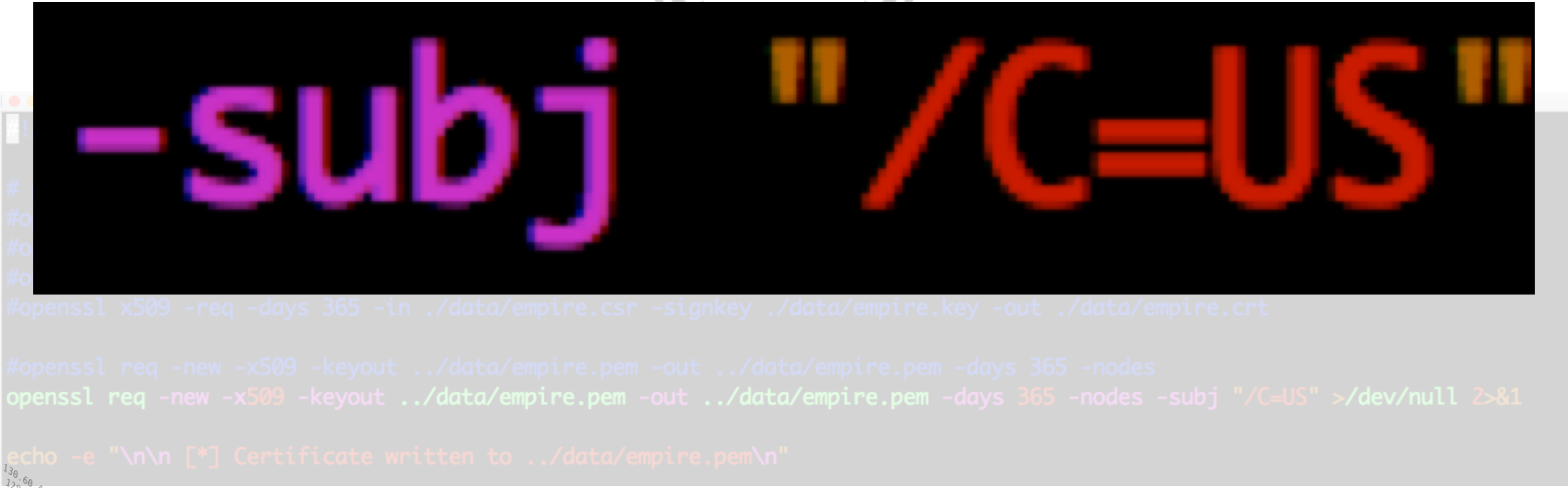
SSL Hunting Allows You To Find Hidden Adversaries



1. root@LAGER: ~/Empire-master/setup (ssh)

```
#!/bin/bash

# generate a self-signed CERT
#openssl genrsa -des3 -out ./data/empire.orig.key 2048
#openssl rsa -in ./data/empire.orig.key -out ./data/empire.key
#openssl req -new -key ./data/empire.key -out ./data/empire.csr
#openssl x509 -req -days 365 -in ./data/empire.csr -signkey ./data/empire.key -out ./data/empire.crt

#openssl req -new -x509 -keyout ../data/empire.pem -out ../data/empire.pem -days 365 -nodes
openssl req -new -x509 -keyout ../data/empire.pem -out ../data/empire.pem -days 365 -nodes -subj "/C=US" >/dev/null 2>&1

echo -e "\n\n [*] Certificate written to ../data/empire.pem\n"
```

SSL Hunting Allows You To Find Hidden Adversaries

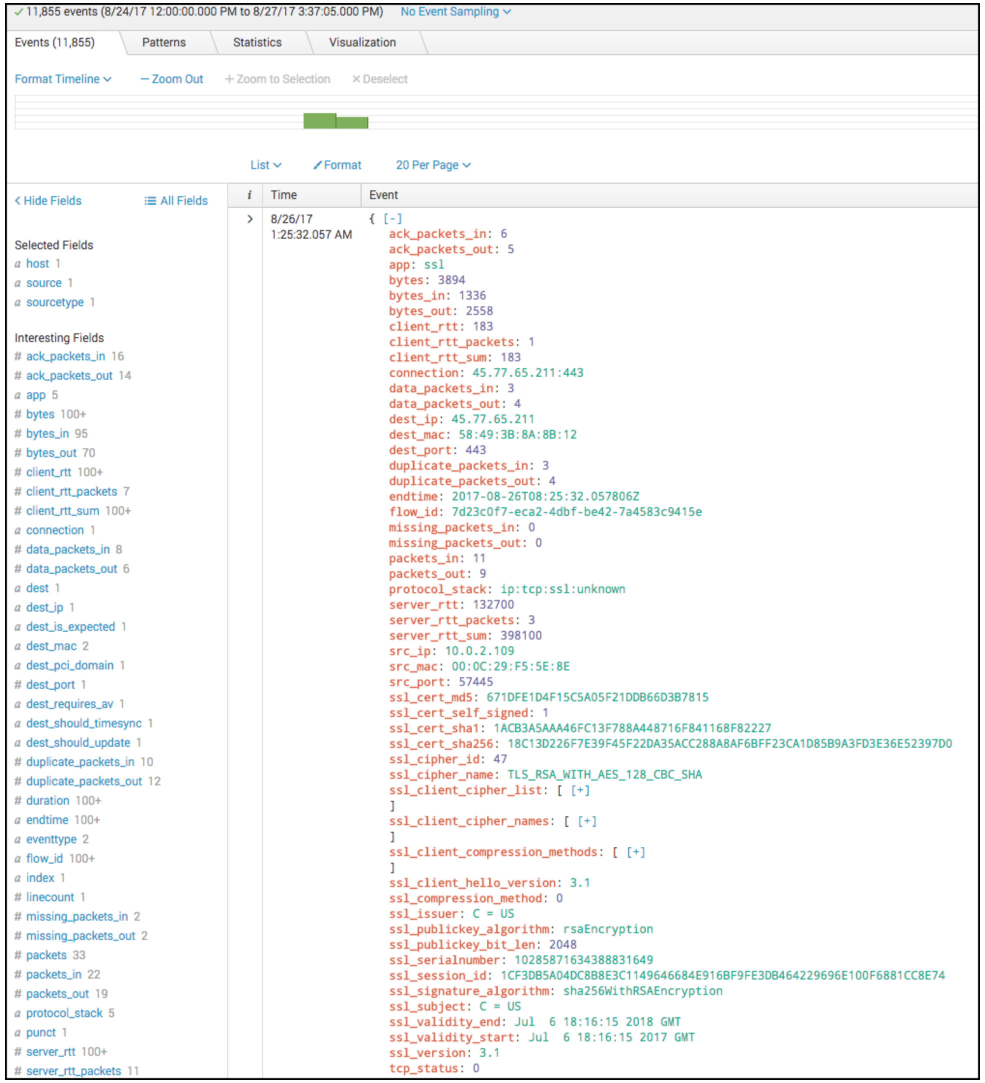


```
-subj "/C=US"
```

```
#!

#
#o
#o
#o
#openssl x509 -req -days 365 -in ./data/empire.csr -signkey ./data/empire.key -out ./data/empire.crt

#openssl req -new -x509 -keyout ../data/empire.pem -out ../data/empire.pem -days 365 -nodes
openssl req -new -x509 -keyout ../data/empire.pem -out ../data/empire.pem -days 365 -nodes -subj "/C=US" >/dev/null 2>&1

echo -e "\n\n [*] Certificate written to ../data/empire.pem\n"
```

splunk> .conf2017

SSL Hunting Allows You To Find Hidden Adversaries



✓ 11,855 events (8/24/17 12:00:00.000 PM to 8/27/17 3:37:05.000 PM) No Event Sampling

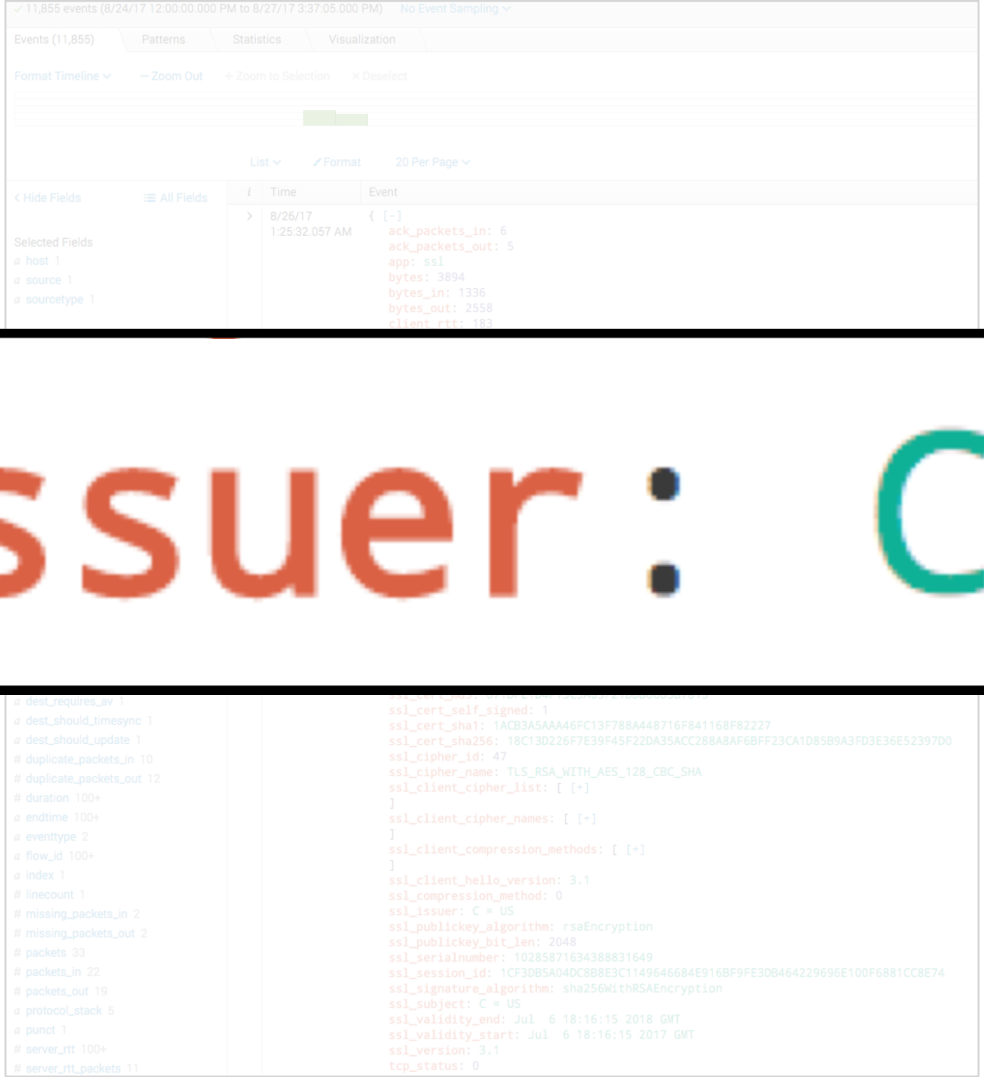
Selected Fields
- a host 1
- a source 1
- a sourcetype 1

Interesting Fields
- # ack_packets_in 16
- # ack_packets_out 14
- a app 5
- # bytes 100+
- # bytes_in 95
- # bytes_out 70
- # client_rtt 100+
- # client_rtt_packets 7
- # client_rtt_sum 100+
- a connection 1
- # data_packets_in 8
- # data_packets_out 6
- a dest 1
- a dest_ip 1
- a dest_is_expected 1
- a dest_mac 2
- a dest_pci_domain 1
- # dest_port 1
- a dest_requires_av 1
- a dest_should_timesync 1
- a dest_should_update 1
- # duplicate_packets_in 10
- # duplicate_packets_out 12
- # duration 100+
- a endtime 100+
- a eventtype 2
- a flow_id 100+
- a index 1
- # linecount 1
- # missing_packets_in 2
- # missing_packets_out 2
- # packets 33
- # packets_in 22
- # packets_out 19
- a protocol_stack 5
- a punct 1
- # server_rtt 100+
- # server_rtt_packets 11

8/26/17
1:25:32.057 AM

```
{ [-]
   ack_packets_in: 6
   ack_packets_out: 5
   app: ssl
   bytes: 3894
   bytes_in: 1336
   bytes_out: 2558
   client_rtt: 183
   client_rtt_packets: 1
   client_rtt_sum: 183
   connection: 45.77.65.211:443
   data_packets_in: 3
   data_packets_out: 4
   dest_ip: 45.77.65.211
   dest_mac: 58:49:3B:8A:8B:12
   dest_port: 443
   duplicate_packets_in: 3
   duplicate_packets_out: 4
   endtime: 2017-08-26T08:25:32.057806Z
   flow_id: 7d23c0f7-eca2-4dbf-be42-7a4583c9415e
   missing_packets_in: 0
   missing_packets_out: 0
   packets_in: 11
   packets_out: 9
   protocol_stack: ip:tcp:ssl:unknown
   server_rtt: 132700
   server_rtt_packets: 3
   server_rtt_sum: 398100
   src_ip: 10.0.2.109
   src_mac: 00:0C:29:F5:5E:8E
   src_port: 57445
   ssl_cert_md5: 671DFE1D4F15C5A05F21DDB66D3B7815
   ssl_cert_self_signed: 1
   ssl_cert_sha1: 1ACB3A5AAA46FC13F788A448716F841168F82227
   ssl_cert_sha256: 18C13D226F7E39F45F22DA35ACC288A8AF6BFF23CA1D85B9A3FD3E36E52397D0
   ssl_cipher_id: 47
   ssl_cipher_name: TLS_RSA_WITH_AES_128_CBC_SHA
   ssl_client_cipher_list: [ [+]
   ]
   ssl_client_cipher_names: [ [+]
   ]
   ssl_client_compression_methods: [ [+]
   ]
   ssl_client_hello_version: 3.1
   ssl_compression_method: 0
   ssl_issuer: C = US
   ssl_publickey_algorithm: rsaEncryption
   ssl_publickey_bit_len: 2048
   ssl_serialnumber: 10285871634388831649
   ssl_session_id: 1CF3DB5A04DC8B8E3C1149646684E916BF9FE3DB464229696E100F6881CC8E74
   ssl_signature_algorithm: sha256WithRSAEncryption
   ssl_subject: C = US
   ssl_validity_end: Jul  6 18:16:15 2018 GMT
   ssl_validity_start: Jul  6 18:16:15 2017 GMT
   ssl_version: 3.1
   tcp_status: 0
```

SSL Hunting Allows You To Find Hidden Adversaries

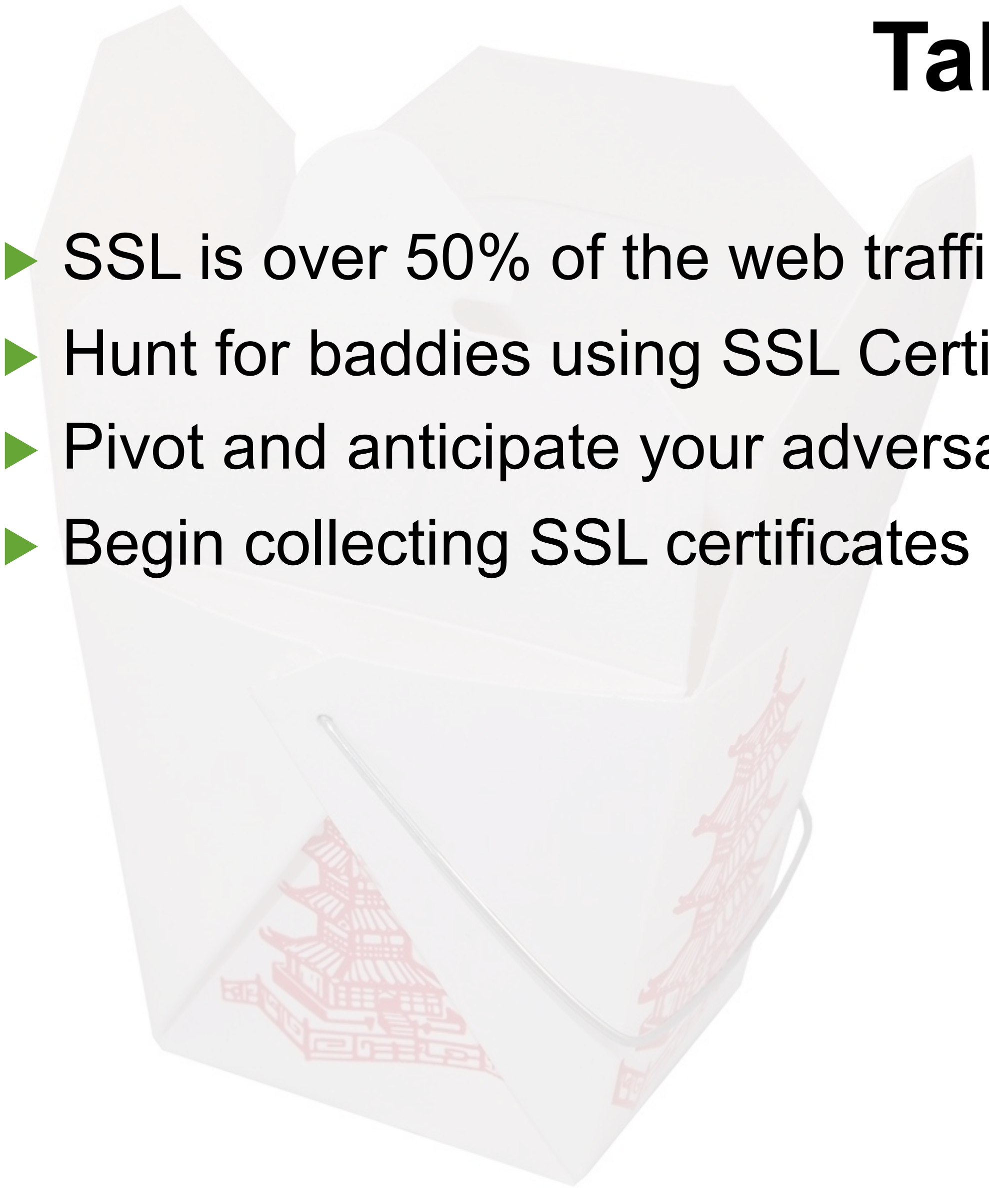


```
{ [-]
   ack_packets_in: 6
   ack_packets_out: 5
   app: ssl
   bytes: 3894
   bytes_in: 1336
   bytes_out: 2558
   client_rtt: 183
```

```
   ssl_cert_self_signed: 1
   ssl_cert_sha1: 1ACB3A5AAA46FC13F788A448716F841168F82227
   ssl_cert_sha256: 18C13D226F7E39F45F22DA35ACC288A8AF6BFF23CA1D85B9A3FD3E36E52397D0
   ssl_cipher_id: 47
   ssl_cipher_name: TLS_RSA_WITH_AES_128_CBC_SHA
   ssl_client_cipher_list: [ [+]
   ]
   ssl_client_cipher_names: [ [+]
   ]
   ssl_client_compression_methods: [ [+]
   ]
   ssl_client_hello_version: 3.1
   ssl_compression_method: 0
   ssl_issuer: C = US
   ssl_publickey_algorithm: rsaEncryption
   ssl_publickey_bit_len: 2048
   ssl_serialnumber: 10285871634388831649
   ssl_session_id: 1CF3DB5A04DC8B8E3C1149646684E916BF9FE3DB464229696E100F6881CC8E74
   ssl_signature_algorithm: sha256WithRSAEncryption
   ssl_subject: C = US
   ssl_validity_end: Jul  6 18:16:15 2018 GMT
   ssl_validity_start: Jul  6 18:16:15 2017 GMT
   ssl_version: 3.1
   tcp_status: 0
```

ssl_issuer: C = US

Takeaways



- SSL is over 50% of the web traffic in your network
- Hunt for baddies using SSL Certificates and Fingerprints
- Pivot and anticipate your adversary!
- Begin collecting SSL certificates and create your own Passive SSL database

Resources

- https://github.com/rkovar/splunk-hunting-helpers
  - The lookup files and workflow actions used in this presentation.
- https://censys.io/
  - Pivot on SSL certificates and websites. Only valid since their last scan
- https://github.com/rkovar/splunk-hunting-helpers/tree/master/workflow_actions
  - Workflow actions with censys.io
- https://engineering.salesforce.com/open-sourcing-ja3-92c9e53c3c41
  - Info on JA3 and adding it to Bro
- https://sslbl.abuse.ch/
  - Known bad SSL certificate
- https://github.com/trisulnsm/trisul-scripts/blob/master/lua/frontend_scripts/reassembly/ja3/prints/ja3fingerprint.json
  - JA3 fingerprint json. Just convert to csv

Special Thanks

- Mark Parsons
- William Salusky
- Ben Withnell
- IKBD

Thank You

Don't forget to rate this session in the .conf2017 mobile app

splunk> .conf2017