



Search on Splunk

By: Ryan Stewart

Let's explore the Search page together and clarify some essential aspects.

The screenshot displays the Splunk Search interface. At the top, the navigation bar includes 'splunk>enterprise', 'Apps', and various user options like 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. Below this, the 'Search' tab is active, showing a 'New Search' page. The search query is 'index=*winlog_clients*' and the time range is 'during Sep 2022'. The results show 2,835 events from 9/1/22 12:00:00.000 AM to 10/1/22 12:00:00.000 AM. The interface includes a 'Format Timeline' dropdown, 'Zoom Out' and 'Zoom to Selection' buttons, and a 'Deselect' button. The results are displayed in a table with columns for 'Time' and 'Event'. The table shows four events, each with a timestamp and a detailed log entry. The left sidebar contains a list of fields, including 'SELECTED FIELDS' (host, source, sourcetype) and 'INTERESTING FIELDS' (ComputerName, Domain, EventCode, EventType, ID de sécurité, ID d'ouverture de session, index, Keywords, linecount, LogName, Message, Nom du compte, OpCode, punct, RecordNumber, Sid, SidType, SourceName, splunk_server, TaskCategory, Type, User). The bottom of the sidebar shows '140 more fields' and a button to 'Extract New Fields'.

New Search Save As Create Table View Close

index=*winlog_clients* during Sep 2022 Q

✓ 2,835 events (9/1/22 12:00:00.000 AM to 10/1/22 12:00:00.000 AM) No Event Sampling Job || || → ⌵ ⌴ Smart Mode

Events (2,835) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 day per column

List Format 20 Per Page < Prev 1 2 3 4 5 6 7 8 ... Next >

i	Time	Event
>	9/2/22 4:36:47.000 AM	09/02/2022 01:36:47 PM LogName=Application EventCode=16384 EventType=4 ComputerName=DESKTOP-4L9QKFS Show all 12 lines host = DESKTOP-4L9QKFS source = WinEventLog:Application sourcetype = WinEventLog:Application
>	9/2/22 4:36:18.000 AM	09/02/2022 01:36:18 PM LogName=Setup EventCode=1 EventType=0 ComputerName=DESKTOP-4L9QKFS Show all 15 lines host = DESKTOP-4L9QKFS source = WinEventLog:Setup sourcetype = WinEventLog:Setup
>	9/2/22 4:36:17.000 AM	09/02/2022 01:36:17 PM LogName=Security EventCode=4799 EventType=0 ComputerName=DESKTOP-4L9QKFS Show all 27 lines host = DESKTOP-4L9QKFS source = WinEventLog:Security sourcetype = WinEventLog:Security
>	9/2/22 4:36:17.000 AM	09/02/2022 01:36:17 PM LogName=Security EventCode=4799 EventType=0 ComputerName=DESKTOP-4L9QKFS Show all 27 lines host = DESKTOP-4L9QKFS source = WinEventLog:Security sourcetype = WinEventLog:Security
>	9/2/22 4:36:17.000 AM	09/02/2022 01:36:17 PM LogName=Security EventCode=4799 EventType=0 ComputerName=DESKTOP-4L9QKFS Show all 27 lines host = DESKTOP-4L9QKFS source = WinEventLog:Security sourcetype = WinEventLog:Security

< Hide Fields All Fields

SELECTED FIELDS
a host 1
a source 4
a sourcetype 4

INTERESTING FIELDS
a ComputerName 2
a Domaine du compte 8
EventCode 100+
EventType 4
a ID de sécurité 38
a ID d'ouverture de session 43
a index 1
a Keywords 9
linecount 30
a LogName 4
a Message 100+
a Nom du compte 32
a OpCode 11
a punct 100+
RecordNumber 100+
a Sid 5
SidType 1
a SourceName 41
a splunk_server 1
a TaskCategory 35
a Type 3
a User 1

140 more fields
[+ Extract New Fields](#)

****Traps and Tips:****

- Field names are case-sensitive.
- Field values are not case-sensitive.
- The wildcard character "*" is available for use.
- Operators such as AND, OR, and NOT can be utilized.

****Date Selection:****

The first step is selecting the data range. You have various options:

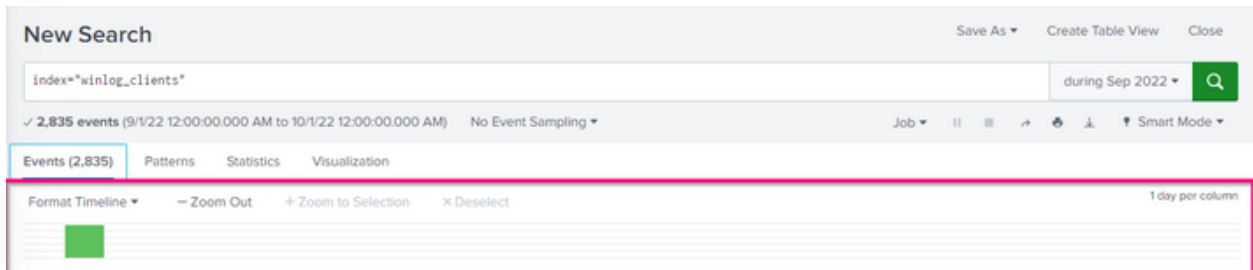
- Presets (today, last week, last year, last 24 hours, etc.).
- Relative (beginning of the hour, X minutes ago, X weeks ago, etc.).
- Real-time.
- Date range (between 00:00 DD/MM/YYYY and 24:00 DD/MM/YYYY).
- Date & time range (same but with the option to choose an hour).

The screenshot shows the Splunk Search interface. At the top, the search bar contains the query `index=*winlog_clients*`. To the right of the search bar, there is a dropdown menu showing `during Sep 2022` and a green search button. Below the search bar, the interface displays the results of the search, including a timeline view and a table of events. The table has columns for Time and Event. The first event is dated 9/2/22 at 4:36:47 AM, with LogName=Application and EventCode=16384.

Time	Event
9/2/22 4:36:47 AM	LogName=Application EventCode=16384

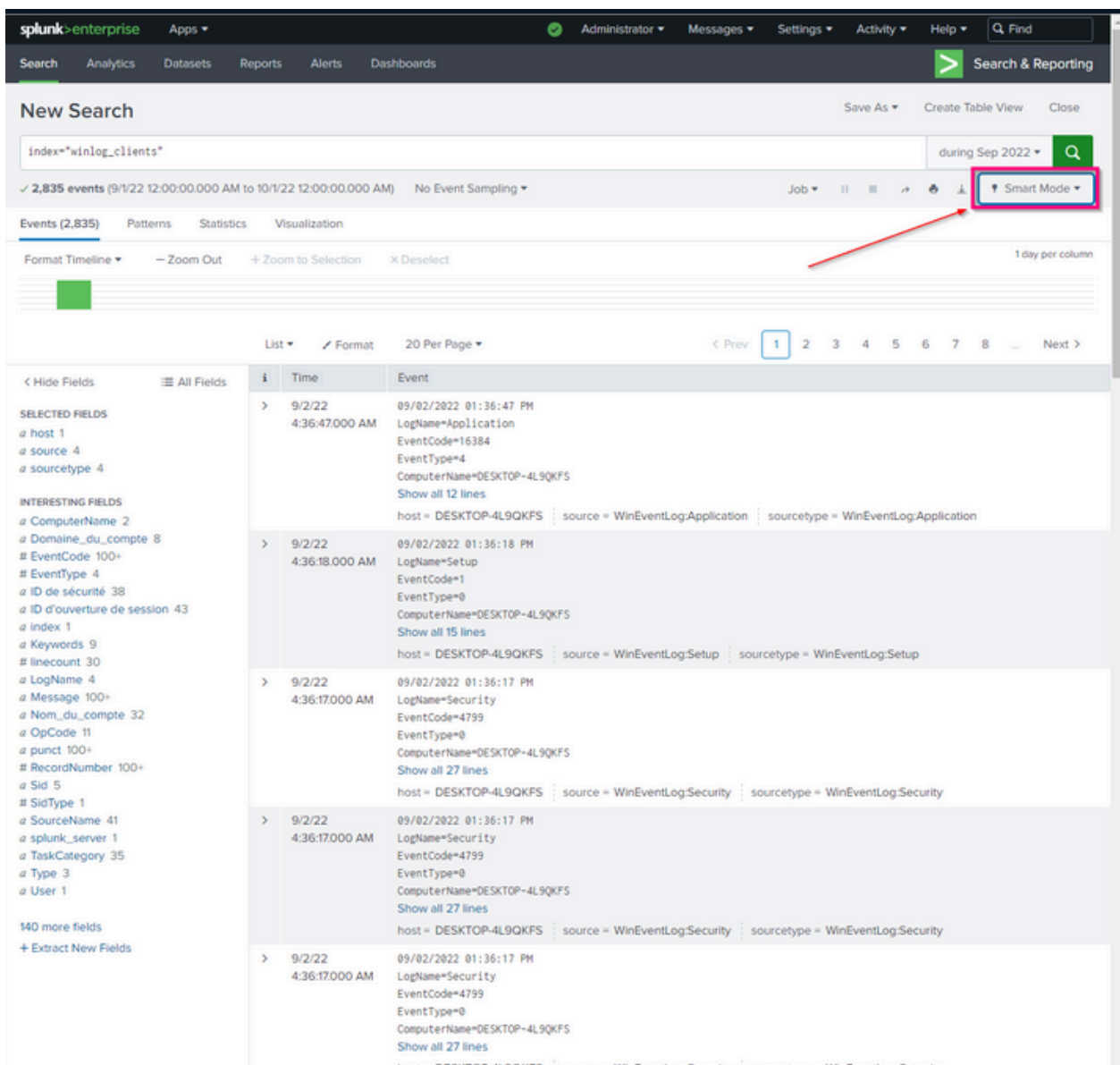
****Timeline:****

Upon conducting a search, Splunk displays a Timeline.



Search Mode:

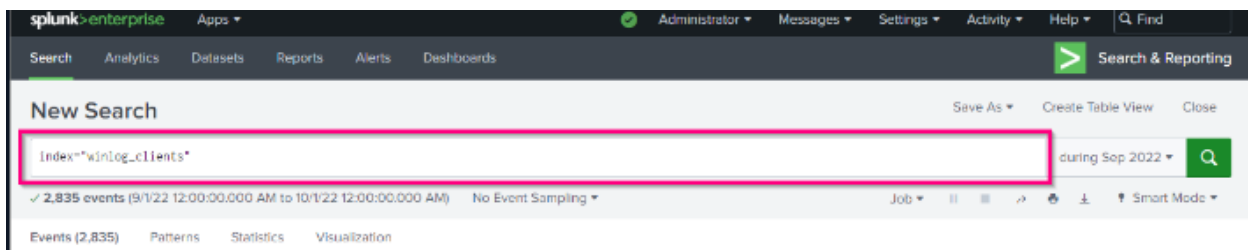
There are three modes, with Smart Mode being the most frequently used.



****Search Bar:****

This is where you formulate your requests. As mentioned earlier, utilize the wildcard character ("*") and operators. Examples include:

- Search for a username with "Je" in it: "Username=Je*"
- Search for connections on the computer named computer1: "eventid=4624 AND computername=computer1"
- Search for every connection on the computer except the domain controller: "eventid=4624 NOT computername=domaincontroller"
- Utilize "Search History."



****Fields:****

Fields are listed on the left, providing information about each field in your search. Select a field to view details.

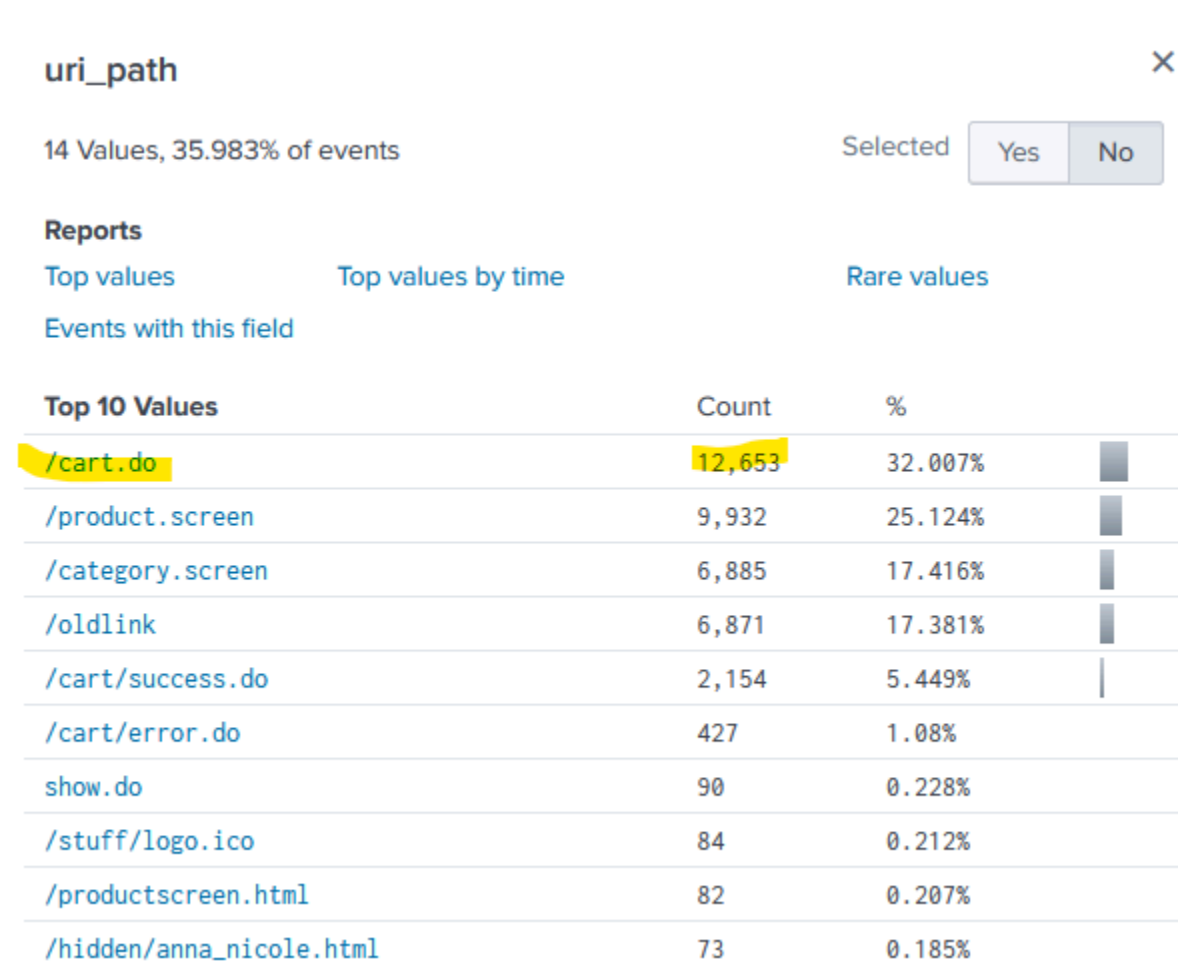


****Save As:****

In this menu, you can opt to save your request as a report, alert, or dashboard.

Quiz Questions

1. Path with the highest number of web requests from the client IP address "128.241.220.82":



i	Time	Event
>	9/8/22 6:20:56.000 PM	182.236.164.11 - - [08/Sep/2022:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=BS-AG-G09&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 2252 "http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 506 host = ip-172-31-30-208.us-east-2.compute.internal source = tutorialdata.zip:/www1/access.log sourcetype = access_combined_wcookie

2. Number of unique client IP addresses requesting the
"/productscreen.html" path:**

uri_path



14 Values, 35.983% of events

Selected

Yes

No

Reports

Top values

Top values by time

Rare values

Events with this field


Top 10 Values	Count	%	
/cart.do	12,653	32.007%	<div></div>
/product.screen	9,932	25.124%	<div></div>
/category.screen	6,885	17.416%	<div></div>
/oldlink	6,871	17.381%	<div></div>
/cart/success.do	2,154	5.449%	<div></div>
/cart/error.do	427	1.08%	<div></div>
show.do	90	0.228%	<div></div>
/stuff/logo.ico	84	0.212%	<div></div>
/productscreen.html	82	0.207%	<div></div>
/hidden/anna_nicole.html	73	0.185%	<div></div>






In Splunk, I'll use the `stats` command along with the `count` function to find the count of unique IP addresses. According to the source data the IP addresses are stored in a field named `clientip`, the search command would look like this:

New Search

Save As ▾Create Table ViewClose

source="tutorialdata.zip:*" host="ip-172-31-30-208.us-east-2.compute.internal" index="letsdefend" uri_path="/productscreen.html" | stats count by clientip

All time ▾

✓ 82 events (before 2/19/24 7:32:10.000 PM)No Event Sampling ▾Job ▾Smart Mode ▾

EventsPatternsStatistics (65)Visualization

clientip

65 Values, 100% of eventsSelecte

Reports

Top valuesTop values by timeRare va

Events with this field

Top 10 Values	Count	%
12.130.60.4	3	3.658%
128.241.220.82	3	3.658%
216.221.226.11	3	3.658%
87.194.216.51	3	3.658%
111.161.27.20	2	2.439%
123.118.73.155	2	2.439%
124.160.192.241	2	2.439%
125.17.14.100	2	2.439%
198.35.3.23	2	2.439%
211.166.11.101	2	2.439%