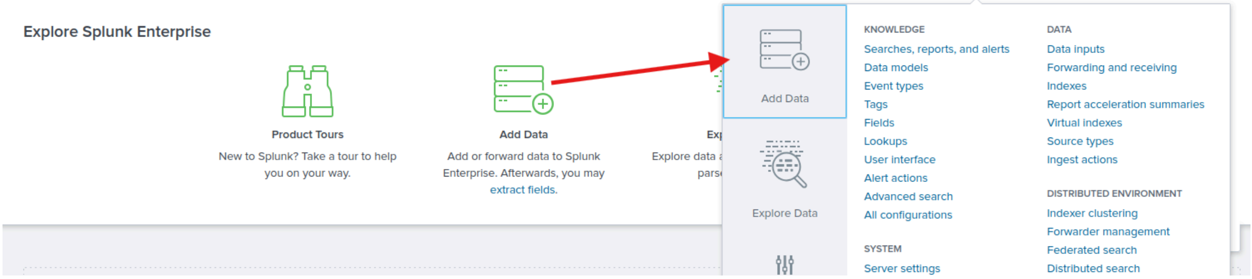
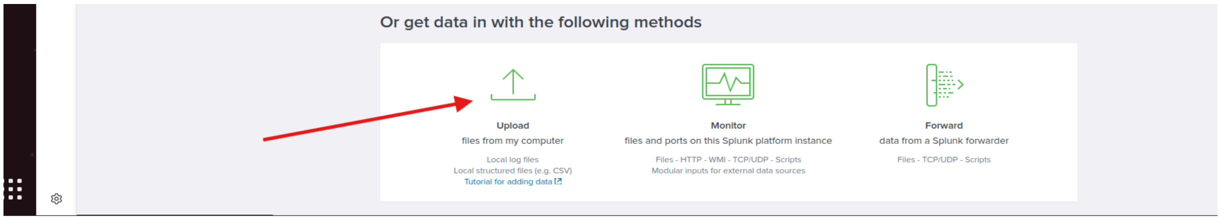
- ## Uploading and Indexing Log Data in Splunk for Analysis

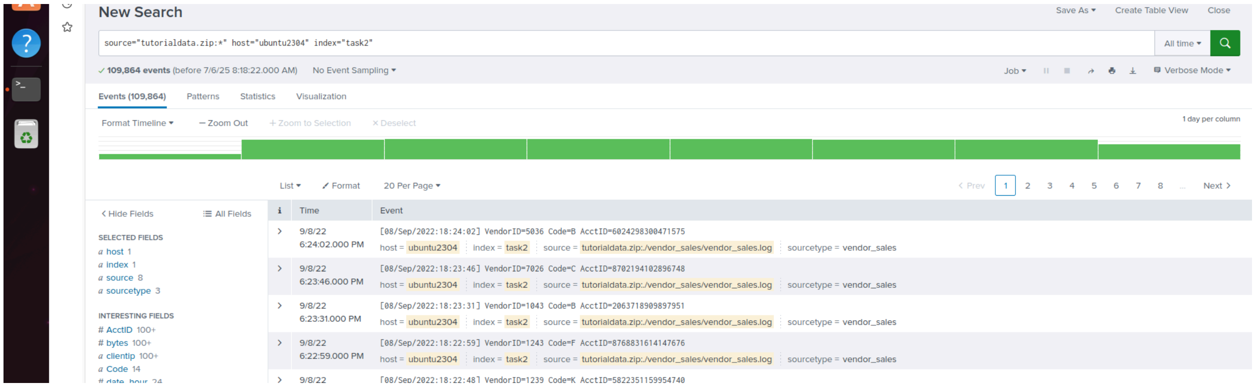
  1-Click "Add Data" from the Splunk Home or Settings menu.

  2-Choose **"Upload"** to upload a file from your local machine.

  3-Click **"Select File"** and browse to the extracted log file location.




Or get data in with the following methods
Upload
files from my computer
Local log files
Local structured files (e.g. CSV)
Tutorial for adding data
Monitor
files and ports on this Splunk platform instance
Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources
Forward
data from a Splunk forwarder
Files - TCP/UDP - Scripts



```
source="tutorialdata.zip:*" host="ubuntu2304" index="task2"
```

✓ 109,864 events (before 7/6/25 8:18:22.000 AM) No Event Sampling

SELECTED FIELDS
a host 1
a index 1
a source 8
a sourcetype 3

INTERESTING FIELDS
AcctID 100+
# bytes 100+
a clientip 100+
a Code 14
# date_hour 24

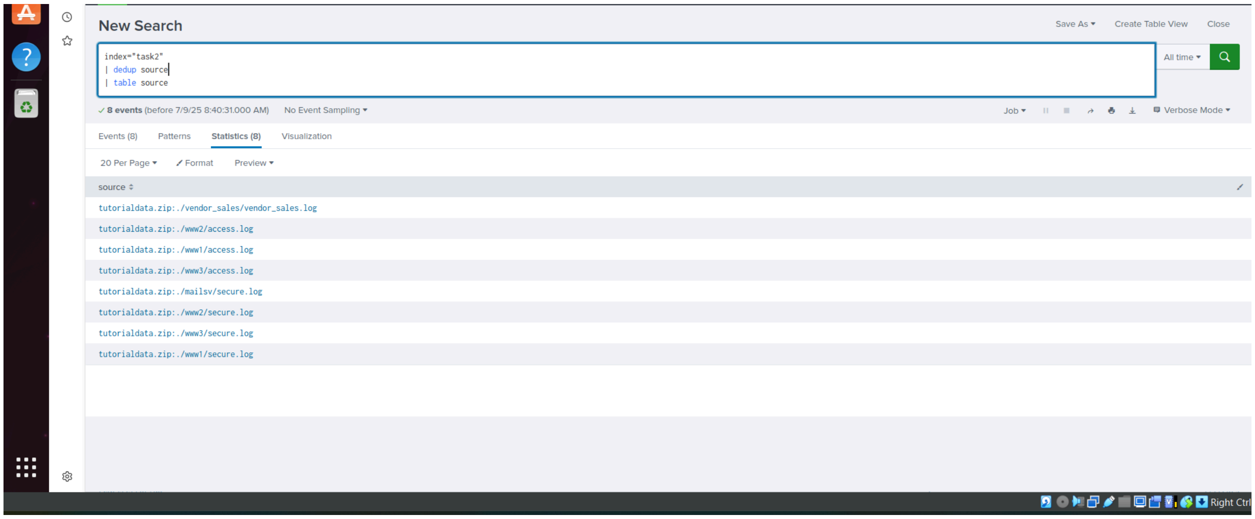
i	Time	Event
>	9/8/22 6:24:02.000 PM	[08/Sep/2022:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575 host = ubuntu2304 index = task2 source = tutorialdata.zip:./vendor_sales/vendor_sales.log sourcetype = vendor_sales
>	9/8/22 6:23:46.000 PM	[08/Sep/2022:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748 host = ubuntu2304 index = task2 source = tutorialdata.zip:./vendor_sales/vendor_sales.log sourcetype = vendor_sales
>	9/8/22 6:23:31.000 PM	[08/Sep/2022:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951 host = ubuntu2304 index = task2 source = tutorialdata.zip:./vendor_sales/vendor_sales.log sourcetype = vendor_sales
>	9/8/22 6:22:59.000 PM	[08/Sep/2022:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676 host = ubuntu2304 index = task2 source = tutorialdata.zip:./vendor_sales/vendor_sales.log sourcetype = vendor_sales
>	9/8/22	[08/Sep/2022:18:22:48] VendorID=1239 Code=K AcctID=5822351159954740

How many events are in this source?

ANS : 109,864

1- How many sources we got after upload the file ?

SPL Used: *index="task2" | dedup source | table source*



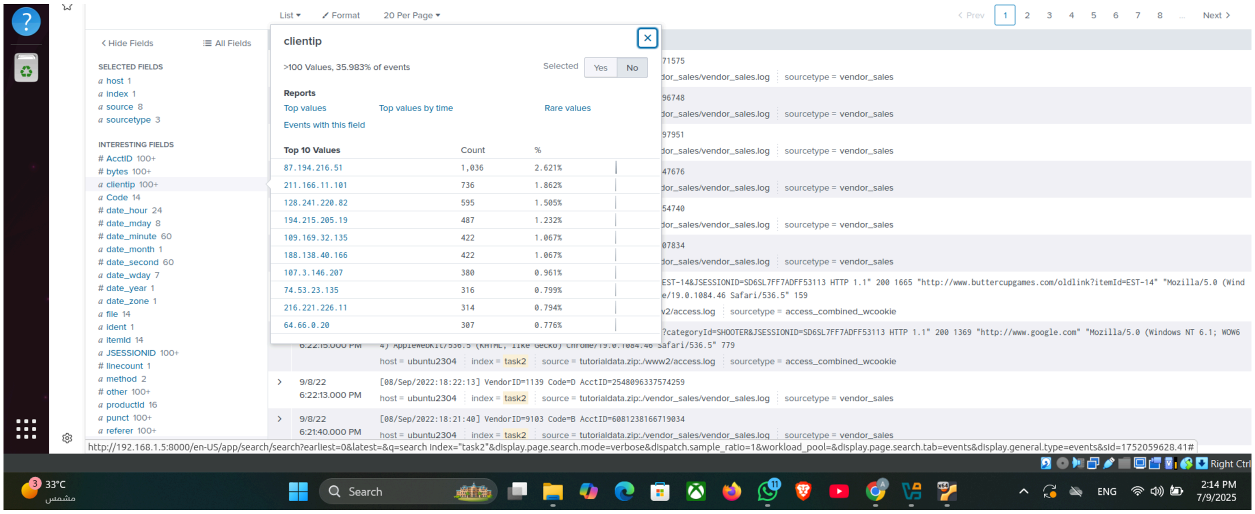
```
index="task2"
| dedup source
| table source
```

✓ 8 events (before 7/9/25 8:40:31.000 AM) No Event Sampling

source
tutorialdata.zip:./vendor_sales/vendor_sales.log
tutorialdata.zip:./www2/access.log
tutorialdata.zip:./www1/access.log
tutorialdata.zip:./www3/access.log
tutorialdata.zip:./mailsv/secure.log
tutorialdata.zip:./www2/secure.log
tutorialdata.zip:./www3/secure.log
tutorialdata.zip:./www1/secure.log

Ans:The number of sources is: 8

2- what is the most client IP mad requests and how many requests he made?



clientip

>100 Values, 35.983% of events

Selected Yes No

Reports

Top values Top values by time Rare values

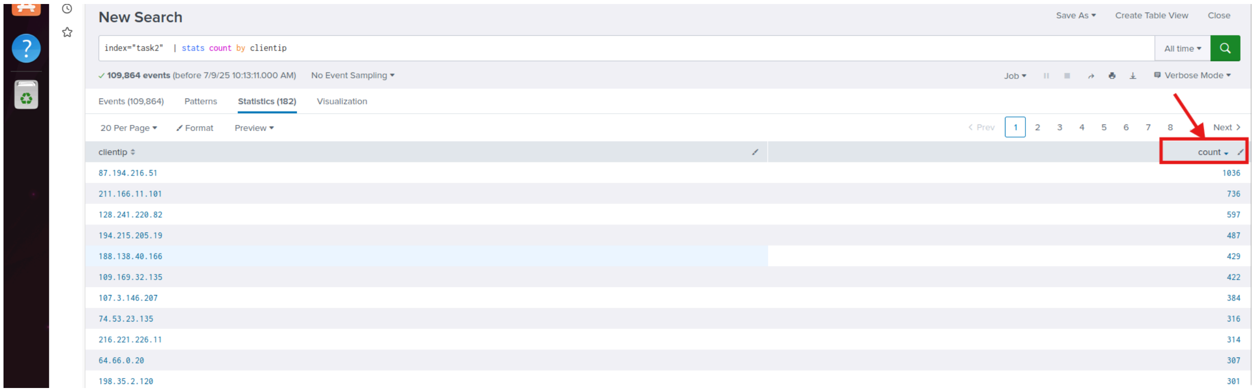
Events with this field

Top 10 Values	Count	%
87.194.216.51	1,036	2.621%
211.166.11.101	736	1.862%
128.241.220.82	595	1.505%
194.215.205.19	487	1.232%
109.169.32.135	422	1.067%
188.138.40.166	422	1.067%
107.3.146.207	380	0.961%
74.53.23.135	316	0.799%
216.221.226.11	314	0.794%
64.66.0.20	307	0.776%

SPL Used:

index="task2" | stats count by clientip

And Click the **count**



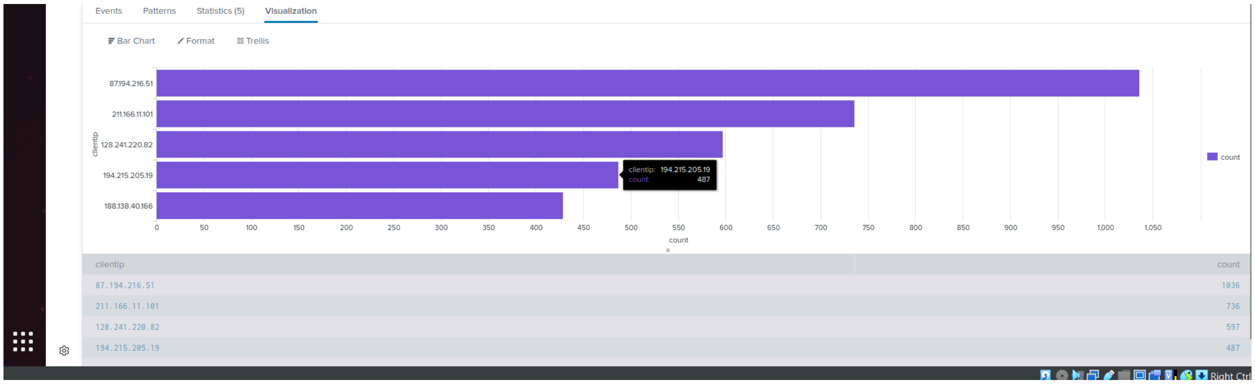
New Search

```
index="task2"  | stats count by clientip
```

✓ 109,864 events (before 7/9/25 10:13:11.000 AM) No Event Sampling

Events (109,864) Patterns Statistics (182) Visualization

clientip	count
87.194.216.51	1036
211.166.11.101	736
128.241.220.82	597
194.215.205.19	487
188.138.40.166	429
109.169.32.135	422
107.3.146.207	384
74.53.23.135	316
216.221.226.11	314
64.66.0.20	307
198.35.2.120	301



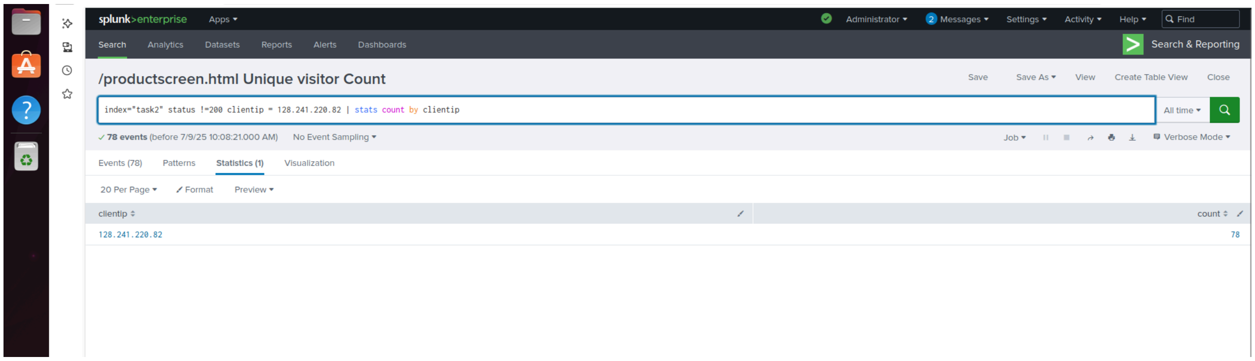
clientip	count
87.194.216.51	1036
211.166.11.101	736
128.241.220.82	597
194.215.205.19	487

Ans:Most Active Client IP: 87.194.216.51

3- how many requests the client IP address “128.241.220.82” sends with status not equal 200?

SPL Used:

index="task2" status!=200 clientip = "128.241.220.82" | stats count by clientip



/productscreen.html Unique visitor Count

```
index="task2" status !=200 clientip = 128.241.220.82 | stats count by clientip
```

✓ 78 events (before 7/9/25 10:08:21.000 AM) No Event Sampling

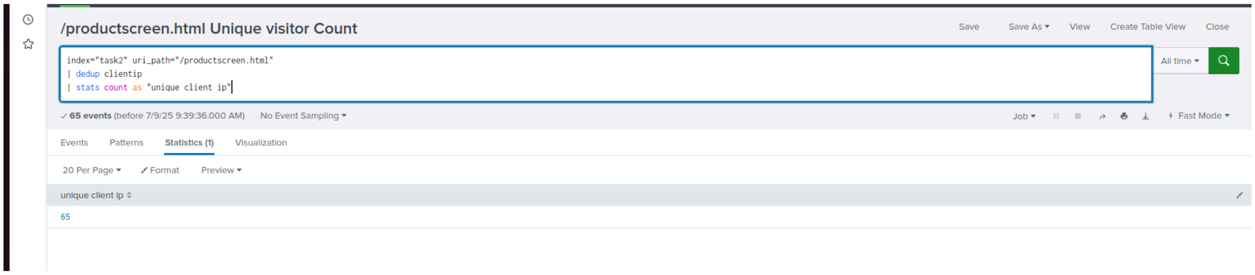
clientip	count
128.241.220.82	78

Ans:Requests with Status Not 200 : 78

4- How many different client IPs are there requesting the "/productscreen.html" path?

SPL Used :

index="task2" uri_path="/productscreen.html" | dedup clientip | stats count as "unique client ip"



/productscreen.html Unique visitor Count

```
index="task2" uri_path="/productscreen.html"
| dedup clientip
| stats count as "unique client ip"
```

✓ 65 events (before 7/9/25 9:39:36.000 AM)

unique client ip
65

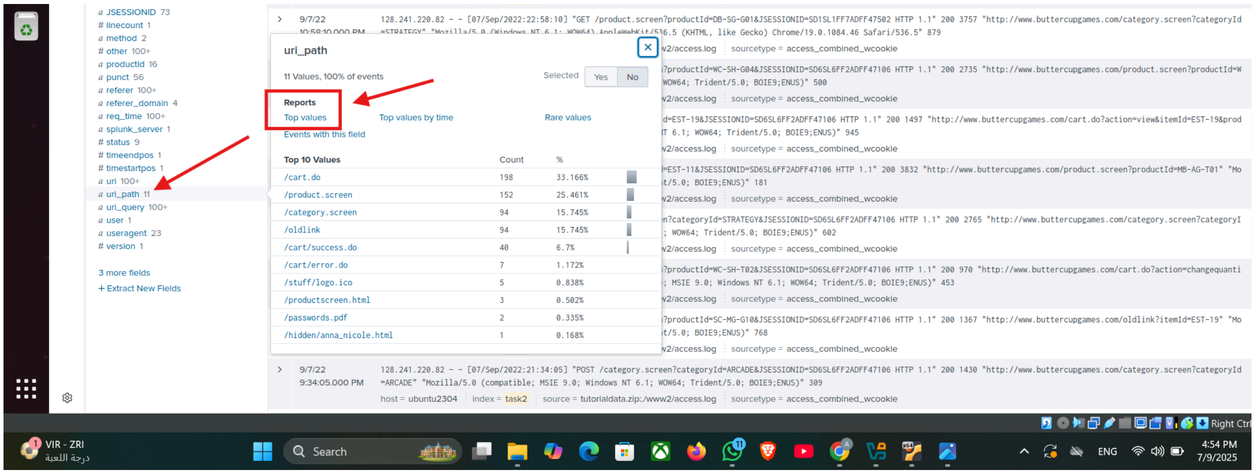
Ans:Number of Different Client IPs: 65

5- What is the path where the client IP address "128.241.220.82" sends the most web requests?

SPL Used:

index="task2" clientip = "128.241.220.82"

1. Click on the `uri_path` field.
2. Select **Top Values**.



uri_path

11 Values, 100% of events

Selected Yes No

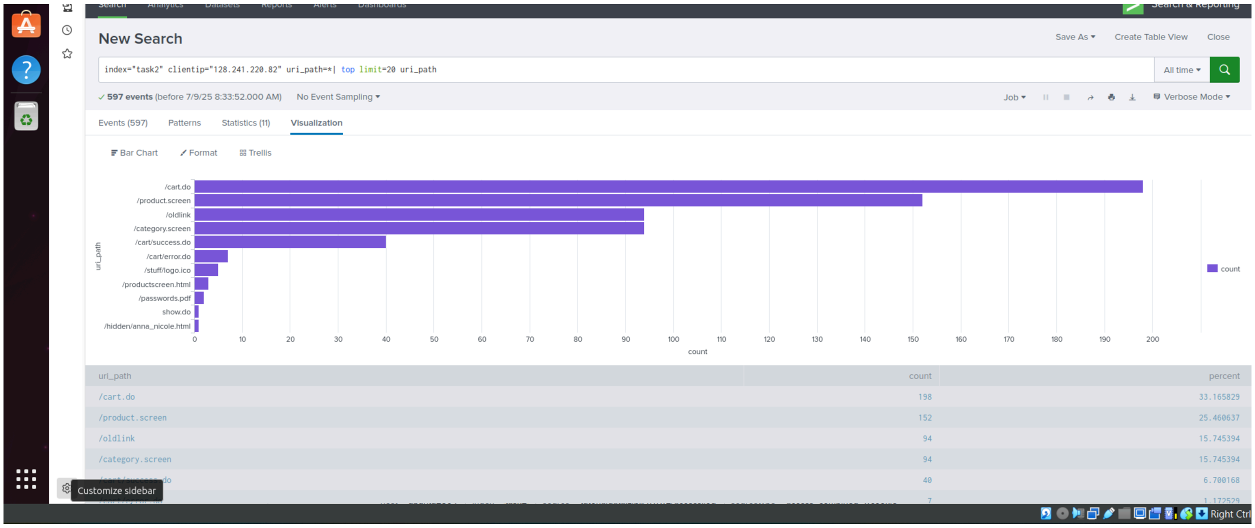
Reports

Top values · Top values by time · Rare values

Events with this field

Top 10 Values	Count	%
/cart.do	198	33.166%
/product.screen	152	25.461%
/category.screen	94	15.745%
/oldlink	94	15.745%
/cart/success.do	40	6.7%
/cart/error.do	7	1.172%
/stuff/logo.ico	5	0.838%
/productscreen.html	3	0.502%
/passwords.pdf	2	0.335%
/hidden/anna_nicole.html	1	0.168%

```
9/7/22          128.241.220.82 - - [07/Sep/2022:22:58:10] "GET /product.screen?productId=DB-SG-G01&JSESSIONID=SD1SL1FF7ADFF47502 HTTP 1.1" 200 3757 "http://www.buttercupgames.com/category.screen?categoryId
10:58:10.000 PM =STRATEGY" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 879
w2/access.log   sourcetype = access_combined_wcookie
?productId=WC-SH-G04&JSESSIONID=SD6SL6FF2ADFF47106 HTTP 1.1" 200 2735 "http://www.buttercupgames.com/product.screen?productId=W
WOW64; Trident/5.0; BOIE9;ENUS)" 500
w2/access.log   sourcetype = access_combined_wcookie
d=EST-19&JSESSIONID=SD6SL6FF2ADFF47106 HTTP 1.1" 200 1497 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-19&prod
T 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 945
w2/access.log   sourcetype = access_combined_wcookie
=EST-11&JSESSIONID=SD6SL6FF2ADFF47106 HTTP 1.1" 200 3832 "http://www.buttercupgames.com/product.screen?productId=MB-AG-T01" "Mo
t/5.0; BOIE9;ENUS)" 181
w2/access.log   sourcetype = access_combined_wcookie
n?categoryId=STRATEGY&JSESSIONID=SD6SL6FF2ADFF47106 HTTP 1.1" 200 2765 "http://www.buttercupgames.com/category.screen?categoryI
; WOW64; Trident/5.0; BOIE9;ENUS)" 602
w2/access.log   sourcetype = access_combined_wcookie
?productId=WC-SH-T02&JSESSIONID=SD6SL6FF2ADFF47106 HTTP 1.1" 200 970 "http://www.buttercupgames.com/cart.do?action=changequanti
; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 453
w2/access.log   sourcetype = access_combined_wcookie
?productId=SC-MG-G10&JSESSIONID=SD6SL6FF2ADFF47106 HTTP 1.1" 200 1367 "http://www.buttercupgames.com/oldlink?itemId=EST-19" "Mo
t/5.0; BOIE9;ENUS)" 768
w2/access.log   sourcetype = access_combined_wcookie
9/7/22          128.241.220.82 - - [07/Sep/2022:21:34:05] "POST /category.screen?categoryId=ARCADE&JSESSIONID=SD6SL6FF2ADFF47106 HTTP 1.1" 200 1430 "http://www.buttercupgames.com/category.screen?categoryId
9:34:05.000 PM  =ARCADE" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 309
                host = ubuntu2304   index = task2   source = tutorialdata.zip:./www2/access.log   sourcetype = access_combined_wcookie
```

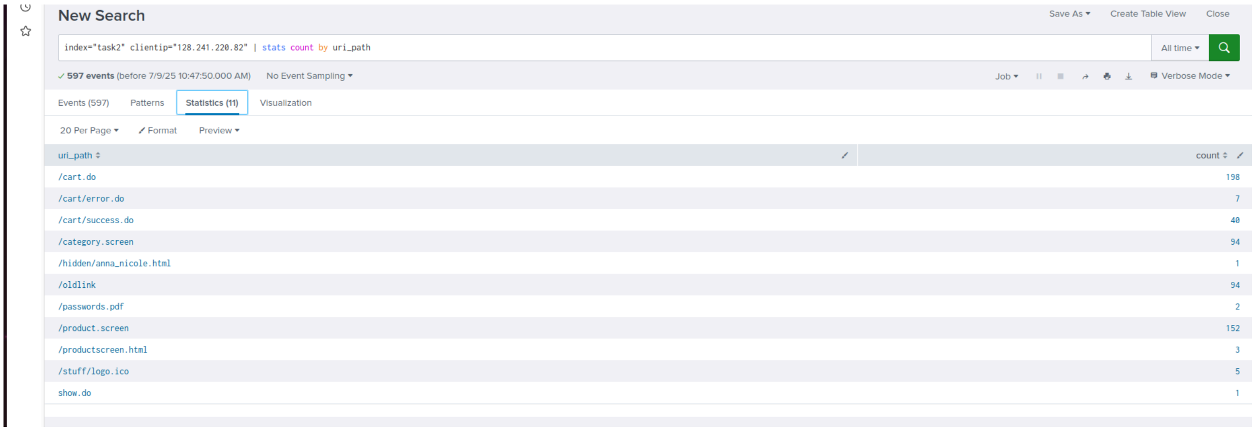


New Search

```
index="task2" clientip="128.241.220.82" uri_path=*| top limit=20 uri_path
```

✓ 597 events (before 7/9/25 8:33:52.000 AM) No Event Sampling ▾

uri_path	count	percent
/cart.do	198	33.165829
/product.screen	152	25.460637
/oldlink	94	15.745394
/category.screen	94	15.745394
/cart/success.do	40	6.700168
/cart/error.do	7	1.172529



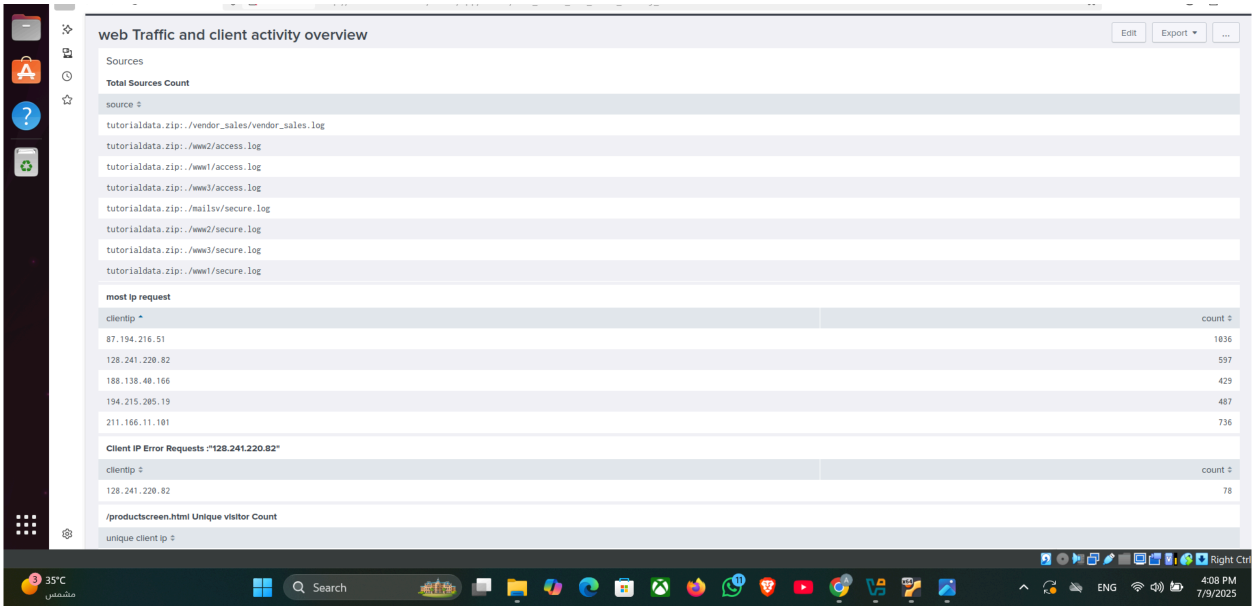
```
index="task2" clientip="128.241.220.82" | stats count by uri_path
```

✓ **597 events** (before 7/9/25 10:47:50.000 AM) No Event Sampling

uri_path	count
/cart.do	198
/cart/error.do	7
/cart/success.do	40
/category.screen	94
/hidden/anna_nicole.html	1
/oldlink	94
/passwords.pdf	2
/product.screen	152
/productscreen.html	3
/stuff/logo.ico	5
show.do	1

Ans: Most Requested Path: /cart.do

Dashboard Overview:



web Traffic and client activity overview

Sources

Total Sources Count

source ⇕
tutorialdata.zip:./vendor_sales/vendor_sales.log
tutorialdata.zip:./www2/access.log
tutorialdata.zip:./www1/access.log
tutorialdata.zip:./www3/access.log
tutorialdata.zip:./mailsv/secure.log
tutorialdata.zip:./www2/secure.log
tutorialdata.zip:./www3/secure.log
tutorialdata.zip:./www1/secure.log

most Ip request

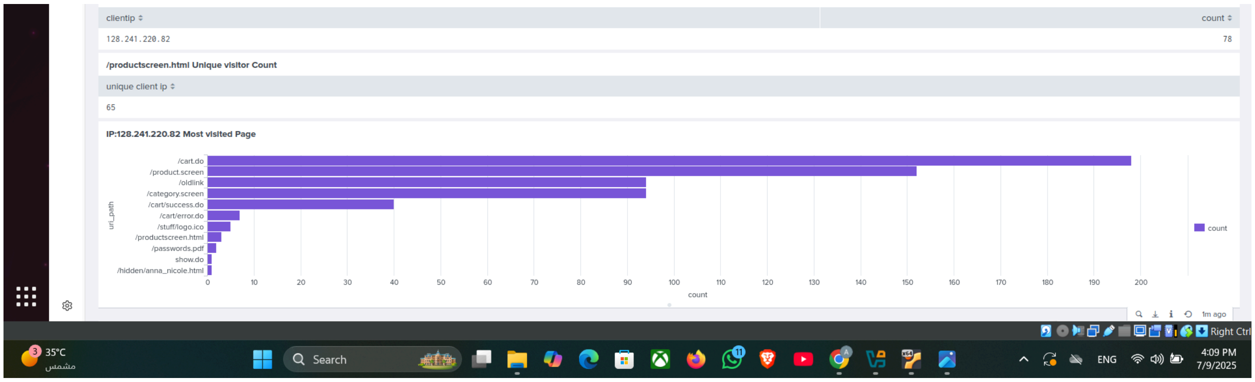
clientip ˄	count ⇕
87.194.216.51	1036
128.241.220.82	597
188.138.40.166	429
194.215.205.19	487
211.166.11.101	736

Client IP Error Requests :"128.241.220.82"

clientip ⇕	count ⇕
128.241.220.82	78

/productscreen.html Unique visitor Count

unique client ip ⇕



clientip ⇕	count ⇕
128.241.220.82	78

/productscreen.html Unique visitor Count

unique client ip ⇕
65

IP:128.241.220.82 Most visited Page