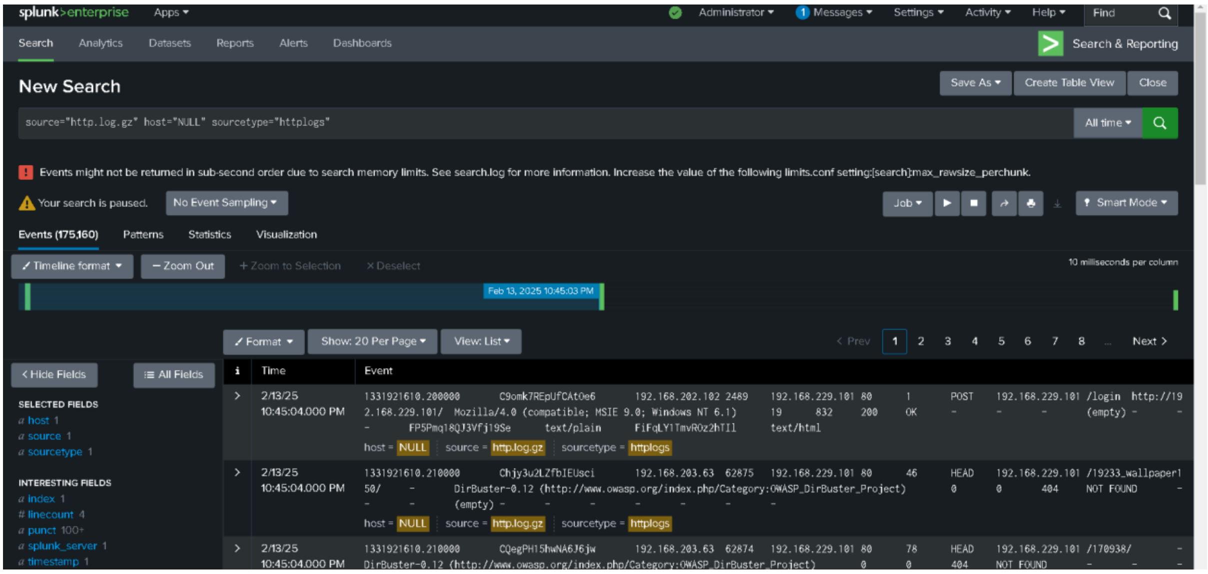
# HTTP Log Analysis Using Splunk

Analyzing the HTTP Log file using Splunk SIEM

HTTP Log Ingestion



New Search

```
source="http.log.gz" host="NULL" sourcetype="httplogs"
```

Events might not be returned in sub-second order due to search memory limits. See search.log for more information. Increase the value of the following limits.conf setting:[search]:max_rawsize_perchunk.

Your search is paused. No Event Sampling ▾

Events (175,160)

10 milliseconds per column

Feb 13, 2025 10:45:03 PM

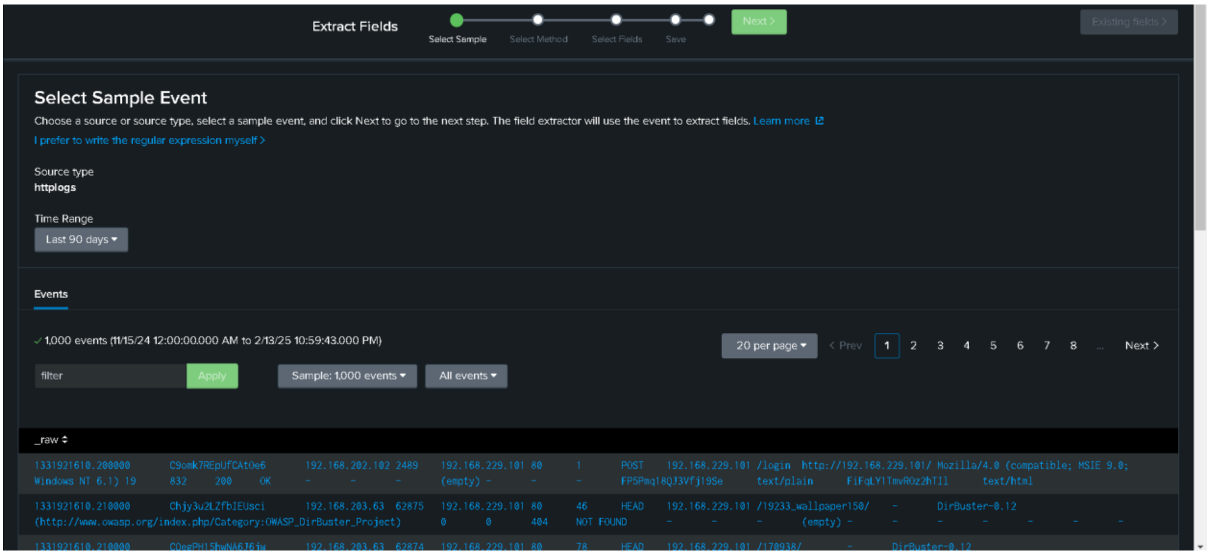
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a index 1
# linecount 4
a punct 100+
a splunk_server 1
a timestamp 1

```
i  Time                 Event
>  2/13/25              1331921610.200000       C9omk7REpUfCAtOe6       192.168.202.102 2489    192.168.229.101 80      1       POST    192.168.229.101 /login  http://19
   10:45:04.000 PM      2.168.229.101/  Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1)      19      832     200     OK      -       -       -       (empty) -       -
                        -       FP5Pmq18QJ3Vfj19Se      text/plain      FiFqLY1TmvROz2hTIl      text/html
                        host = NULL   source = http.log.gz   sourcetype = httplogs
>  2/13/25              1331921610.210000       Chjy3u2LZfbIEUsci       192.168.203.63  62875   192.168.229.101 80      46      HEAD    192.168.229.101 /19233_wallpaper1
   10:45:04.000 PM      50/     -       DirBuster-0.12 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)       0       0       404     NOT FOUND       -
                        -       -       (empty) -       -       -       -       -       -
                        host = NULL   source = http.log.gz   sourcetype = httplogs
>  2/13/25              1331921610.210000       CQegPH15hwNA6J6jw       192.168.203.63  62874   192.168.229.101 80      78      HEAD    192.168.229.101 /170938/        -
   10:45:04.000 PM      DirBuster-0.12 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)       0       0       404     NOT FOUND       -       -       -
```

Parsing the data by extracting new fields

Selecting a sample event for field extraction



Select Sample Event

Choose a source or source type, select a sample event, and click Next to go to the next step. The field extractor will use the event to extract fields.

Source type
**httplogs**

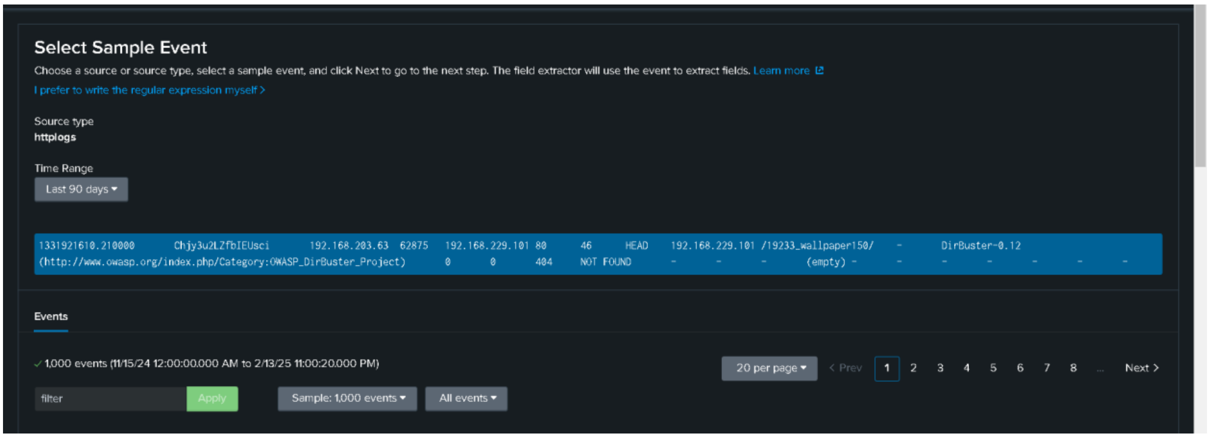
Time Range
Last 90 days ▾

Events

✓ 1,000 events (11/15/24 12:00:00.000 AM to 2/13/25 10:59:43.000 PM)

Sample: 1,000 events ▾

```
_raw ⇕
1331921610.200000       C9omk7REpUfCAtOe6       192.168.202.102 2489    192.168.229.101 80      1       POST    192.168.229.101 /login  http://192.168.229.101/ Mozilla/4.0 (compatible; MSIE 9.0;
Windows NT 6.1) 19      832     200     OK      -       -       -       (empty) -       -       -       FP5Pmq18QJ3Vfj19Se      text/plain      FiFqLY1TmvROz2hTIl      text/html
1331921610.210000       Chjy3u2LZfbIEUsci       192.168.203.63  62875   192.168.229.101 80      46      HEAD    192.168.229.101 /19233_wallpaper150/    -       DirBuster-0.12
(http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)       0       0       404     NOT FOUND       -       -       -       (empty) -       -       -       -       -       -
1331921610.210000       CQegPH15hwNA6J6jw       192.168.203.63  62874   192.168.229.101 80      78      HEAD    192.168.229.101 /170938/        -       DirBuster-0.12
```



**Select Sample Event**

Choose a source or source type, select a sample event, and click Next to go to the next step. The field extractor will use the event to extract fields. Learn more

I prefer to write the regular expression myself >

Source type
**httplogs**

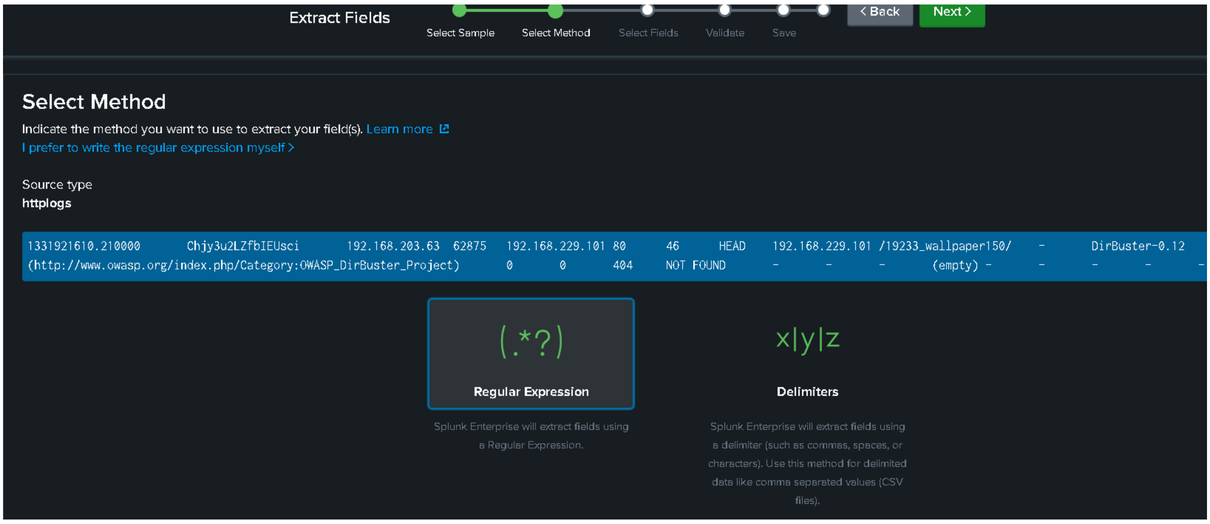
Time Range
Last 90 days ▾

```
1331921610.210000       Chjy3u2LZfbIEUsci       192.168.203.63  62875   192.168.229.101 80      46      HEAD    192.168.229.101 /19233_wallpaper150/    -       DirBuster-0.12
(http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)       0       0       404     NOT FOUND       -       -       -       (empty) -       -       -       -       -       -       -
```

Events

✓ 1,000 events (11/15/24 12:00:00.000 AM to 2/13/25 11:00:20.000 PM)

selecting regular expression method



**Select Method**

Indicate the method you want to use to extract your field(s). Learn more

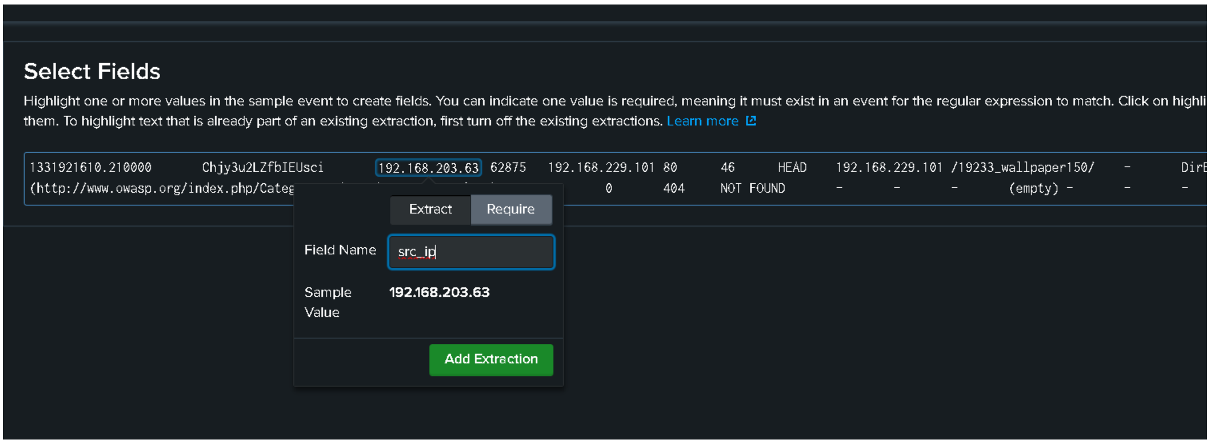
I prefer to write the regular expression myself >

Source type
**httplogs**

```
1331921610.210000       Chjy3u2LZfbIEUsci       192.168.203.63  62875   192.168.229.101 80      46      HEAD    192.168.229.101 /19233_wallpaper150/    -       DirBuster-0.12
(http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)       0       0       404     NOT FOUND       -       -       -       (empty) -       -       -       -
```

Splunk Enterprise will extract fields using a Regular Expression.

Splunk Enterprise will extract fields using a delimiter (such as commas, spaces, or characters). Use this method for delimited data like comma separated values (CSV files).



**Select Fields**

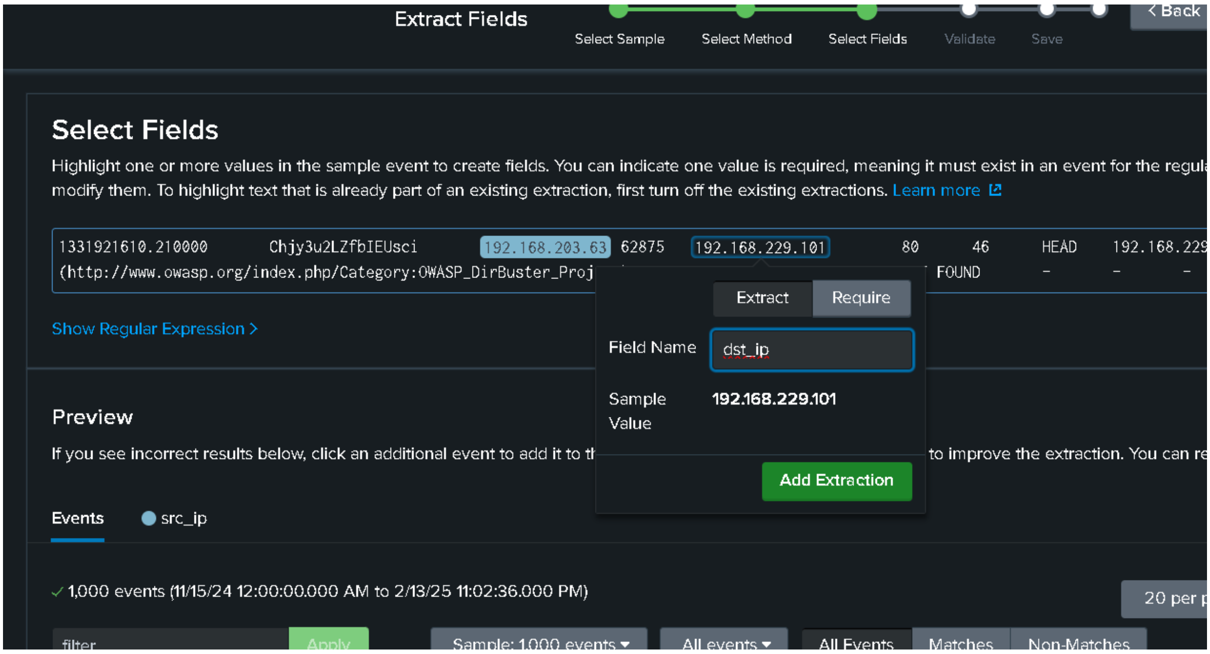
Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression to match. Click on highli them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. Learn more

```
1331921610.210000       Chjy3u2LZfbIEUsci       192.168.203.63  62875   192.168.229.101 80      46      HEAD    192.168.229.101 /19233_wallpaper150/    -       DirE
(http://www.owasp.org/index.php/Categ                                   0       404     NOT FOUND       -       -       -       (empty) -       -       -
```

Field Name: src_ip

Sample Value: 192.168.203.63

selecting 192.168.203.63 as the source ip src_ip



Select Fields

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regul
modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. Learn more

```
1331921610.210000        Chjy3u2LZfbIEUsci        192.168.203.63  62875  192.168.229.101        80     46      HEAD     192.168.229
(http://www.owasp.org/index.php/Category:OWASP_DirBuster_Proj                                       FOUND      -        -       -
```

Field Name: dst_ip

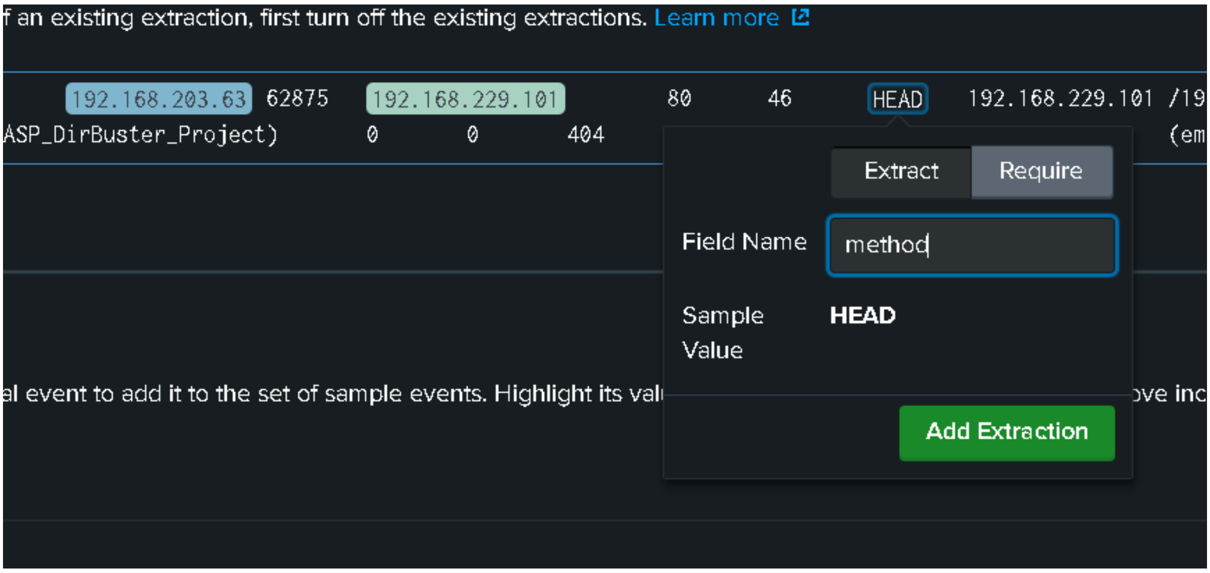
Sample Value: 192.168.229.101

Preview

If you see incorrect results below, click an additional event to add it to th … to improve the extraction. You can re

✓ 1,000 events (11/15/24 12:00:00.000 AM to 2/13/25 11:02:36.000 PM)

192.168.229.101 as the destination ip dst_ip



f an existing extraction, first turn off the existing extractions. Learn more

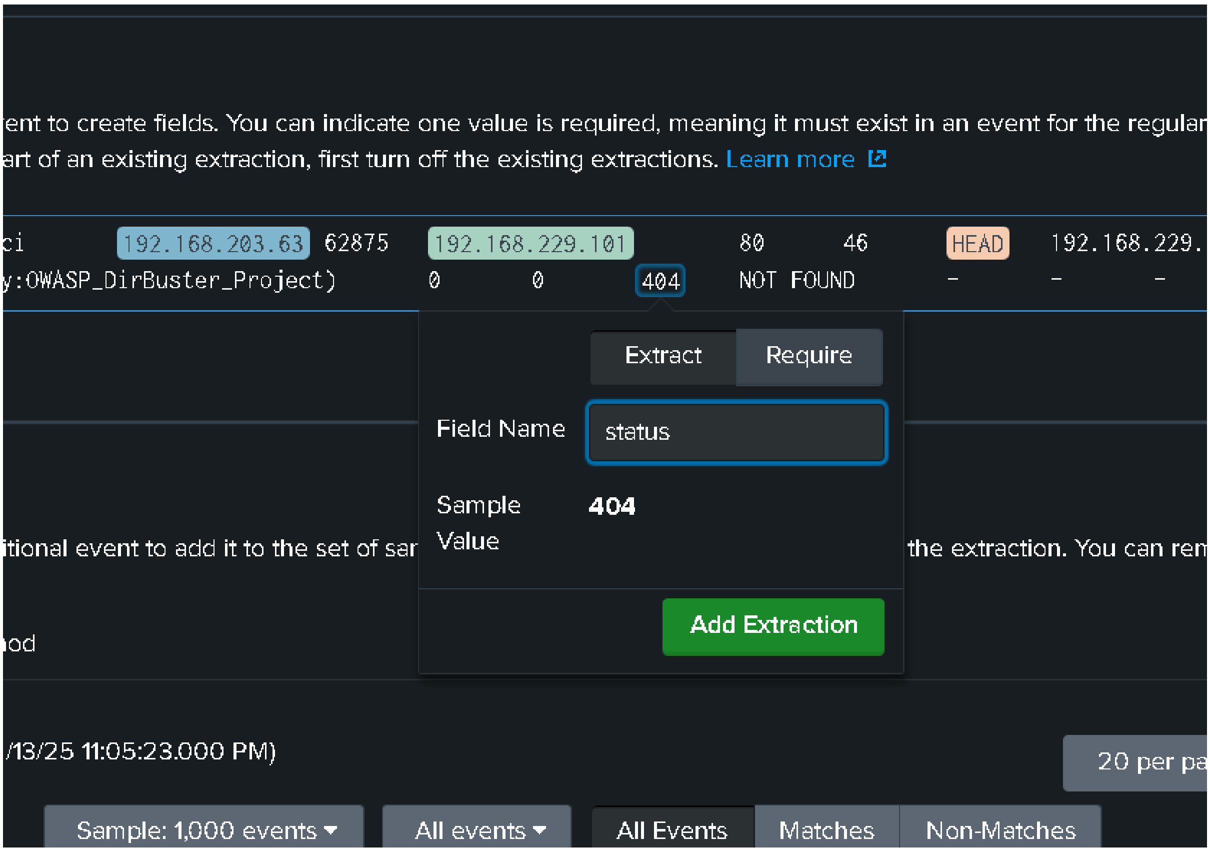
```
 192.168.203.63  62875   192.168.229.101       80      46      HEAD    192.168.229.101  /19
ASP_DirBuster_Project)   0         0       404                                           (em
```

Field Name: method

Sample Value: HEAD

al event to add it to the set of sample events. Highlight its valu … ove inc

HEAD – the http request method



ent to create fields. You can indicate one value is required, meaning it must exist in an event for the regular
art of an existing extraction, first turn off the existing extractions. Learn more

```
ci          192.168.203.63  62875   192.168.229.101     80    46     HEAD   192.168.229.
y:OWASP_DirBuster_Project)          0        0      404  NOT FOUND    -      -       -
```

Field Name: status

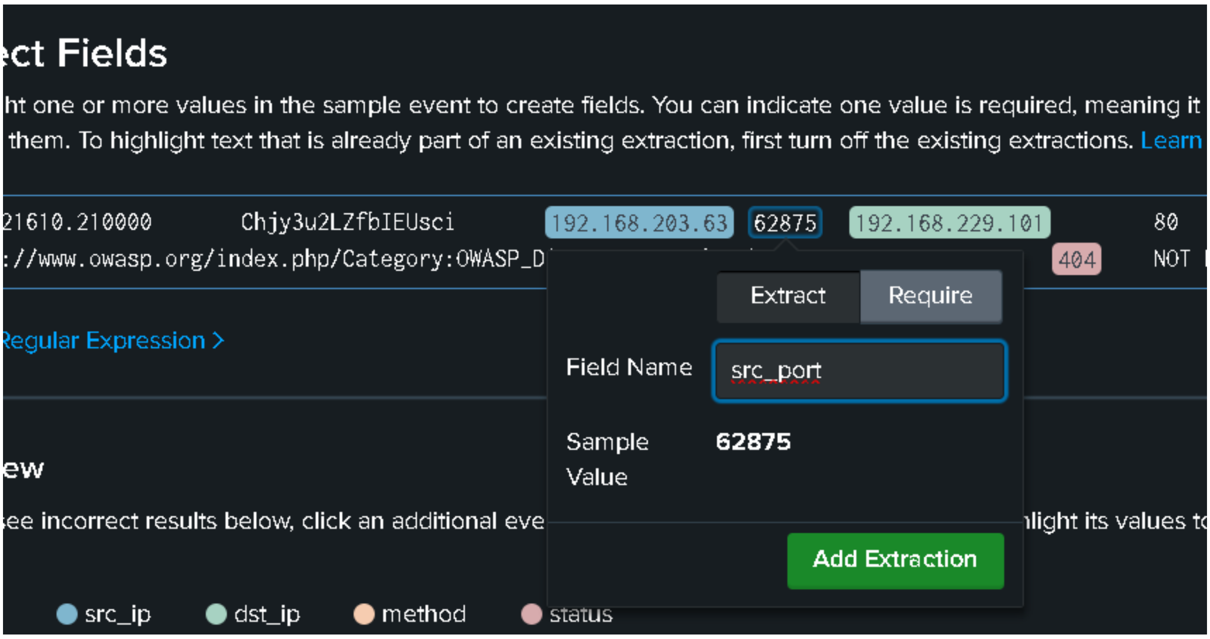
Sample Value: **404**

itional event to add it to the set of sar … the extraction. You can rem

od

/13/25 11:05:23.000 PM)

extracting the status code of the response



ct Fields

ht one or more values in the sample event to create fields. You can indicate one value is required, meaning it
them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. Learn

```
21610.210000        Chjy3u2LZfbIEUsci        192.168.203.63  62875   192.168.229.101     80
://www.owasp.org/index.php/Category:OWASP_D                                     404      NOT
```

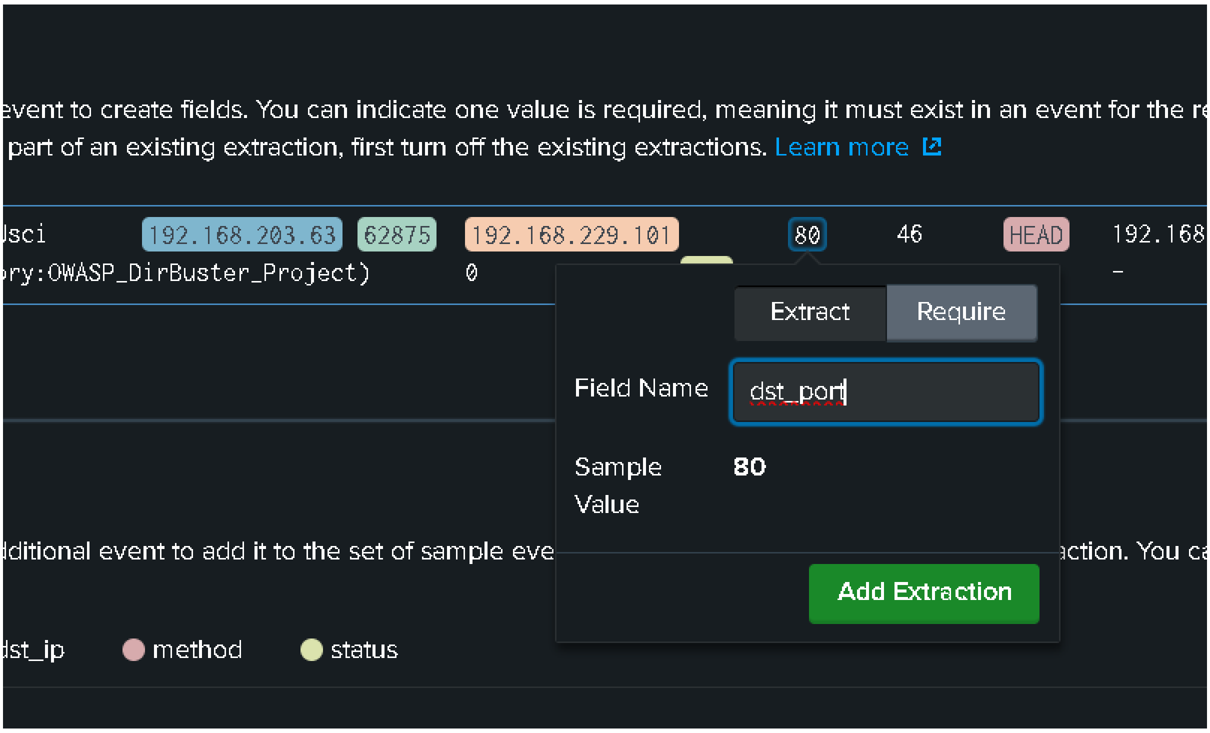
Field Name: src_port

Sample Value: **62875**

ew

ee incorrect results below, click an additional eve … hlight its values to

src_port



event to create fields. You can indicate one value is required, meaning it must exist in an event for the re
part of an existing extraction, first turn off the existing extractions. Learn more

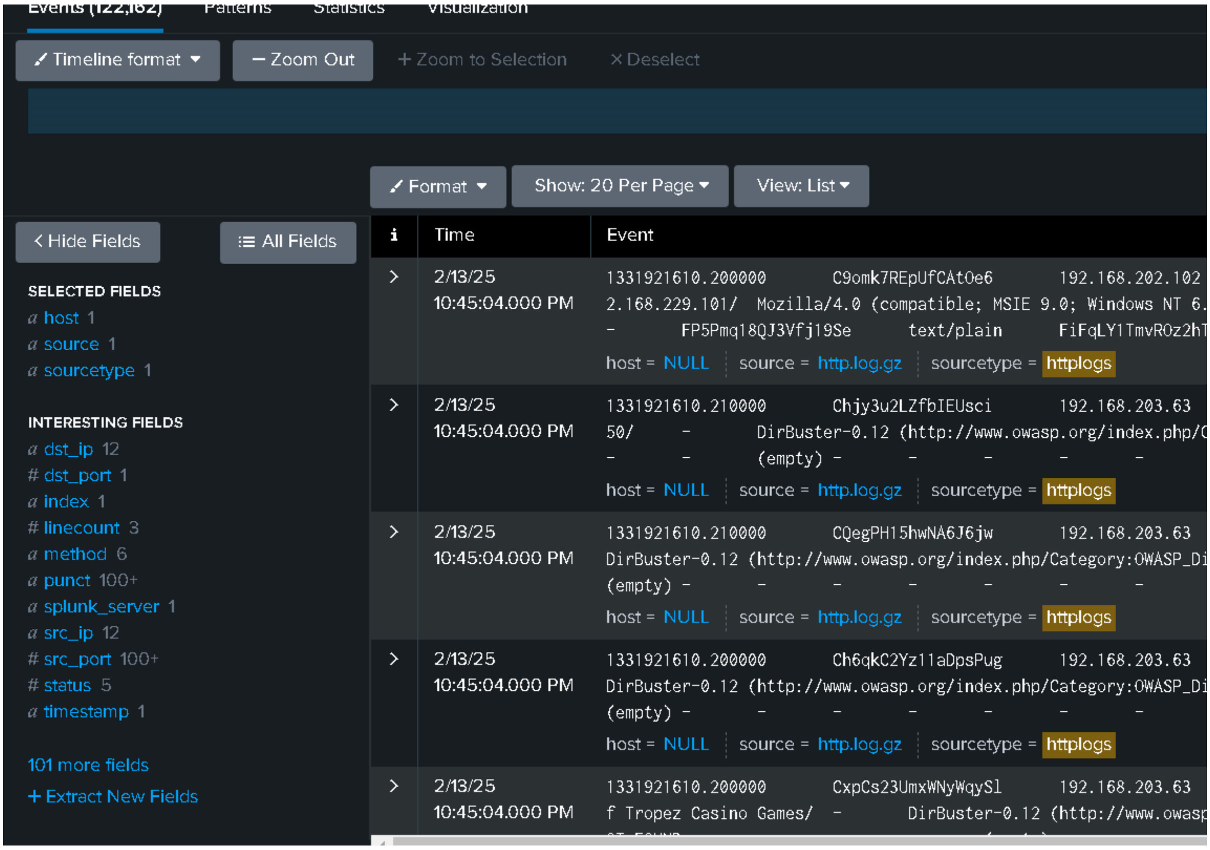
```
Jsci          192.168.203.63  62875  192.168.229.101     80     46    HEAD    192.168
ory:OWASP_DirBuster_Project)          0                                       -
```

Field Name: dst_port

Sample Value: 80

dditional event to add it to the set of sample eve … action. You ca

destination port no.



SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

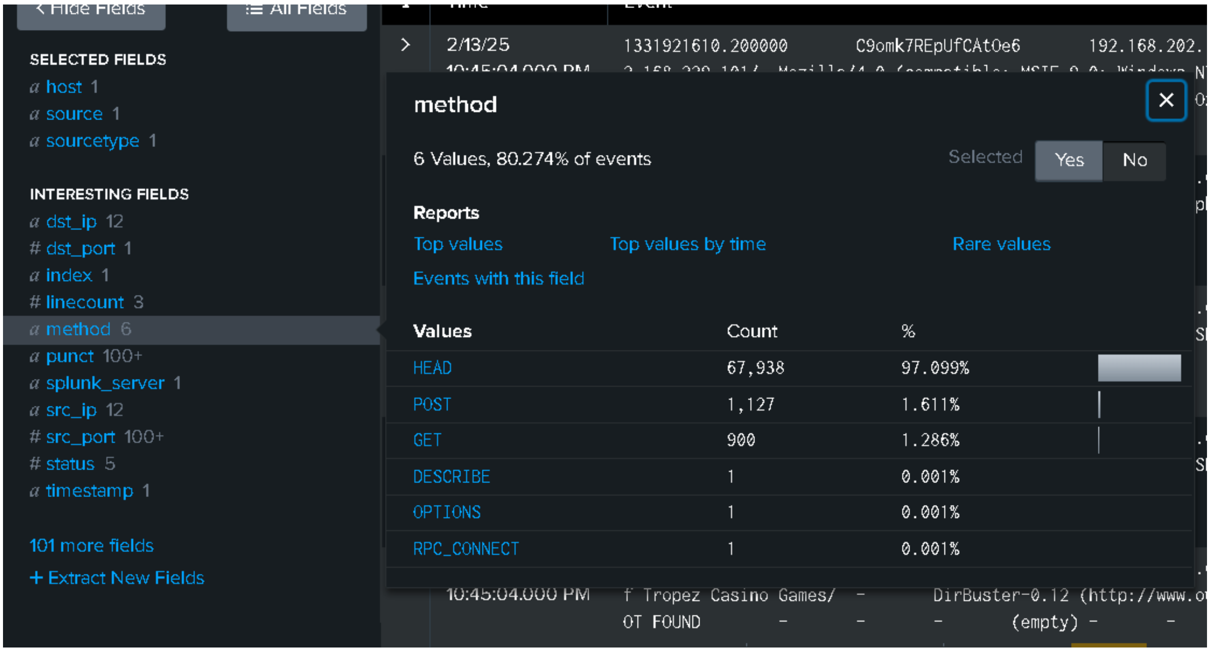
INTERESTING FIELDS
- a dst_ip 12
- # dst_port 1
- a index 1
- # linecount 3
- a method 6
- a punct 100+
- a splunk_server 1
- a src_ip 12
- # src_port 100+
- # status 5
- a timestamp 1

101 more fields

+ Extract New Fields

| i | Time | Event |
|---|---|---|
| > | 2/13/25<br>10:45:04.000 PM | 1331921610.200000 C9omk7REpUfCAtOe6 192.168.202.102<br>2.168.229.101/ Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.<br>- FP5Pmq18QJ3Vfj19Se text/plain FiFqLY1TmvROz2hT<br>host = NULL source = http.log.gz sourcetype = httplogs |
| > | 2/13/25<br>10:45:04.000 PM | 1331921610.210000 Chjy3u2LZfbIEUsci 192.168.203.63<br>50/ - DirBuster-0.12 (http://www.owasp.org/index.php/C<br>- - (empty) - - - - -<br>host = NULL source = http.log.gz sourcetype = httplogs |
| > | 2/13/25<br>10:45:04.000 PM | 1331921610.210000 CQegPH15hwNA6J6jw 192.168.203.63<br>DirBuster-0.12 (http://www.owasp.org/index.php/Category:OWASP_Di<br>(empty) - - - - - - -<br>host = NULL source = http.log.gz sourcetype = httplogs |
| > | 2/13/25<br>10:45:04.000 PM | 1331921610.200000 Ch6qkC2Yz11aDpsPug 192.168.203.63<br>DirBuster-0.12 (http://www.owasp.org/index.php/Category:OWASP_Di<br>(empty) - - - - - - -<br>host = NULL source = http.log.gz sourcetype = httplogs |
| > | 2/13/25<br>10:45:04.000 PM | 1331921610.200000 CxpCs23UmxWNyWqySl 192.168.203.63<br>f Tropez Casino Games/ - DirBuster-0.12 (http://www.owasp |

The extracted fields



SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a dst_ip 12
# dst_port 1
a index 1
# linecount 3
a method 6
a punct 100+
a splunk_server 1
a src_ip 12
# src_port 100+
# status 5
a timestamp 1

101 more fields
+ Extract New Fields

**method**

6 Values, 80.274% of events

Selected: [✓ Yes] No

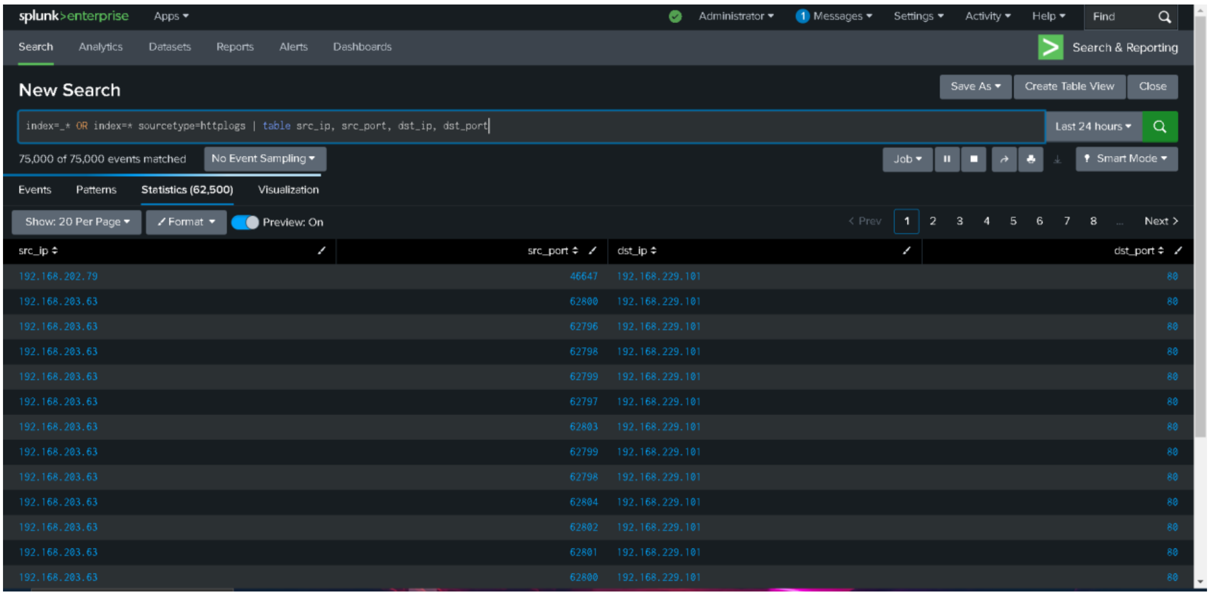
**Reports**

Top values | Top values by time | Rare values

Events with this field

| Values | Count | % |
|---|---|---|
| HEAD | 67,938 | 97.099% |
| POST | 1,127 | 1.611% |
| GET | 900 | 1.286% |
| DESCRIBE | 1 | 0.001% |
| OPTIONS | 1 | 0.001% |
| RPC_CONNECT | 1 | 0.001% |

Table view of the source and destination ip, ports



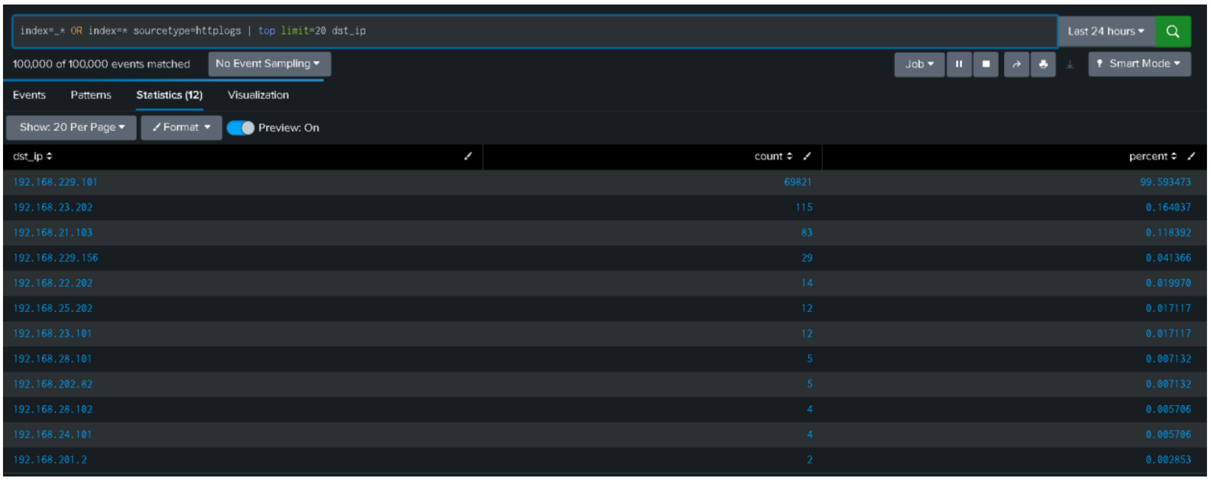
New Search

```
index=_* OR index=* sourcetype=httplogs | table src_ip, src_port, dst_ip, dst_port
```

75,000 of 75,000 events matched | No Event Sampling

| src_ip | src_port | dst_ip | dst_port |
|---|---|---|---|
| 192.168.202.79 | 46647 | 192.168.229.101 | 80 |
| 192.168.203.63 | 62800 | 192.168.229.101 | 80 |
| 192.168.203.63 | 62796 | 192.168.229.101 | 80 |
| 192.168.203.63 | 62798 | 192.168.229.101 | 80 |
| 192.168.203.63 | 62799 | 192.168.229.101 | 80 |
| 192.168.203.63 | 62797 | 192.168.229.101 | 80 |
| 192.168.203.63 | 62803 | 192.168.229.101 | 80 |
| 192.168.203.63 | 62799 | 192.168.229.101 | 80 |
| 192.168.203.63 | 62798 | 192.168.229.101 | 80 |
| 192.168.203.63 | 62804 | 192.168.229.101 | 80 |
| 192.168.203.63 | 62802 | 192.168.229.101 | 80 |
| 192.168.203.63 | 62801 | 192.168.229.101 | 80 |
| 192.168.203.63 | 62800 | 192.168.229.101 | 80 |

Top count through filtering of destination ip address



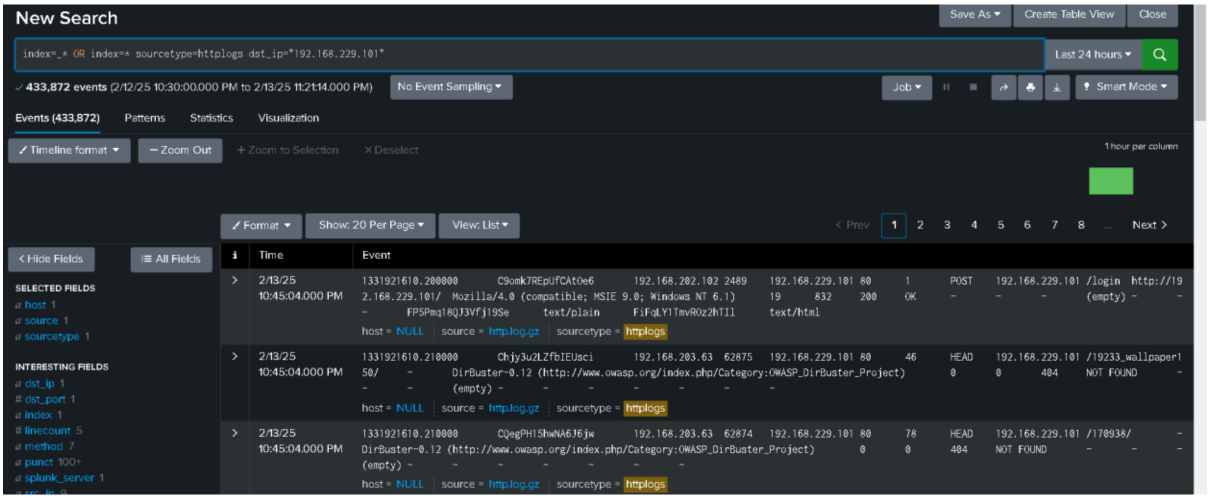
```
index=_* OR index=* sourcetype=httplogs | top limit=20 dst_ip
```

100,000 of 100,000 events matched

| dst_ip | count | percent |
|---|---|---|
| 192.168.229.101 | 69821 | 99.593473 |
| 192.168.23.202 | 115 | 0.164037 |
| 192.168.21.103 | 83 | 0.118392 |
| 192.168.229.156 | 29 | 0.041366 |
| 192.168.22.202 | 14 | 0.019970 |
| 192.168.25.202 | 12 | 0.017117 |
| 192.168.23.101 | 12 | 0.017117 |
| 192.168.28.101 | 5 | 0.007132 |
| 192.168.202.82 | 5 | 0.007132 |
| 192.168.28.102 | 4 | 0.005706 |
| 192.168.24.101 | 4 | 0.005706 |
| 192.168.201.2 | 2 | 0.002853 |

As we can see 192.168.229.101 Ip address has got 433872 requests

To get all the events of the 192.168.229.101 ip address



New Search

```
index=_* OR index=* sourcetype=httplogs dst_ip="192.168.229.101"
```

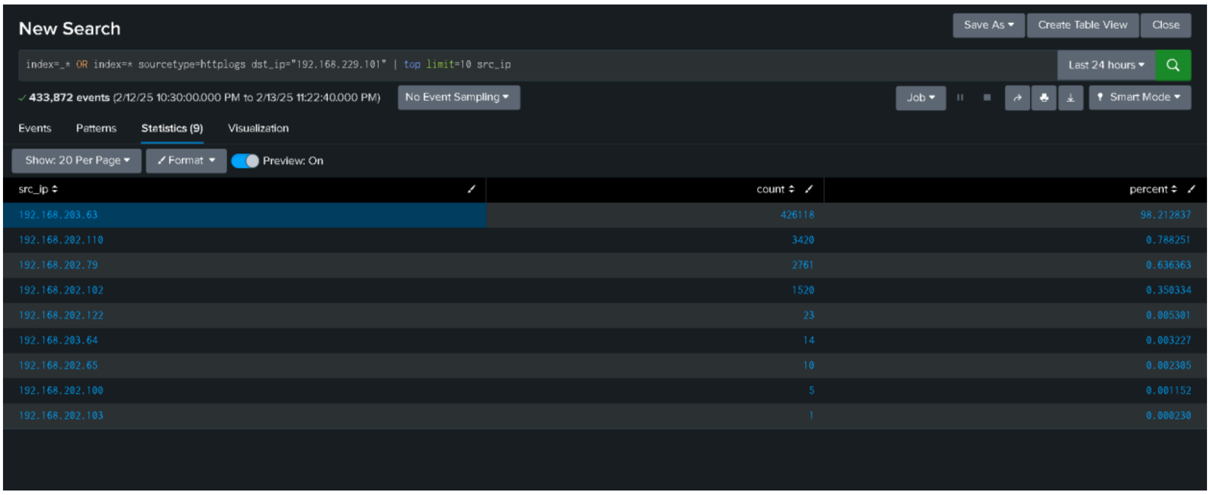
✓ 433,872 events (2/12/25 10:30:00.000 PM to 2/13/25 11:21:14.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a dst_ip 1
# dst_port 1
a index 1
# linecount 5
a method 7
a punct 100+
a splunk_server 1

```
i  Time                   Event
>  2/13/25                1331921610.200000       C9omk7REpUfCAtOe6       192.168.202.102 2489    192.168.229.101 80      1       POST    192.168.229.101 /login  http://19
   10:45:04.000 PM        2.168.229.101/  Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1)      19      832     200     OK      -       -       -       (empty) -       -
                          -       FP5Pmq18QJ3Vfj19Se      text/plain      FiFqLY1TmvROz2hTIl      text/html
                          host = NULL   source = http.log.gz   sourcetype = httplogs
>  2/13/25                1331921610.210000       Chjy3u2LZfbIEUsci       192.168.203.63  62875   192.168.229.101 80      46      HEAD    192.168.229.101 /19233_wallpaper1
   10:45:04.000 PM        50/     -       DirBuster-0.12 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)        0       0       404     NOT FOUND       -
                          -       -       (empty) -       -       -       -       -       -       -
                          host = NULL   source = http.log.gz   sourcetype = httplogs
>  2/13/25                1331921610.210000       CQegPH15hwNA6J6jw       192.168.203.63  62874   192.168.229.101 80      78      HEAD    192.168.229.101 /170938/        -
   10:45:04.000 PM        DirBuster-0.12 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)        0       0       404     NOT FOUND       -       -       -
                          (empty) -       -       -       -       -       -       -
                          host = NULL   source = http.log.gz   sourcetype = httplogs
```

To view top 10 source ip address which has requested to the destination ip 192.168.229.101

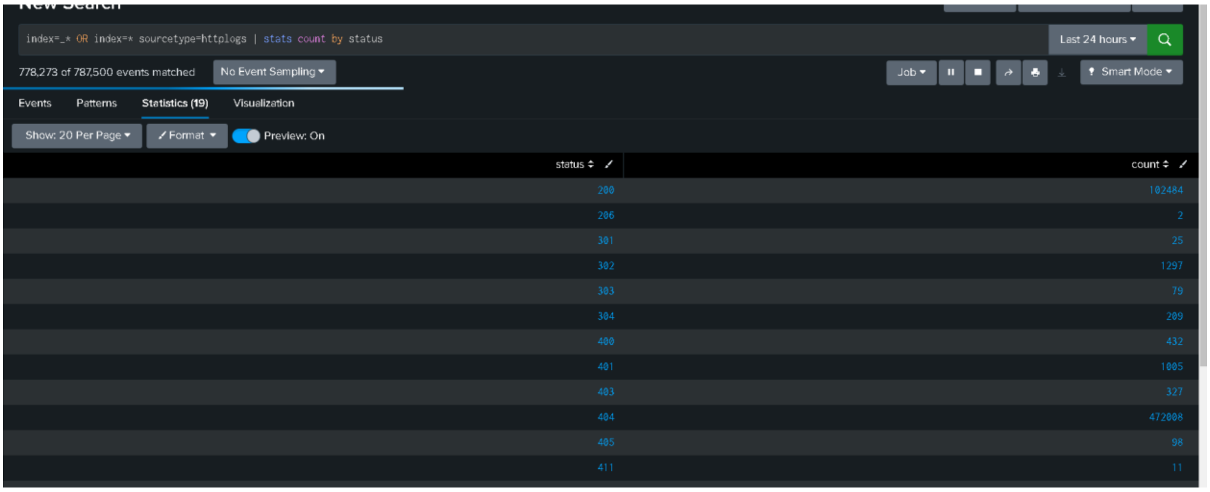


```
index=_* OR index=* sourcetype=httplogs dst_ip="192.168.229.101" | top limit=10 src_ip
```

✓ 433,872 events (2/12/25 10:30:00.000 PM to 2/13/25 11:22:40.000 PM)

| src_ip | count | percent |
|---|---|---|
| 192.168.203.63 | 426118 | 98.212837 |
| 192.168.202.110 | 3420 | 0.788251 |
| 192.168.202.79 | 2761 | 0.636363 |
| 192.168.202.102 | 1520 | 0.350334 |
| 192.168.202.122 | 23 | 0.005301 |
| 192.168.203.64 | 14 | 0.003227 |
| 192.168.202.65 | 10 | 0.002305 |
| 192.168.202.100 | 5 | 0.001152 |
| 192.168.202.103 | 1 | 0.000230 |

Analyze response codes to identify errors or successful requests.

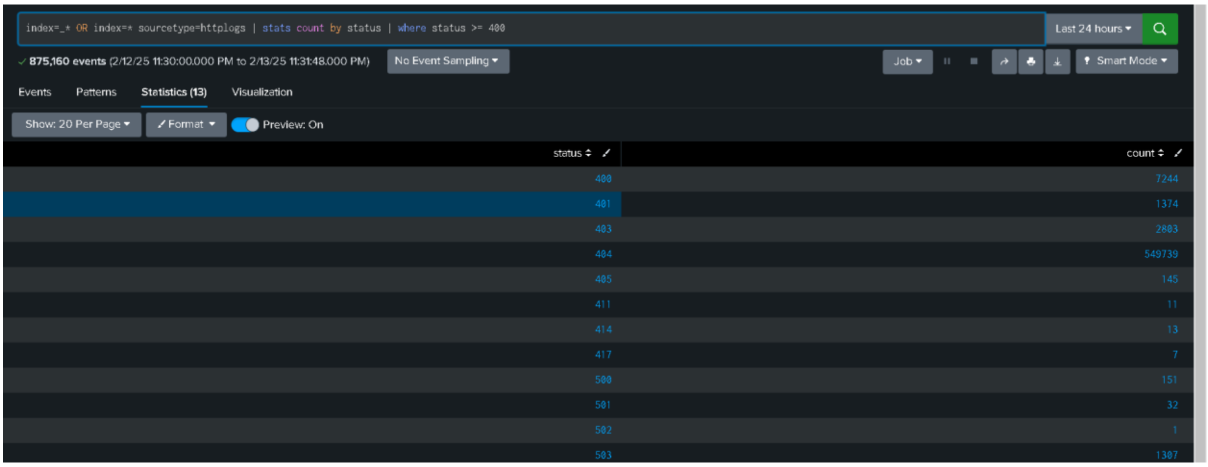


```
index=_* OR index=* sourcetype=httplogs | stats count by status
```

778,273 of 787,500 events matched

| status | count |
|---|---|
| 200 | 102484 |
| 206 | 2 |
| 301 | 25 |
| 302 | 1297 |
| 303 | 79 |
| 304 | 209 |
| 400 | 432 |
| 401 | 1005 |
| 403 | 327 |
| 404 | 472008 |
| 405 | 98 |
| 411 | 11 |

Analyze high volumes of error responses by checking the response codes higher than or equal to 400



```
index=_* OR index=* sourcetype=httplogs | stats count by status | where status >= 400
```

✓ 875,160 events (2/12/25 11:30:00.000 PM to 2/13/25 11:31:48.000 PM)

| status | count |
|---|---|
| 400 | 7244 |
| 401 | 1374 |
| 403 | 2803 |
| 404 | 549739 |
| 405 | 145 |
| 411 | 11 |
| 414 | 13 |
| 417 | 7 |
| 500 | 151 |
| 501 | 32 |
| 502 | 1 |
| 503 | 1307 |