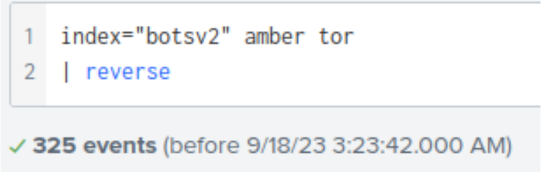
Splunk 2 -
200 series questions

Question 1:

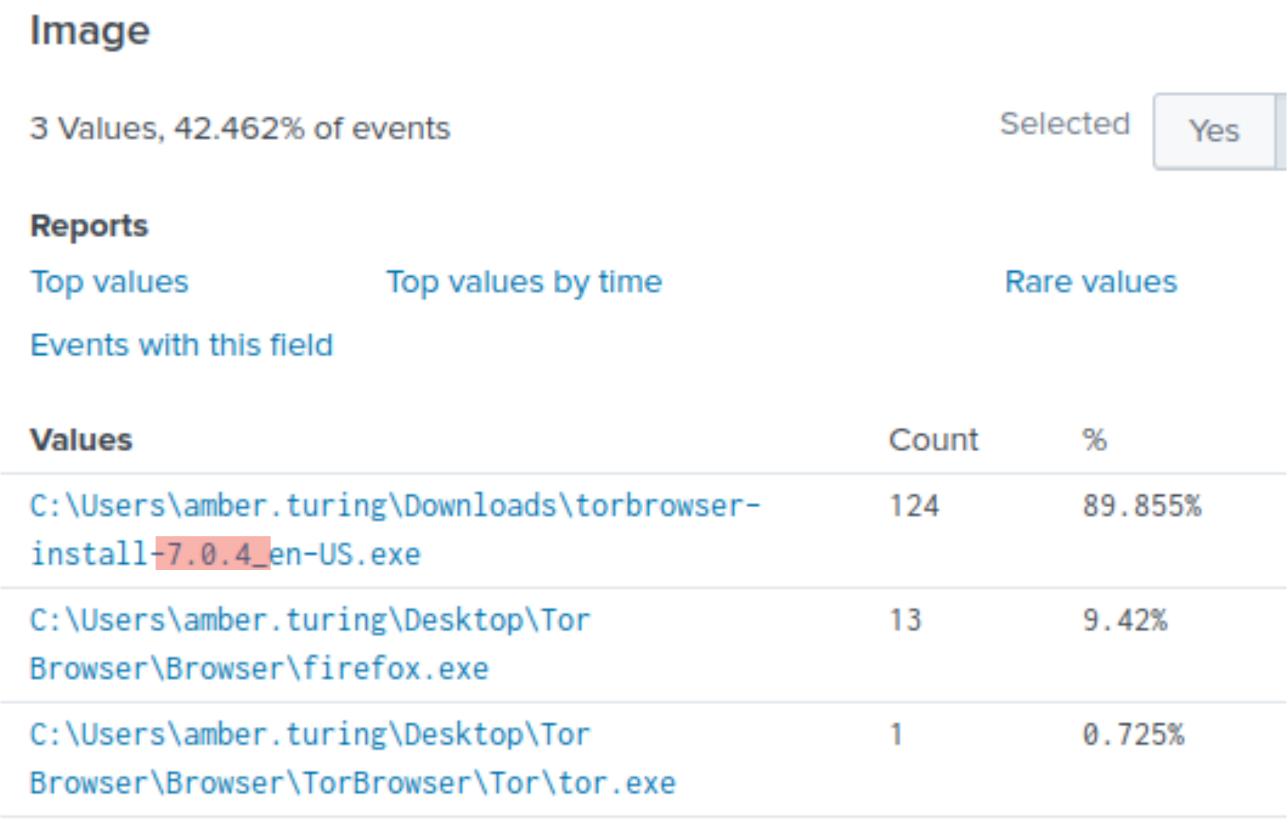
What version of Tor that Amber have installed?
7.0.4

Findings



```
index="botsv2" amber tor
| reverse
```

✓ 325 events (before 9/18/23 3:23:42.000 AM)



Image

3 Values, 42.462% of events

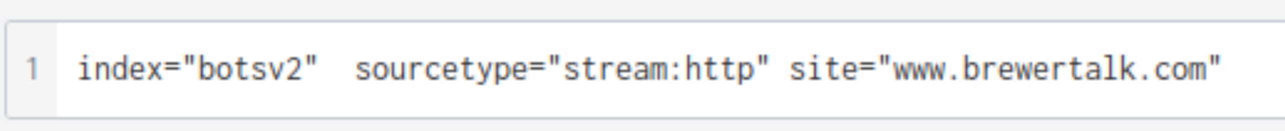
Values	Count	%
C:\Users\amber.turing\Downloads\torbrowser-install-7.0.4_en-US.exe	124	89.855%
C:\Users\amber.turing\Desktop\Tor Browser\Browser\firefox.exe	13	9.42%
C:\Users\amber.turing\Desktop\Tor Browser\Browser\TorBrowser\Tor\tor.exe	1	0.725%

Question 2:

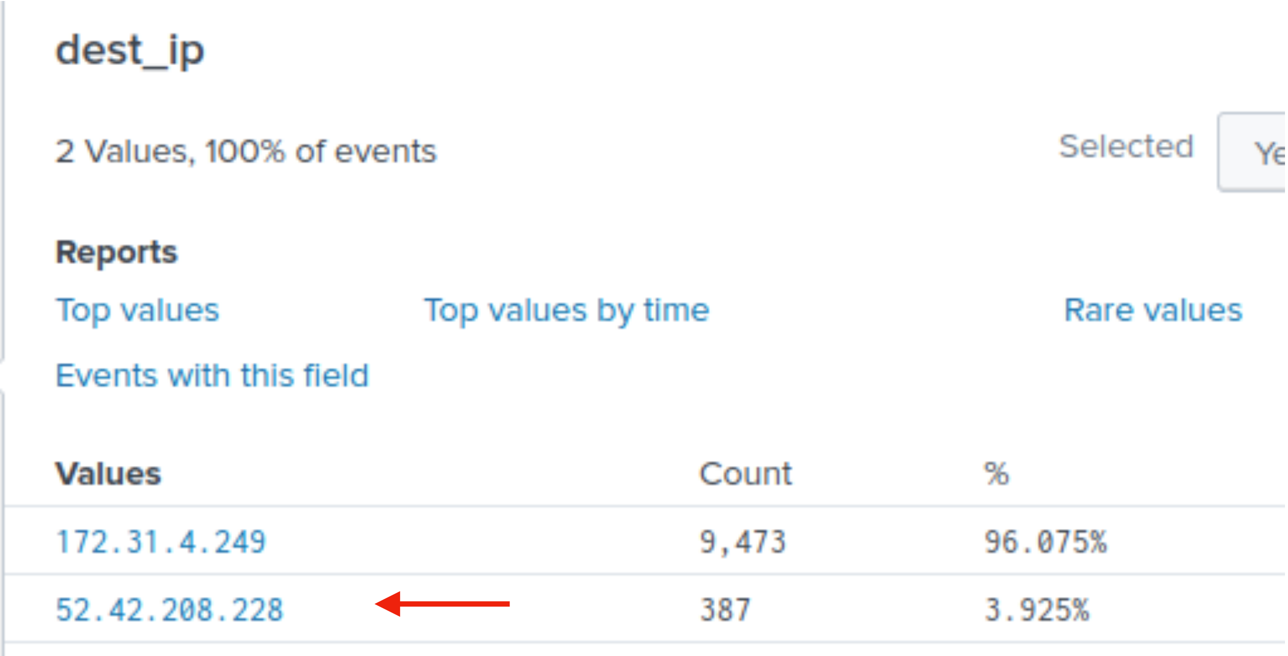
What is the public IPv4 address of the server running www.brewertalk.com?
52.42.208.228

Findings

There are 2 IpV4s addresses, the first one is the private and the second one is the Public.



```
index="botsv2"  sourcetype="stream:http" site="www.brewertalk.com"
```



dest_ip

2 Values, 100% of events

Values	Count	%
172.31.4.249	9,473	96.075%
52.42.208.228	387	3.925%

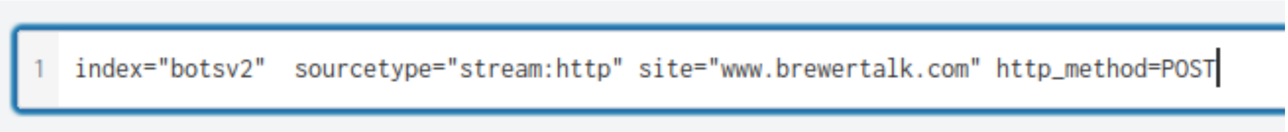
Question 3:

Provide the IP address of the system used to run a web vulnerability scan against www.brewertalk.com.

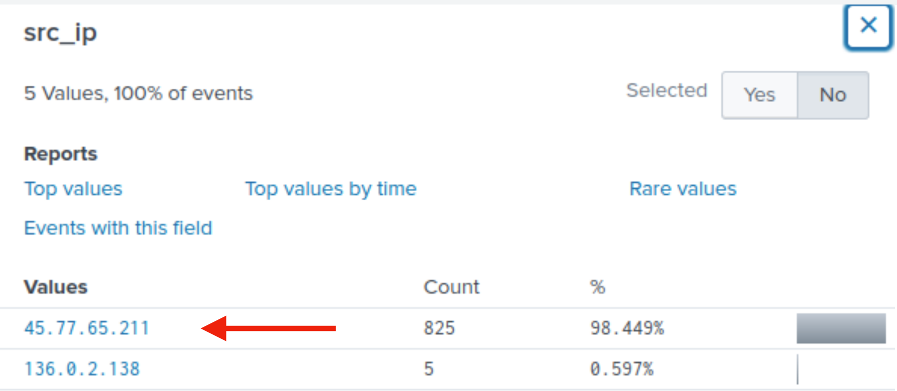
45.77.65.211

Findings

Adding the http_method=POST would show the src_ip address with the highest traffic.



```
index="botsv2"  sourcetype="stream:http" site="www.brewertalk.com" http_method=POST
```



src_ip

5 Values, 100% of events

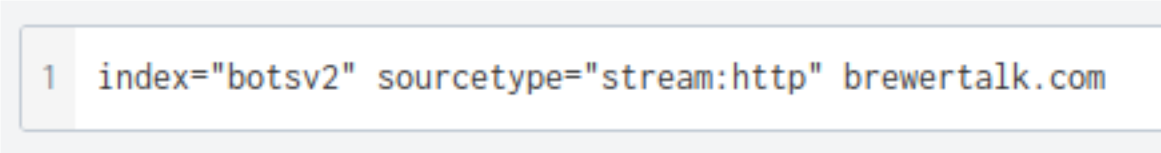
Values	Count	%
45.77.65.211	825	98.449%
136.0.2.138	5	0.597%

Question 4:

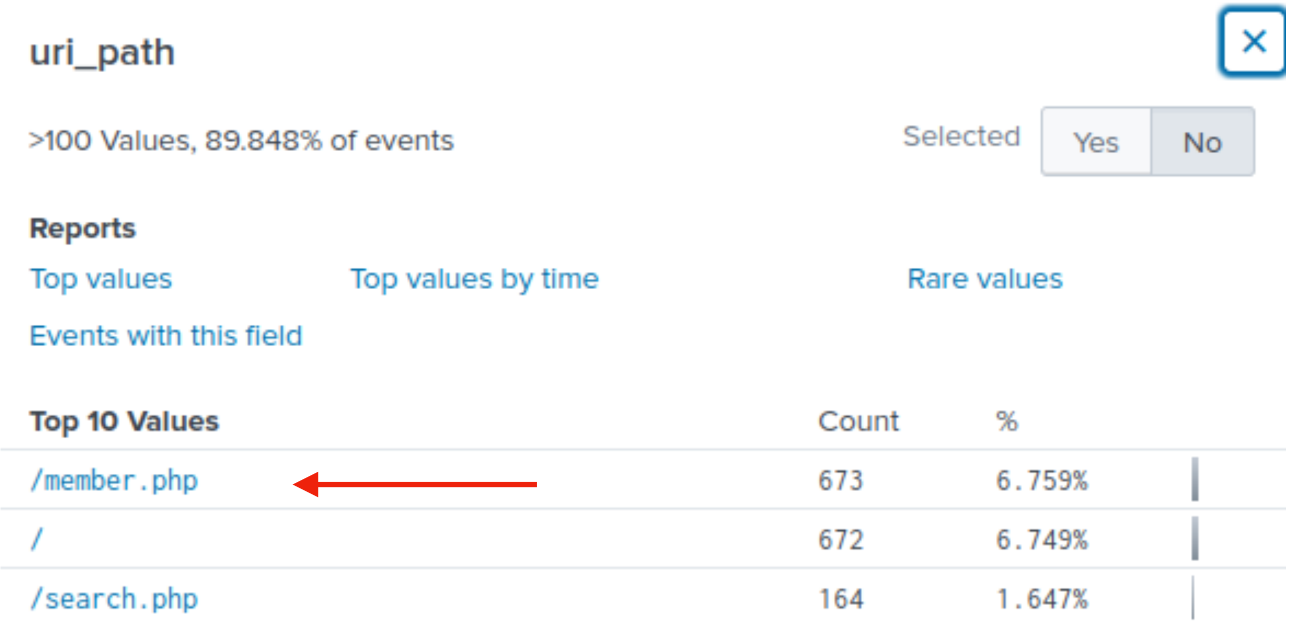
The IP address from Q#2 is also being used by a likely different piece of software to attack a URI path. What is the URI path? Answer guidance: Include the leading forward slash in your answer. Do not include the query string or other parts of the URI. Answer example: /phpinfo.php

/member.php

Findings



```
index="botsv2" sourcetype="stream:http" brewertalk.com
```



uri_path

>100 Values, 89.848% of events

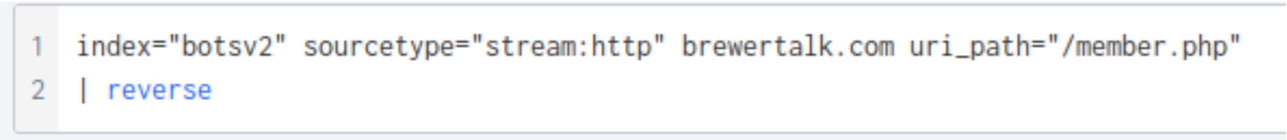
Top 10 Values	Count	%
/member.php	673	6.759%
/	672	6.749%
/search.php	164	1.647%

Question 5:

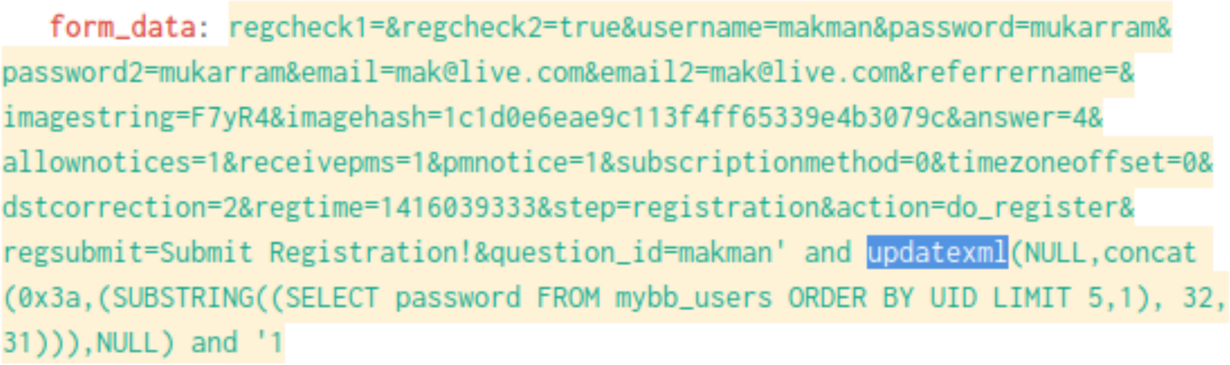
What SQL function is being abused on the URI path from the previous question?

updatexml

Findings



```
index="botsv2" sourcetype="stream:http" brewertalk.com uri_path="/member.php"
| reverse
```



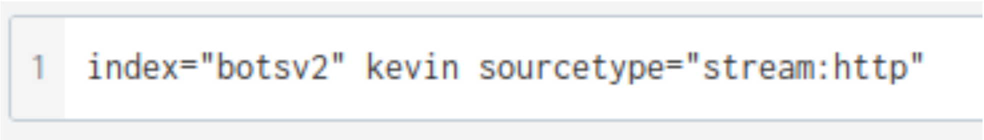
```
form_data: regcheck1=&regcheck2=true&username=makman&password=mukarram&
password2=mukarram&email=mak@live.com&email2=mak@live.com&referrername=&
imagestring=F7yR4&imagehash=1c1d0e6eae9c113f4ff65339e4b3079c&answer=4&
allownotices=1&receivepms=1&pmnotice=1&subscriptionmethod=0&timezoneoffset=0&
dstcorrection=2&regtime=1416039333&step=registration&action=do_register&
regsubmit=Submit Registration!&question_id=makman' and updatexml(NULL,concat
(0x3a,(SUBSTRING((SELECT password FROM mybb_users ORDER BY UID LIMIT 5,1), 32,
31))),NULL) and '1
```

Question 6:

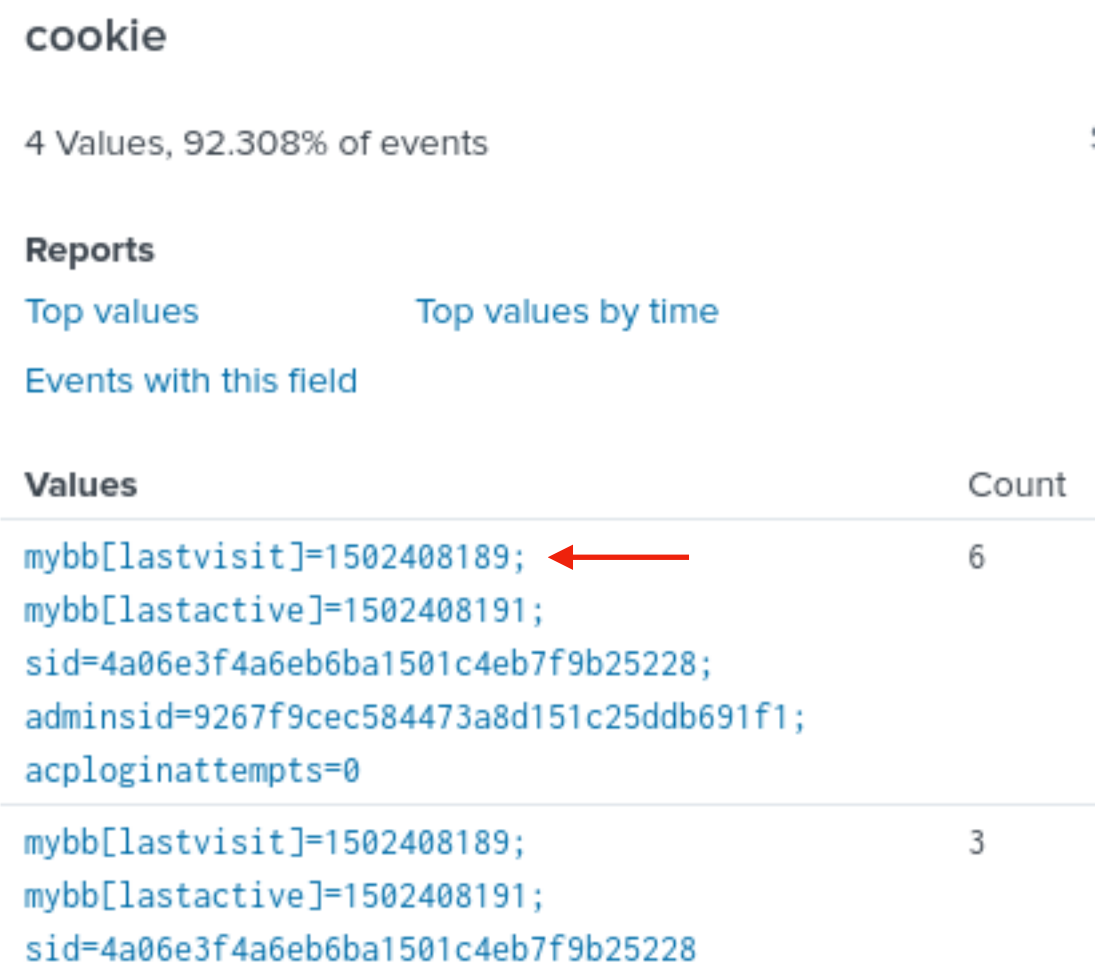
What was the value of the cookie that Kevin's browser transmitted to the malicious URL as part of an XSS attack? Answer guidance: All digits. Not the cookie name or symbols like an equal sign.

1502408189

Findings



```
index="botsv2" kevin sourcetype="stream:http"
```



cookie

4 Values, 92.308% of events

Reports

```
Values                                                  Count
mybb[lastvisit]=1502408189;                             6
mybb[lastactive]=1502408191;
sid=4a06e3f4a6eb6ba1501c4eb7f9b25228;
adminsid=9267f9cec584473a8d151c25ddb691f1;
acploginattempts=0
mybb[lastvisit]=1502408189;                             3
mybb[lastactive]=1502408191;
sid=4a06e3f4a6eb6ba1501c4eb7f9b25228
```

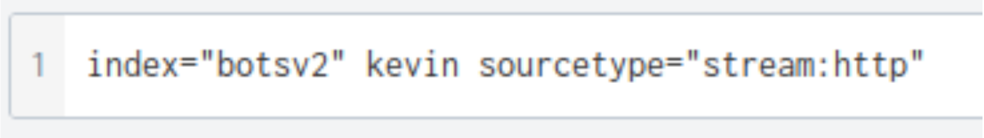
Question 7:

What brewertalk.com username was maliciously created by a spear phishing attack?

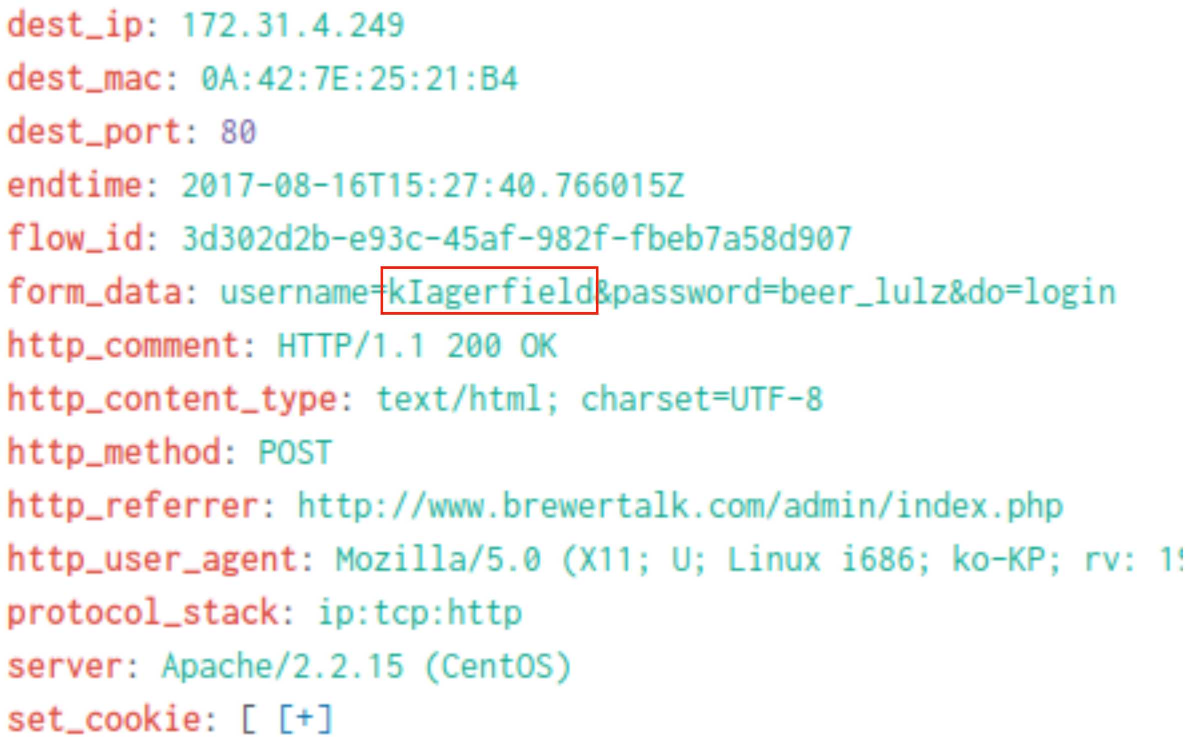
klargerfield

Findings

Using the same search by check the form_data in the interesting field, you will clearly see the newly created username.



```
index="botsv2" kevin sourcetype="stream:http"
```



```
dest_ip: 172.31.4.249
dest_mac: 0A:42:7E:25:21:B4
dest_port: 80
endtime: 2017-08-16T15:27:40.766015Z
flow_id: 3d302d2b-e93c-45af-982f-fbeb7a58d907
form_data: username=kIagerfield&password=beer_lulz&do=login
http_comment: HTTP/1.1 200 OK
http_content_type: text/html; charset=UTF-8
http_method: POST
http_referrer: http://www.brewertalk.com/admin/index.php
http_user_agent: Mozilla/5.0 (X11; U; Linux i686; ko-KP; rv: 1
protocol_stack: ip:tcp:http
server: Apache/2.2.15 (CentOS)
set_cookie: [ [+]
```