

# Splunk

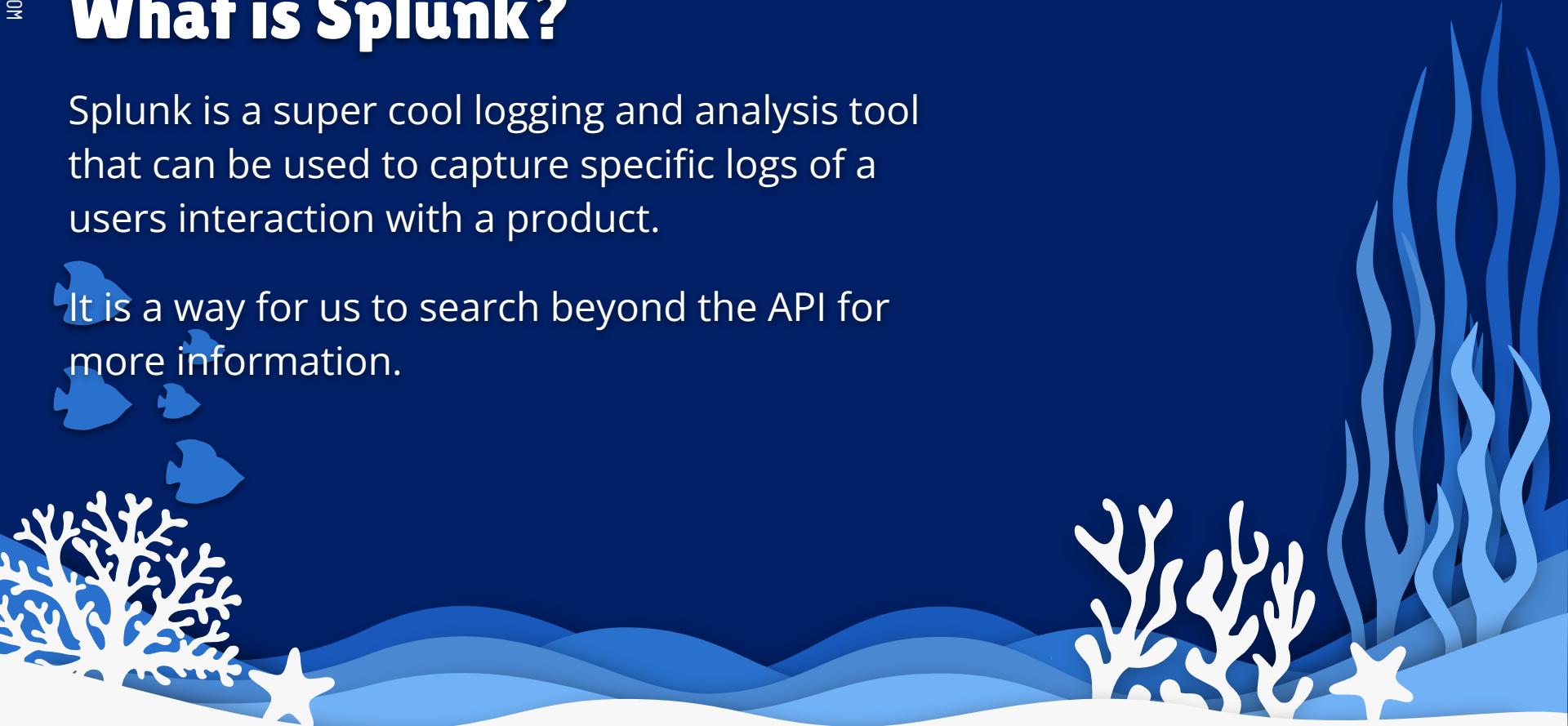
The How to Guide



# What is Splunk?

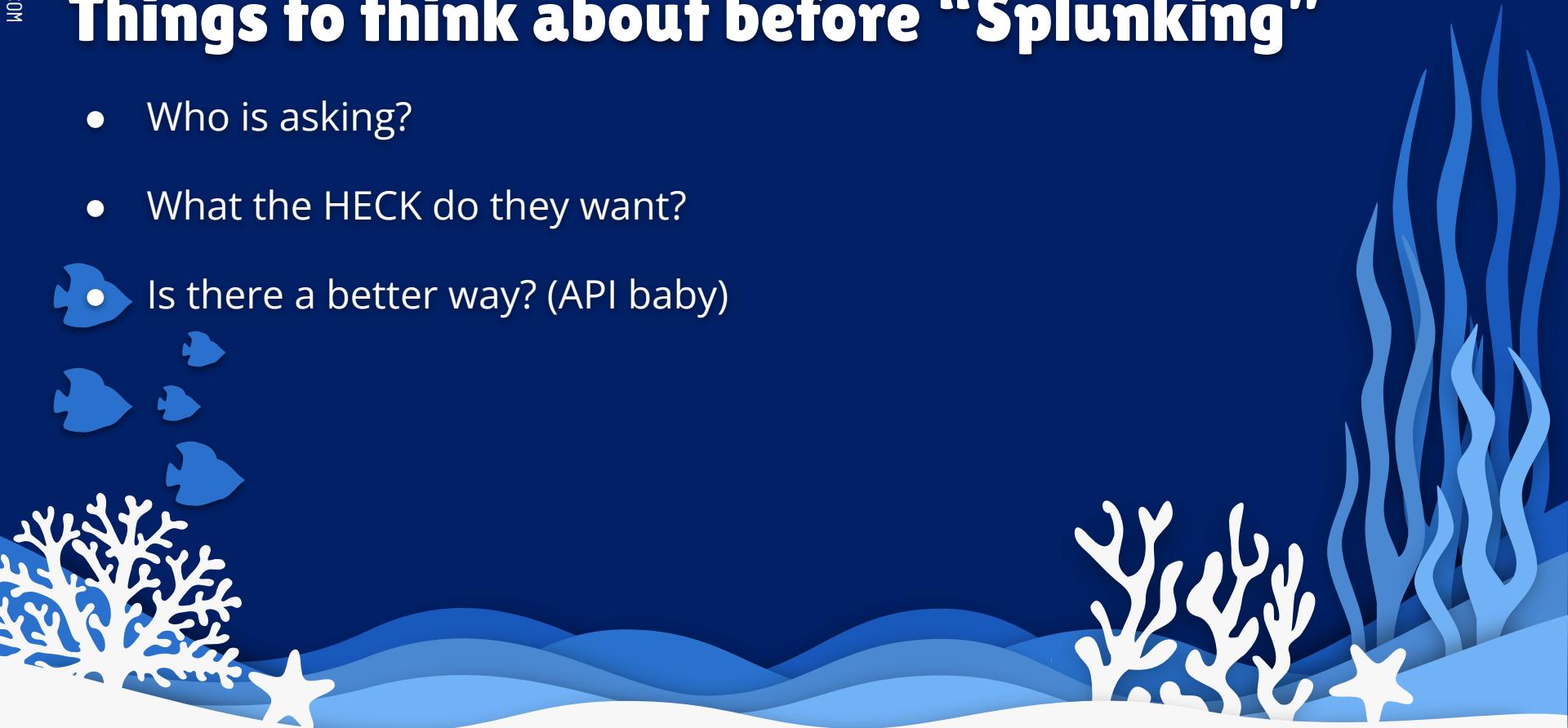
Splunk is a super cool logging and analysis tool that can be used to capture specific logs of a users interaction with a product.

It is a way for us to search beyond the API for more information.



# Things to think about before “Splunking”

- Who is asking?
- What the HECK do they want?
- Is there a better way? (API baby)



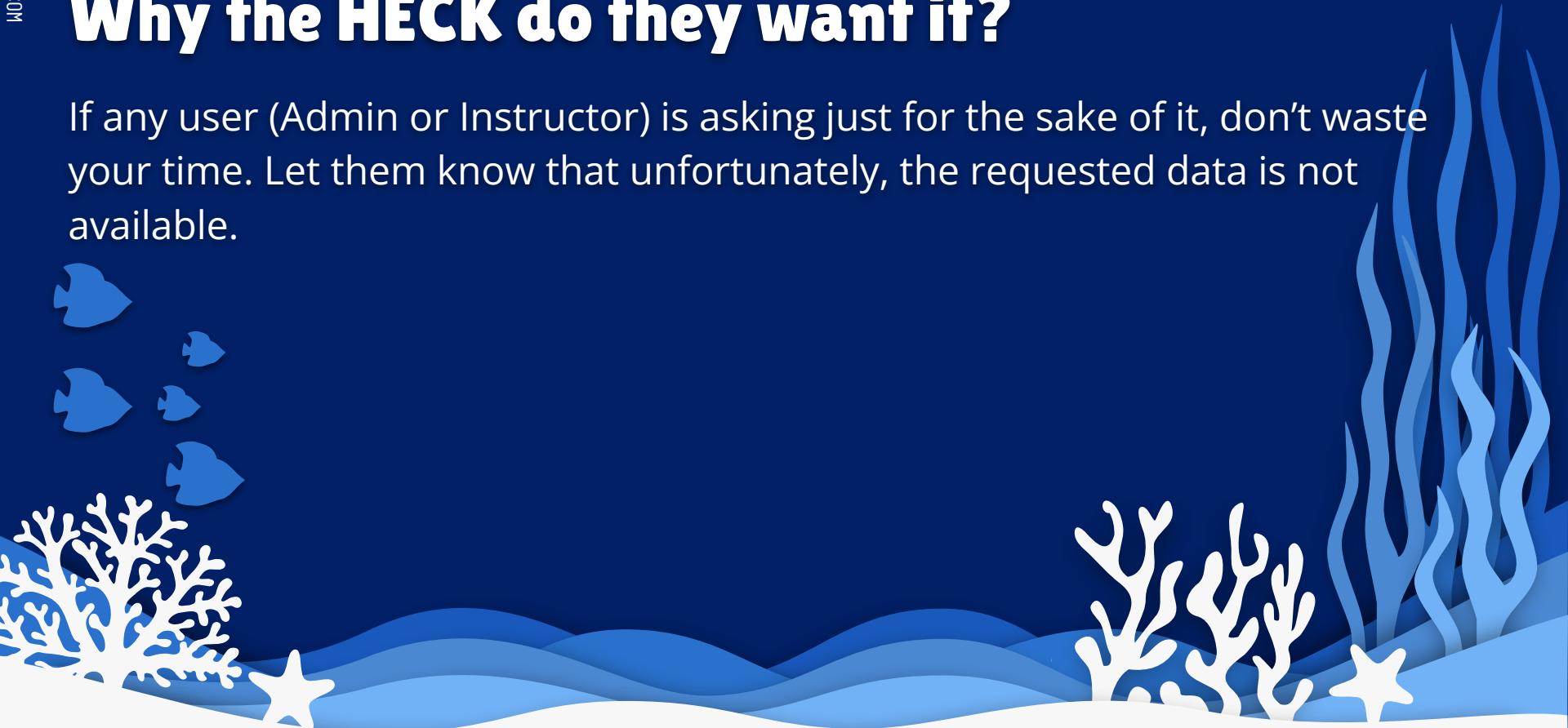
# Who is asking?

If an instructor is asking, tell them that we cannot give this information to them directly. The request must come from the Canvas Administrator at their institution. They should contact their school/university.

If any user (Admin or Instructor) is asking just for the sake of it, don't waste your time. Let them know that unfortunately, the requested data is not available.

# Why the HECK do they want it?

If any user (Admin or Instructor) is asking just for the sake of it, don't waste your time. Let them know that unfortunately, the requested data is not available.



# Is there a better way? (API baby)

When you get a Splunk request you must think to yourself, "Is there a better way to do this?"

Answer: There probably is!

Many of the things we are looking for can be found using the API, making the need to use Splunk not so necessary in certain situations. You can check out our [API documentation](#) to see what types of requests you can make.

1. Who made a change to my course?
2. When was a user added to a course?
3. When was a course cross-listed?

# How to search in Splunk?

1. Dig to find the index
2. Find the Shard ID or Global Root Account ID
3. Network tab to find HTTP Request and HTTP Method
4. Time Frame
5. Construct your query

# How to dig to find the index

1. Open up Terminal on your computer
2. Type dig followed by the schools Canvas Instance  
(you will not need to add https://)

3. Hit enter and look under the action section for  
canvas-\*index\*

Knowing this will also allow us to know what version of  
Splunk to use incase this School is out of the Country

```
c02yn4m6jg5h:~ swynn$ dig swynn.instructure.com
; <>> DiG 9.10.6 <>> swynn.instructure.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 44948
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
;
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;swynn.instructure.com. IN A
;
;; ANSWER SECTION:
swynn.instructure.com. 300 IN CNAME cluster203.instructure.com.
cluster203.instructure.com. 846 IN CNAME canvas-pdx-prod-c203-1198785952.us-west-2.elb.amazonaws.com.
canvas-pdx-prod-c203-1198785952.us-west-2.elb.amazonaws.com. 6 IN A 54.68.191.17
;
;canvas-pdx-prod-c203-1198785952.us-west-2.elb.amazonaws.com. 6 IN A 44.240.126.2
;
```

# How to find a Shard ID?

There are a couple ways you can find the Shard ID for an instance. The first way is to use Siteadmin and search for the school name. You can then click on the info button to find the shard ID listed.

The second way is to save this really cool bookmarklet to your browser. By saving it to your browser, you can click on it anytime you are in an instance and it will automatically pop up on your screen with the shard ID. You will take the first numbers to the left of all the zeros.

```
javascript:(alert(ENV.DOMAIN_ROOT_ACCOUNT_ID))
```

The screenshot shows the Siteadmin interface with the 'Root Accounts' section selected. On the left, there is a sidebar with links: People, Jobs, Developer Keys, Badgr Analytics, and Settings. The main area has a search bar containing 'salt lake', followed by dropdown menus for Region (<All>), Database Server (<All>), and External Status (<All>). A 'Filter' button is also present. Below this, under 'Paid accounts', there is a list: 'Real Salt Lake Academy' (with an info icon), 'Salt Lake City Schools' (with an info icon, highlighted with a red arrow), and 'Salt Lake Community College'. Under 'Partner Sandbox accounts', there is a single entry: 'United Way of Salt Lake' (with an info icon).

# Find the Global Root Account ID

1. Search Siteadmin for the Instance you are needing the Global Root Account ID.
2. Click on the title of the Instance from the list
3. Copy the numbers in the URL bar that have the ~ between them (this is the Global Root Account)

Root Accounts

People  
Jobs  
Developer Keys  
Badgr Analytics  
Settings

Root Accounts

Search: noble finsand

Region: <All>

Database Server: <All>

External Status: <All>

Filter

Employee Sandbox accounts

- Noble Finsand's Sandbox ⓘ

https://nfinsand.instructure.com/accounts/9758~2569/settings

Apps Instructure - My A... Training Flow 202... New Courses - Train... Expose Medi...

Employee Sandboxes > Noble Finsand's Sandbox > Settings

Courses People Statistics Permissions Outcomes

Settings Privacy Quotas Notifications

Account Settings

Account Name: Noble Finsand's Sandbox

# How to find HTTP Request and HTTP Method

1. To find the HTTP Request and Method you will need to be under Inspect > Network
2. Make sure you have the gear icon and "use large request rows" on
3. In your sandbox make the same change they did while under the network tab to find the request and method

The screenshot shows the Network tab of the Chrome DevTools interface. At the top left of the tab, there is a checkbox labeled "Use large request rows" which is checked. Below the tabs, there is a "Filter" section with several checkboxes: "Hide data URLs" (unchecked), "XHR" (checked), "JS" (checked), "CSS" (checked), "Img" (checked), "Media" (checked), "Font" (checked), "Doc" (checked), "WS" (checked), "Manifest" (checked), "Other" (checked), "Has blocked cookies" (unchecked), "Blocked Requests" (unchecked), "Group by frame" (unchecked), and "Capture screenshots" (unchecked). The main area displays a list of network requests. One request is highlighted: "update\_nav" with the URL "/courses/18906". The "Headers" tab is selected in the bottom navigation bar. In the bottom-right panel, detailed information about this request is shown:

- General**:
  - Request URL: https://swynn.instructure.com/courses/18906/update\_nav
  - Request Method: POST
  - Status Code: 302
  - Remote Address: 50.112.81.191:443
  - Referrer Policy: no-referrer-when-downgrade
- Response Headers**:
  - cache-control: no-cache, no-store
  - content-encoding: br
  - content-type: text/html; charset=utf-8
  - date: Mon, 03 May 2021 18:01:58 GMT
  - location: https://swynn.instructure.com/courses/18906/details
  - p3p: CP="None, see http://www.instructure.com/privacy-policy"
  - pragma: no-cache

# Time Frame

The time frame is the most important. If you can be as specific as you can with the time frame the better your results. Searching Splunk also costs the company money and searching longer timeframes will result in a higher fee. We want to try to search ideally within a 3 hour window if possible to limit these costs.

The time frame will need to be converted to UTC which is +6 or +7 hours to MST depending on if Daylight savings. Aka spring time +7 Fall time +6

If you are using the “Presets” filter, no need to worry about time conversion

# Construct your query

Now that we have gone through each of the steps on how to get the different parts of the call we can make it.

```
index=canvas_xxx global_root_account=xxx~xx | spath  
http_request | search http_request=/.... | spath http_method  
| search http_method=....
```

We will be using | = pipeline or bar to create this and spaces are super important as well.

Note: We also have a super cool bookmarklet that will automatically open Splunk and input a basic query with the schools index, and global\_root\_account. You must be within the school's instance in order for it to work.

```
javascript:(function(){var locationInfo=document.location.pathname;var shardID;var globRootID;var masquerading;var currentUser;var garbageRemoval=' AND action!=ping AND controller!=page_views AND action!=unread_count';getPageInfo('https://'+document.domain);function splunk(regionInfo){var query='search index=canvas_'+regionInfo.index+' global_root_account='+globRootID+' http_request '+locationInfo+getMasqueradingQuery()+garbageRemoval;targe tURL='https://inst'+regionInfo.splunkBit+'.splunkcloud.com/en-US/app/ca nvas/search?q='+encodeURIComponent(query);var win>window.open(targetURL, '_blank')}function getMasqueradingQuery(){return(masquerading==!0)?' AND user_id='+'+currentUser:''}function getPageInfo(url){var request=new XMLHttpRequest;request.open("GET",url,!1);request.send(null);var xmlDoc=request.responseText;masquerading=/users\/\d+\/masquerade/g.test(xmlDoc);currentUser=xmlDoc.match(/current_user_id":([\w"]+)/)[1];var header=request.getResponseHeader("x-canvas-meta");var region=header.match(/z=(\w+-\w+\d+)/)[1];var s=header.match(/s=(\d+)/)[1];var a=header.match(/a=(\d+)/)[1];globRootID=s+"~"+a;splunk(getRegionInfo(region))}function getRegionInfo(input){var output=[];switch(input){case 'us-east-1':output.index='iad';output.splunkBit='';break;case 'us-west-2':output.index='pdx';output.splunkBit='';break;case 'ap-southeast-1':output.index='sin';output.splunkBit='syd';break;case 'ap-southeast-2':output.index='syd';output.splunkBit='syd';break;case 'eu-west-1':output.index='dub';output.splunkBit='dub';break;case 'eu-central-1':output.index='fra';output.splunkBit='dub';break;case 'ca-central-1':output.index='yul';output.splunkBit='yul';break;default:output.index='1'}return output}})()
```

# Additional information

- UTC is set to a 24 hour clock
- We can use the “Global Root Account ID” but it is preferred to use the “Shard ID”
- Grab the User ID and check to see who the mysterious user is
- The value for “real\_user\_id” should be null – otherwise, that means someone was masquerading as this user
- PLEASE post a note in the case with the “Last Updated” date/time from the undelete page when sending up the case

# Conclusion

- Here is documentation on Splunk searches
- Checkout the search tutorials
- As well check out the HUB for more information as well
- Please be mindful that each search costs money



**Questions?**

