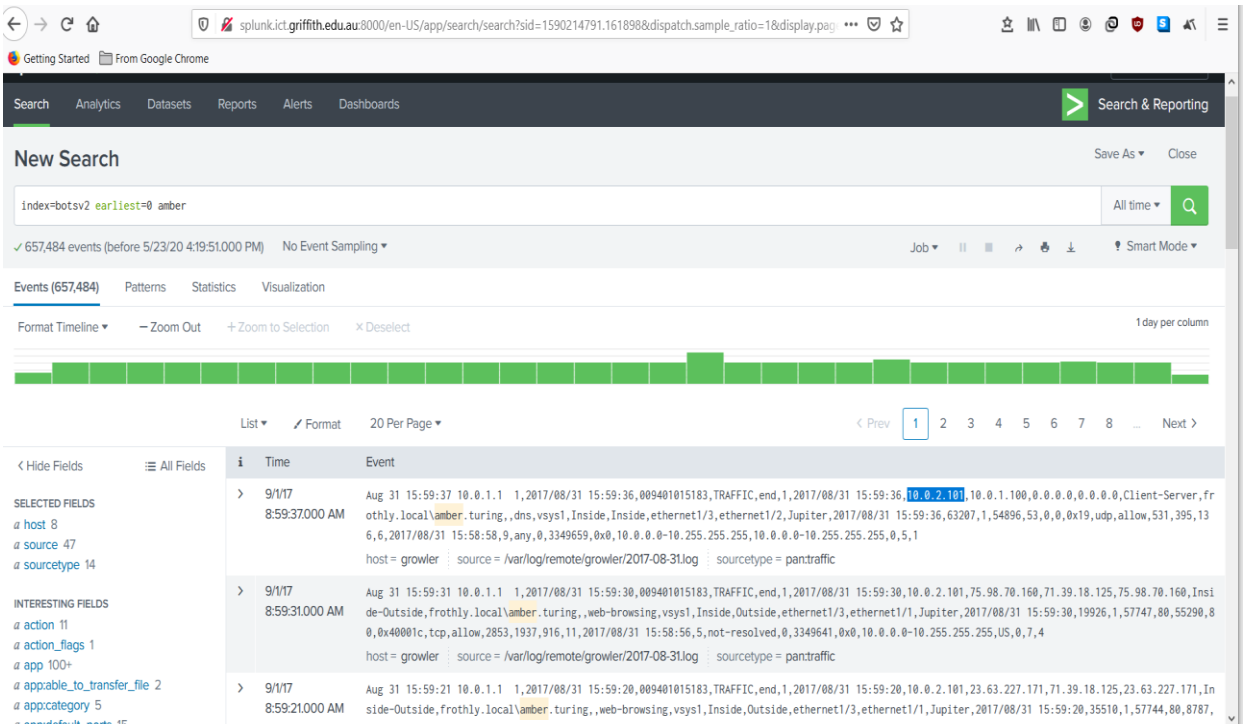
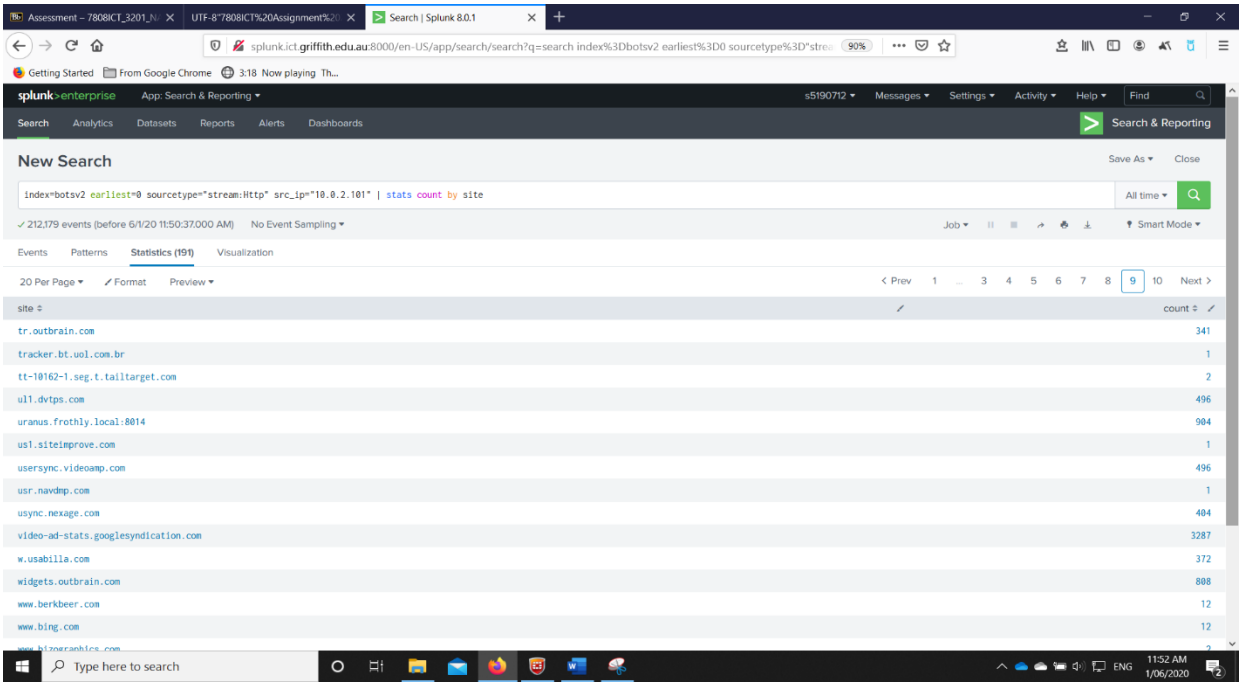
Task A

1) To find the amber IP address, the command **“index=botsv2 earliest=0 amber”** is used. The IP address 10.0.2.101 suggest it is the address of amber as it is used most.



The command **index=botsv2 earliest=0 sourcetype="stream:Http" src_ip="10.0.2.101" | stats count by site** views websites that were visited by Amber’s system:

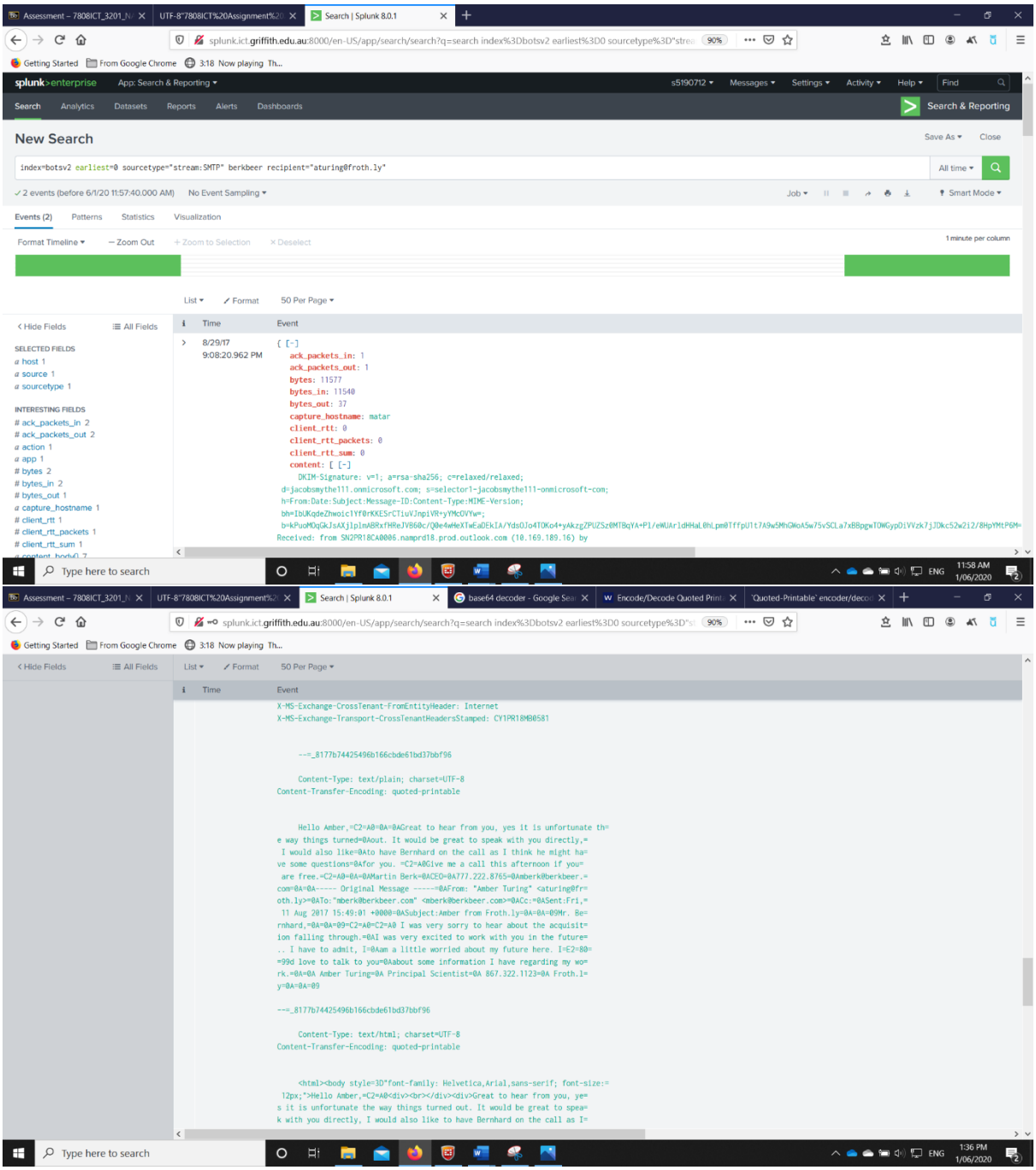
It is found that the competitor website name is **berkbeer.com**

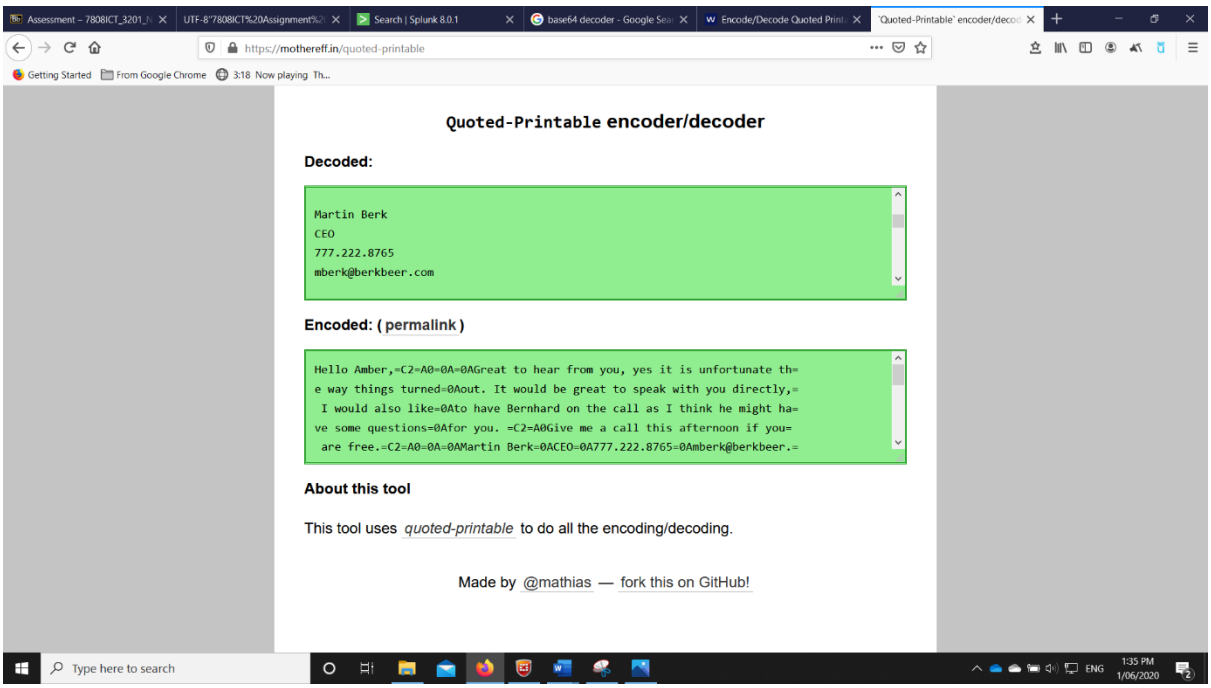


2) Amber's email is identified using the command:

index=botsv2 earliest=0 sourcetype="stream:SMTP" berkbeer recipient="aturing@froth.ly"

Decoding body content of the email, it can be found that the name of the CEO is:





Martin Berk

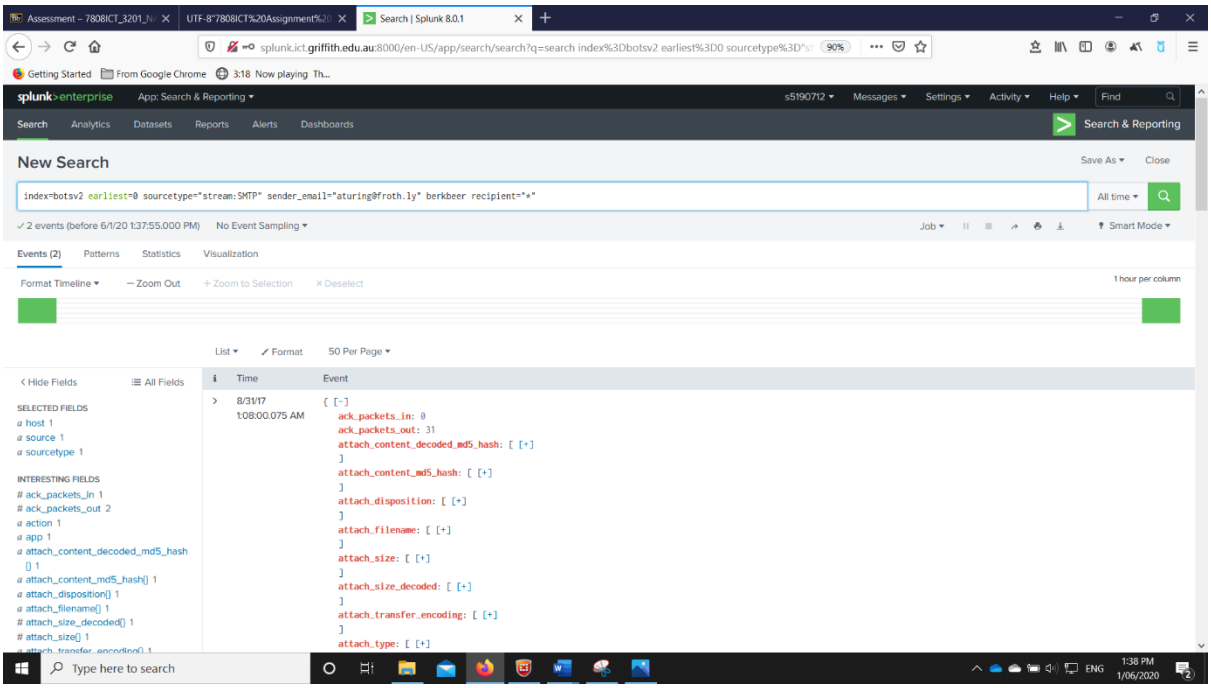
3)

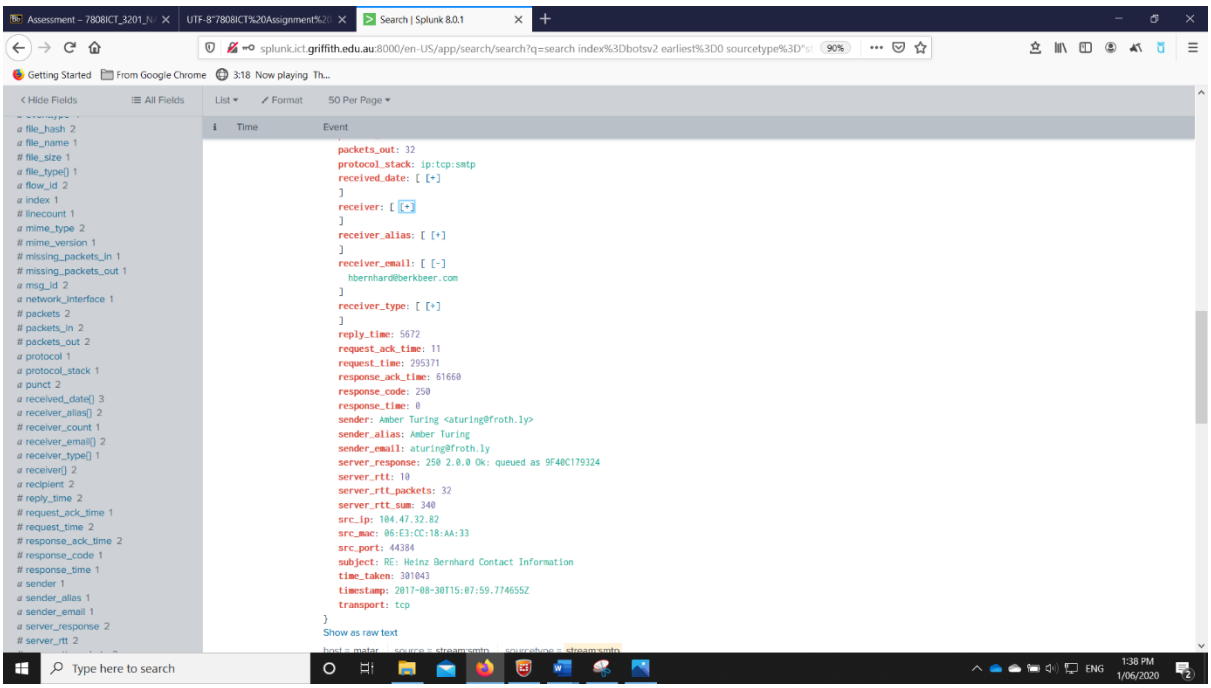
Amber contact with another employee can be searched with the following command:

index=botsv2 earliest=0 sourcetype="stream:SMTP" sender_email="aturing@froth.ly" berkbeer recipient="*"

The employee's email address is:

hbernhard@berkbeer.com



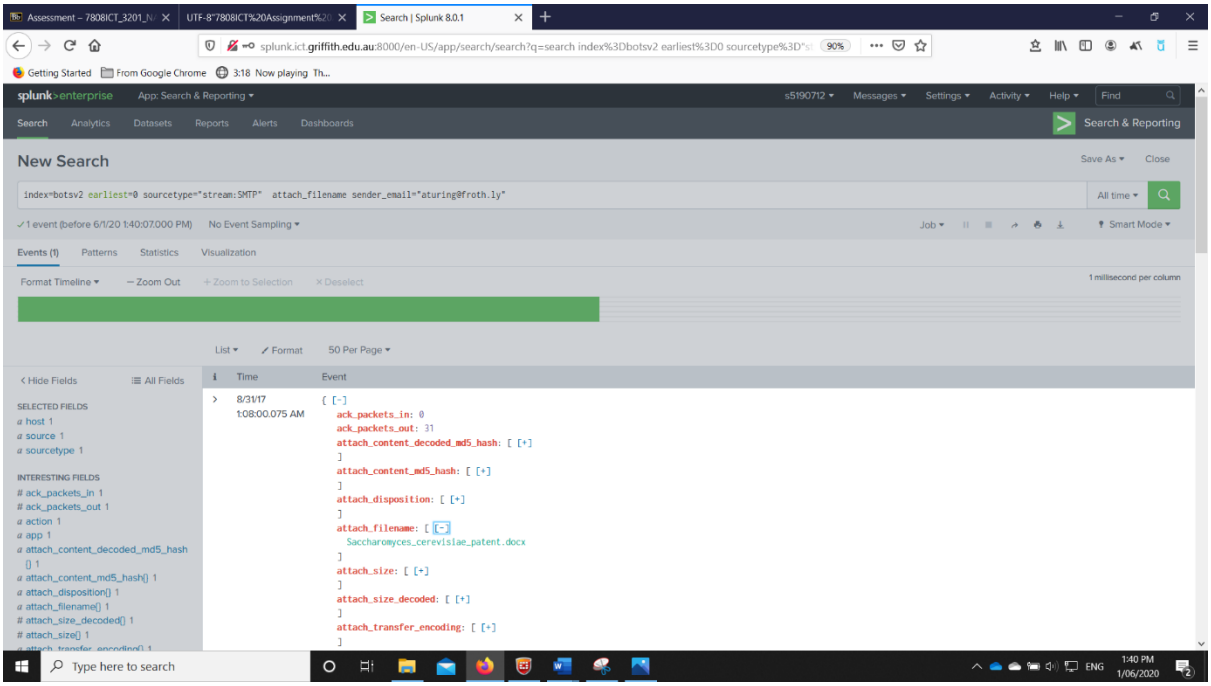


4)

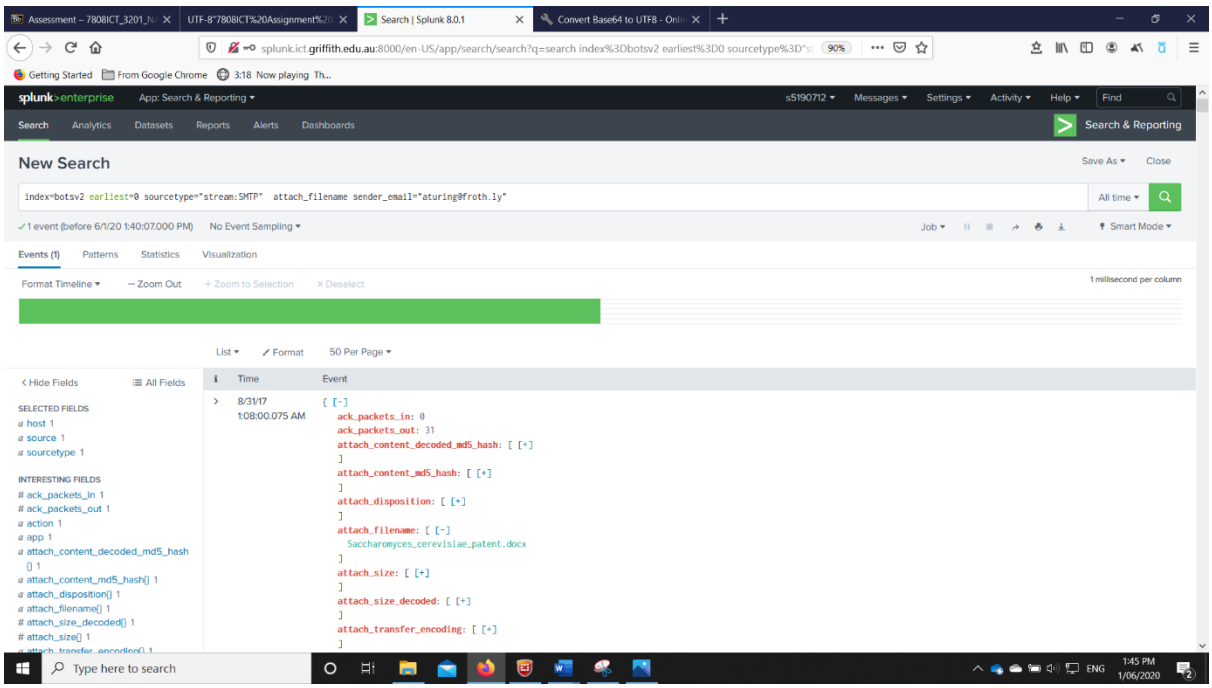
The command **index=botsv2 earliest=0 sourcetype="stream:SMTP" attach_filename sender_email="aturing@froth.ly"** is used to identify the attached file associated with the sender's email:

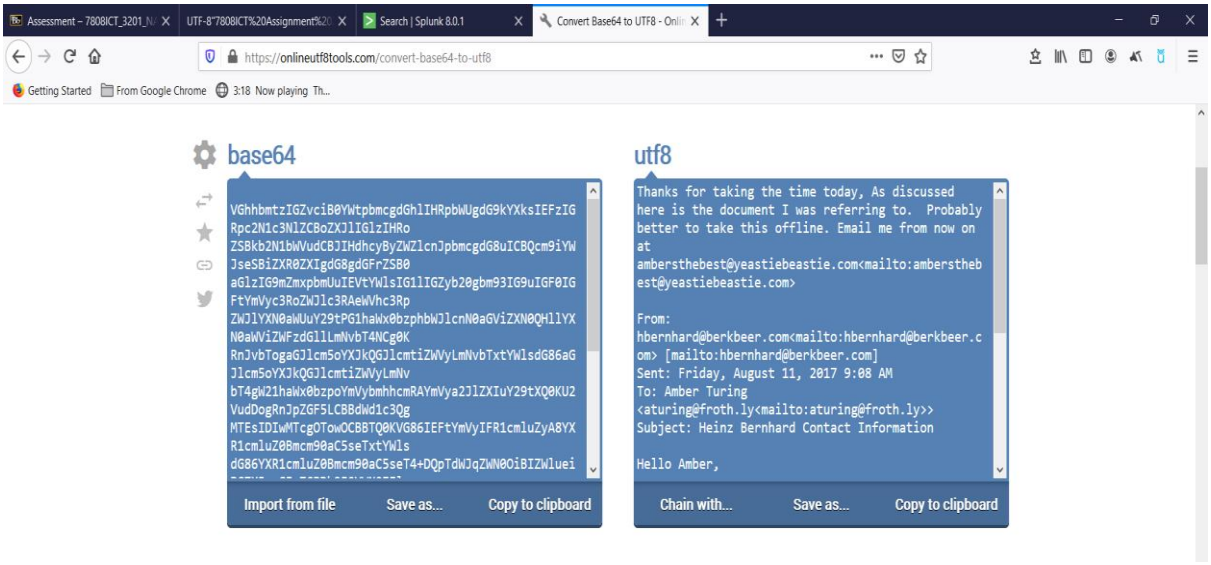
The attached file name is :

Saccharomyces_cerevisiae_patent.docx



5) The attachment was founded using the command **index=botsv2 earliest=0 sourcetype="stream:SMTP" attach_filename sender_email="aturing@froth.ly"** and monitoring the attachment , the message was encoded in base 64. After decoding the message, Amber's personal email address is found as: **ambersthebest@yeastiebeastie.com**

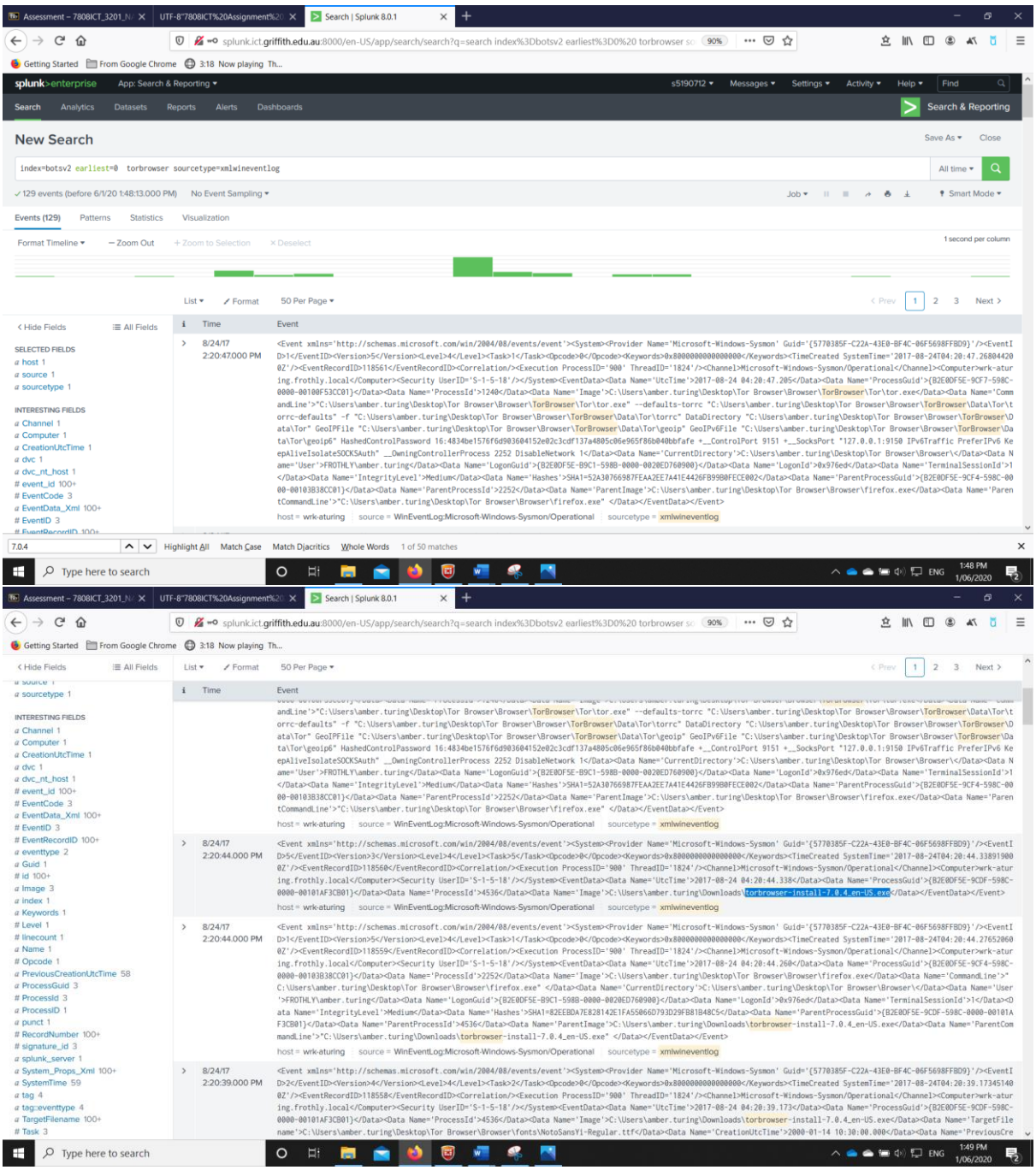




6)

The Tor version can be found using the command **index=botsv2 earliest=0 torbrowser sourcetype=xmlwineventlog.**

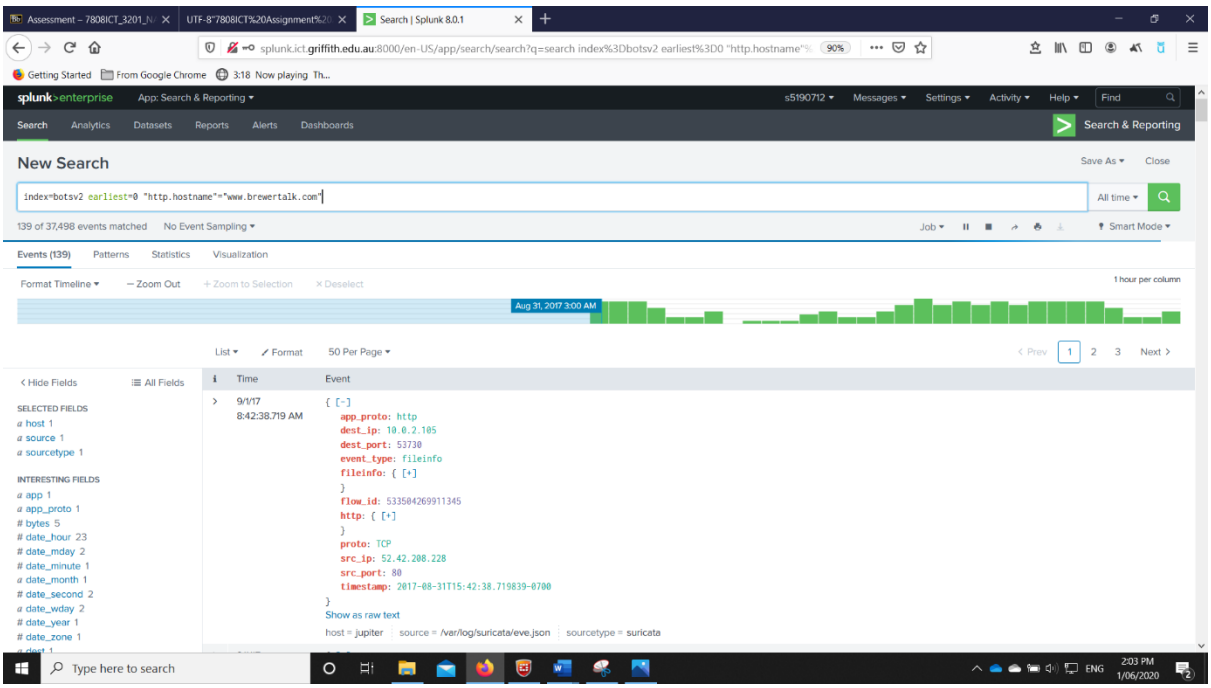
It is found that the tor version is **7.0.4**

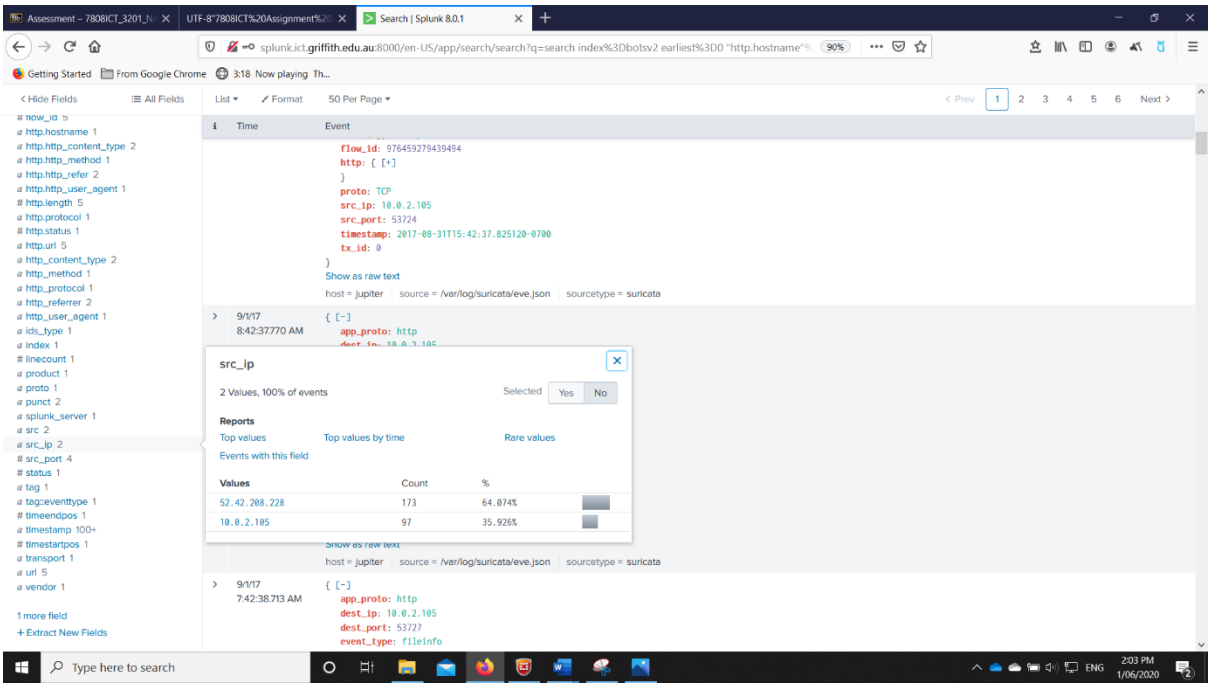


7)

The command **index=botsv2 earliest=0 "http.hostname"="www.brewertalk.com"** is used to find the public ipv4 address of the server.

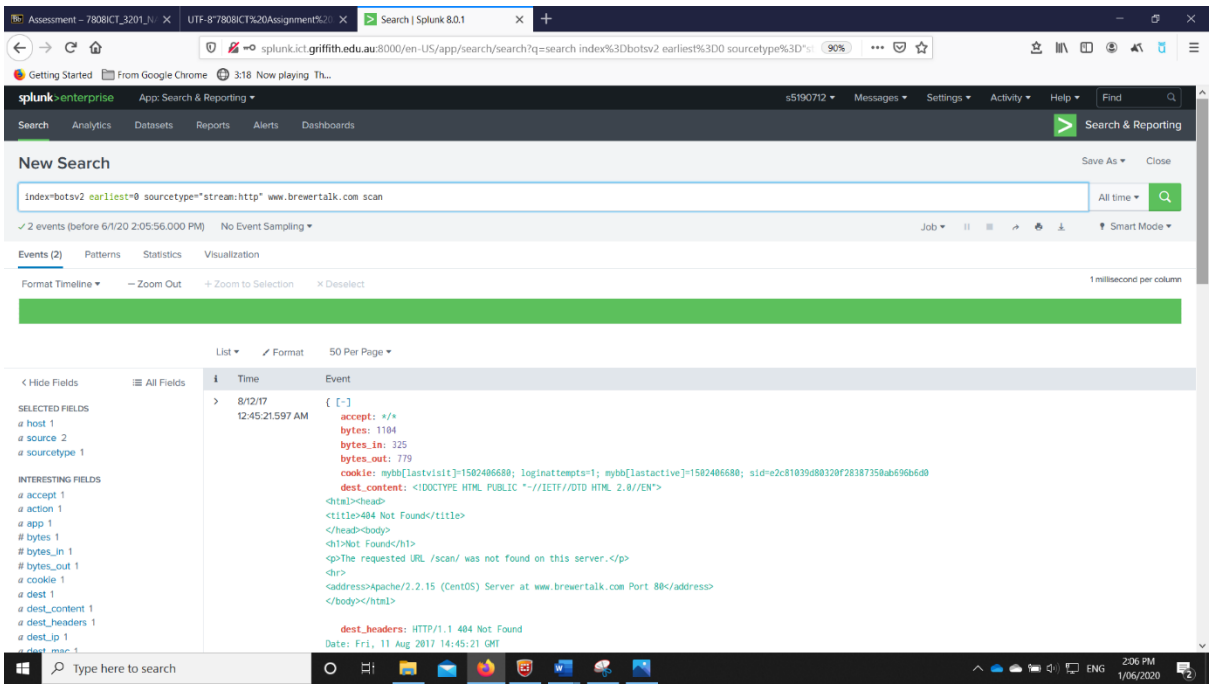
After searching and monitoring, it is found that the public IPV4 address is **52.42.208.228**

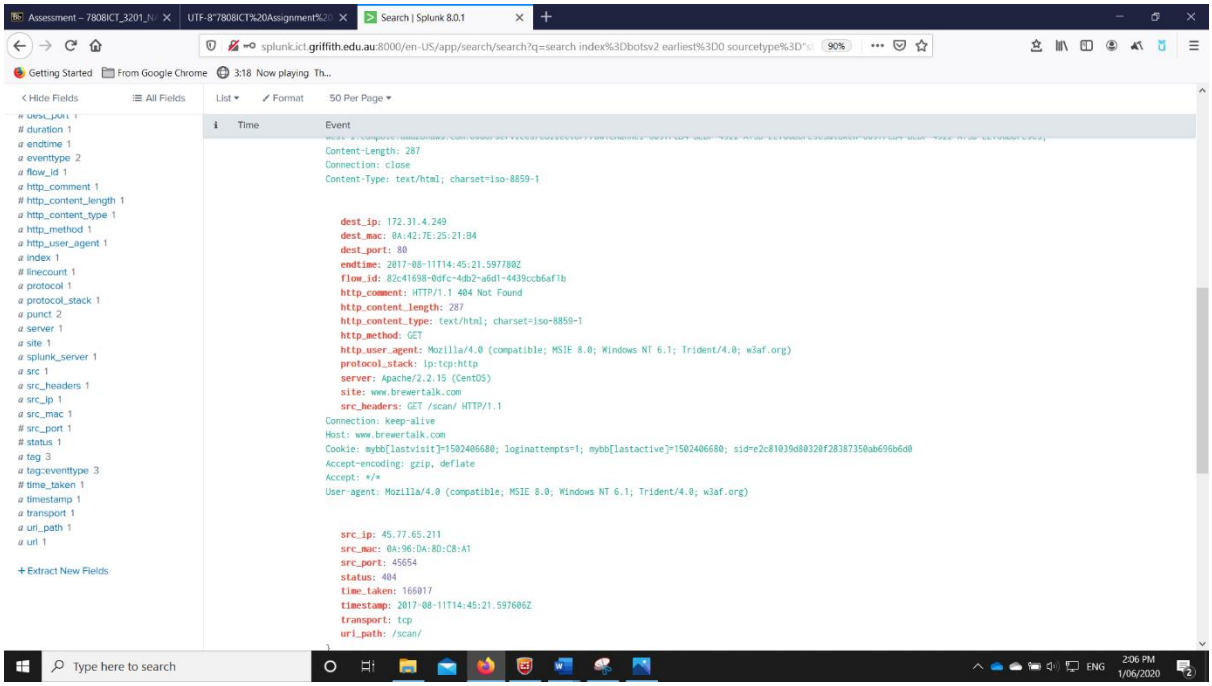




8) The command **index=botsv2 earliest=0 sourcetype="stream:http" www.brewertalk.com scan** is used to find the ip address running the web vulnerability scan. It is visible that the srcip is **45.77.65.211** in the uri path/scan which performs the vulnerability scan.

The ip address **45.77.65.211** is the ip address running the web vulnerability scan.

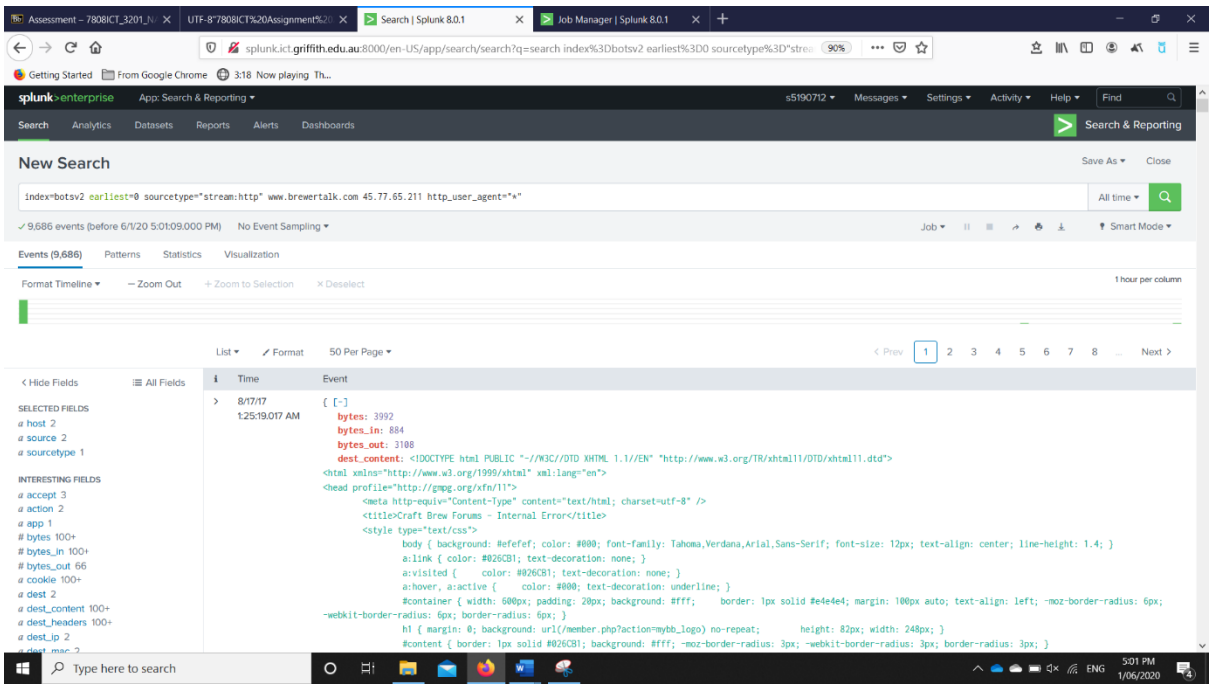


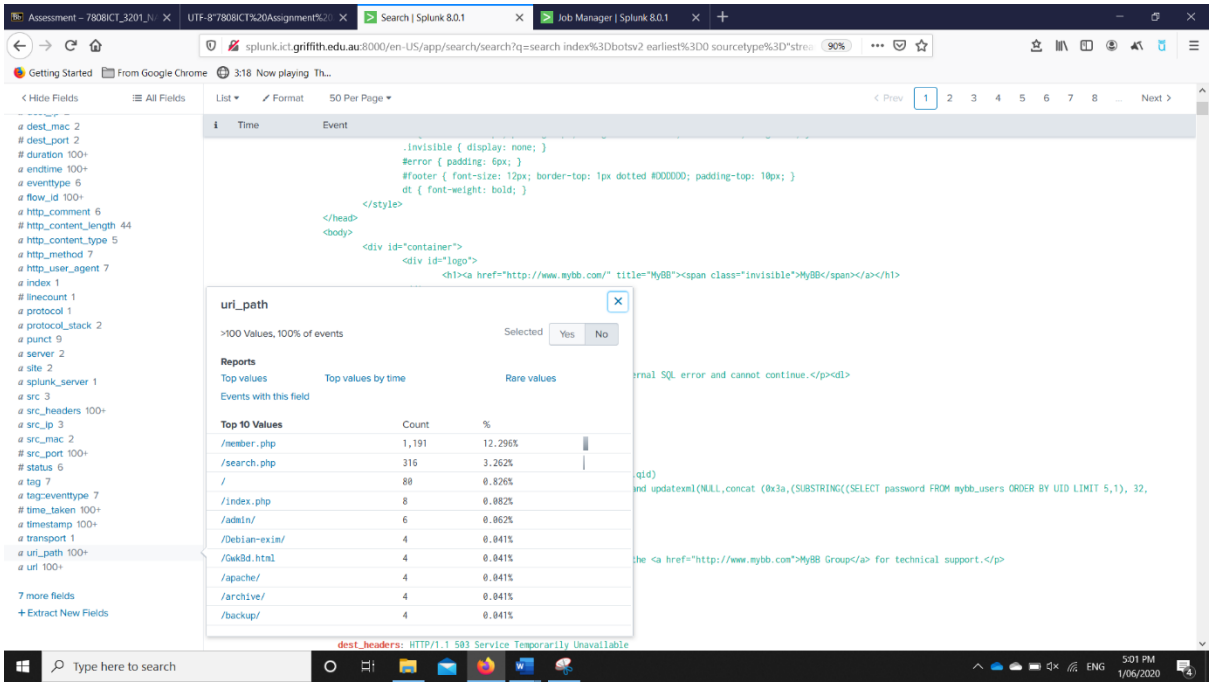


9)

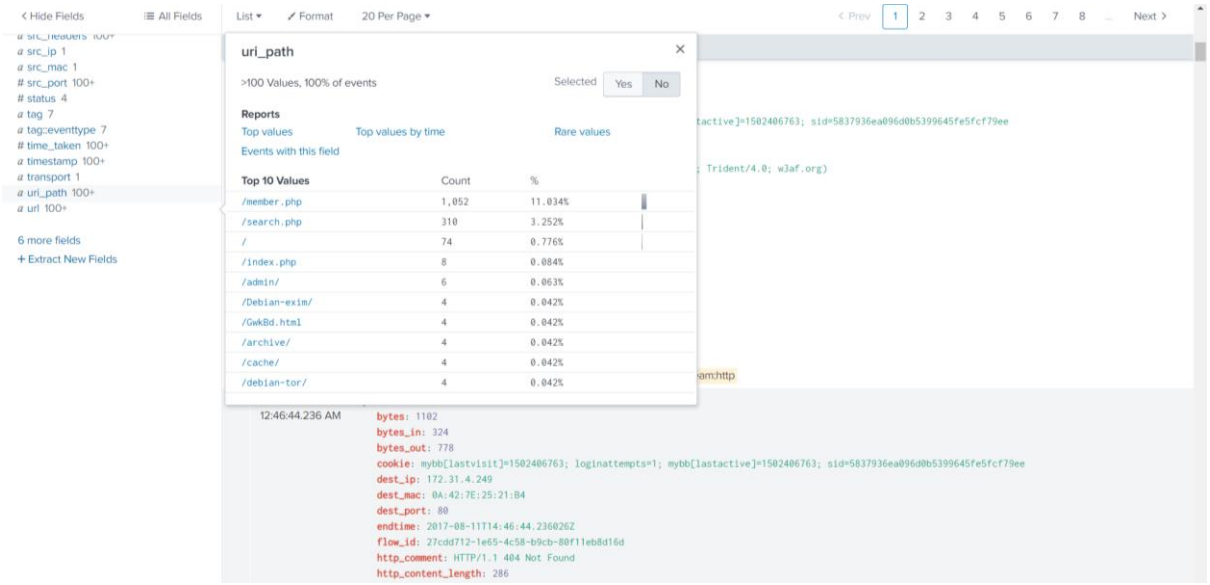
The command **index=botsv2 earliest=0 sourcetype="stream:http" www.brewertalk.com 45.77.65.211 http_user_agent="*"** to find the uri path which is being attacked.

Checking all http user agent, it is found the /member.php is the uri path

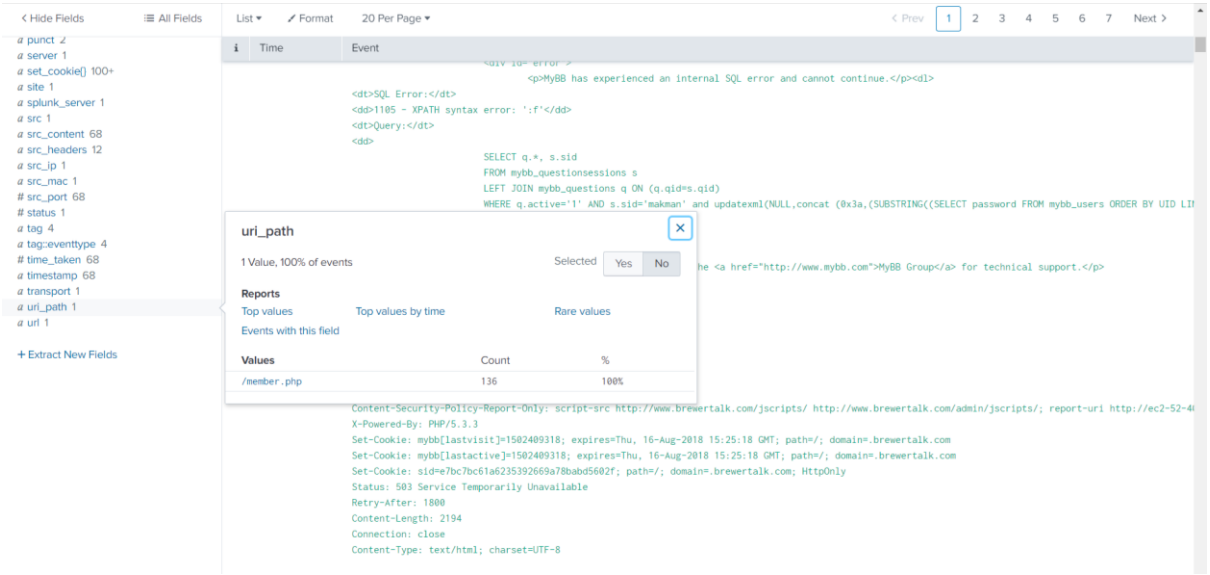




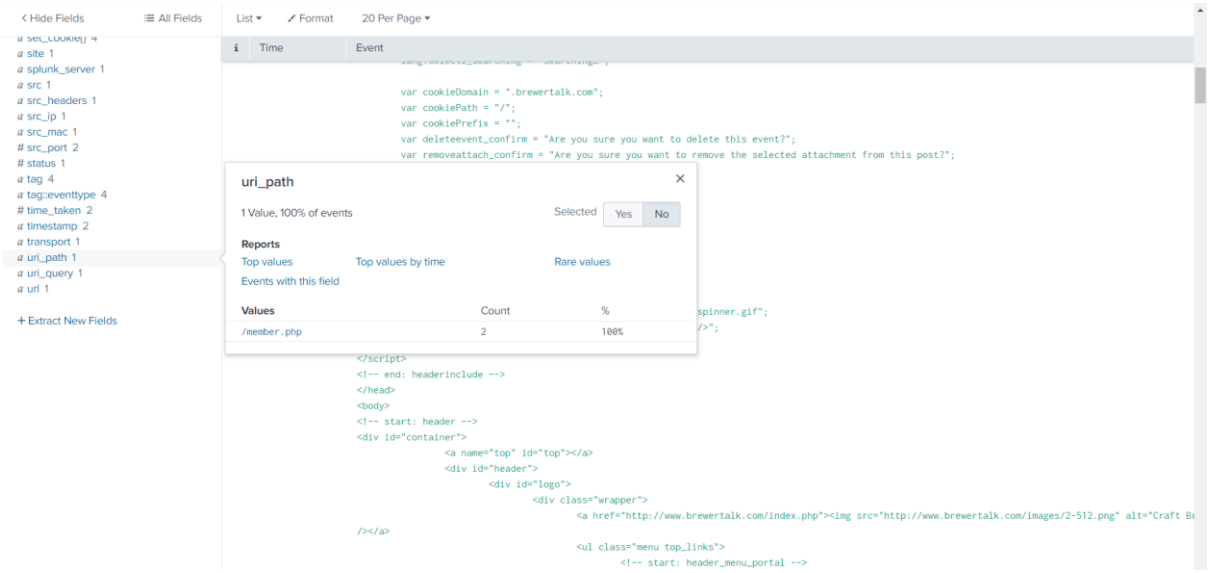
index=botsv2 earliest=0 sourcetype="stream:http" www.brewertalk.com 45.77.65.211 http_user_agent="Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; w3af.org)"



index=botsv2 earliest=0 sourcetype="stream:http" www.brewertalk.com 45.77.65.211 http_user_agent="Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.17 Safari/537.36"



index=botsv2 earliest=0 sourcetype="stream:http" www.brewertalk.com 45.77.65.211 http_user_agent="Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36"



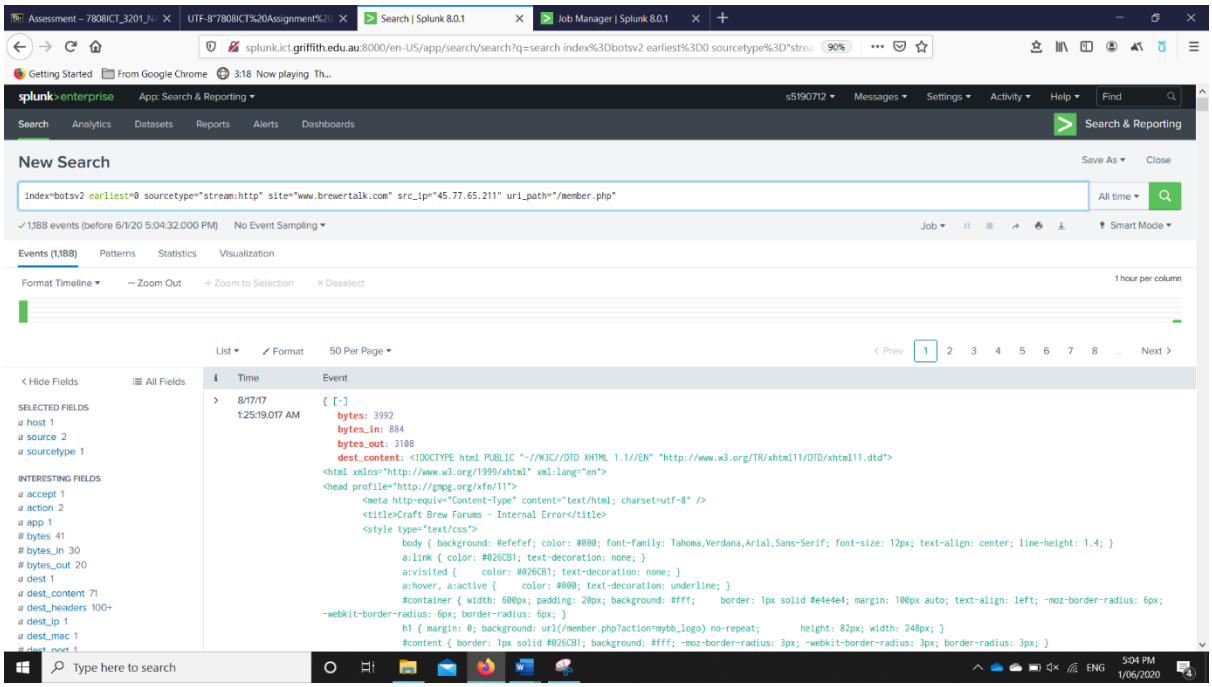
Comparing all http_user_agent, it is found that /member.php is the uri path

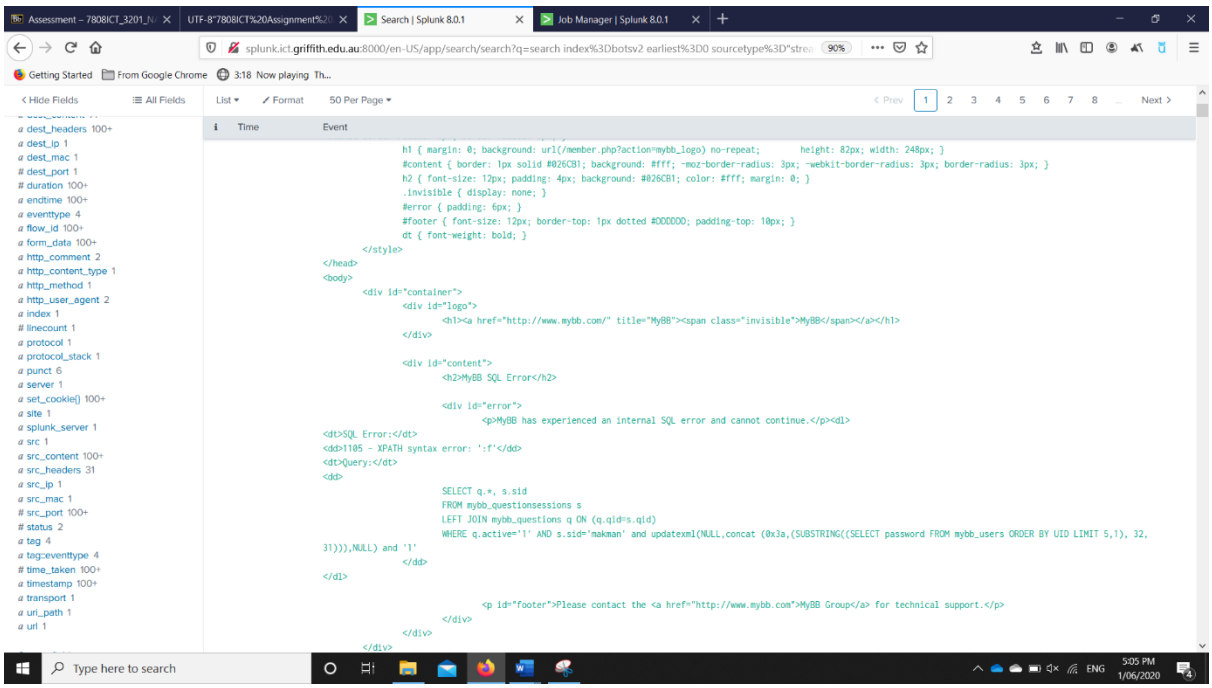
10)

The command **index=botsv2 earliest=0 sourcetype="stream:http" site="www.brewertalk.com" src_ip="45.77.65.211" uri_path="/member.php"** is used to find which sql function is being abused.

The below query is a threat and is an sql injection attack:

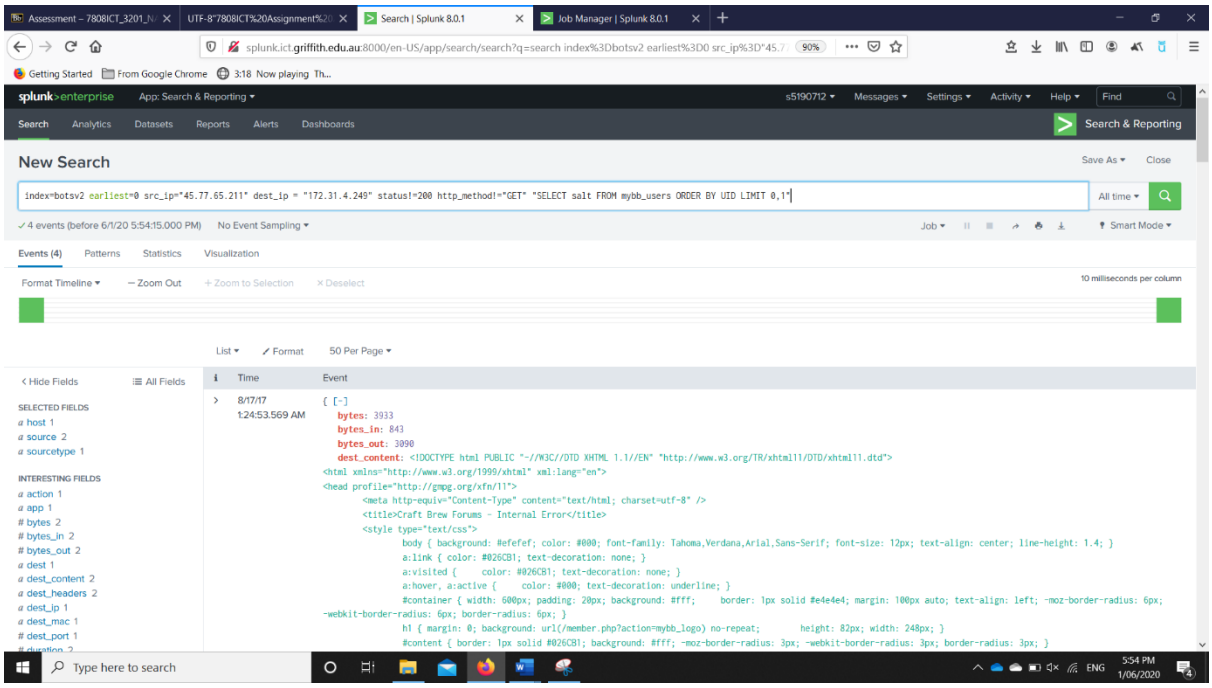
updatexml(NULL,concat (0x3a,(SUBSTRING((SELECT password FROM mybb_users ORDER BY UID LIMIT 5,1), 32, 31))),NULL) and '1'

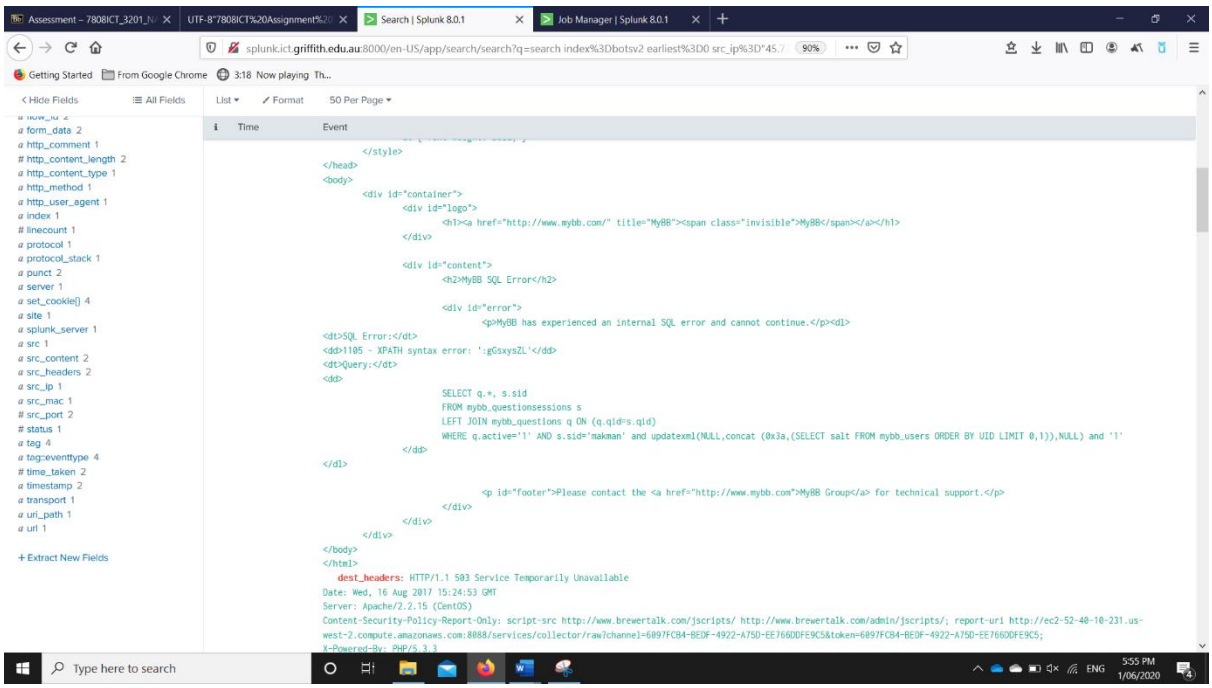




11)

The command **index=botsv2 earliest=0 src_ip="45.77.65.211" dest_ip = "172.31.4.249" status!=200 http_method!="GET" "SELECT salt FROM mybb_users ORDER BY UID LIMIT 0,1"** is used to identify the salt password of Frank Ester.





From the following screenshots, the password value is found as **gGsxysZL.**

12)

The following two command will help in figuring out the answer:

index=botsv2 dest_ip=172.31.4.249 status!=200 http_method=POST XPATH syntax error:btun from with I have found FROM mybb_users ORDER BY UID LIMIT 2,1

index=botsv2 dest_ip=172.31.4.249 status!=200 http_method=POST SELECT password FROM mybb_users ORDER BY UID LIMIT 2,1

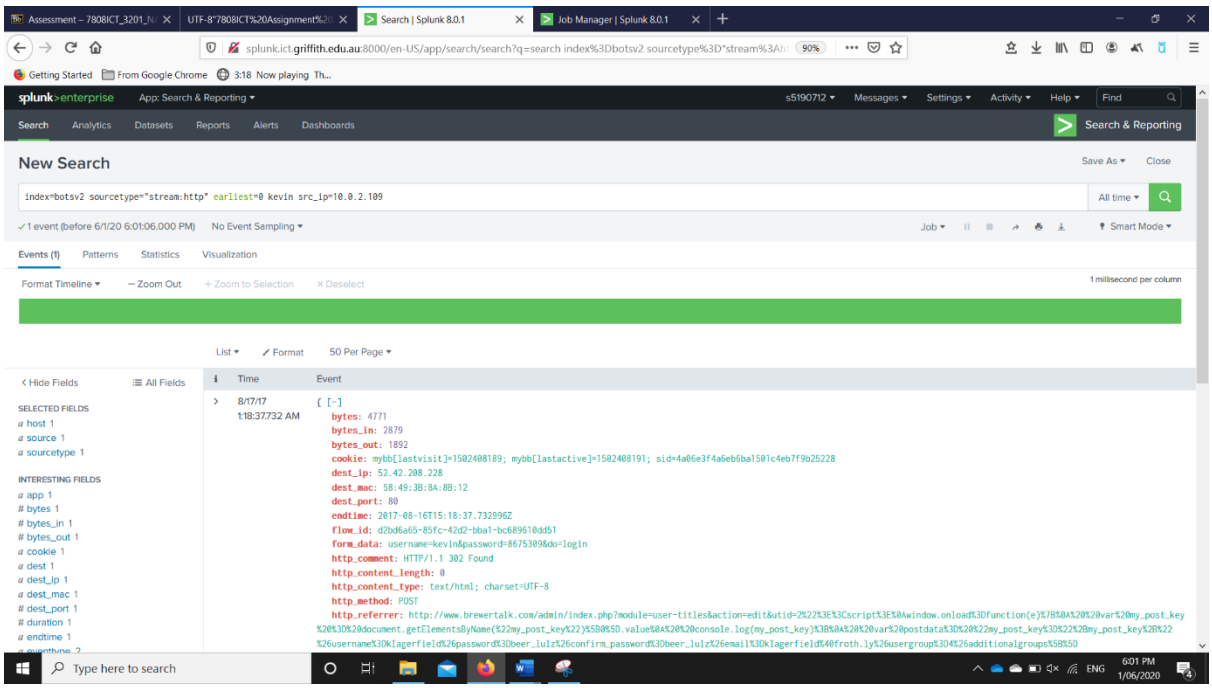
F91904c1dd2723d5911eeba409cc0d1 - hash

t1X7cQPE - salt

We can also find the salt and syntax error and can md5 hash it to find the answer which is **123456**

13)

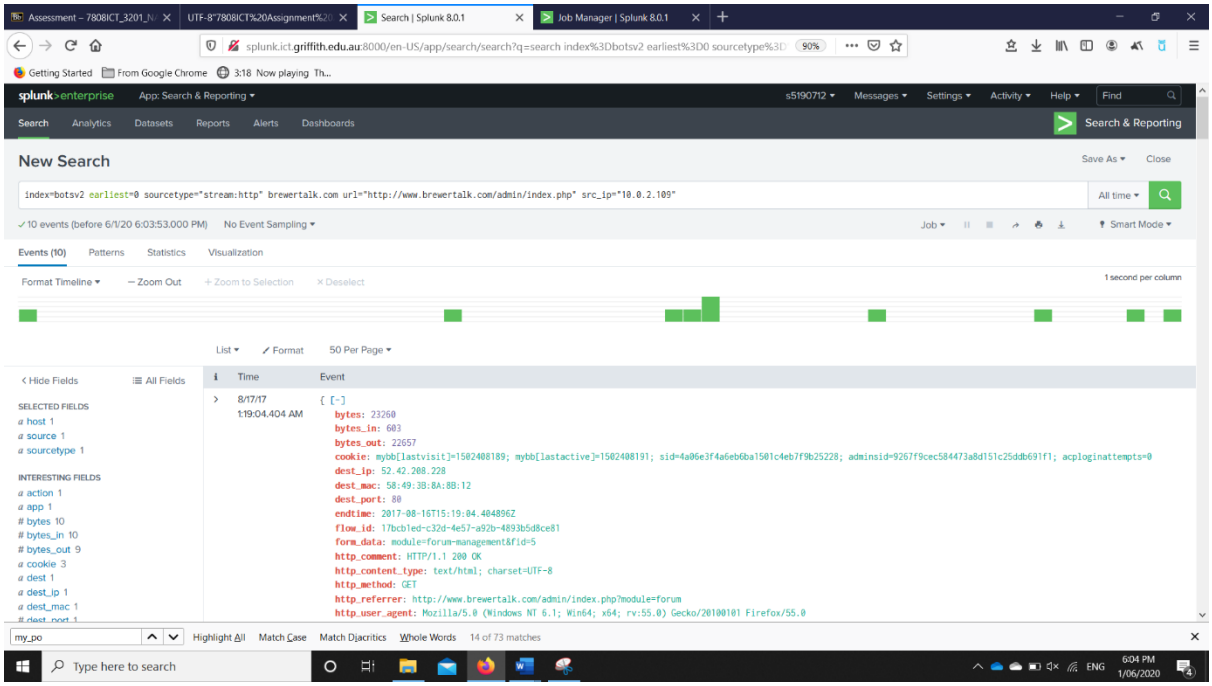
The command **index=botsv2 sourcetype=stream:http earliest=0 kevin src_ip=10.0.2.109** is used to find the value of cookie which Kevin Lagerfield's browser transmitted to the malicious URL.



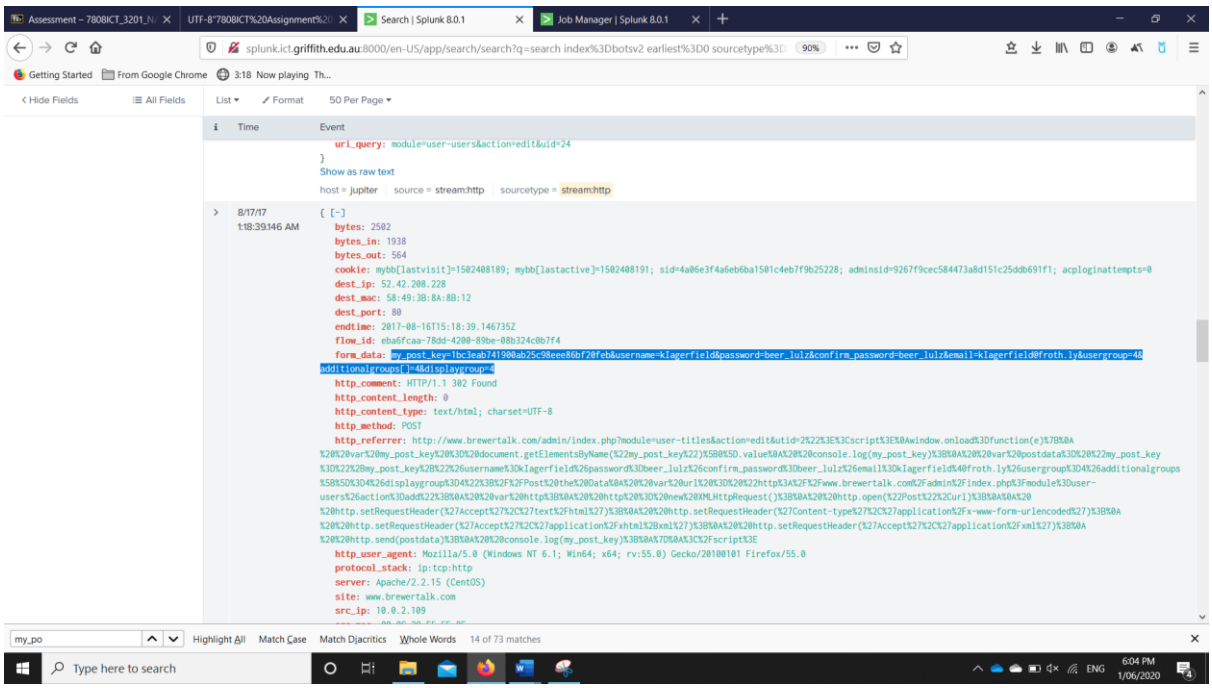
From the above screenshot, the cookie is found out to be **1502408189.**

14)

The command **index=botsv2 earliest=0 sourcetype="stream:http" brewertalk.com url="http://www.brewertalk.com/admin/index.php" src_ip="10.0.2.109"** is used to identify the value of the anti-CSRF token that was stolen from Kevin Lagerfield's computer.

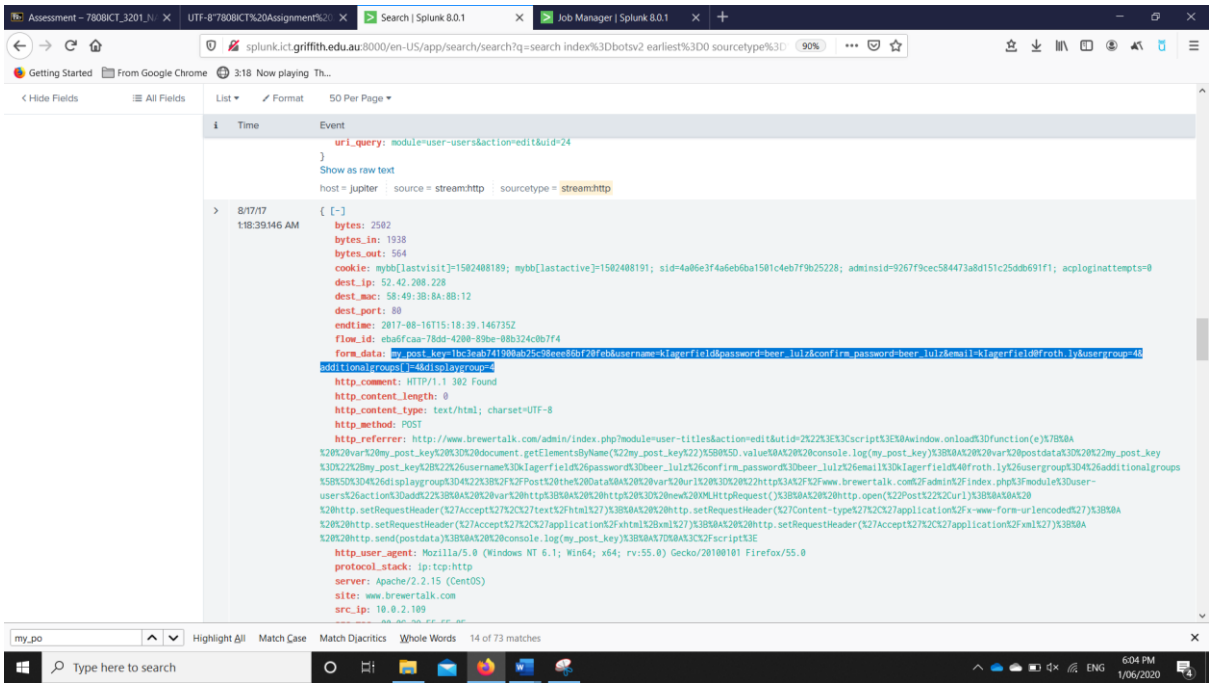


The my_post_key defines the value of anti-CSRF token. From the below screenshot, the value of anti-CSRF token which is my_post_key=**1bc3eab741900ab25c98eee86bf20feb**

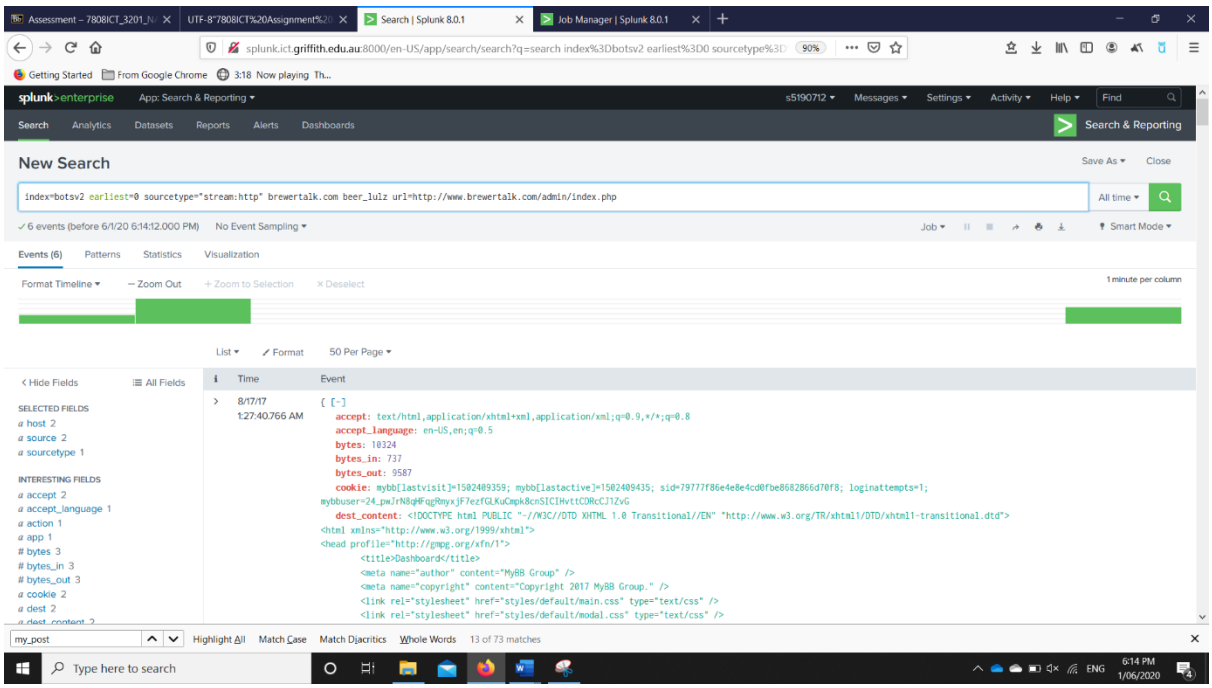


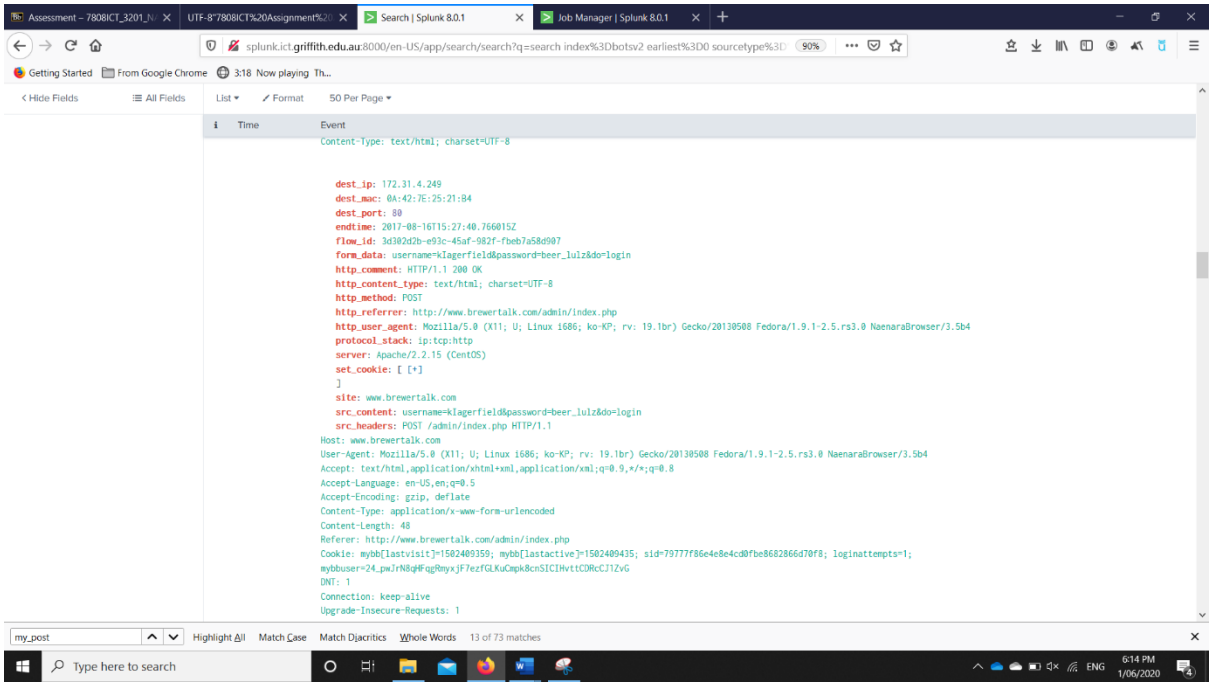
15)

From the above question, it is found that password of required username is beer_lulz.



The command **index=botsv2 earliest=0 sourcetype="stream:http" brewertalk.com beer_lulz url=http://www.brewertalk.com/admin/index.php** is used to find the username as the my_post_key and password has been already found.

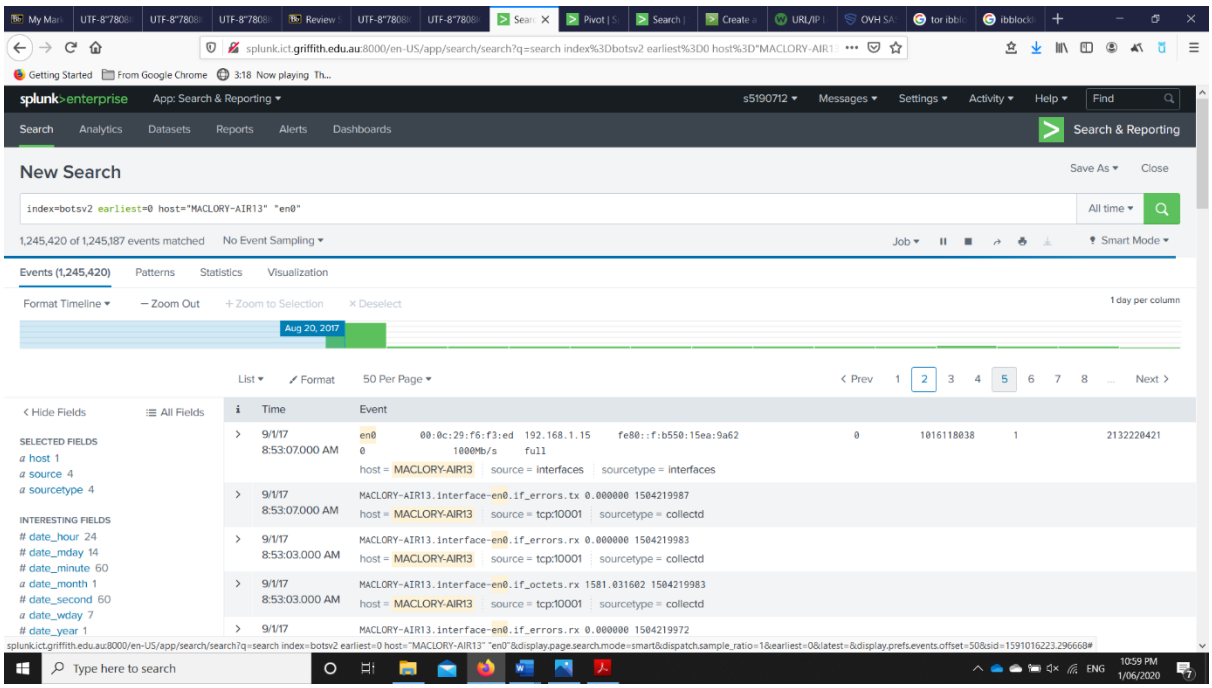




From the above screenshot, it is found that the username which was created maliciously by a spear phishing attack is **klagerfield.**

16)

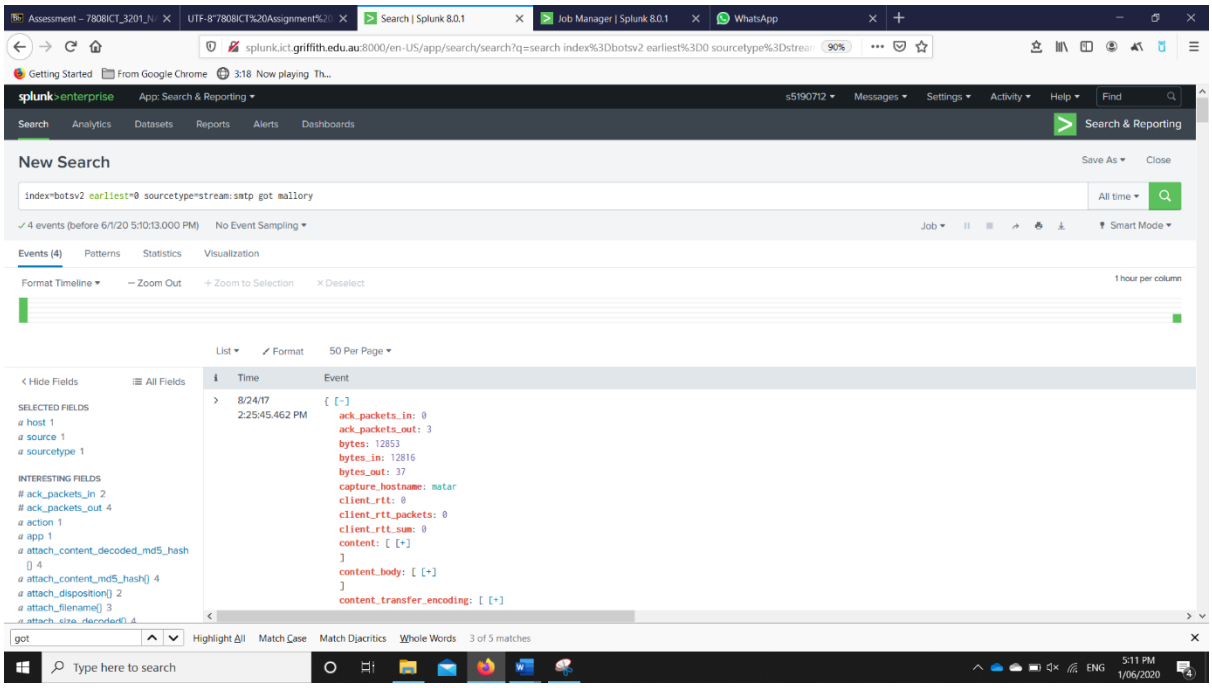
The command **index=botsv2 earliest=0 host="MACLORY-AIR13" "en0"**



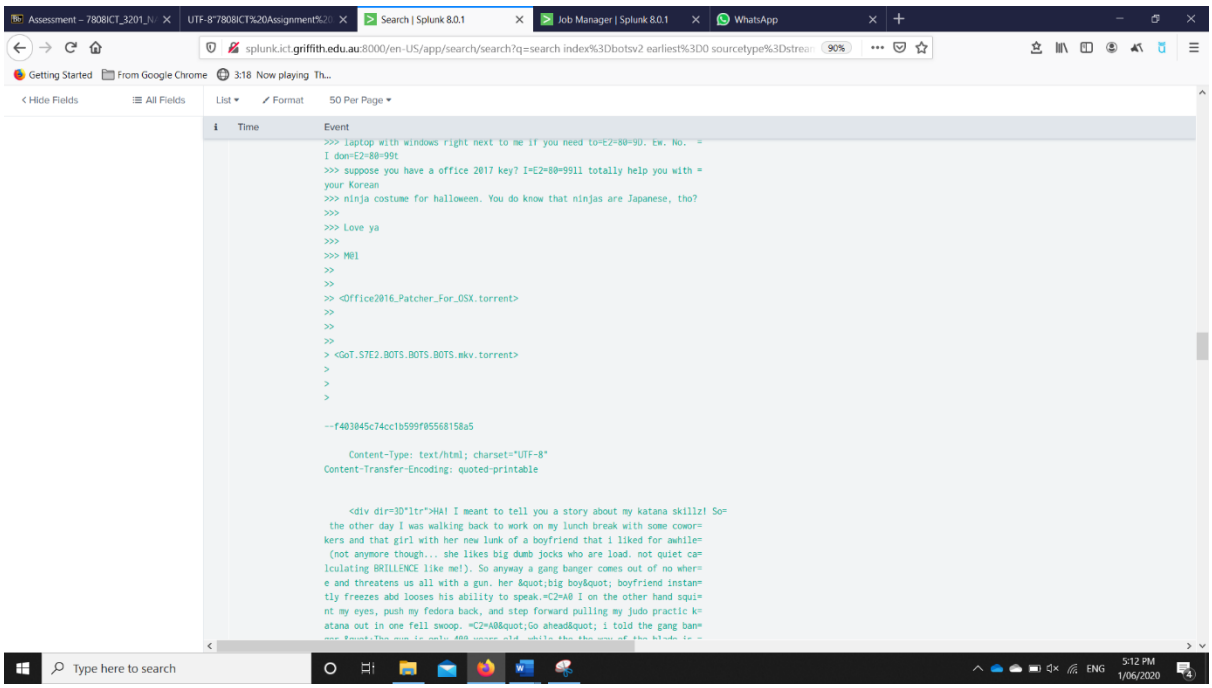
From the above screenshot, the mac address is found out to be 00:0c:29:f6:f3:ed

17)

The command **index=botsv2 earliest=0 sourcetype=stream:smtp got Mallory** is used to find the episode of the game of thrones which Mallory is excited to watch.

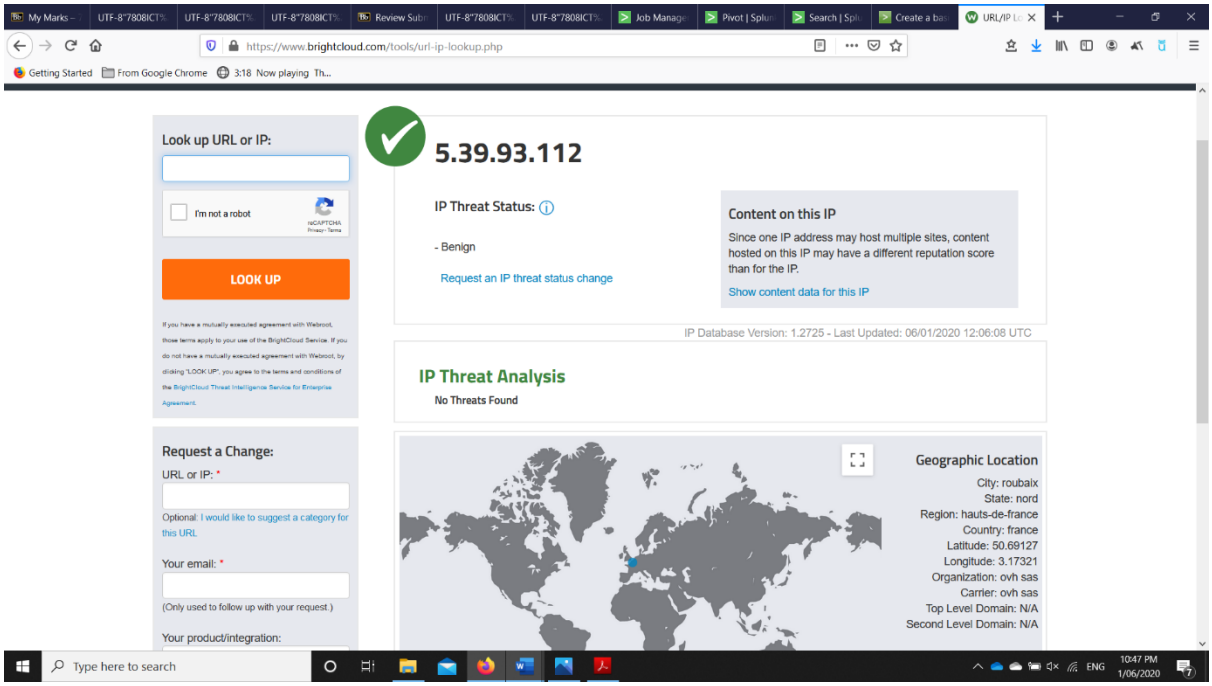


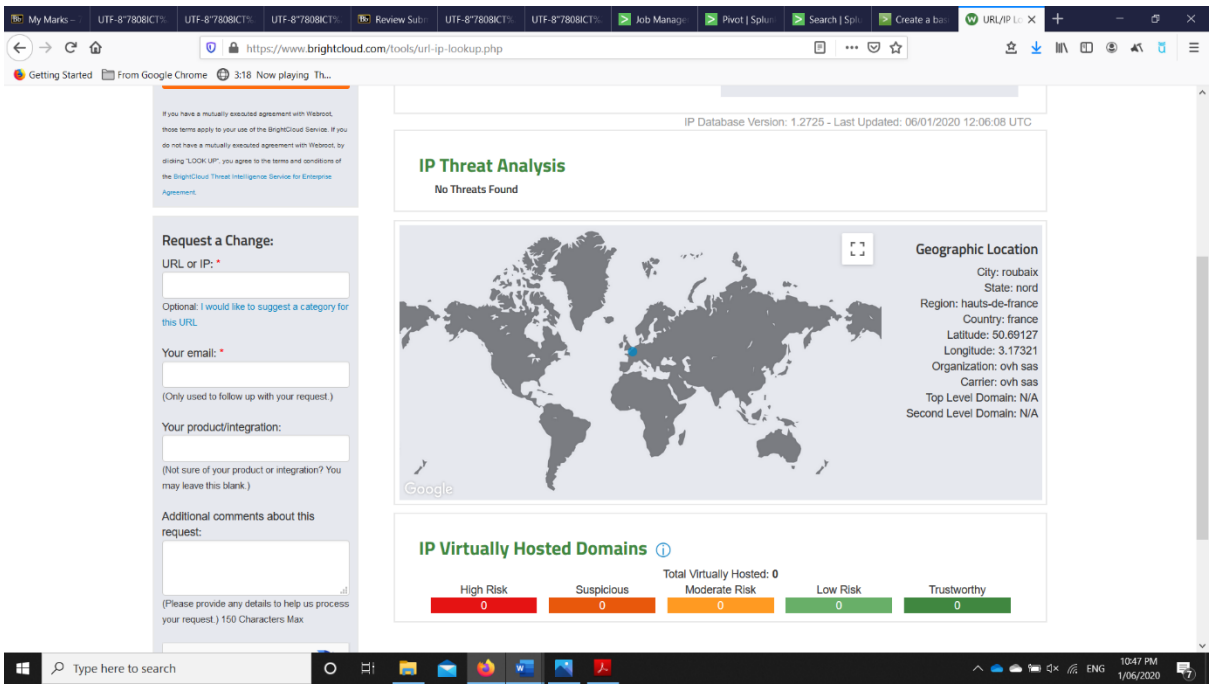
From the following conversation, it is found that Mallory was excited to watch Game of Thrones Episode 2 in Season 2 which is **Stormborn.**



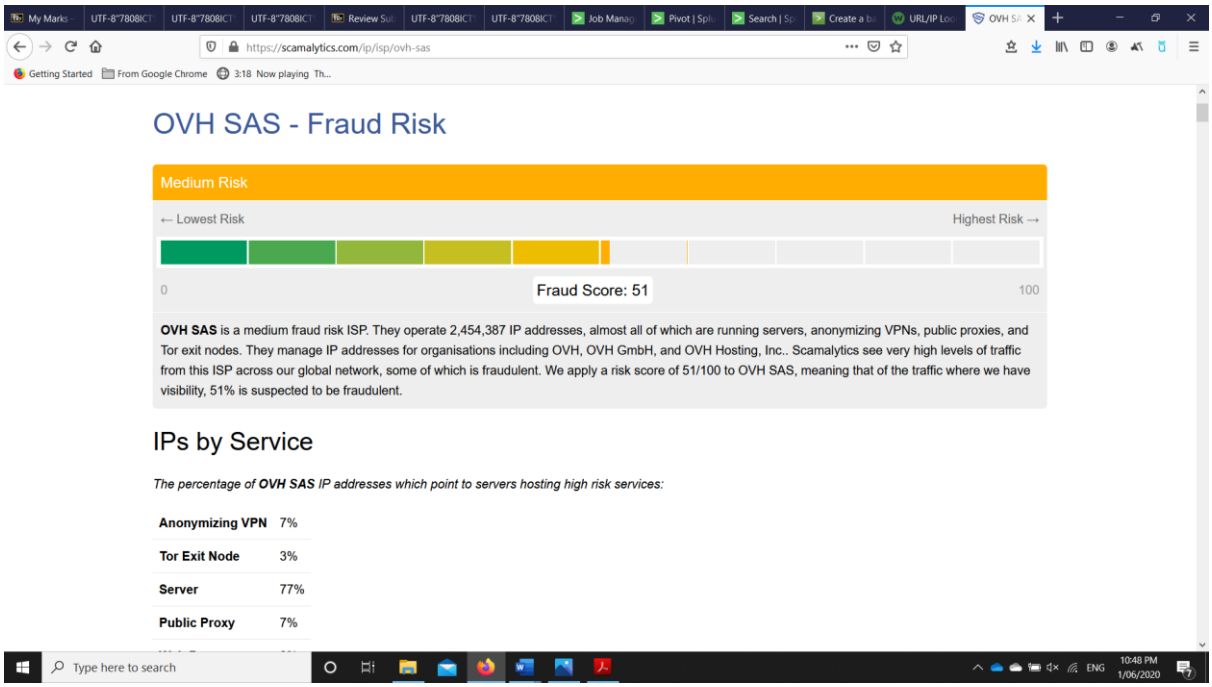
19)

The Ovh SAS organization is identified by running the suspected IP address in the threat status





The OVH SAS organization is searched in the scammylatics website which shows the result of fraud risk score : 51



The Tor exit node shows an 3% high risk service.

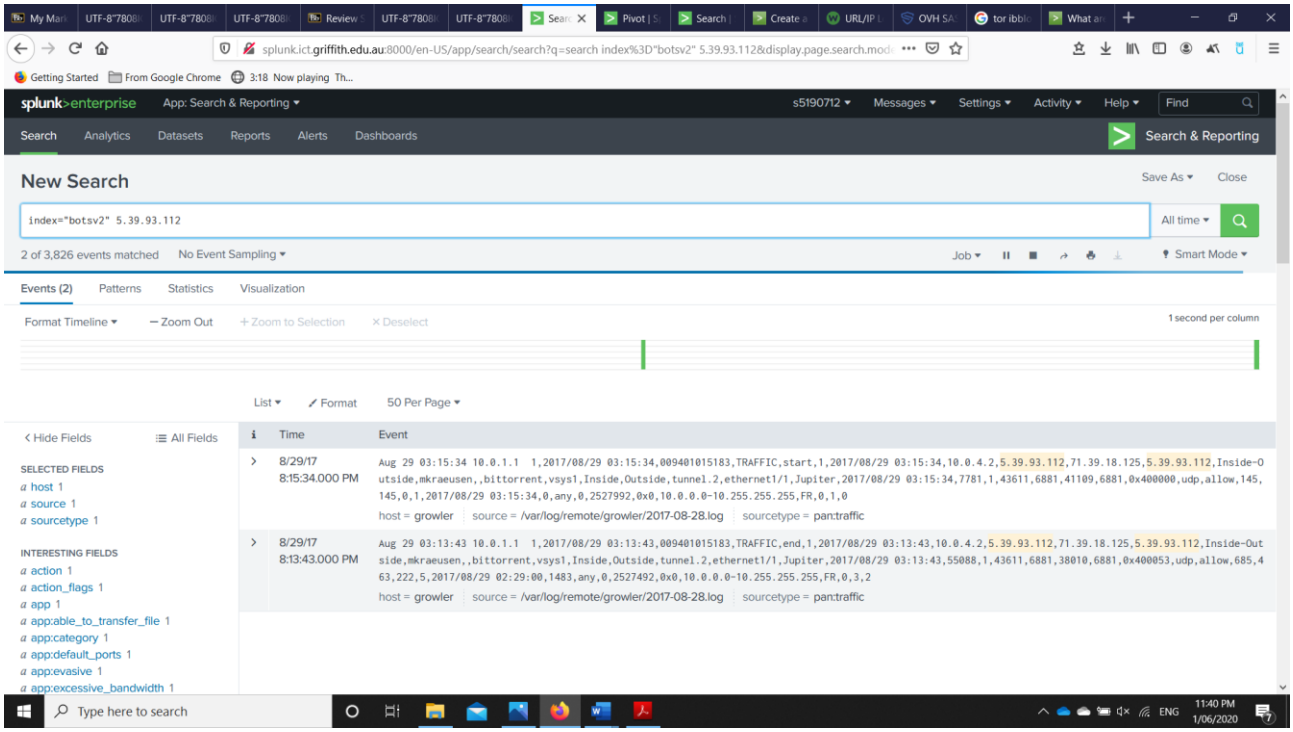
Default Data Downloads

Threat Provider	Threat Source	Source site
Alexa Internet*	Top 1 Million Sites	http://s3.amazonaws.com/alexa-static/
Emerging Threats	compromised IPs blocklist	http://rules.emergingthreats.net/blockrules
	fwip rules	http://rules.emergingthreats.net/fwrules
Hail a TAXII.com	Malware domain host list	http://hailataxii.com
I-Blocklist	Logmein, Piratebay, Proxy, Rapidshare, Spyware, Tor, Web attacker	http://list.iblocklist.com
IANA*	ICANN Top-level Domains List	http://data.iana.org
Malware Domains	Malware Domain Blocklist	http://mirror1.malwaredomains.com
Mozilla*	Mozilla Public Suffix List	https://publicsuffix.org
Phishtank	Phishtank Database	http://data.phishtank.com
SANS	SANS blocklist	http://isc.sans.edu
abuse.ch	Palevo C&C IP Blocklist	https://palevotracker.abuse.ch
abuse.ch	ZeuS blocklist (standard & bad IPs only)	https://zeustracker.abuse.ch

the Tor exit node belongs to the **iblocklist**

20)

The command index="botsv2" 5.39.93.112 is used to find the protocol. The protocol found is **UDP**



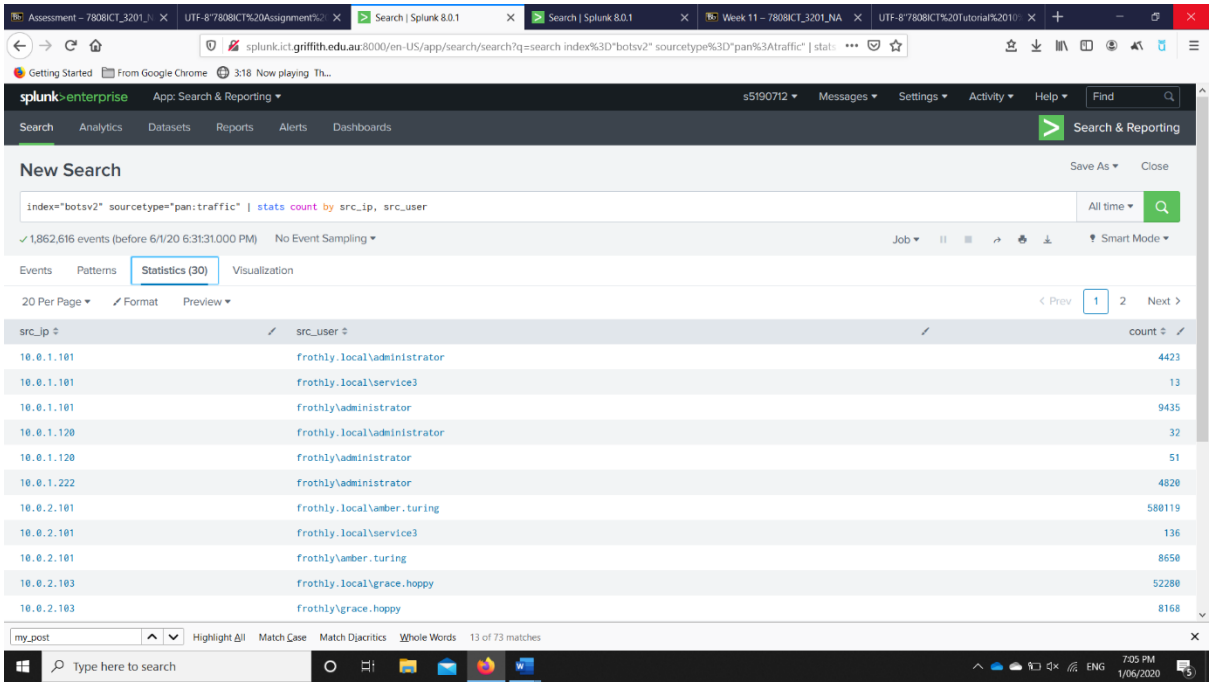
Task 2

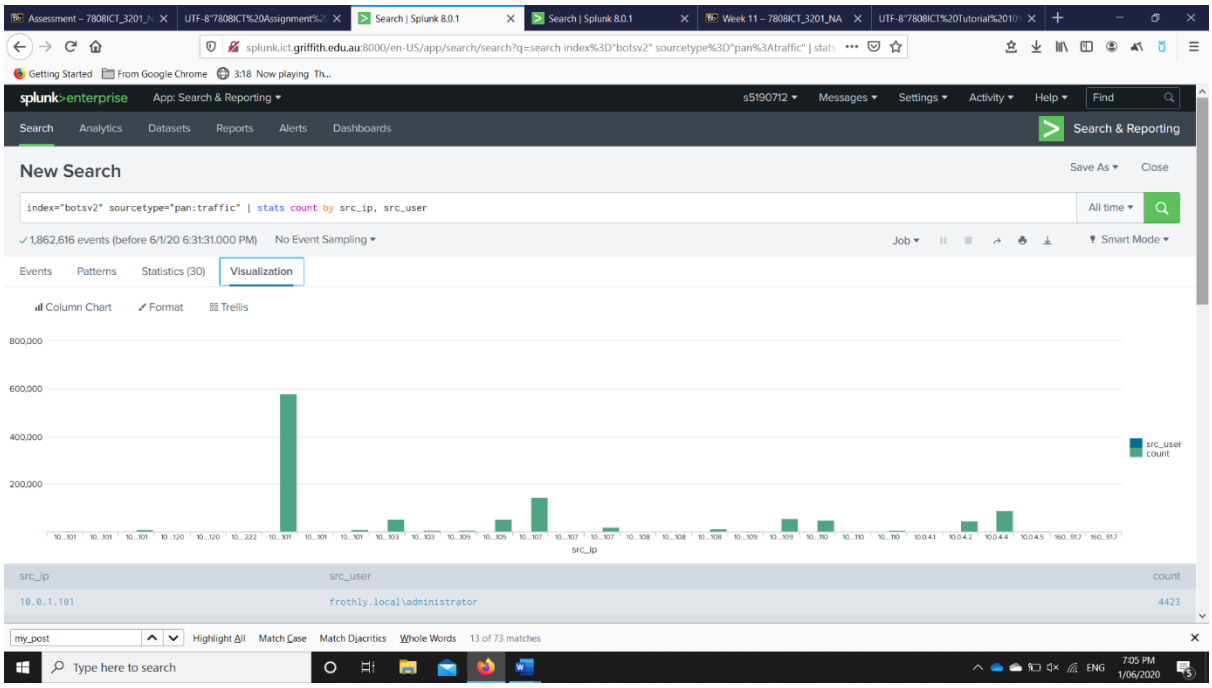
The Palo Alto network logs ingested data are explored using different panels.

Panel 1

The first panel shows the command **index="botsv2" sourcetype="pan:traffic" | stats count by src_ip, src_user** which shows the stats count function.

The stats command is used to calculate statistics depending on the field. In this panel, the stats count is used to count the number of source ip address and source users in the database.



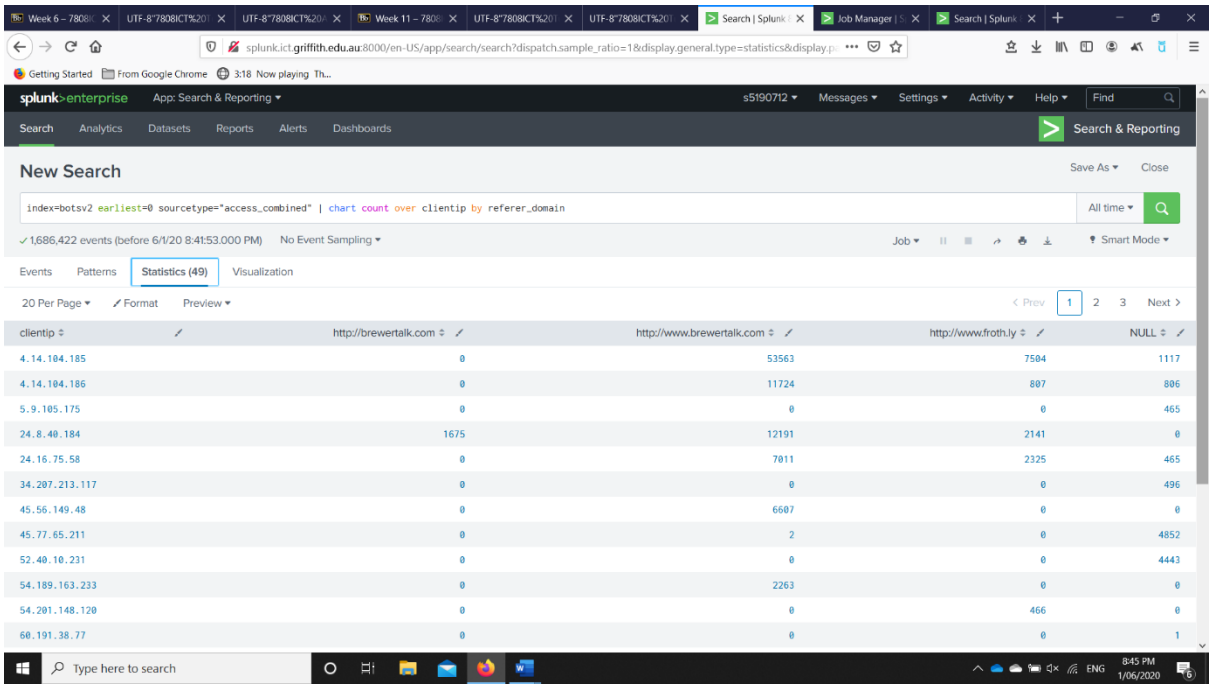


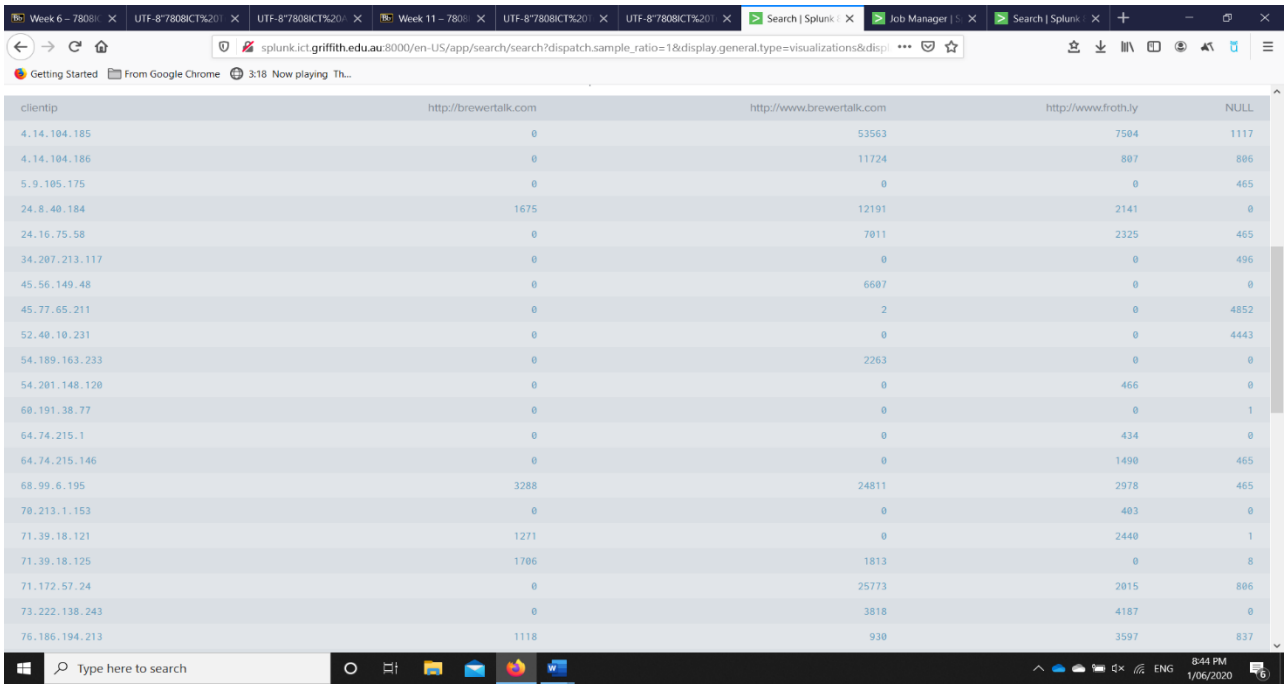
The Virtualization is used to view the chart of each source_ip counts and the difference between each source_ip counts are viewed.

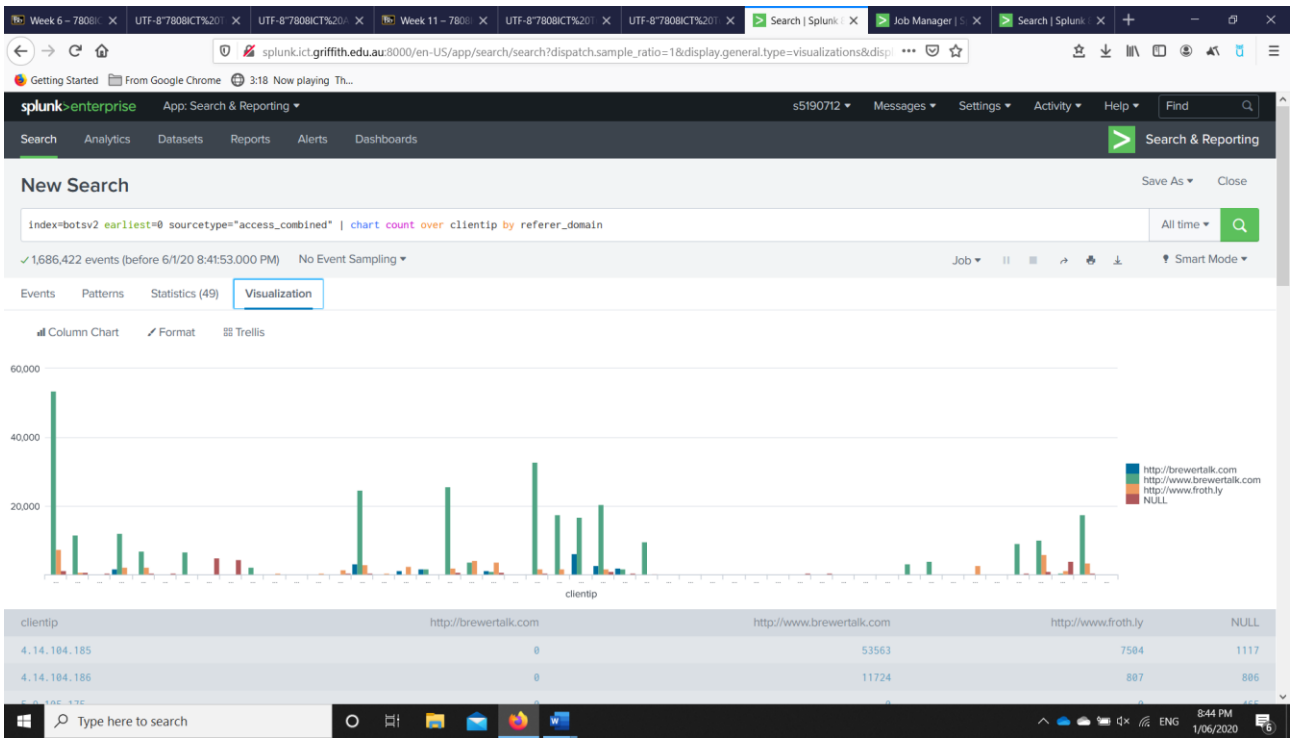
Panel 2

The second panel shows the command **index=botsv2 earliest=0 sourcetype="access_combined" | chart count over clientip by referer_domain** which shows the chart count function.

The chart count command is used count the number of times the field is viewed. In this panel 2, the chart count command is used to count the number of times the website is viewed by the clientip.



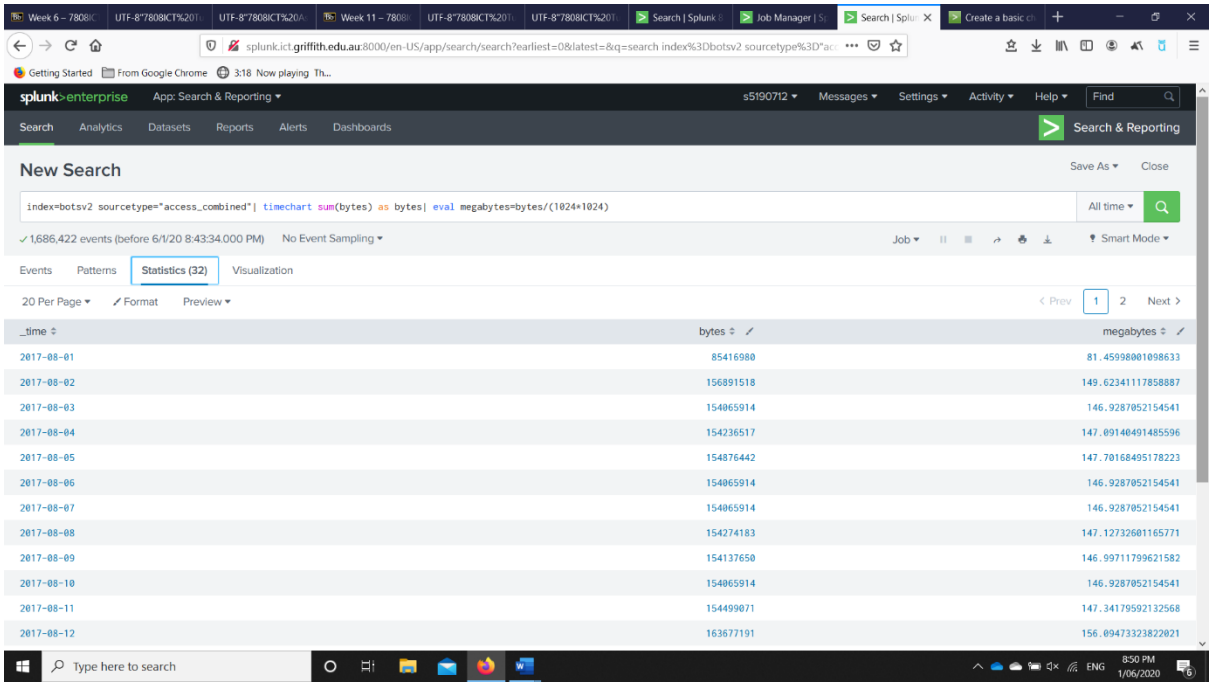


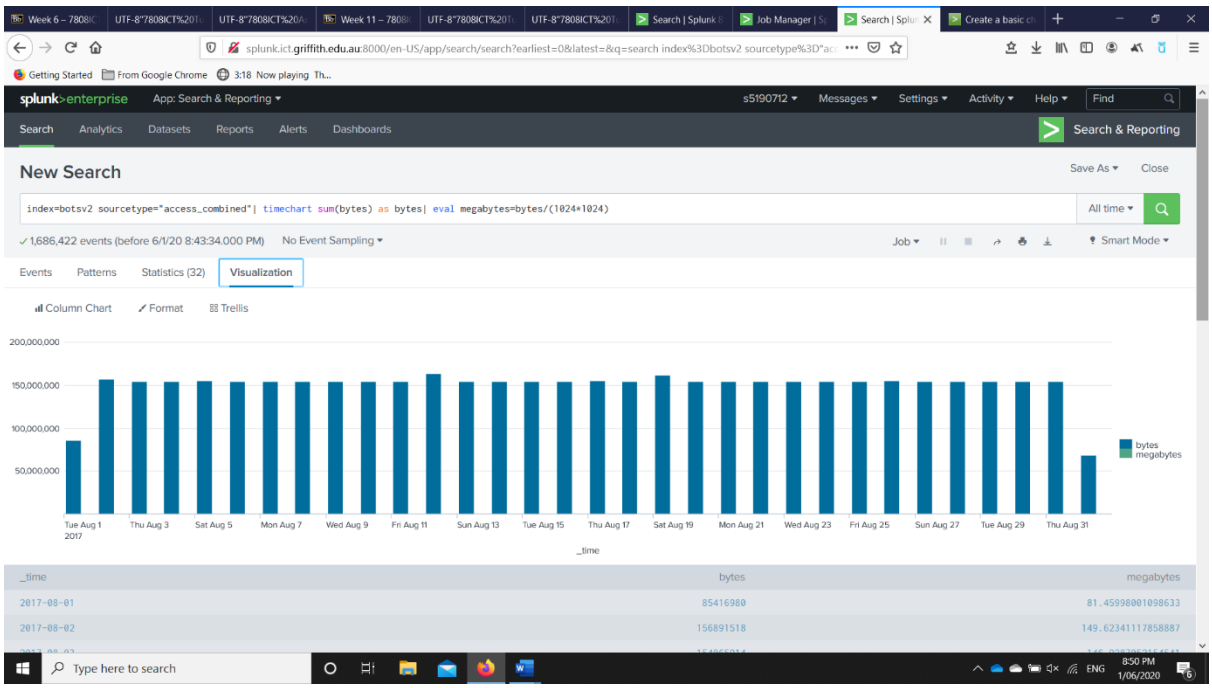


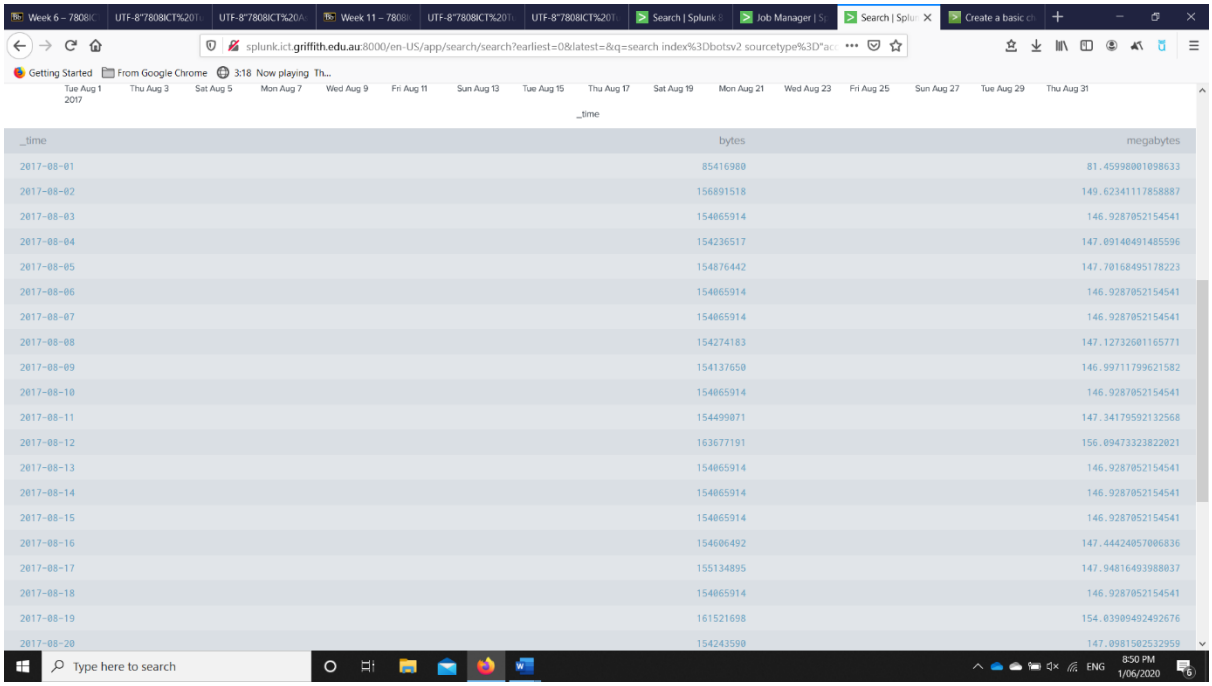
Panel 3

The Panel 3 shows the command **index=botsv2 sourcetype="access_combined"| timechart sum(bytes) as bytes| eval megabytes=bytes/(1024*1024)**

The Panel 3 visualization shows the web servers daily volume usage in Mega Bytes. The eval command is used to convert from bytes to megabytes.

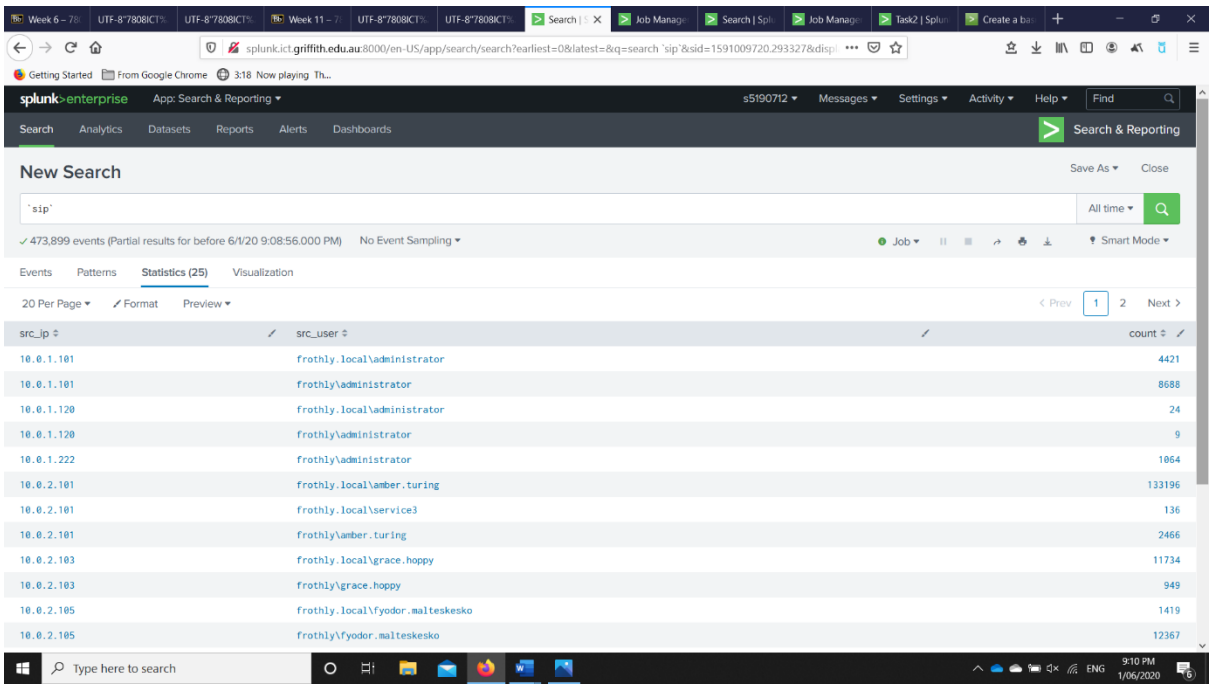






Panel 4

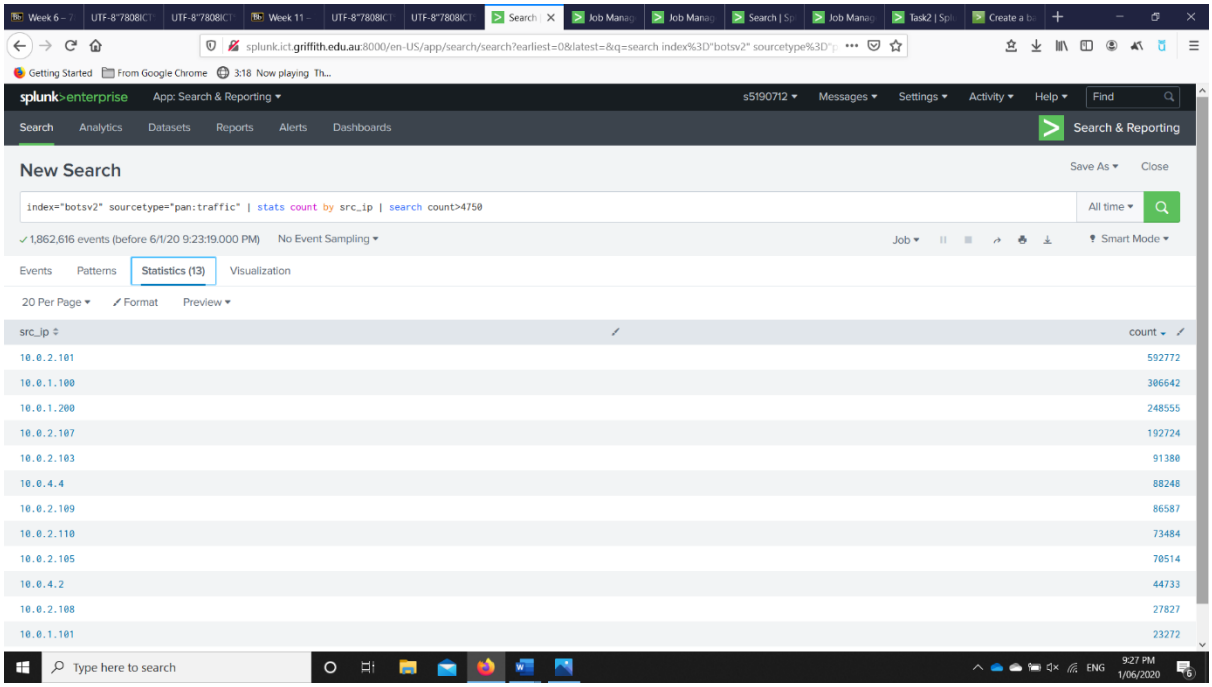
Initially navigated to settings in the splunk and clicked the advanced search which shows the New Macro tab. A new Macro is created with the name sip and definition is given as **index="botsv2" sourcetype="pan:traffic" | stats count by src_ip, src_user.** The created Macro is searched with the name `sip` and the statistics is retrieved.

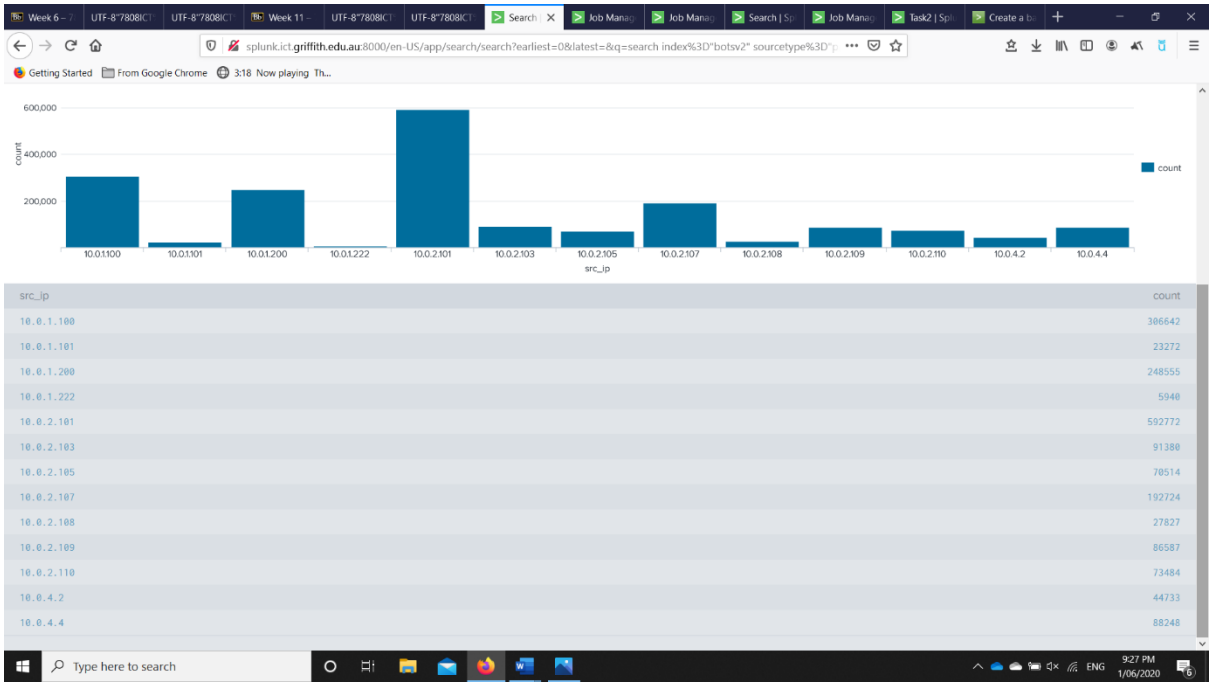


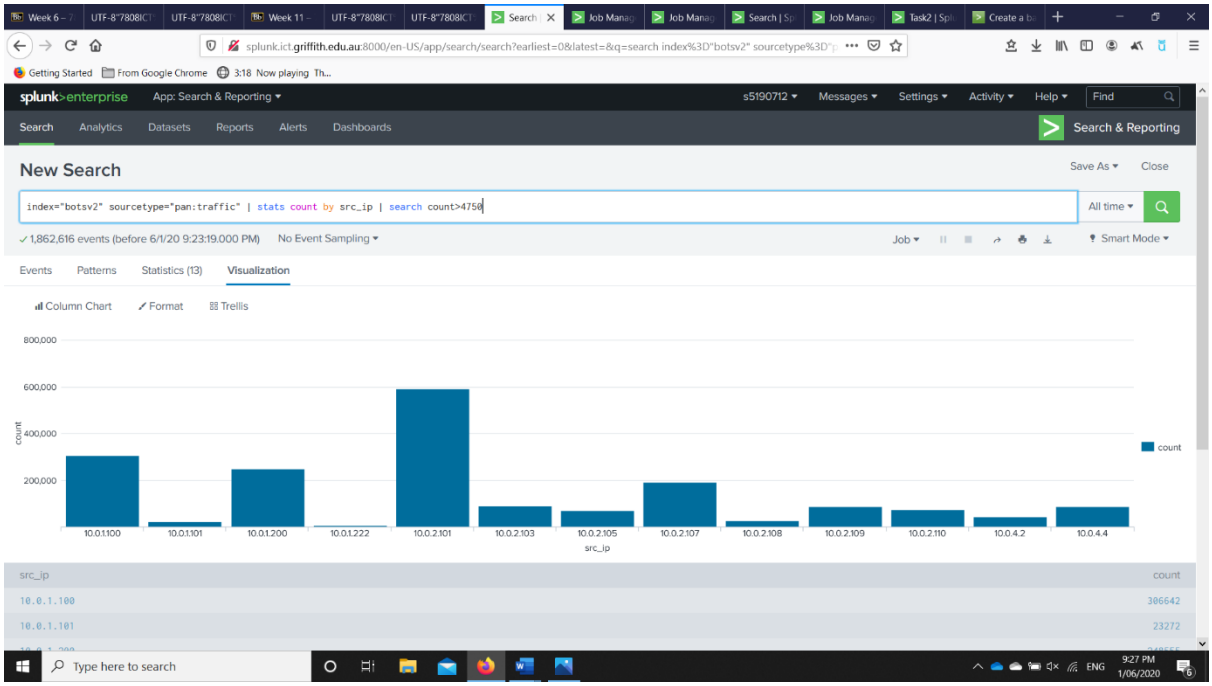
Panel 5

The panel 5 shows the command **index="botsv2" sourcetype="pan:traffic" | stats count by src_ip | search count>4750.** The search is used to limit the data to particular requirement and filtered.

The panel 5 visualization shows that the source ip address with the count greater than 4750 is shown.

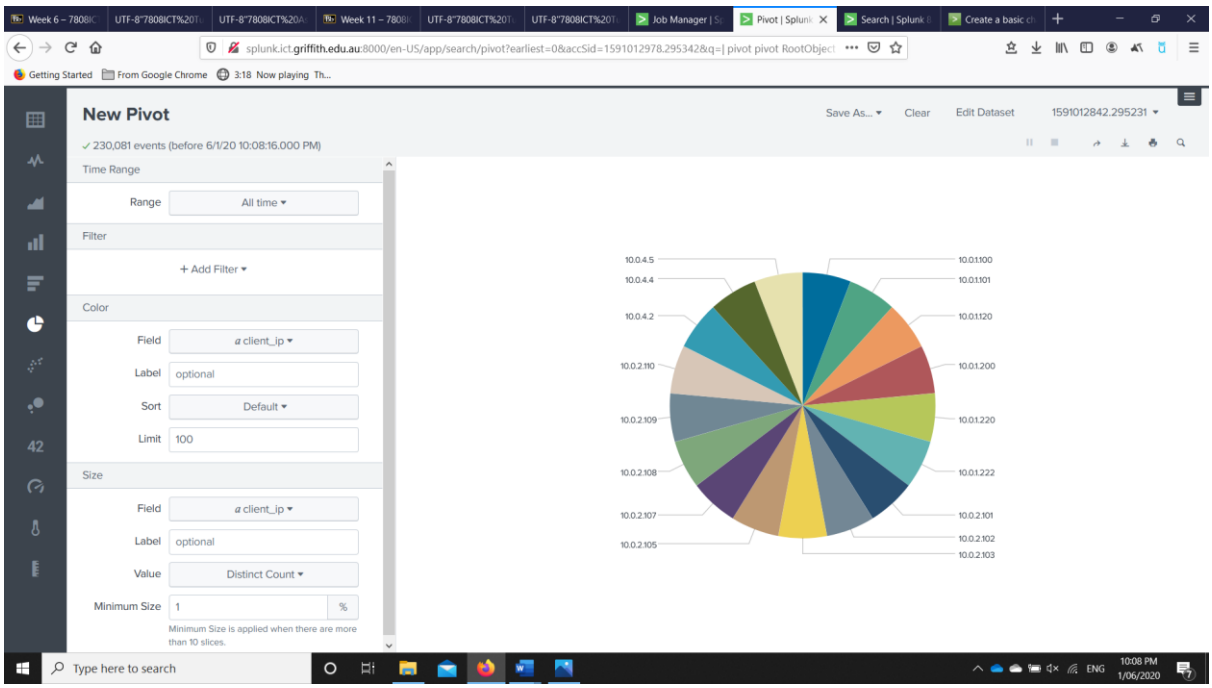






Panel 6

The Panel 6 shows the command index=botsv2 sourcetype="pan:traffic" which is used to create a new pivot. The client_ip field is choosen to view the pivot.


New Pivot
Save As...
Clear
Edit Dataset
1591012842.295231
230,081 events (before 6/1/20 10:08:16.000 PM)
Time Range
Range
All time
Filter
+ Add Filter
Color
Field
a client_ip
Label
optional
Sort
Default
Limit
100
Size
Field
a client_ip
Label
optional
Value
Distinct Count
Minimum Size
1
%
Minimum Size is applied when there are more than 10 slices.
10.0.4.5
10.0.4.4
10.0.4.2
10.0.2.110
10.0.2.109
10.0.2.108
10.0.2.107
10.0.2.105
10.0.1.100
10.0.1.101
10.0.1.120
10.0.1.200
10.0.1.220
10.0.1.222
10.0.2.101
10.0.2.102
10.0.2.103
Type here to search
ENG
10:08 PM
1/06/2020