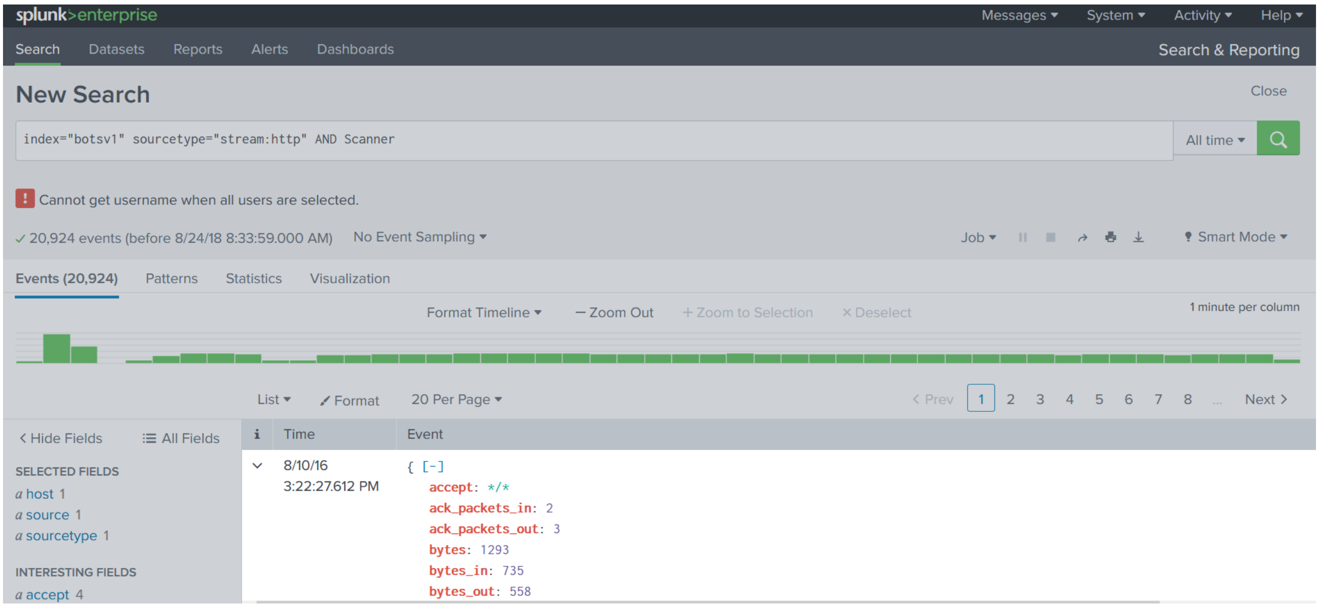
BOTSv1 Writeups

Level 1: Finding Attack Servers

BOTSv1 1.1: Scanner Name (5 pts)

Question: What is the brand name of the vulnerability scanner, covered by a green box in the image above?

SPL: `index="botsv1" sourcetype="stream:http" AND Scanner`



```
index="botsv1" sourcetype="stream:http" AND Scanner
```

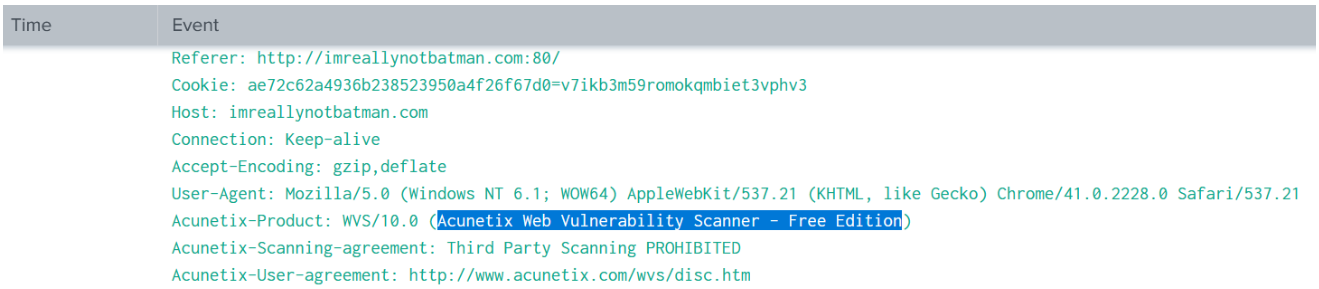
! Cannot get username when all users are selected.

✓ 20,924 events (before 8/24/18 8:33:59.000 AM)   No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a accept 4

```
8/10/16            { [-]
3:22:27.612 PM        accept: */*
                      ack_packets_in: 2
                      ack_packets_out: 3
                      bytes: 1293
                      bytes_in: 735
                      bytes_out: 558
```



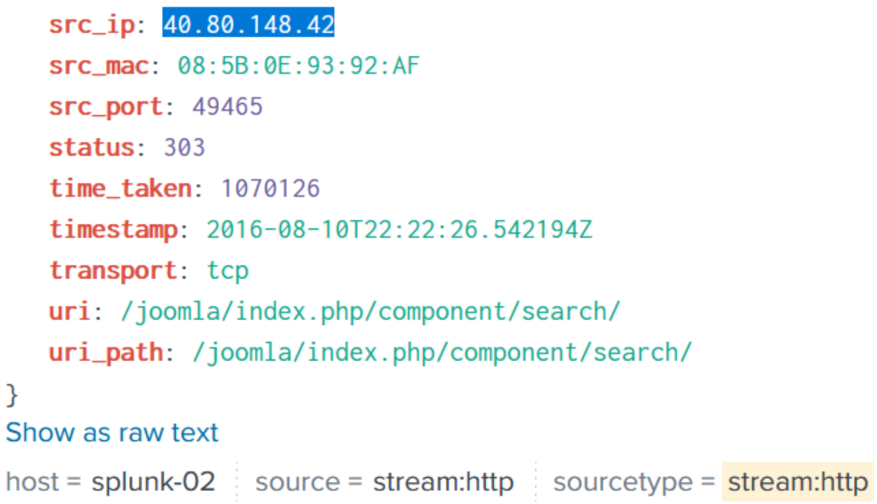
```
Time   Event
       Referer: http://imreallynotbatman.com:80/
       Cookie: ae72c62a4936b238523950a4f26f67d0=v7ikb3m59romokqmbiet3vphv3
       Host: imreallynotbatman.com
       Connection: Keep-alive
       Accept-Encoding: gzip,deflate
       User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
       Acunetix-Product: WVS/10.0 (Acunetix Web Vulnerability Scanner - Free Edition)
       Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
       Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

A: `Acunetix`

BOTSv1 1.2: Attacker IP (5 pts)

Question: What is the attacker's IP address?

SPL: *same as above*



```
    src_ip: 40.80.148.42
    src_mac: 08:5B:0E:93:92:AF
    src_port: 49465
    status: 303
    time_taken: 1070126
    timestamp: 2016-08-10T22:22:26.542194Z
    transport: tcp
    uri: /joomla/index.php/component/search/
    uri_path: /joomla/index.php/component/search/
}
```

Show as raw text

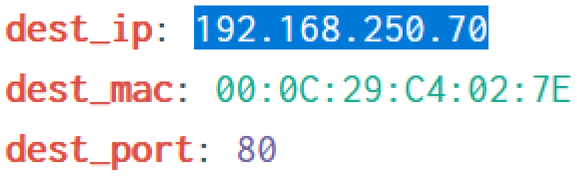
host = splunk-02 | source = stream:http | sourcetype = stream:http

A: `40.80.148.42`

BOTSv1 1.3: Web Server IP (5 pts)

Question: What is the IP address of the web server serving "imreallynotbatman.com"?

SPL: `index="botsv1" sourcetype="stream:http" AND Scanner` *or* `index="botsv1" sourcetype="stream:http" AND "imnotreallybatman.com"`



```
dest_ip: 192.168.250.70
dest_mac: 00:0C:29:C4:02:7E
dest_port: 80
```

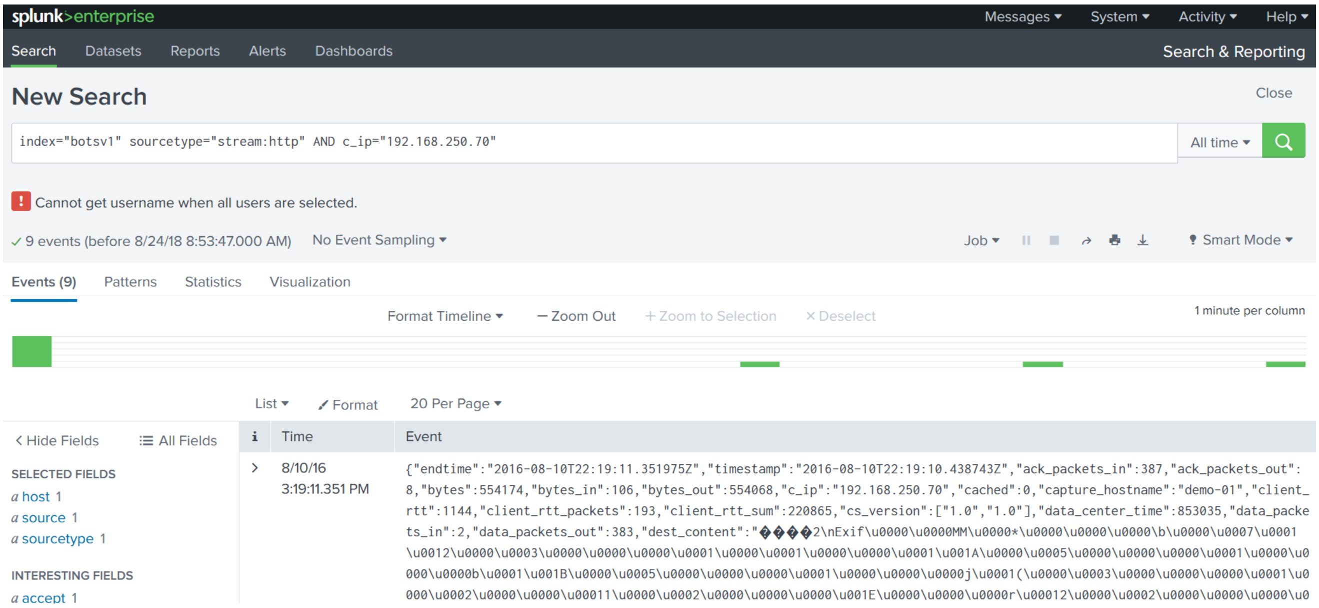
A: `192.168.250.70`

BOTSv1 1.4: Defacement Filename (10 pts)

Question: What is the name of the file used to deface the web server serving "imreallynotbatman.com"?

> Hints:
>
> - It was downloaded by the Web server, so the server's IP is a client address, not a destination address.
> - Remove the filter to see all 9 such events. Examine the **uri** values.

SPL: `index="botsv1" sourcetype="stream:http" AND c_ip="192.168.250.70"`


splunk>enterprise
Messages ▾ System ▾ Activity ▾ Help ▾
Search Datasets Reports Alerts Dashboards
Search & Reporting
Close
All time ▾
Job ▾
Smart Mode ▾
Events (9) Patterns Statistics Visualization
Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect
1 minute per column
List ▾ Format 20 Per Page ▾
< Hide Fields ☰ All Fields

New Search

```
index="botsv1" sourcetype="stream:http" AND c_ip="192.168.250.70"
```

! Cannot get username when all users are selected.

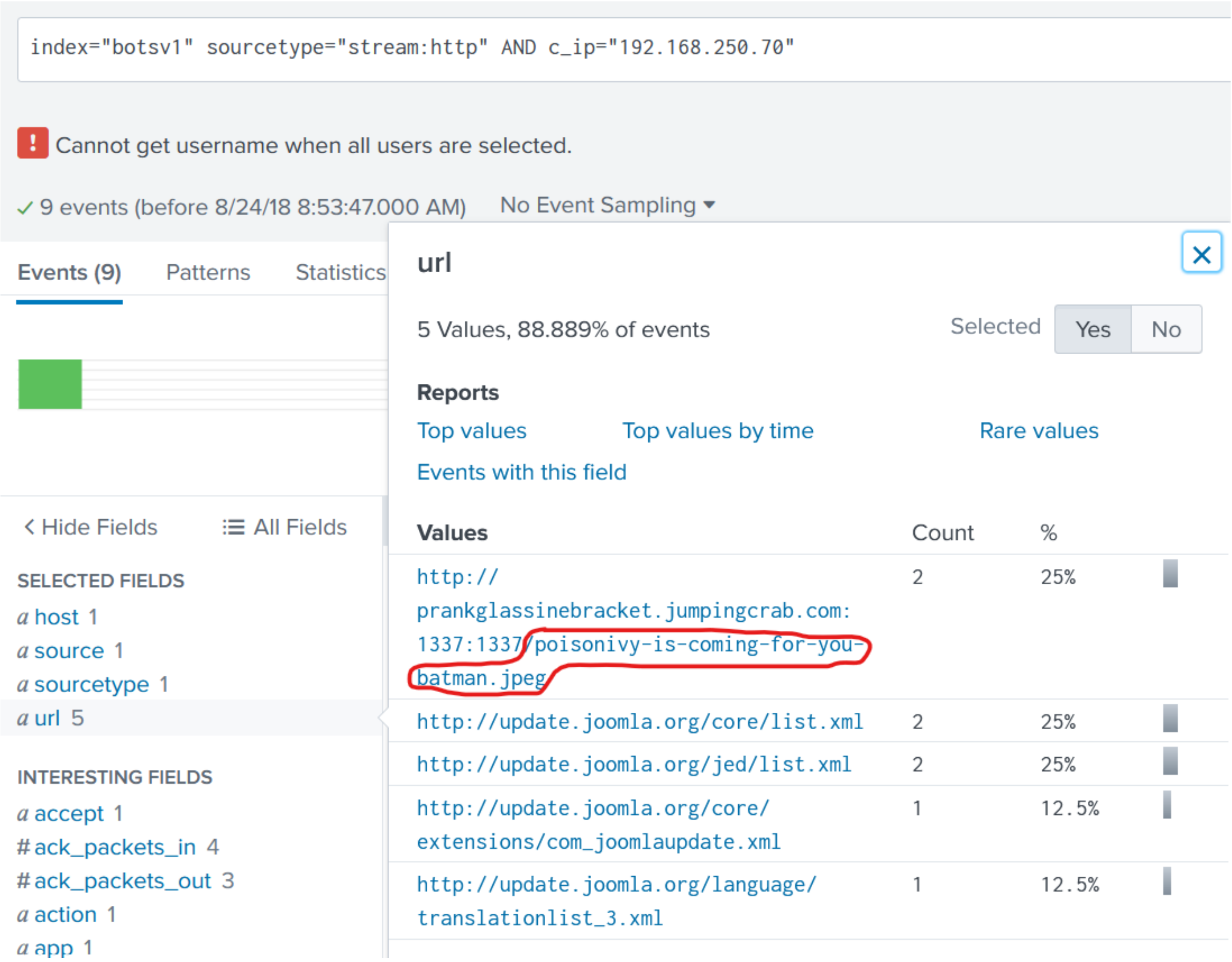
✓ 9 events (before 8/24/18 8:53:47.000 AM) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a accept 1

i	Time	Event
>	8/10/16 3:19:11.351 PM	{"endtime":"2016-08-10T22:19:11.351975Z","timestamp":"2016-08-10T22:19:10.438743Z","ack_packets_in":387,"ack_packets_out":8,"bytes":554174,"bytes_in":106,"bytes_out":554068,"c_ip":"192.168.250.70","cached":0,"capture_hostname":"demo-01","client_rtt":1144,"client_rtt_packets":193,"client_rtt_sum":220865,"cs_version":["1.0","1.0"],"data_center_time":853035,"data_packets_in":2,"data_packets_out":383,"dest_content":"����2\nExif\u0000\u0000MM\u0000*\u0000\u0000\u0000\b\u0000\u0007\u0001\u0012\u0000\u0003\u0000\u0000\u0000\u0001\u0000\u0001\u0000\u0000\u0001\u001A\u0000\u0005\u0000\u0000\u0000\u0001\u0000\u0000\u0000b\u0001\u001B\u0000\u0005\u0000\u0000\u0000\u0001\u0000\u0000\u0000j\u0001(\u0000\u0003\u0000\u0000\u0000\u0001\u0000\u0002\u0000\u0000\u00011\u0000\u0002\u0000\u0000\u0000\u001E\u0000\u0000\u0000r\u00012\u0000\u0002\u0000\u0000\u0000\u0

Go to Interesting Fields > `uri` > move to selected field (i.e. `yes`)


Events (9) Patterns Statistics
< Hide Fields ☰ All Fields
Reports
Top values Top values by time Rare values
Events with this field

```
index="botsv1" sourcetype="stream:http" AND c_ip="192.168.250.70"
```

! Cannot get username when all users are selected.

✓ 9 events (before 8/24/18 8:53:47.000 AM) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
a url 5

INTERESTING FIELDS
a accept 1
# ack_packets_in 4
# ack_packets_out 3
a action 1
a app 1

url

5 Values, 88.889% of events

Selected [✓ Yes] No

Values	Count	%
http://prankglassinebracket.jumpingcrab.com:1337:1337/poisonivy-is-coming-for-you-batman.jpeg	2	25%
http://update.joomla.org/core/list.xml	2	25%
http://update.joomla.org/jed/list.xml	2	25%
http://update.joomla.org/core/extensions/com_joomlaupdate.xml	1	12.5%
http://update.joomla.org/language/translationlist_3.xml	1	12.5%

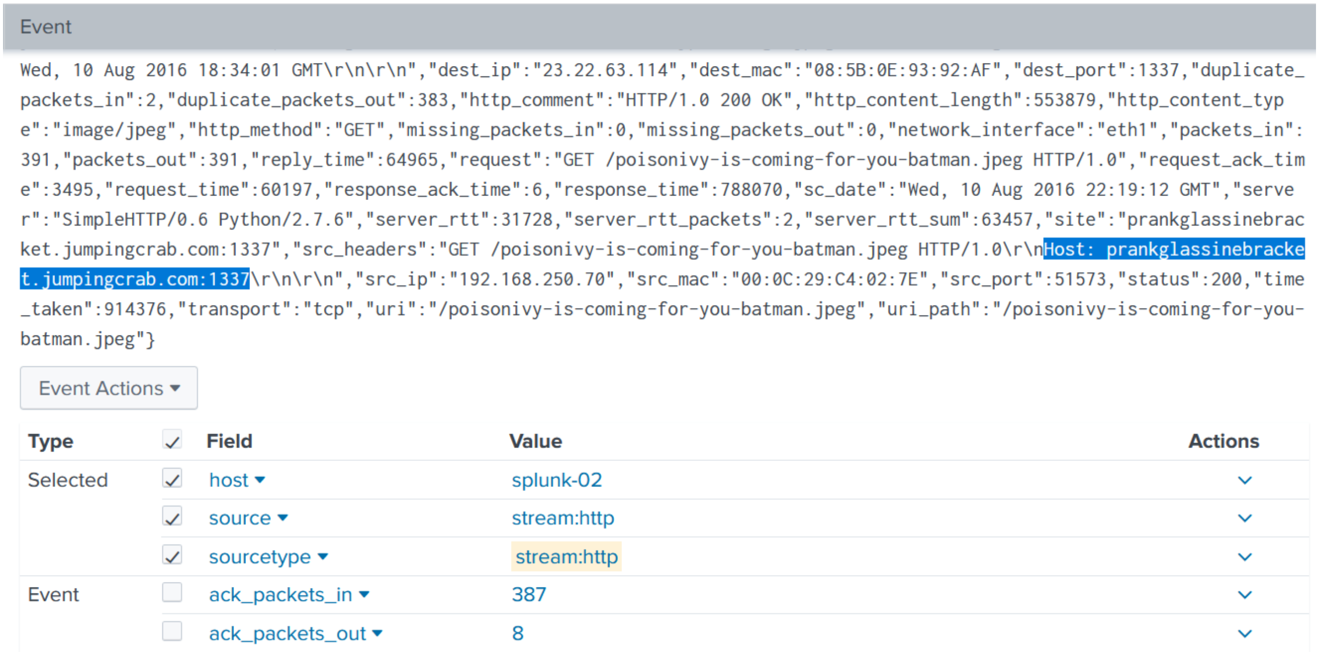
A: `poisonivy-is-coming-for-you-batman.jpeg`

BOTSv1 1.5: Domain Name (10 pts)

Question: What is the fully qualified domain name (FQDN) used by the staging server hosting the defacement file?

> Hints:
>
> - Examine the 9 events from the previous challenge. Look at the **url** values.

SPL: *same as above*



Event

```
Wed, 10 Aug 2016 18:34:01 GMT\r\n\r\n","dest_ip":"23.22.63.114","dest_mac":"08:5B:0E:93:92:AF","dest_port":1337,"duplicate_
packets_in":2,"duplicate_packets_out":383,"http_comment":"HTTP/1.0 200 OK","http_content_length":553879,"http_content_typ
e":"image/jpeg","http_method":"GET","missing_packets_in":0,"missing_packets_out":0,"network_interface":"eth1","packets_in":
391,"packets_out":391,"reply_time":64965,"request":"GET /poisonivy-is-coming-for-you-batman.jpeg HTTP/1.0","request_ack_tim
e":3495,"request_time":60197,"response_ack_time":6,"response_time":788070,"sc_date":"Wed, 10 Aug 2016 22:19:12 GMT","serve
r":"SimpleHTTP/0.6 Python/2.7.6","server_rtt":31728,"server_rtt_packets":2,"server_rtt_sum":63457,"site":"prankglassinebrac
ket.jumpingcrab.com:1337","src_headers":"GET /poisonivy-is-coming-for-you-batman.jpeg HTTP/1.0\r\nHost: prankglassinebracke
t.jumpingcrab.com:1337\r\n\r\n","src_ip":"192.168.250.70","src_mac":"00:0C:29:C4:02:7E","src_port":51573,"status":200,"time
_taken":914376,"transport":"tcp","uri":"/poisonivy-is-coming-for-you-batman.jpeg","uri_path":"/poisonivy-is-coming-for-you-
batman.jpeg"}
```

Type	✓	Field	Value	Actions
Selected	☑	host ▾	splunk-02	⌄
	☑	source ▾	stream:http	⌄
	☑	sourcetype ▾	stream:http	⌄
Event	□	ack_packets_in ▾	387	⌄
	□	ack_packets_out ▾	8	⌄

A: `prankglassinebracket.jumpingcrab.com:1337`

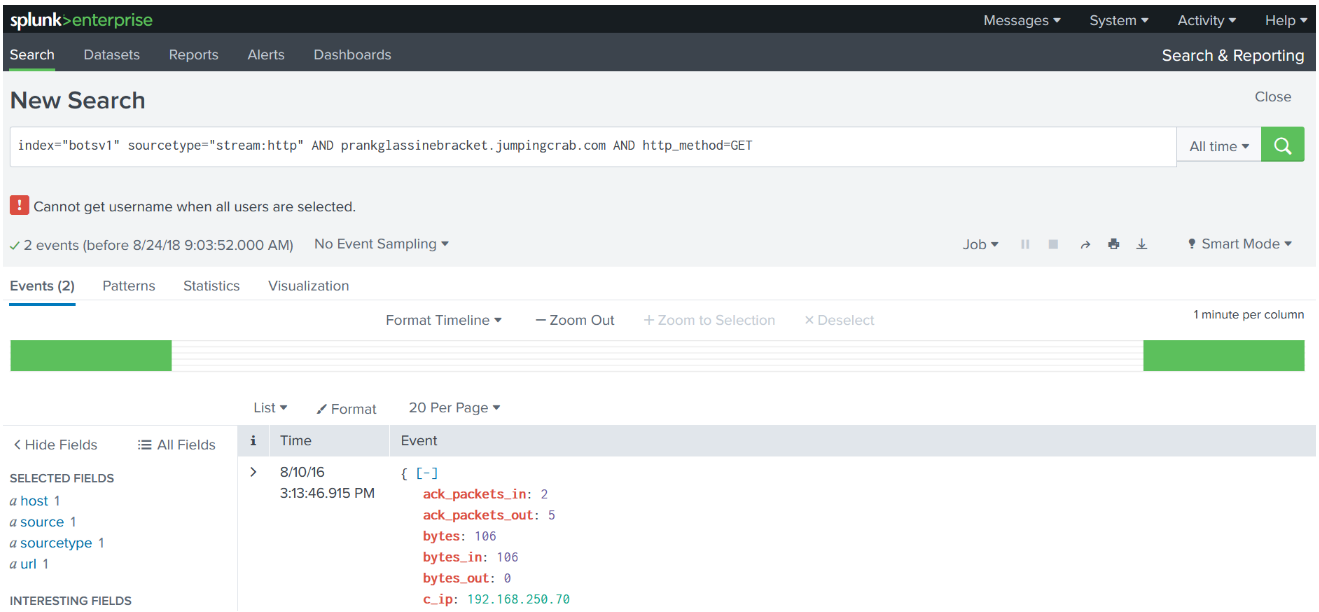
Level 2: Identifying Threat Actors

BOTSv1 2.1: Staging Server IP (10 pts)

Question: What is the IP address of the staging server hosting the defacement file?

> Hints:
>
> - Search for HTTP GET events containing the target FQDN.

SPL: `index="botsv1" sourcetype="stream:http" AND prankglassinebracket.jumpingcrab.com AND http_method=GET`


splunk>enterprise
Messages ▾ System ▾ Activity ▾ Help ▾
Search Datasets Reports Alerts Dashboards
Search & Reporting
New Search
Close
All time ▾
Job ▾
Smart Mode ▾
Events (2) Patterns Statistics Visualization
Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect
1 minute per column
List ▾ Format 20 Per Page ▾
< Hide Fields ☰ All Fields
i Time Event

```
index="botsv1" sourcetype="stream:http" AND prankglassinebracket.jumpingcrab.com AND http_method=GET
```

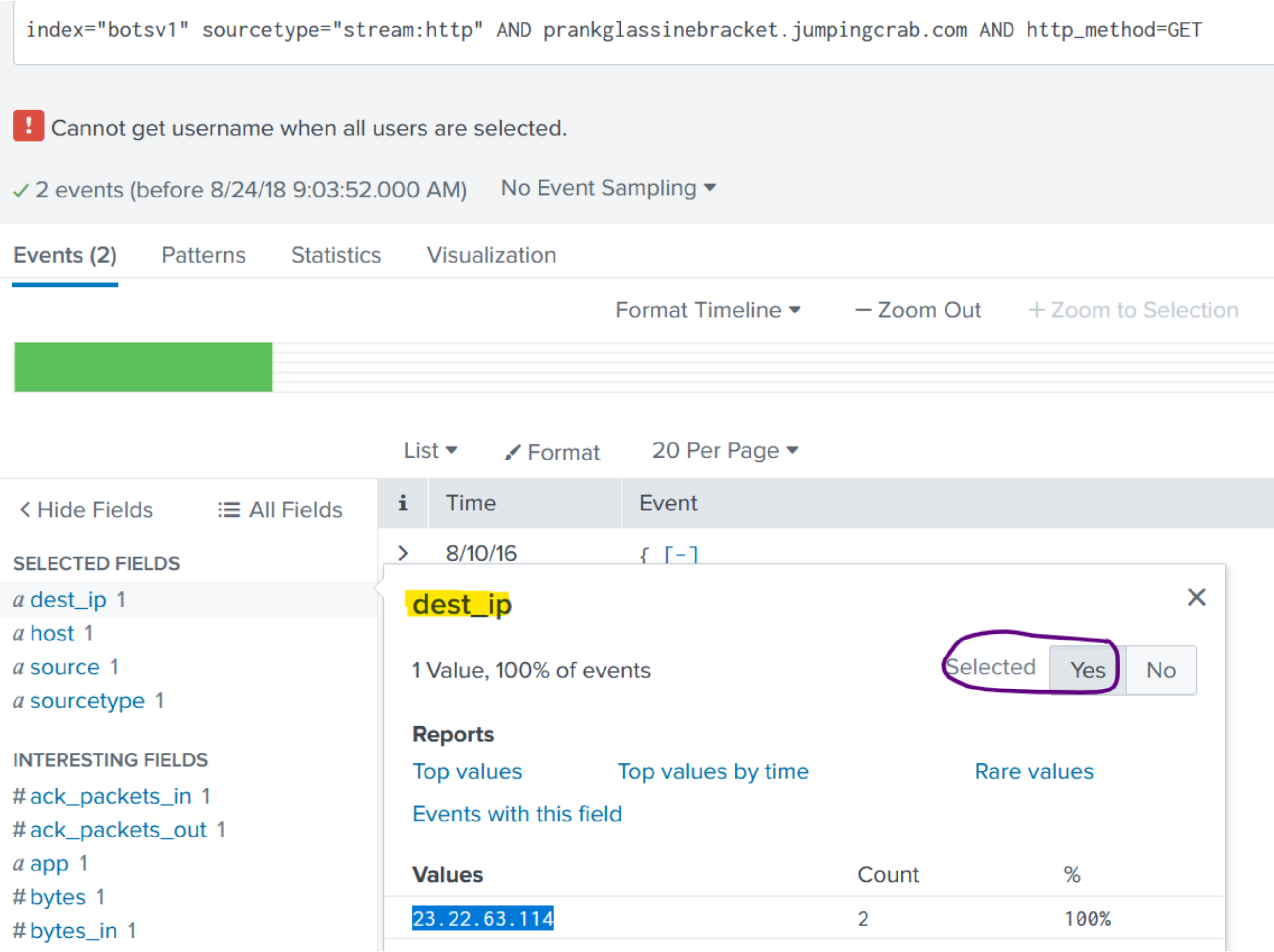
! Cannot get username when all users are selected.

✓ 2 events (before 8/24/18 9:03:52.000 AM) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
a url 1

INTERESTING FIELDS

```
> 8/10/16            { [-]
  3:13:46.915 PM       ack_packets_in: 2
                       ack_packets_out: 5
                       bytes: 106
                       bytes_in: 106
                       bytes_out: 0
                       c_ip: 192.168.250.70
```


Events (2) Patterns Statistics Visualization
Format Timeline ▾ — Zoom Out + Zoom to Selection
List ▾ Format 20 Per Page ▾
< Hide Fields ☰ All Fields
i Time Event
Reports
Top values Top values by time Rare values
Events with this field

```
index="botsv1" sourcetype="stream:http" AND prankglassinebracket.jumpingcrab.com AND http_method=GET
```

! Cannot get username when all users are selected.

✓ 2 events (before 8/24/18 9:03:52.000 AM) No Event Sampling ▾

SELECTED FIELDS
a dest_ip 1
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# ack_packets_in 1
# ack_packets_out 1
a app 1
# bytes 1
# bytes_in 1

> 8/10/16 { [-]

dest_ip ✕

1 Value, 100% of events Selected [✓ Yes] No

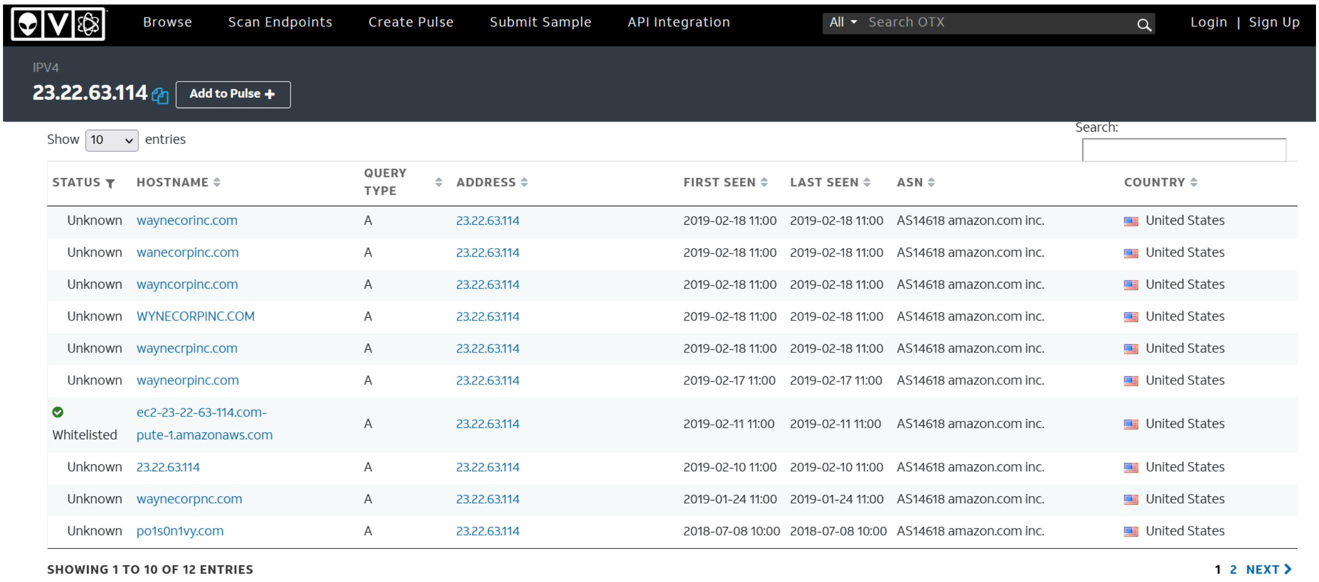
Values	Count	%
23.22.63.114	2	100%

A: `23.22.63.114`

BOTSv1 2.2: Leetspeak Domain (10 pts)

Question: What is the Leetspeak domain found on the staging server? Use a search engine (outside Splunk) to find other domains on the staging server. Search for that IP address. Find a domain with an name in Leetspeak (like "1337sp33k.com").

SPL: *N.A.*



23.22.63.114

STATUS	HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN	ASN	COUNTRY
Unknown	waynecorinc.com	A	23.22.63.114	2019-02-18 11:00	2019-02-18 11:00	AS14618 amazon.com inc.	United States
Unknown	wanecorpinc.com	A	23.22.63.114	2019-02-18 11:00	2019-02-18 11:00	AS14618 amazon.com inc.	United States
Unknown	wayncorpinc.com	A	23.22.63.114	2019-02-18 11:00	2019-02-18 11:00	AS14618 amazon.com inc.	United States
Unknown	WYNECORPINC.COM	A	23.22.63.114	2019-02-18 11:00	2019-02-18 11:00	AS14618 amazon.com inc.	United States
Unknown	waynecrpinc.com	A	23.22.63.114	2019-02-18 11:00	2019-02-18 11:00	AS14618 amazon.com inc.	United States
Unknown	wayneorpinc.com	A	23.22.63.114	2019-02-17 11:00	2019-02-17 11:00	AS14618 amazon.com inc.	United States
✓ Whitelisted	ec2-23-22-63-114.compute-1.amazonaws.com	A	23.22.63.114	2019-02-11 11:00	2019-02-11 11:00	AS14618 amazon.com inc.	United States
Unknown	23.22.63.114	A	23.22.63.114	2019-02-10 11:00	2019-02-10 11:00	AS14618 amazon.com inc.	United States
Unknown	waynecorpnc.com	A	23.22.63.114	2019-01-24 11:00	2019-01-24 11:00	AS14618 amazon.com inc.	United States
Unknown	po1s0n1vy.com	A	23.22.63.114	2018-07-08 10:00	2018-07-08 10:00	AS14618 amazon.com inc.	United States

SHOWING 1 TO 10 OF 12 ENTRIES

A: `po1s0n1vy.com`

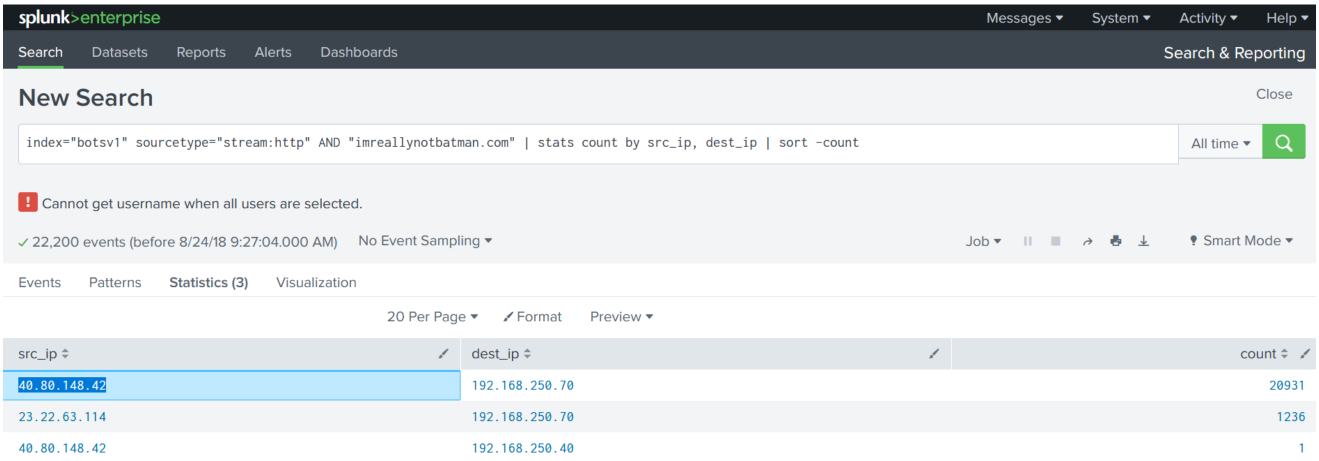
BOTSv1 2.3: Brute Force Attack (15 pts)

Question: What is the IP address performing a brute force attack against "imreallynotbatman.com"?

Initial Try

SPL: `index="botsv1" sourcetype="stream:http" AND "imreallynotbatman.com" | stats count by src_ip, dest_ip | sort -count`

- obtain results counted by source and destination ip by descending count to pinpoint likely attacker address (source) -> may be both 23.22.x.x or 40.80.x.x
- answer limited to target web site



```
index="botsv1" sourcetype="stream:http" AND "imreallynotbatman.com" | stats count by src_ip, dest_ip | sort -count
```

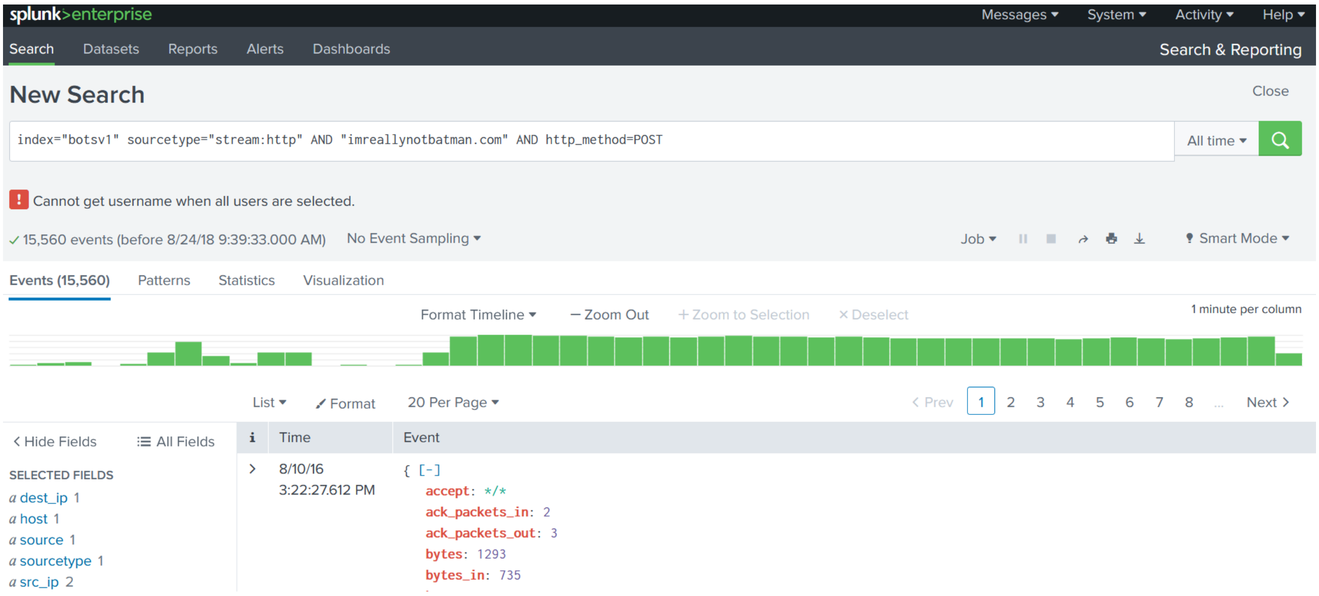
! Cannot get username when all users are selected.

✓ 22,200 events (before 8/24/18 9:27:04.000 AM)

src_ip	dest_ip	count
40.80.148.42	192.168.250.70	20931
23.22.63.114	192.168.250.70	1236
40.80.148.42	192.168.250.40	1

> Hints
>
> - Find the 15,570 HTTP events using the POST method.
> - Exclude the events from the vulnerability scanner.
> - Examine the **form_data** of the remaining 441 events.

> - To make a useful table, add this to your query:
>   `| table _time, form_data`



New Search

```
index="botsv1" sourcetype="stream:http" AND "imreallynotbatman.com" AND http_method=POST
```

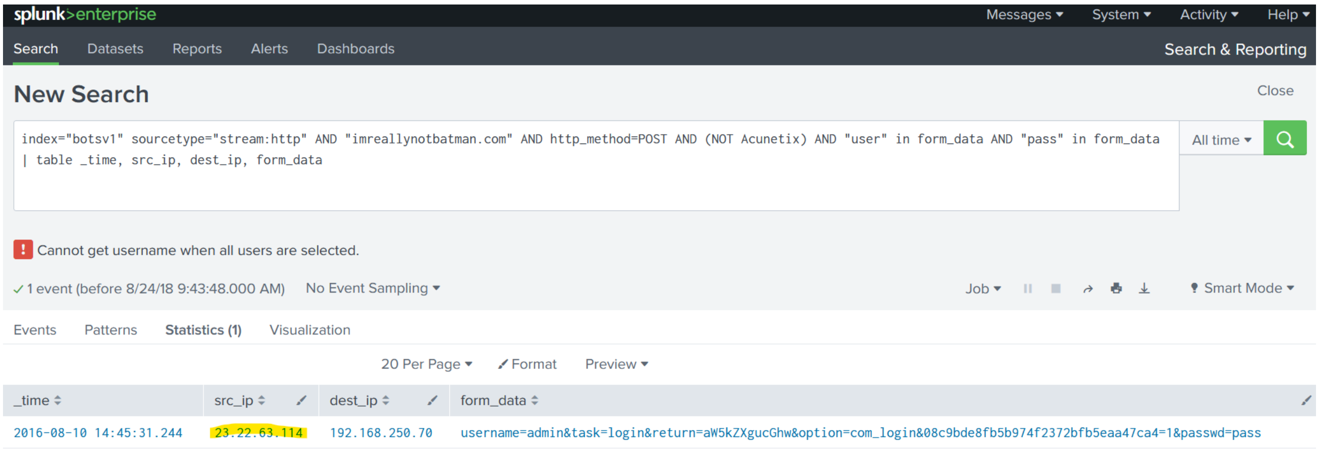
! Cannot get username when all users are selected.

✓ 15,560 events (before 8/24/18 9:39:33.000 AM) No Event Sampling ▾

SELECTED FIELDS
a dest_ip 1
a host 1
a source 1
a sourcetype 1
a src_ip 2

i	Time	Event
›	8/10/16 3:22:27.612 PM	{ [-] accept: */* ack_packets_in: 2 ack_packets_out: 3 bytes: 1293 bytes_in: 735

SPL: `index="botsv1" sourcetype="stream:http" AND "imreallynotbatman.com" AND http_method=POST AND (NOT Acunetix) AND "user" in form_data AND "pass" in form_data | table _time, src_ip, dest_ip, form_data`



New Search

```
index="botsv1" sourcetype="stream:http" AND "imreallynotbatman.com" AND http_method=POST AND (NOT Acunetix) AND "user" in form_data AND "pass" in form_data
| table _time, src_ip, dest_ip, form_data
```

! Cannot get username when all users are selected.

✓ 1 event (before 8/24/18 9:43:48.000 AM) No Event Sampling ▾

_time	src_ip	dest_ip	form_data
2016-08-10 14:45:31.244	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&08c9bde8fb5b974f2372bfb5eaa47ca4=1&passwd=pass

A: `23.22.63.114`

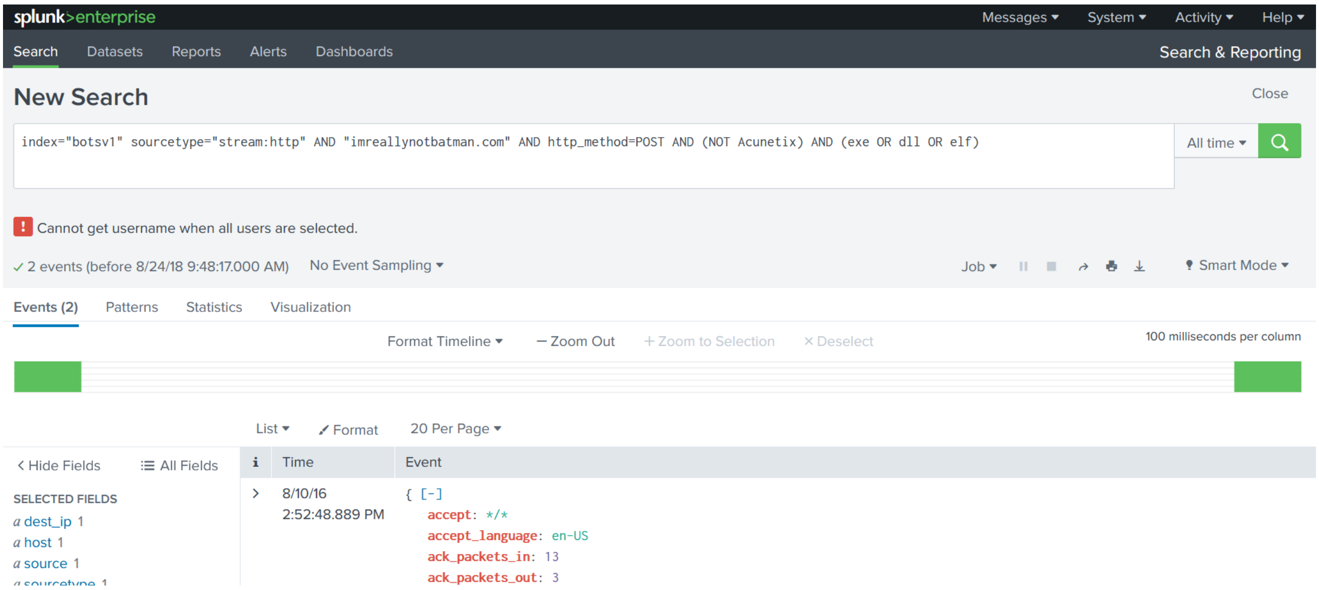
BOTSv1 2.4: Uploaded Executable File Name (15 pts)

Question: What is the name of the executable file the attacker uploaded to the server?

> Hints
>
> - Find the 15,570 HTTP events using the POST method.
> - Exclude the events from the vulnerability scanner.
> - Search for common Windows executable filename extensions.

SPL: `index="botsv1" sourcetype="stream:http" AND "imreallynotbatman.com" AND http_method=POST AND (NOT Acunetix) AND (exe OR dll OR elf)`

- search on the most common executable formats



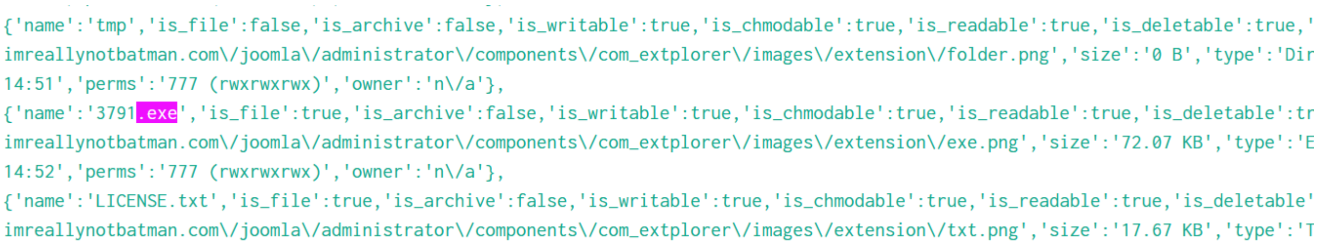
```
index="botsv1" sourcetype="stream:http" AND "imreallynotbatman.com" AND http_method=POST AND (NOT Acunetix) AND (exe OR dll OR elf)
```

Cannot get username when all users are selected.

✓ 2 events (before 8/24/18 9:48:17.000 AM) No Event Sampling ▾

```
8/10/16
2:52:48.889 PM   { [-]
                   accept: */*
                   accept_language: en-US
                   ack_packets_in: 13
                   ack_packets_out: 3
```

Next we can do a `Ctrl-F` for `.exe`, `.dll` and `.elf`. The first yields `3791.exe`, while the latter two yield no results.



```
{'name':'tmp','is_file':false,'is_archive':false,'is_writable':true,'is_chmodable':true,'is_readable':true,'is_deletable':true,'
imreallynotbatman.com\/joomla\/administrator\/components\/com_extplorer\/images\/extension\/folder.png','size':'0 B','type':'Dir
14:51','perms':'777 (rwxrwxrwx)','owner':'n\/a'},
{'name':'3791.exe','is_file':true,'is_archive':false,'is_writable':true,'is_chmodable':true,'is_readable':true,'is_deletable':tr
imreallynotbatman.com\/joomla\/administrator\/components\/com_extplorer\/images\/extension\/exe.png','size':'72.07 KB','type':'E
14:52','perms':'777 (rwxrwxrwx)','owner':'n\/a'},
{'name':'LICENSE.txt','is_file':true,'is_archive':false,'is_writable':true,'is_chmodable':true,'is_readable':true,'is_deletable'
imreallynotbatman.com\/joomla\/administrator\/components\/com_extplorer\/images\/extension\/txt.png','size':'17.67 KB','type':'T
```

A: `3791.exe`

Level 3: Using Sysmon and Stream

BOTSv1 3.1: MD5 (10 pts)

Question: What is the MD5 hash of the uploaded executable file?

SPL: ``

A:

BOTSv1 3.2: Brute Force (10 pts)

Question: What was the first brute force password used?

SPL: ``

A:

BOTSv1 3.3: Correct Password (10 pts)

Question: What was the correct password found in the brute force attack?

SPL: ``

A:

BOTSv1 3.4: Time Interval (10 pts)

Question: How many seconds elapsed between the time the brute force password scan identified the correct password and the compromised login? Round to 2 decimal places.

SPL: ``

A:

BOTSv1 3.5: Number of Passwords (10 pts)

Question: How many unique passwords were attempted in the brute force attack?

SPL: ``

A:

Level 4: Analyzing a Ransomware Attack

BOTSv1 4.1: IP Address (5 pts)

Question: What was the most likely IP address of we8105desk on 24AUG2016?

SPL: ``

A:

BOTSv1 4.2: Signature ID (5 pts)

Question: Amongst the Suricata signatures that detected the Cerber malware, which one alerted the fewest number of times? Submit ONLY the signature ID value as the answer. (No punctuation, just 7 integers.)

SPL: ``

A:

BOTSv1 4.3: FQDN (15 pts)

Question: What fully qualified domain name (FQDN) does the Cerber ransomware attempt to direct the user to at the end of its encryption phase?

SPL: ``

A:

BOTSv1 4.4: Suspicious Domain (15 pts)

Question: What was the first suspicious domain visited by we8105desk on 24AUG2016?

SPL: ``

A:

BOTSv1 4.5: VB Script (15 pts)

Question: During the initial Cerber infection, a VB script is run. What is the name of the first function defined in the VB script?

SPL: ``

A:

BOTSv1 4.6: Field Length (15 pts)

Question: During the initial Cerber infection, a VB script is run. What is the length in characters of the value of the field containing the VB script?

SPL: ``

A:

BOTSv1 4.7: USB key (15 pts)

Question: What is the name of the USB key inserted by Bob Smith?

SPL: ``

A:

BOTSv1 4.8: Server Name (5 pts)

Question: Bob Smith's workstation (we8105desk) was connected to a file server during the ransomware outbreak. What is the domain name of the file server?

SPL: ``

A:

BOTSv1 4.9: IP Address (15 pts)

Question: Bob Smith's workstation (we8105desk) was connected to a file server during the ransomware outbreak. What is the IP address of the file server?

SPL: ``

A:

BOTSv1 4.10: PDFs (20 pts)

Question: How many distinct PDFs did the ransomware encrypt on the remote file server?

SPL: ``

A:

BOTSv1 4.11: Process ID (15 pts)

Question: The VBscript found above launches 121214.tmp. What is the ParentProcessId of this initial launch?

SPL: ``

A:

BOTSv1 4.12: Text Files (15 pts)

Question: The Cerber ransomware encrypts files located in Bob Smith's Windows profile. How many .txt files does it encrypt?

SPL: ``

A:

BOTSv1 4.13: File Name (15 pts)

Question: The malware downloads a file that contains the Cerber ransomware cryptor code. What is the name of that file?

SPL: ``

A:

BOTSv1 4.14: Obfuscation (10 pts)

Question: Now that you know the name of the ransomware's encryptor file, what obfuscation technique does it likely use?

SPL: ``

A: