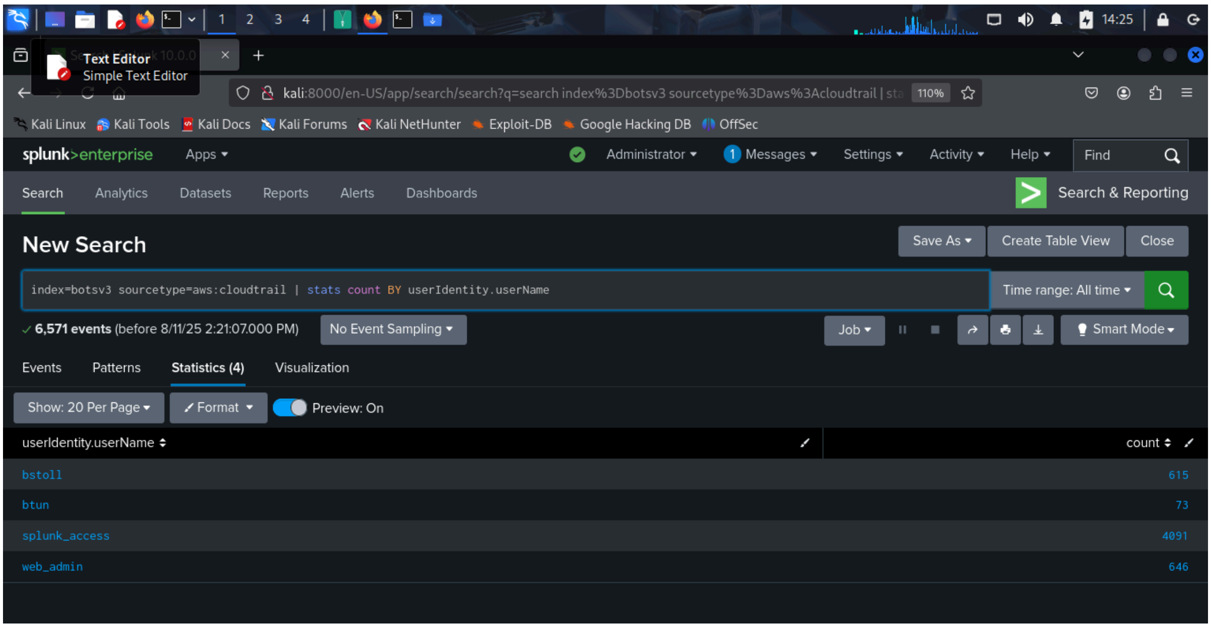
QUESTION 1: List out the IAM users that accessed an AWS service (successfully or unsuccessfully) in Frothly's AWS environment.

ANSWER:

1. splunk_access
2. web_admin
3. bstoll
4. btun



```
index=botsv3 sourcetype=aws:cloudtrail | stats count BY userIdentity.userName
```

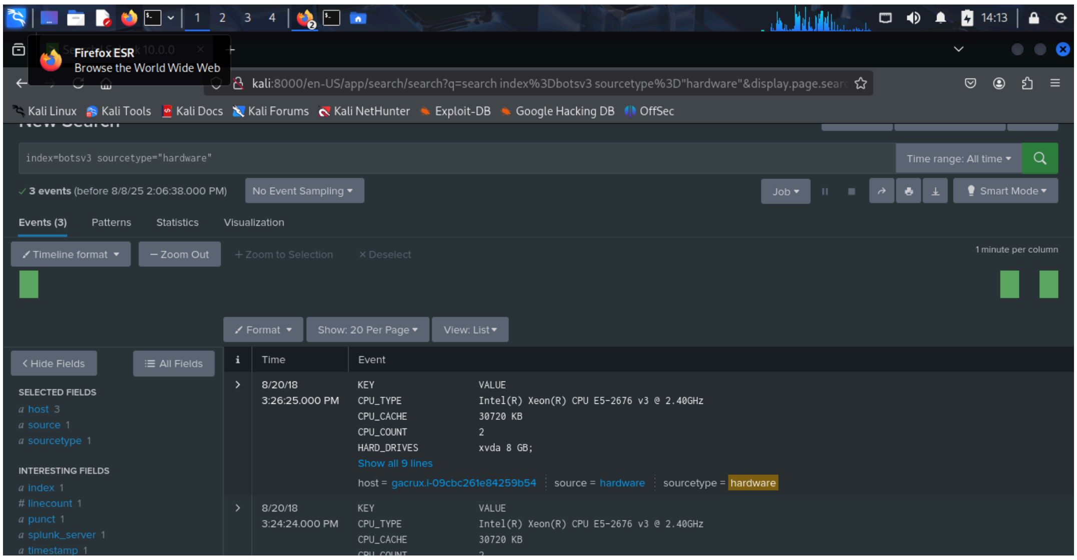
✓ 6,571 events (before 8/11/25 2:21:07.000 PM)

userIdentity.userName	count
bstoll	615
btun	73
splunk_access	4091
web_admin	646

QUESTION 2:
What is the processor number used on the web servers?

ANSWER:

E5-2676 v3



```
index=botsv3 sourcetype="hardware"
```

✓ 3 events (before 8/8/25 2:06:38.000 PM)

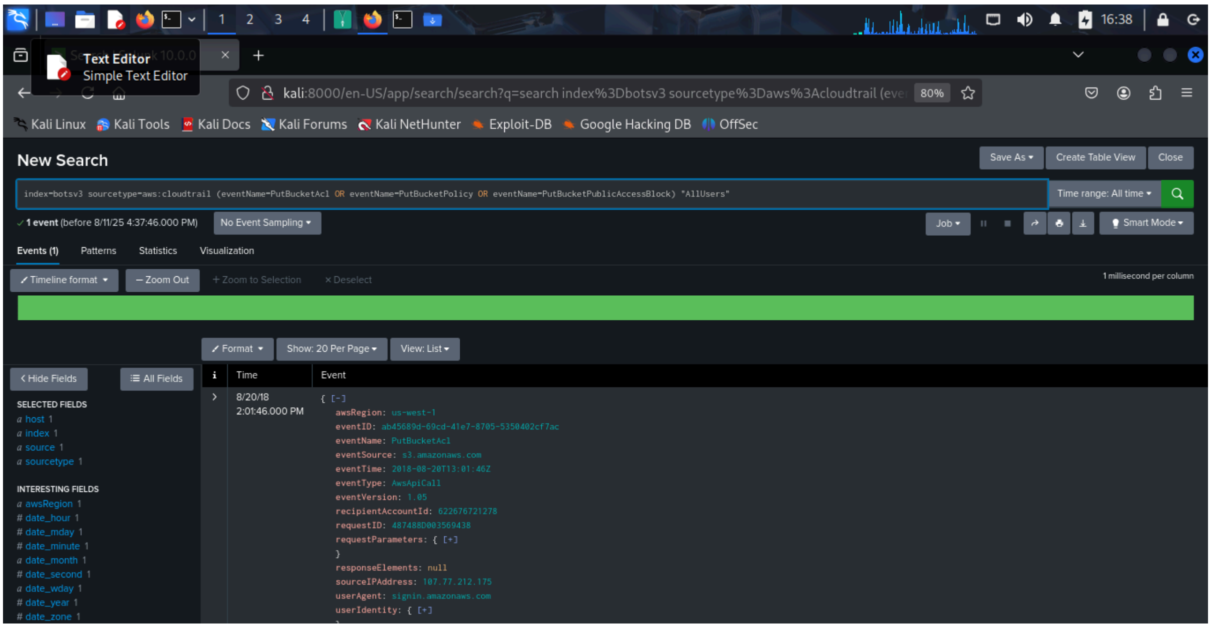
```
Time                    Event
8/20/18                 KEY              VALUE
3:26:25.000 PM          CPU_TYPE         Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz
                        CPU_CACHE        30720 KB
                        CPU_COUNT        2
                        HARD_DRIVES      xvda 8 GB;
                        Show all 9 lines
                        host = gacrux.i-09cbc261e84259b54   source = hardware   sourcetype = hardware
8/20/18                 KEY              VALUE
3:24:24.000 PM          CPU_TYPE         Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz
                        CPU_CACHE        30720 KB
                        CPU_COUNT        2
```

QUESTION 3:

Bud accidentally makes an S3 bucket publicly accessible. What is the event ID of the API call that enabled public access?

ANSWER:

Event ID: ab45689d-69cd-41e7-8705-5350402cf7ac



```
index=botsv3 sourcetype=aws:cloudtrail (eventName=PutBucketAcl OR eventName=PutBucketPolicy OR eventName=PutBucketPublicAccessBlock) "AllUsers"
```

✓ 1 event (before 8/11/25 4:37:46.000 PM)

Time	Event
8/20/18 2:01:46.000 PM	see below

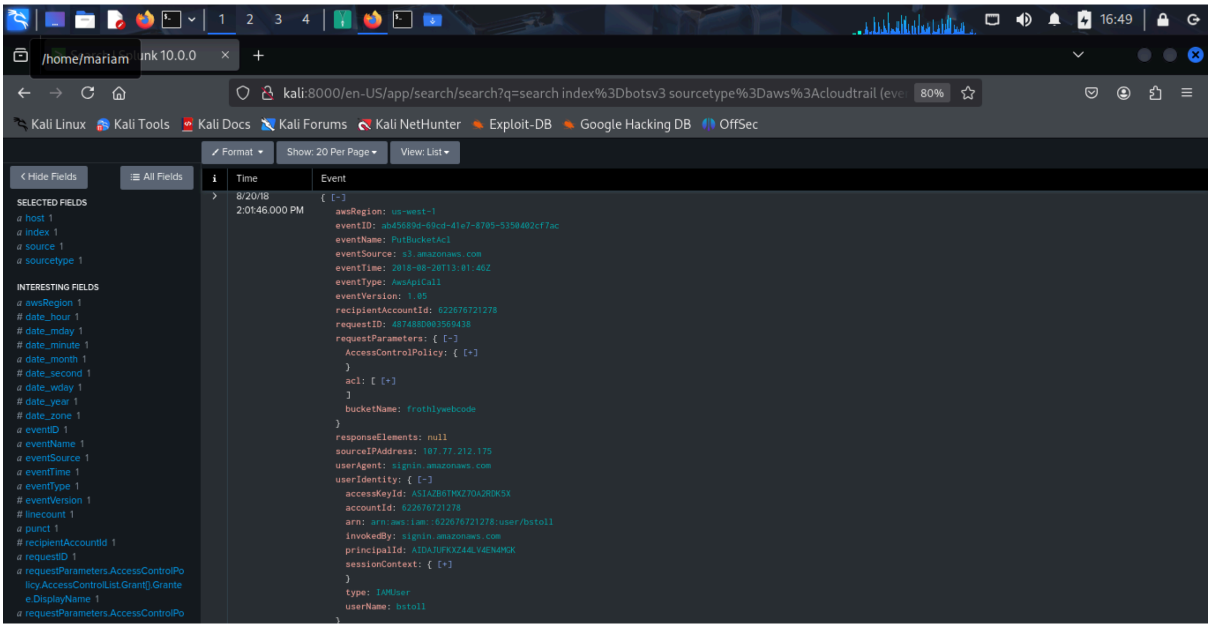
```
{ [-]
  awsRegion: us-west-1
  eventID: ab45689d-69cd-41e7-8705-5350402cf7ac
  eventName: PutBucketAcl
  eventSource: s3.amazonaws.com
  eventTime: 2018-08-20T13:01:46Z
  eventType: AwsApiCall
  eventVersion: 1.05
  recipientAccountId: 622676721278
  requestID: 487488D003569438
  requestParameters: { [+]
  }
  responseElements: null
  sourceIPAddress: 107.77.212.175
  userAgent: signin.amazonaws.com
  userIdentity: { [+]
```

QUESTION 4:

What is the name of the S3 bucket that was made publicly accessible?

ANSWER:

Bucket name: frothlywebcode



Time	Event
8/20/18 2:01:46.000 PM	see below

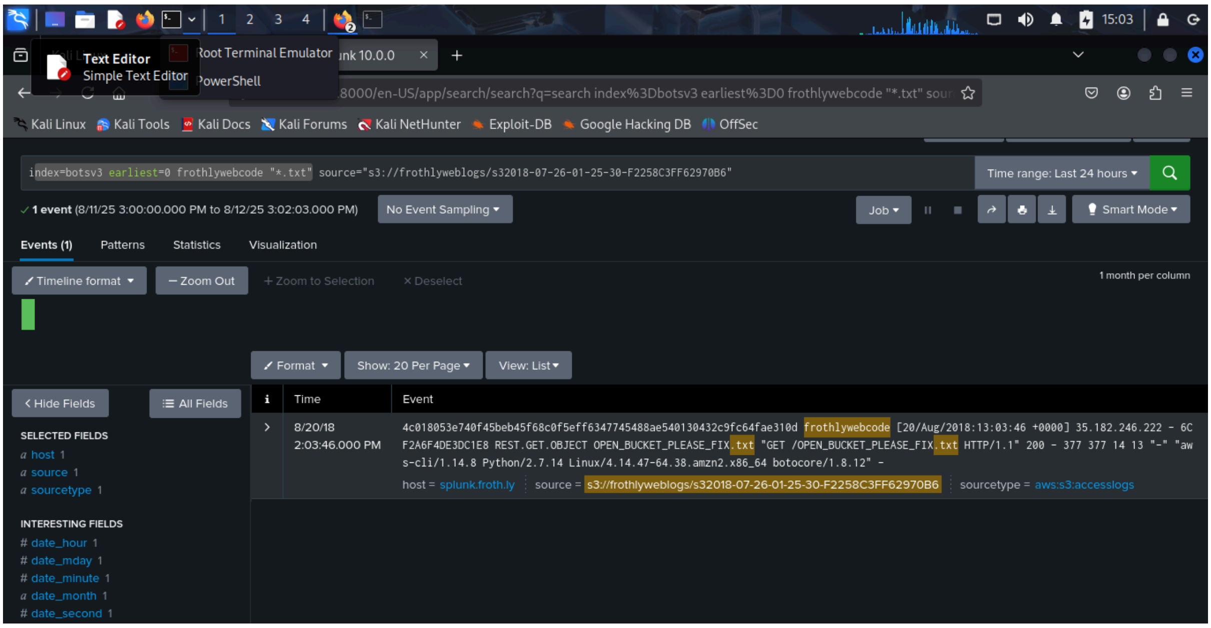
```
{ [-]
  awsRegion: us-west-1
  eventID: ab45689d-69cd-41e7-8705-5350402cf7ac
  eventName: PutBucketAcl
  eventSource: s3.amazonaws.com
  eventTime: 2018-08-20T13:01:46Z
  eventType: AwsApiCall
  eventVersion: 1.05
  recipientAccountId: 622676721278
  requestID: 487488D003569438
  requestParameters: { [-]
    AccessControlPolicy: { [+]
    }
    acl: [ [+]
    ]
    bucketName: frothlywebcode
  }
  responseElements: null
  sourceIPAddress: 107.77.212.175
  userAgent: signin.amazonaws.com
  userIdentity: { [-]
    accessKeyId: ASIAZB6TMXZ7OA2RDK5X
    accountId: 622676721278
    arn: arn:aws:iam::622676721278:user/bstoll
    invokedBy: signin.amazonaws.com
    principalId: AIDAJUFKXZ44LV4EN4MGK
    sessionContext: { [+]
    }
    type: IAMUser
    userName: bstoll
  }
```

QUESTION 5:

What is the name of the text file that was successfully uploaded into the S3 bucket while it was publicly accessible?

ANSWER:

OPEN_BUCKET_PLEASE_FIX.txt



```
index=botsv3 earliest=0 frothlywebcode "*.txt" source="s3://frothlyweblogs/s32018-07-26-01-25-30-F2258C3FF62970B6"
```

✓ 1 event (8/11/25 3:00:00.000 PM to 8/12/25 3:02:03.000 PM)

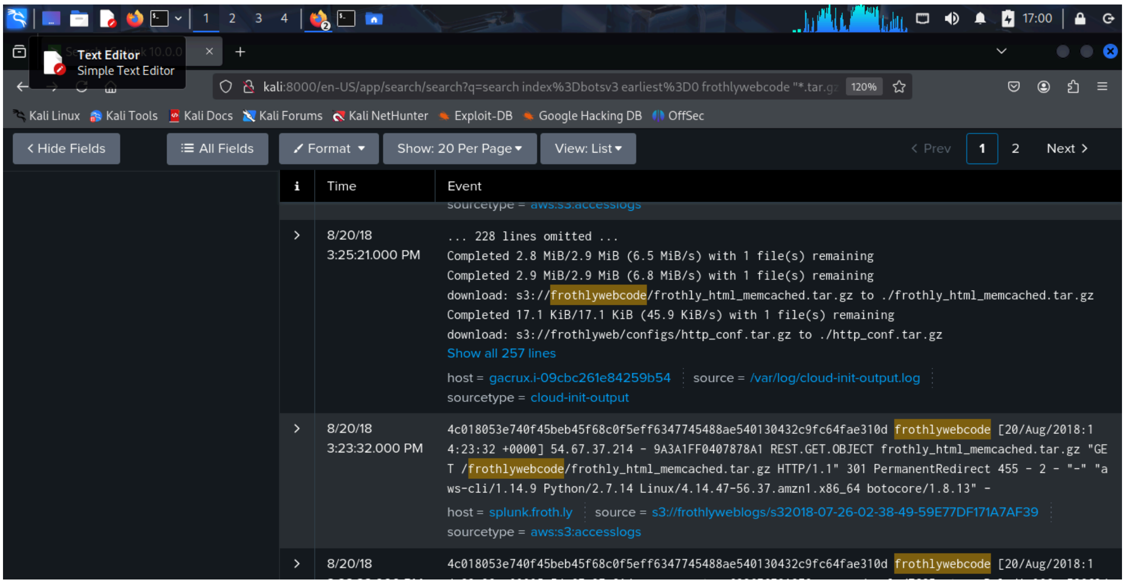
Time	Event
8/20/18 2:03:46.000 PM	4c018053e740f45beb45f68c0f5eff6347745488ae540130432c9fc64fae310d frothlywebcode [20/Aug/2018:13:03:46 +0000] 35.182.246.222 - 6CF2A6F4DE3DC1E8 REST.GET.OBJECT OPEN_BUCKET_PLEASE_FIX.txt "GET /OPEN_BUCKET_PLEASE_FIX.txt HTTP/1.1" 200 - 377 377 14 13 "-" "aws-cli/1.14.8 Python/2.7.14 Linux/4.14.47-64.38.amzn2.x86_64 botocore/1.8.12" - host = splunk.froth.ly source = s3://frothlyweblogs/s32018-07-26-01-25-30-F2258C3FF62970B6 sourcetype = aws:s3:accesslogs

QUESTION 6:

What is the size (in mb) of the .tar.gz file that was successfully uploaded into the S3 bucket while it was publicly accessible? Answer guidance: Round to two decimal places.

ANSWER:

Size: 2.9MB



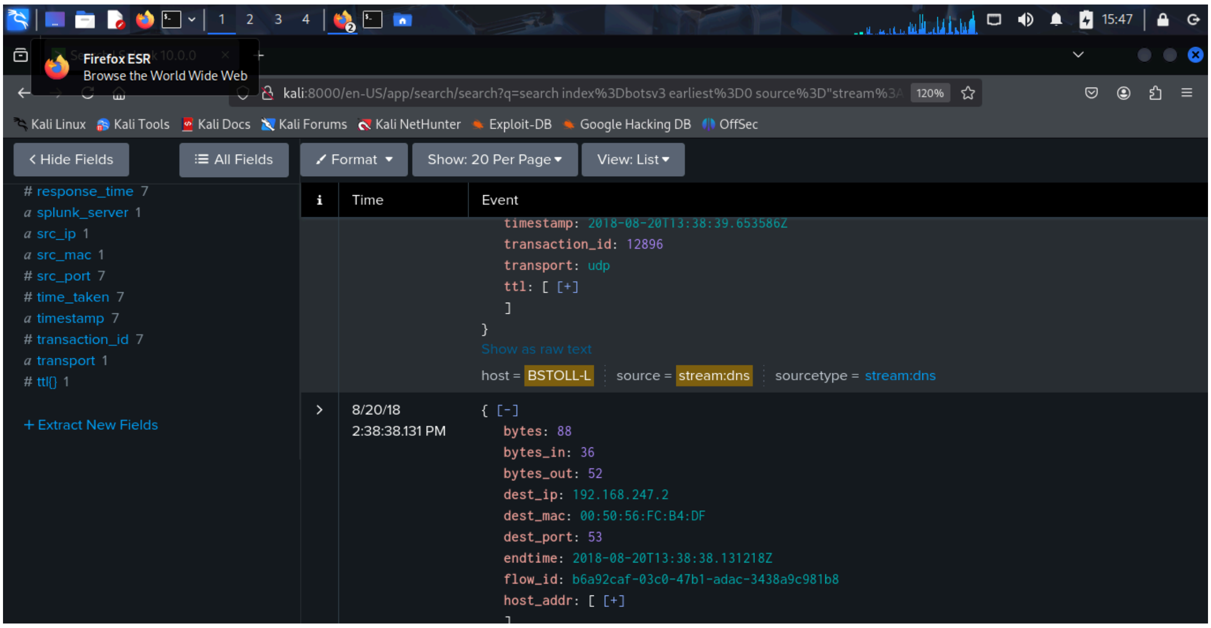
Time	Event
8/20/18 3:25:21.000 PM	... 228 lines omitted ... Completed 2.8 MiB/2.9 MiB (6.5 MiB/s) with 1 file(s) remaining Completed 2.9 MiB/2.9 MiB (6.8 MiB/s) with 1 file(s) remaining download: s3://frothlywebcode/frothly_html_memcached.tar.gz to ./frothly_html_memcached.tar.gz Completed 17.1 KiB/17.1 KiB (45.9 KiB/s) with 1 file(s) remaining download: s3://frothlyweb/configs/http_conf.tar.gz to ./http_conf.tar.gz Show all 257 lines host = gacrux.i-09cbc261e84259b54 source = /var/log/cloud-init-output.log sourcetype = cloud-init-output

8/20/18 3:23:32.000 PM	4c018053e740f45beb45f68c0f5eff6347745488ae540130432c9fc64fae310d frothlywebcode [20/Aug/2018:14:23:32 +0000] 54.67.37.214 - 9A3A1FF0407878A1 REST.GET.OBJECT frothly_html_memcached.tar.gz "GET /frothlywebcode/frothly_html_memcached.tar.gz HTTP/1.1" 301 PermanentRedirect 455 - 2 - "-" "aws-cli/1.14.9 Python/2.7.14 Linux/4.14.47-56.37.amzn1.x86_64 botocore/1.8.13" -
	host = splunk.froth.ly source = s3://frothlyweblogs/s32018-07-26-02-38-49-59E77DF171A7AF39
	sourcetype = aws:s3:accesslogs

8/20/18	4c018053e740f45beb45f68c0f5eff6347745488ae540130432c9fc64fae310d frothlywebcode [20/Aug/2018:1

QUESTION 7:
What is the short hostname of the only Frothly endpoint to actually mine Monero cryptocurrency?

ANSWER:
BSTOLL-L



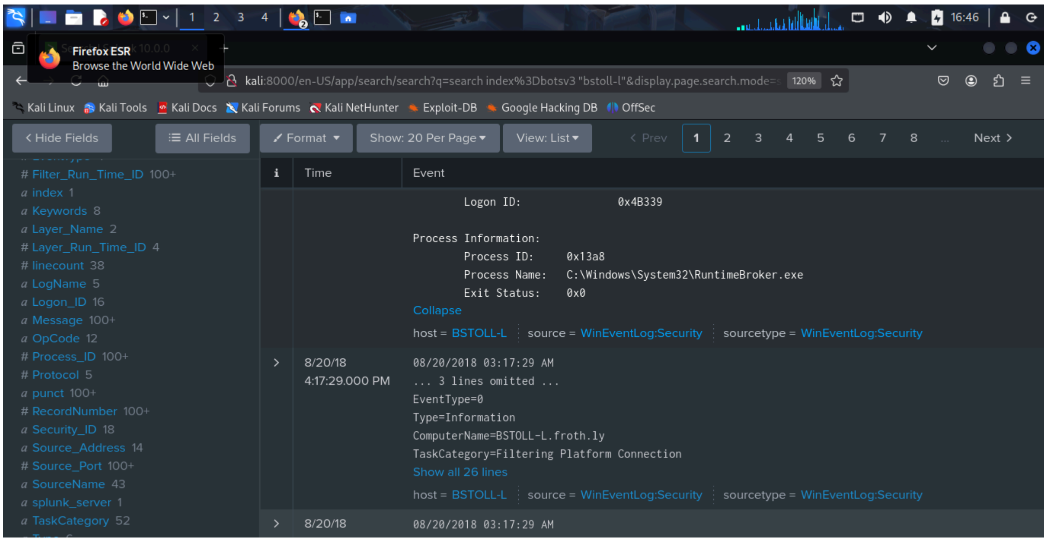
kali:8000/en-US/app/search/search?q=search index%3Dbotsv3 earliest%3D0 source%3D"stream%3A

```
# response_time 7
a splunk_server 1
a src_ip 1
a src_mac 1
# src_port 7
# time_taken 7
a timestamp 7
# transaction_id 7
a transport 1
# ttl{} 1
```

i	Time	Event
		timestamp: 2018-08-20T13:38:39.653586Z transaction_id: 12896 transport: udp ttl: [[+]] } Show as raw text host = BSTOLL-L source = stream:dns sourcetype = stream:dns
>	8/20/18 2:38:38.131 PM	{ [-] bytes: 88 bytes_in: 36 bytes_out: 52 dest_ip: 192.168.247.2 dest_mac: 00:50:56:FC:B4:DF dest_port: 53 endtime: 2018-08-20T13:38:38.131218Z flow_id: b6a92caf-03c0-47b1-adac-3438a9c981b8 host_addr: [[+]]

QUESTION 8
What is the FQDN of the endpoint that is running different windows operating system edition than the others?

ANSWER:
BSTOLL-L.froth.ly



kali:8000/en-US/app/search/search?q=search index%3Dbotsv3 "bstoll-l"&display.page.search.mode=s

```
# Filter_Run_Time_ID 100+
a index 1
a Keywords 8
a Layer_Name 2
# Layer_Run_Time_ID 4
# linecount 38
a LogName 5
a Logon_ID 16
a Message 100+
a OpCode 12
# Process_ID 100+
# Protocol 5
a punct 100+
# RecordNumber 100+
a Security_ID 18
a Source_Address 14
# Source_Port 100+
a SourceName 43
a splunk_server 1
a TaskCategory 52
```

i	Time	Event
		Logon ID: 0x4B339 Process Information: Process ID: 0x13a8 Process Name: C:\Windows\System32\RuntimeBroker.exe Exit Status: 0x0 Collapse host = BSTOLL-L source = WinEventLog:Security sourcetype = WinEventLog:Security

>	8/20/18
	4:17:29.000 PM
		08/20/2018 03:17:29 AM
		... 3 lines omitted ...
		EventType=0
		Type=Information
		ComputerName=BSTOLL-L.froth.ly
		TaskCategory=Filtering Platform Connection
		Show all 26 lines
		host = BSTOLL-L source = WinEventLog:Security sourcetype = WinEventLog:Security

>	8/20/18	08/20/2018 03:17:29 AM