14.1 Diving into an APT investigation

**Sprint 14** Incident Investigation

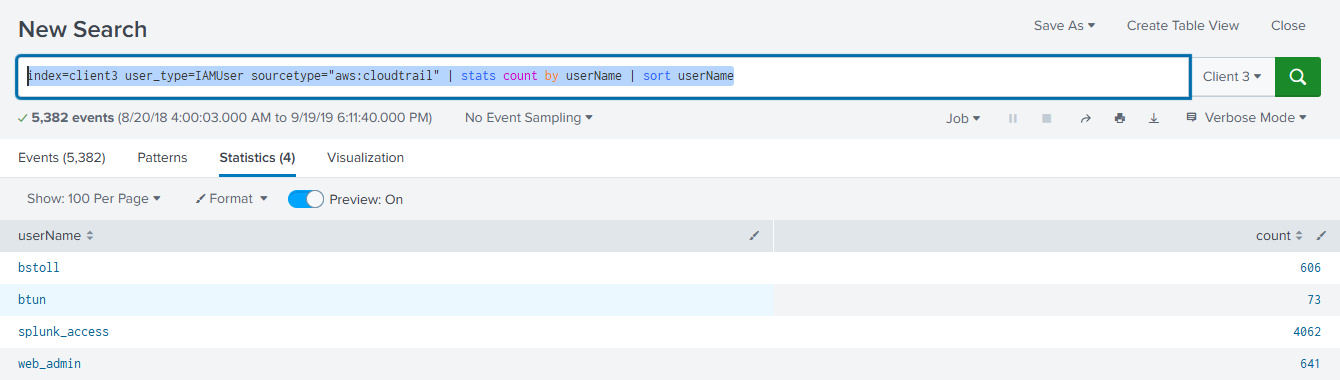
← Use the **Document tabs** to locate the notes for each task in this investigation.

14.1.1 IAM users who accessed AWS

14.1.1 Listing the IAM users who accessed an AWS service

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/0b1d7c5e-4f73-4fa3-baab-cda7cdffa453)**.** Use this worksheet to keep notes as you complete it. |
| --- |

index=client3 user\_type=IAMUser sourcetype="aws:cloudtrail" | stats count by userName | sort userName



Question

Which IAM users accessed an AWS service in Frothly’s AWS environment?

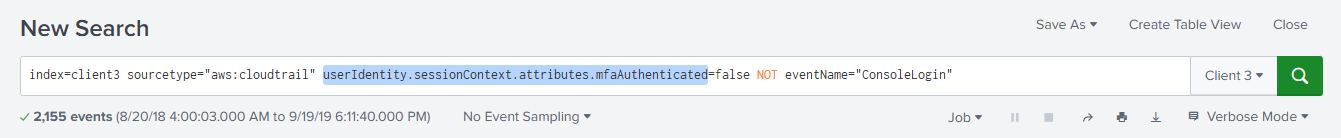
* We don’t care whether that access was successful or unsuccessful — we just want to know *anybody who tried to access resources*.
* For your answer, list all the users in alphabetical order, separated by commas (*e.g.,* adent,fprefect,rdent,zbeeblebrox).

bstoll,btun,splunk\_access,web\_admin

14.1.2 AWS API brute force

14.1.2 Detecting an AWS API brute force

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/0e6200fe-dd54-4b6b-8d3a-15701c46dbe7)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index=client3 sourcetype="aws:cloudtrail" userIdentity.sessionContext.attributes.mfaAuthenticated=false NOT eventName="ConsoleLogin"

Question

What field should we use to determine that AWS API activity have occurred without MFA?

Provide the full JSON path (*e.g.,* tripleten.cyberSecurity.sprintFourteen).

userIdentity.sessionContext.attributes.mfaAuthenticated

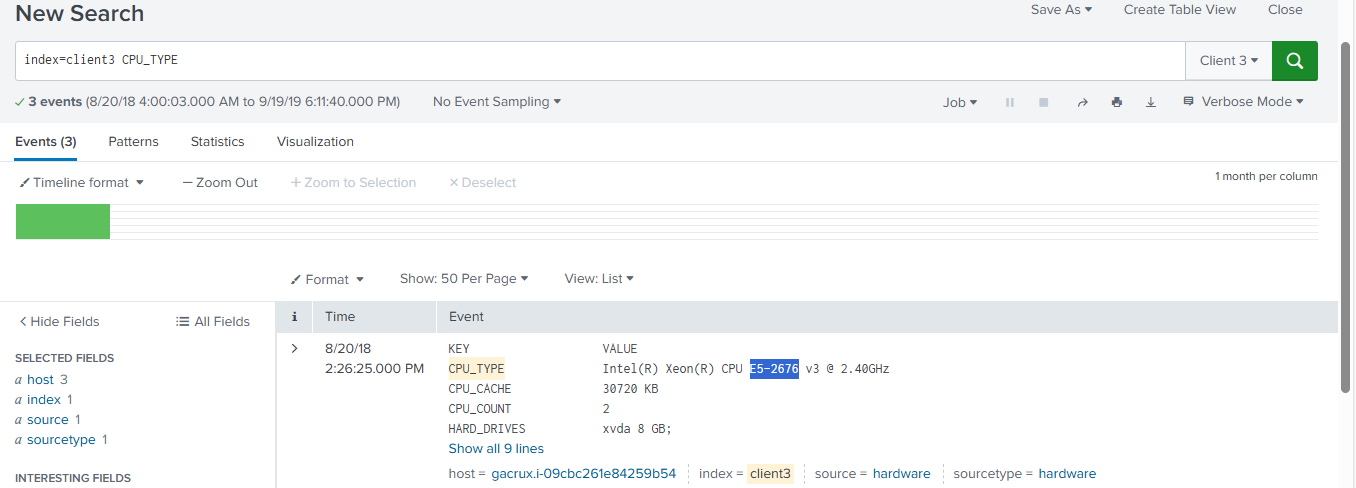
14.1.3 Processor number of web server

14.1.3 Locating the processor number used on the web server

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/146abf44-57ed-483c-be66-864a81b87998)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/20/18

2:26:25.000 PM



index=client3 CPU\_TYPE

Question

What is the processor number used on the web servers?

*Include any special characters. For instance, the correct processor number for* Intel Core i9-12900K *is* i9-12900K*.*

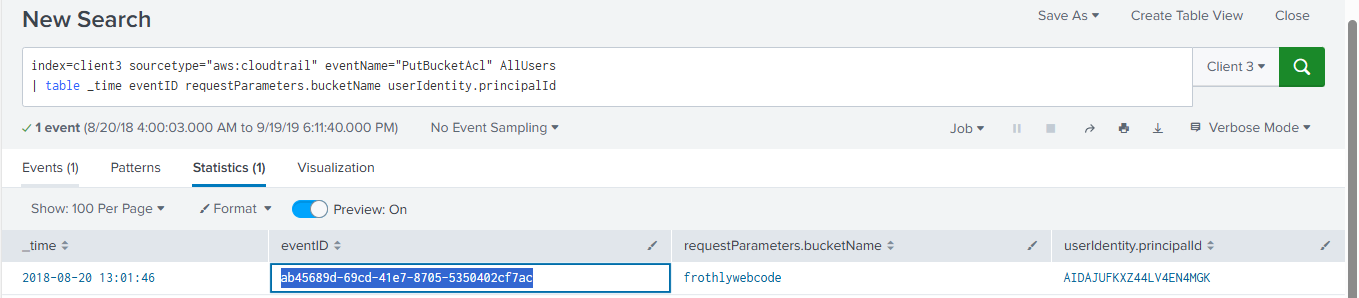
E5-2676

14.1.4 Bud's S3 bucket

14.1.4 Identifying the publicly accessible S3 bucket created by Bud

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/8be256a8-8dc8-4485-a508-bb27cd7d044d)**.** Use this worksheet to keep notes as you complete it. |
| --- |

2018-08-20 13:01:46



index=client3 sourcetype="aws:cloudtrail" eventName="PutBucketAcl" AllUsers

| table \_time eventID requestParameters.bucketName userIdentity.principalId

Question

Bud has accidentally made an S3 bucket publicly accessible.

There is a particular Event ID associated with the API call that enabled that public access.

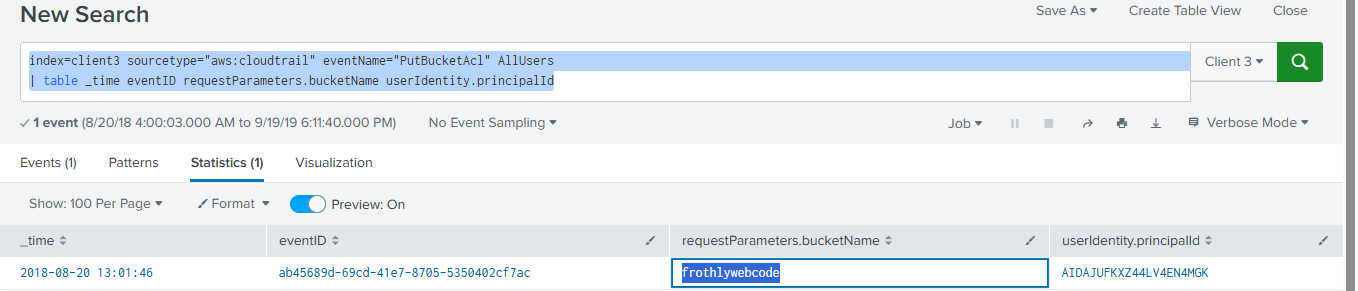
What is that associated Event ID?

ab45689d-69cd-41e7-8705-5350402cf7ac

14.1.5 Public S3 bucket name

14.1.5 Finding the name of the publicly accessible S3 bucket

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/585a9b83-cb5f-4661-8f50-47ddf8b4eaad)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index=client3 sourcetype="aws:cloudtrail" eventName="PutBucketAcl" AllUsers

| table \_time eventID requestParameters.bucketName userIdentity.principalId

Question

What is the name of the S3 bucket that Bud accidentally made public?

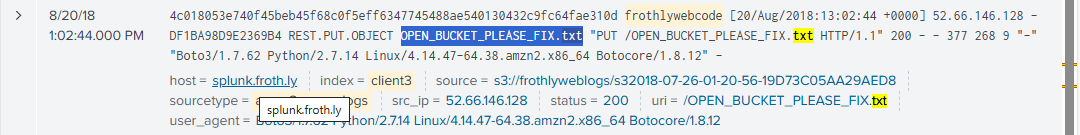
frothlywebcode

14.1.6 Accessed text file's name

14.1.6 Determining the name of an accessed text file

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/0de05e70-6e93-45ce-9755-f4886faef108)**.** Use this worksheet to keep notes as you complete it. |
| --- |

| 8/20/18  1:02:44.000 PM |
| --- |



index="client3" sourcetype=aws:s3:accesslogs frothlywebcode operation="REST.PUT.OBJECT"

Question

Which text file was successfully uploaded into that S3 bucket during its public exposure?

Provide only the filename and extension (*e.g.,* file.txt) — don’t include the full file path (*e.g.,* path/to/file.txt)

OPEN\_BUCKET\_PLEASE\_FIX.txt

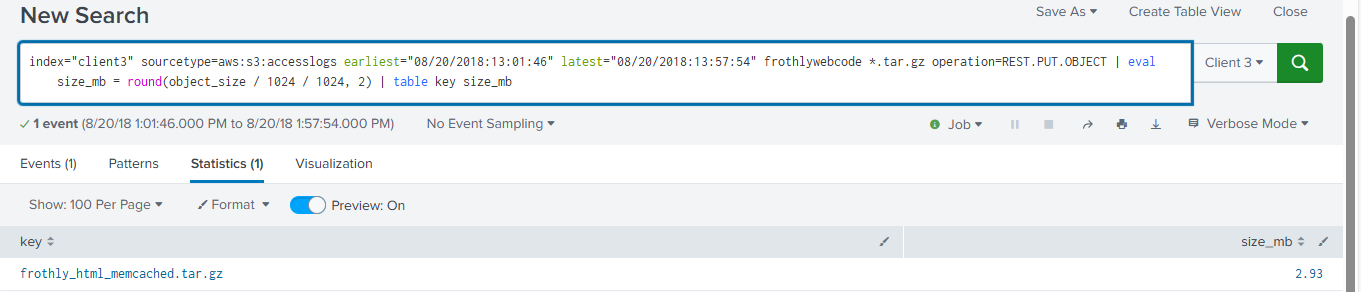
14.1.7 Archive file's size

14.1.7 Measuring the size of the uploaded archive file

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/a1a21619-b6e5-4b19-9be8-c374fcebe6bf)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/20/18

1:04:17.000 PM



index="client3" sourcetype=aws:s3:accesslogs earliest="08/20/2018:13:01:46" latest="08/20/2018:13:57:54" frothlywebcode \*.tar.gz operation=REST.PUT.OBJECT | eval size\_mb = round(object\_size / 1024 / 1024, 2) | table key size\_mb

Question

How large (in megabytes) is the .tar.gz file that was uploaded to the S3 bucket while it was publicly accessible?

*Round to two decimal places. Do not include the unit of measure (”*MB*”). Use 1024 for the byte conversion. Use a period [*.*] (not a comma!) as the radix character. For example, if your answer is “*42.013 MBs*”, you would enter “*42.01*”.*

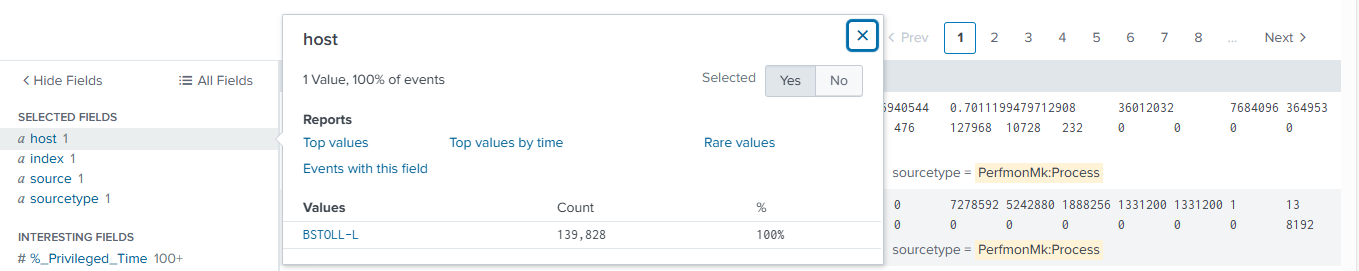
2.93

14.2 Coin mining on endpoints

14.2.1 Cryptomining process

14.2.1 Detecting the cryptocurrency mining process

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/71d4971f-b067-4511-a15a-e0c69904b4d9)**.** Use this worksheet to keep notes as you complete it. |
| --- |

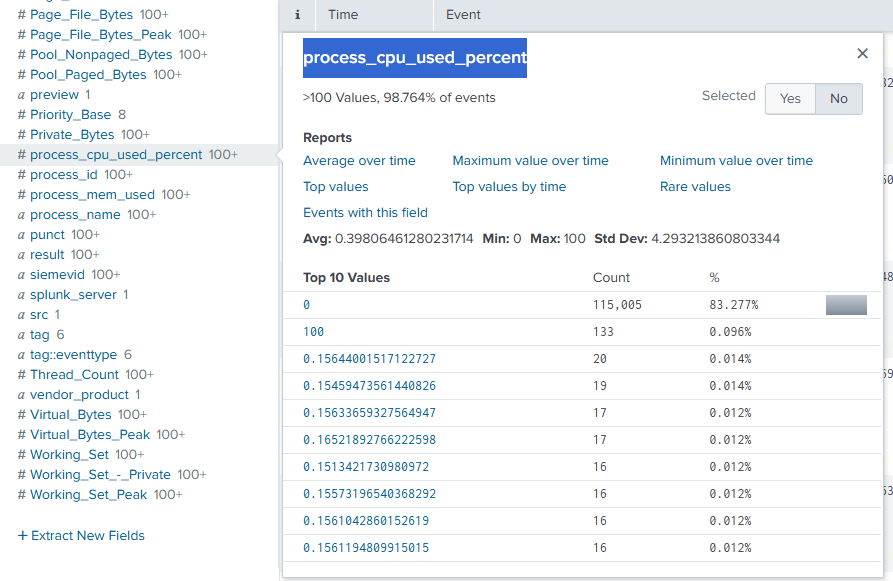


index="client3" sourcetype="PerfmonMk:Process" host="BSTOLL-L"

Question

Which field are hostnames contained within for the PerfmonMk:Process sourcetype?

Host

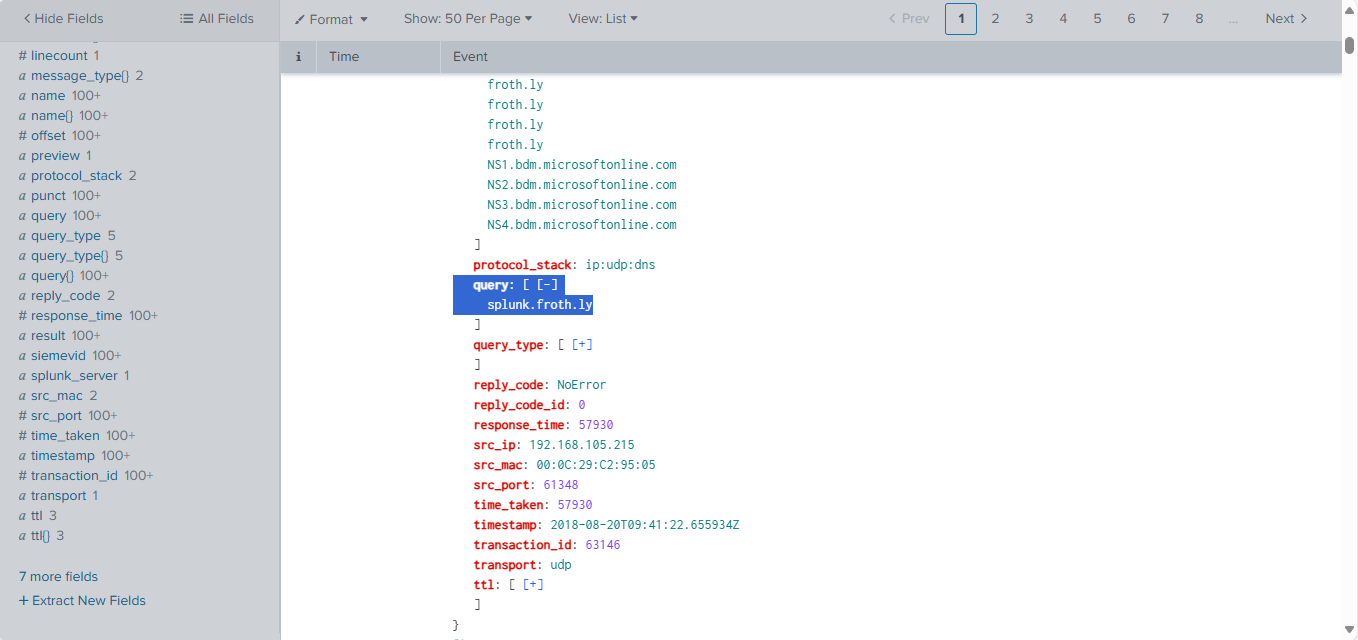


index="client3" sourcetype="PerfmonMk:Process" host="BSTOLL-L"

Question

Which PerfmonMk:Process field contains the information about what percentage of CPU is being used by a given process?

Process\_cpu\_used\_percent

8/20/18

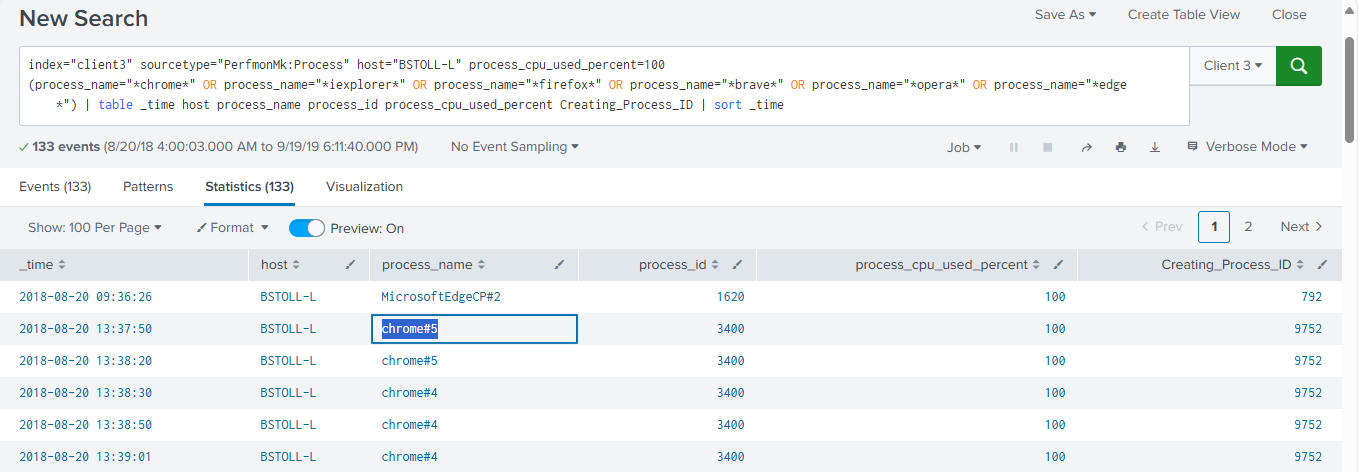
9:36:26.000 AM

index="client3" host="BSTOLL-L" sourcetype="stream:dns"

Question

Which field contains the FQDN data?

Query



index="client3" sourcetype="PerfmonMk:Process" host="BSTOLL-L" process\_cpu\_used\_percent=100

(process\_name="\*chrome\*" OR process\_name="\*iexplorer\*" OR process\_name="\*firefox\*" OR process\_name="\*brave\*" OR process\_name="\*opera\*" OR process\_name="\*edge\*") | table \_time host process\_name process\_id process\_cpu\_used\_percent Creating\_Process\_ID | sort \_time

Question

What is the name of the first process to hit 100% CPU usage due to coin mining on the Frothly Windows endpoint?

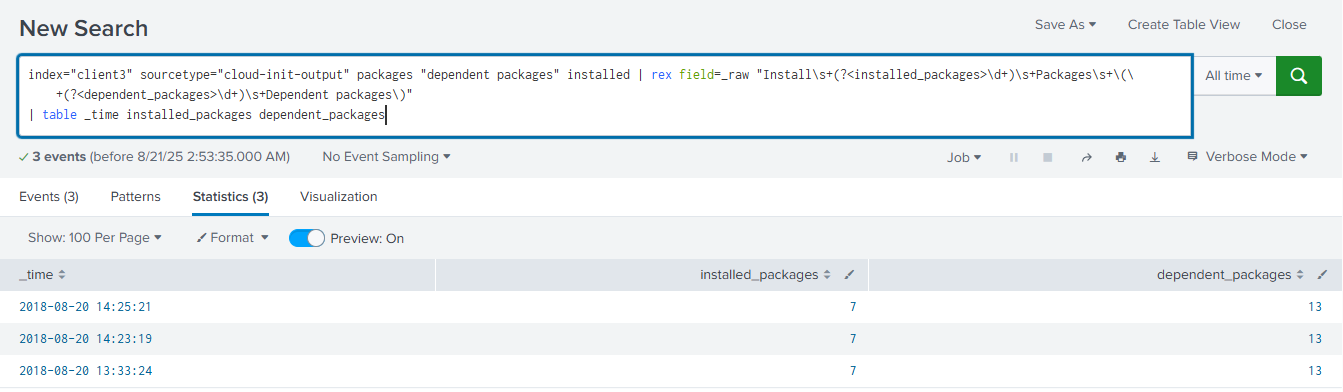
*Include any special characters or punctuation included in the process’s name.*

chrome#5

14.2.2 Cloud init script's packages

14.2.2 Counting packages installed by a cloud initialization script

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/600b272b-1106-42b8-93bf-d422b01f9fb1)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index="client3" sourcetype="cloud-init-output" packages "dependent packages" installed | rex field=\_raw "Install\s+(?<installed\_packages>\d+)\s+Packages\s+\(\+(?<dependent\_packages>\d+)\s+Dependent packages\)"

| table \_time installed\_packages dependent\_packages

Question

How many packages are installed by the EC2 instance’s cloud init script when a Frothly web server is auto-scaled?

7

Question

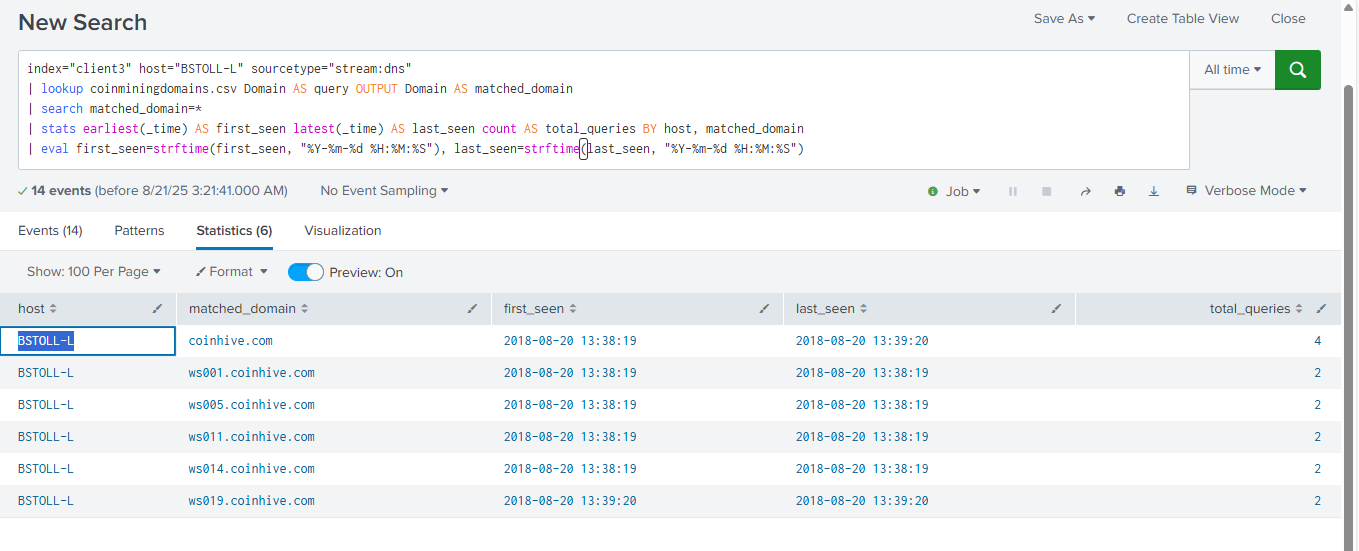
How many dependencies are installed by the EC2 instance’s cloud init script when a Frothly web server is auto-scaled?

13

14.2.3 Monero-mining endpoint

14.2.3 Finding the hostname of the endpoint that mined Monero

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/507b3e41-b876-4d12-9692-cb3e2b077570)**.** Use this worksheet to keep notes as you complete it. |
| --- |

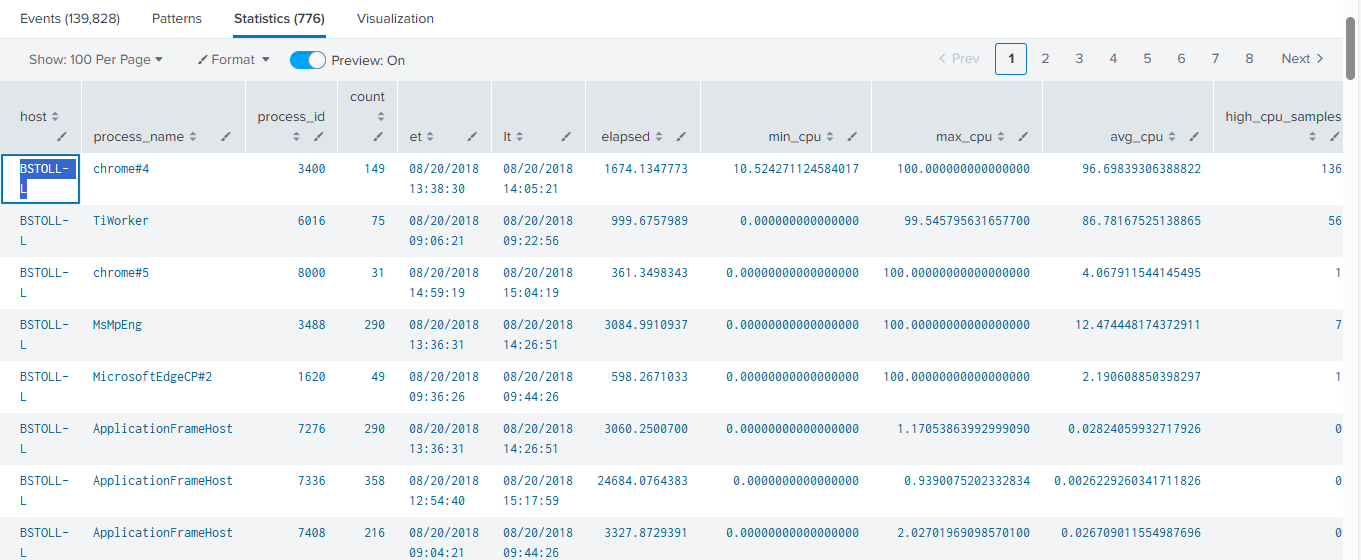
index="client3" host="BSTOLL-L" sourcetype="stream:dns"

| lookup coinminingdomains.csv Domain AS query OUTPUT Domain AS matched\_domain

| search matched\_domain=\*

| stats earliest(\_time) AS first\_seen latest(\_time) AS last\_seen count AS total\_queries BY host, matched\_domain

| eval first\_seen=strftime(first\_seen, "%Y-%m-%d %H:%M:%S"), last\_seen=strftime(last\_seen, "%Y-%m-%d %H:%M:%S")



index=client3 sourcetype=PerfmonMk:Process host="BSTOLL-L" earliest=0 latest=+24h

| eval high\_cpu=if(process\_cpu\_used\_percent>=90,1,0)

| stats count earliest(\_time) AS et latest(\_time) AS lt max(Elapsed\_Time) AS elapsed

min(process\_cpu\_used\_percent) AS min\_cpu

max(process\_cpu\_used\_percent) AS max\_cpu

avg(process\_cpu\_used\_percent) AS avg\_cpu

sum(high\_cpu) AS high\_cpu\_samples

BY host process\_name process\_id

| where elapsed>=300

| eval risk\_score=(high\_cpu\_samples/elapsed)\*100

| convert ctime(et) ctime(lt)

| sort - risk\_score

Question

Which host is appearing in these narrowed results?

BSTOLL-L

Question

What is the short hostname of the sole Frothly system that successfully mined Monero?

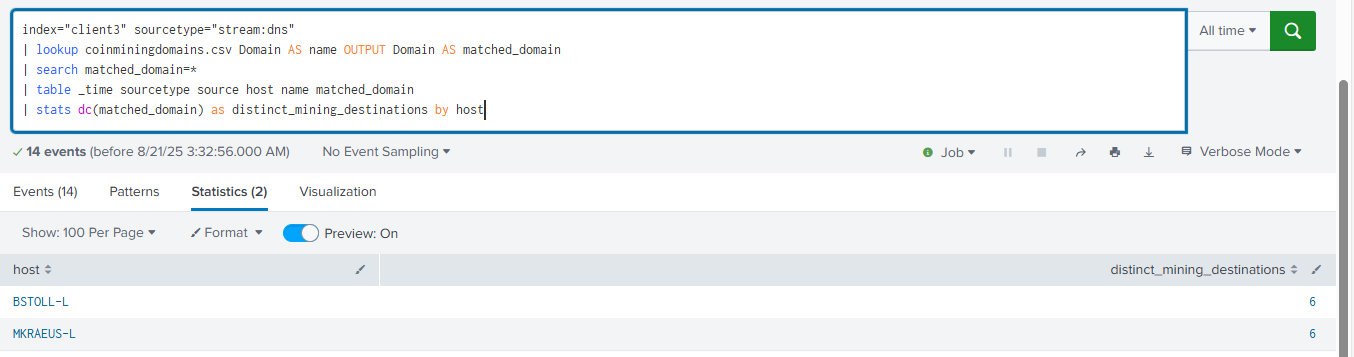
*Provide the hostname only! (e.g.,* fprefect *instead of* fprefect.0x2a.com*)*

BSTOLL-L

14.2.4 Cryptocurrency mining destinations

14.2.4 Calculating the number of cryptocurrency mining destinations

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/64f3755d-29b0-4592-b591-3a117d21dbc7)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index="client3" sourcetype="stream:dns"

| lookup coinminingdomains.csv Domain AS name OUTPUT Domain AS matched\_domain

| search matched\_domain=\*

| table \_time sourcetype source host name matched\_domain

| stats dc(matched\_domain) as distinct\_mining\_destinations by host

Question

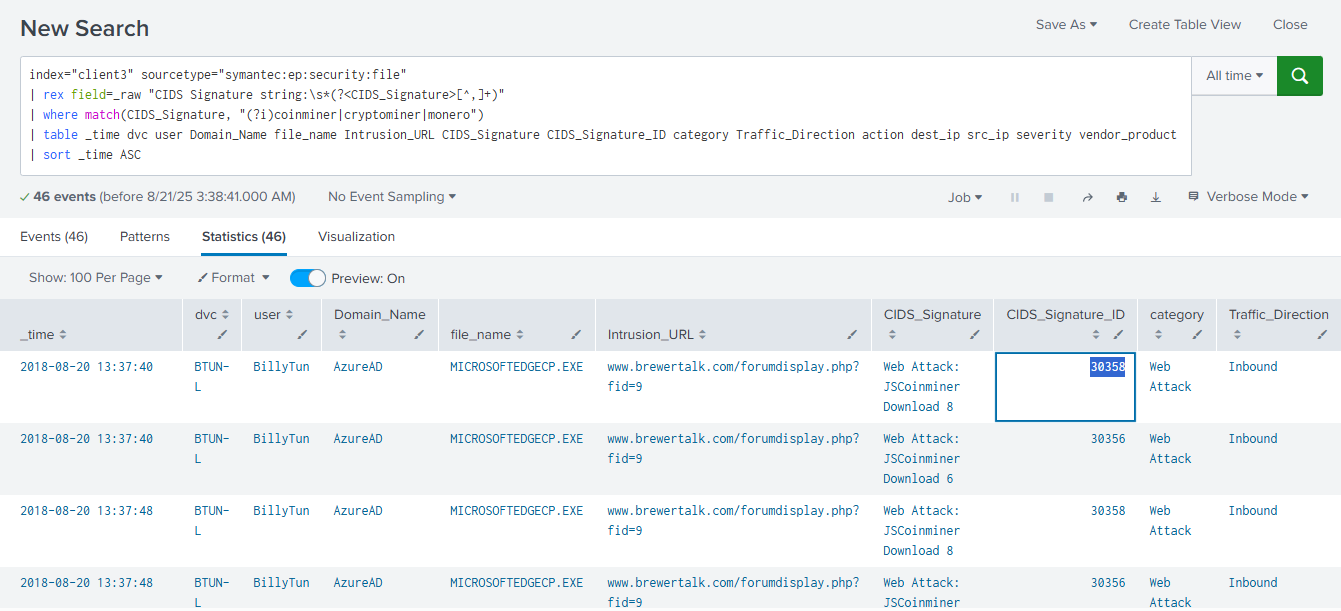
What is the total number of cryptocurrency mining destinations accessed by Frothly endpoints?

6

14.2.5 Suricata detection ID

14.2.5 Determining the ID of the first Suricata detection

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/b8872a86-6cab-4cea-acf0-39bce1cb32e0)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index="client3" sourcetype="symantec:ep:security:file"

| rex field=\_raw "CIDS Signature string:\s\*(?<CIDS\_Signature>[^,]+)"

| where match(CIDS\_Signature, "(?i)coinminer|cryptominer|monero")

| table \_time dvc user Domain\_Name file\_name Intrusion\_URL CIDS\_Signature CIDS\_Signature\_ID category Traffic\_Direction action dest\_ip src\_ip severity vendor\_product

| sort \_time ASC

Question

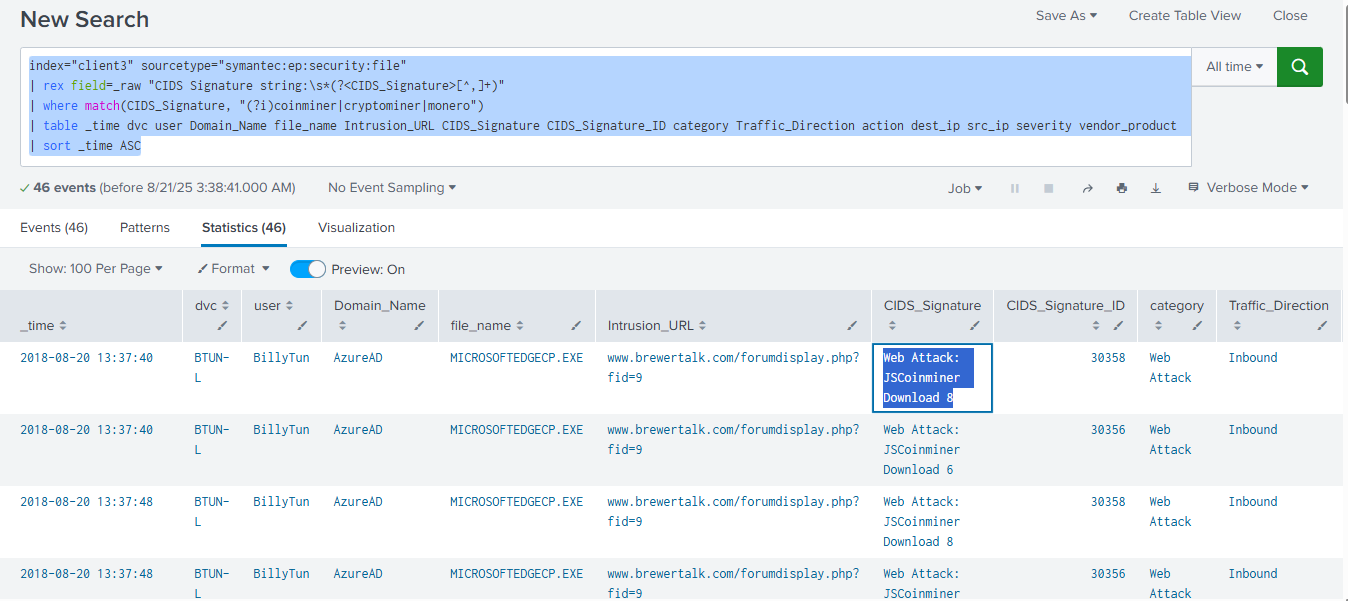
What is the earliest recorded signature ID of the coin miner threat in Frothly’s Symantec Endpoint Protection (SEP) logs?

30358

14.2.6 Malware severity via OSINT

14.2.6 Using OSINT to look up the severity of the malware

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/9e5290cb-0107-4a2e-b17d-709a6280e81e)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index="client3" sourcetype="symantec:ep:security:file"

| rex field=\_raw "CIDS Signature string:\s\*(?<CIDS\_Signature>[^,]+)"

| where match(CIDS\_Signature, "(?i)coinminer|cryptominer|monero")

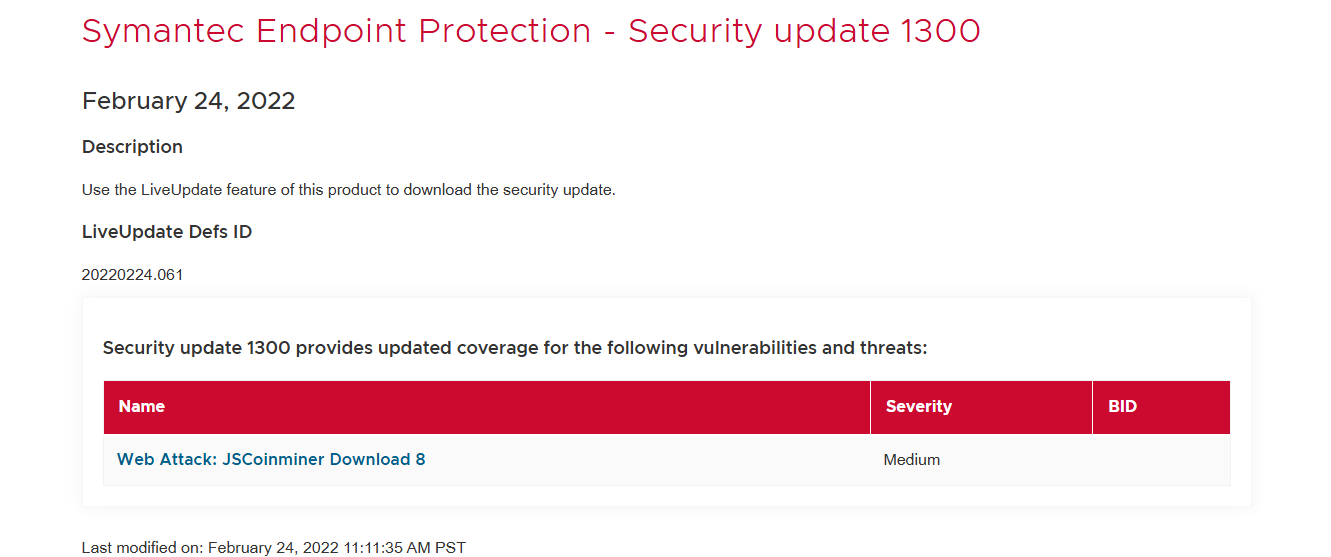
| table \_time dvc user Domain\_Name file\_name Intrusion\_URL CIDS\_Signature CIDS\_Signature\_ID category Traffic\_Direction action dest\_ip src\_ip severity vendor\_product

| sort \_time ASC

Question

What’s the name of the threat (= the value contained in this threat’s CIDS\_Signature field)?

Web Attack: JSCoinminer Download 8



[Symantec Endpoint Protection - Security update 1300](https://www.broadcom.com/support/security-center/securityupdates/detail?fid=sep&pvid=sep14&year=2022&suid=CIDS_Enterprise_SEP_14-SU1300-20220224.061)

Question

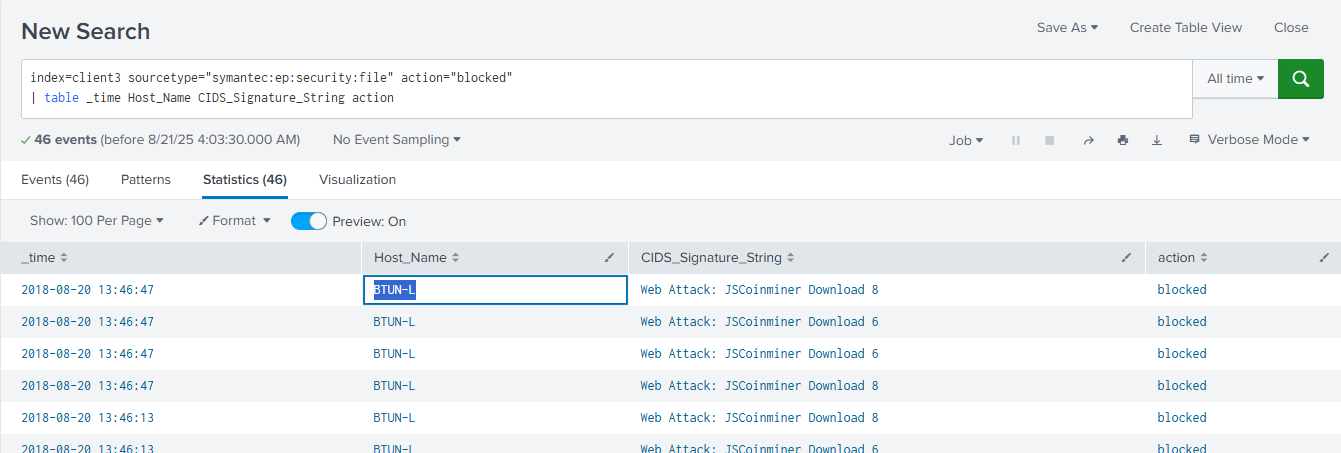
What severity level is assigned to this coin miner threat (according to Symantec’s official documentation)?

Medium

14.2.7 Coinminer-defeating endpoint

14.2.7 Identifying the endpoint that defeated the coin miner

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/3a98487a-ede9-47f1-a40e-aca9e0527f23)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index=client3 sourcetype="symantec:ep:security:file" action="blocked"

| table \_time Host\_Name CIDS\_Signature\_String action

Question

Which Frothly endpoint successfully overcame the cryptocurrency attack?

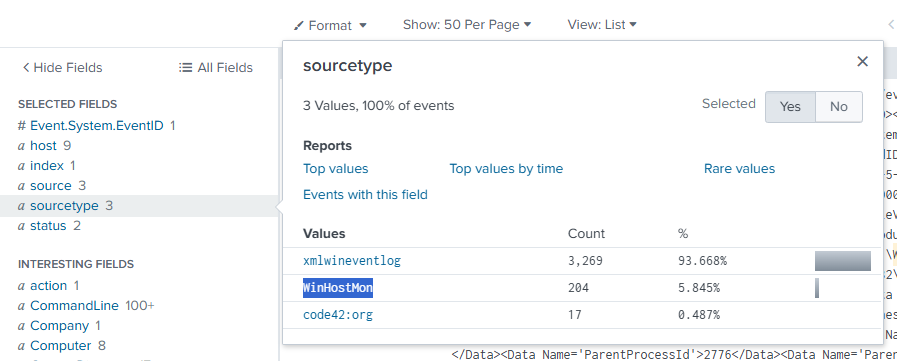
*Provide that device’s short hostname.*

BTUN-L

14.2.8 Different OS endpoint

14.2.8 Finding the endpoint with a different OS version

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/fab4c06a-ee94-401d-9de4-8ae24d94d35c)**.** Use this worksheet to keep notes as you complete it. |
| --- |

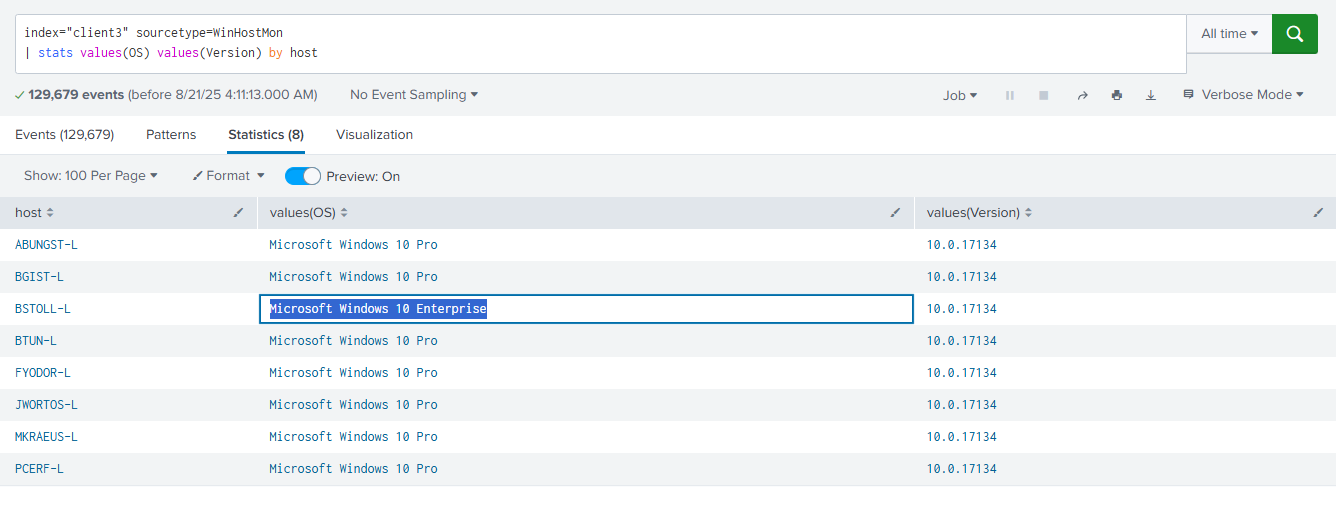


index="client3" sourcetype=\* CASE(Windows) (os OR operating) (ver OR version)

Question

Which sourcetype do all the useful fields appear in?

WinHostMon



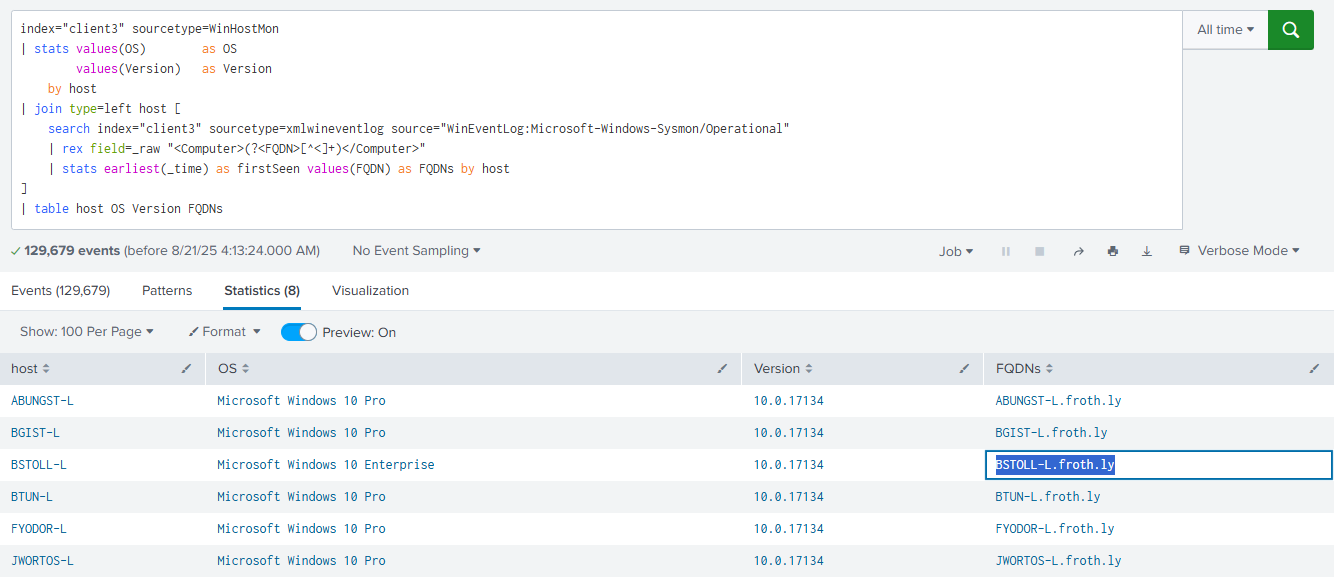
index="client3" sourcetype=WinHostMon

| stats values(OS) values(Version) by host

Question

Which is host has the operating system that is different from everybody else?

BSTOLL-L



index="client3" sourcetype=WinHostMon

| stats values(OS) as OS

values(Version) as Version

by host

| join type=left host [

search index="client3" sourcetype=xmlwineventlog source="WinEventLog:Microsoft-Windows-Sysmon/Operational"

| rex field=\_raw "<Computer>(?<FQDN>[^<]+)</Computer>"

| stats earliest(\_time) as firstSeen values(FQDN) as FQDNs by host

]

| table host OS Version FQDNs

Question

Which endpoint runs a different edition of Windows compared to the rest?

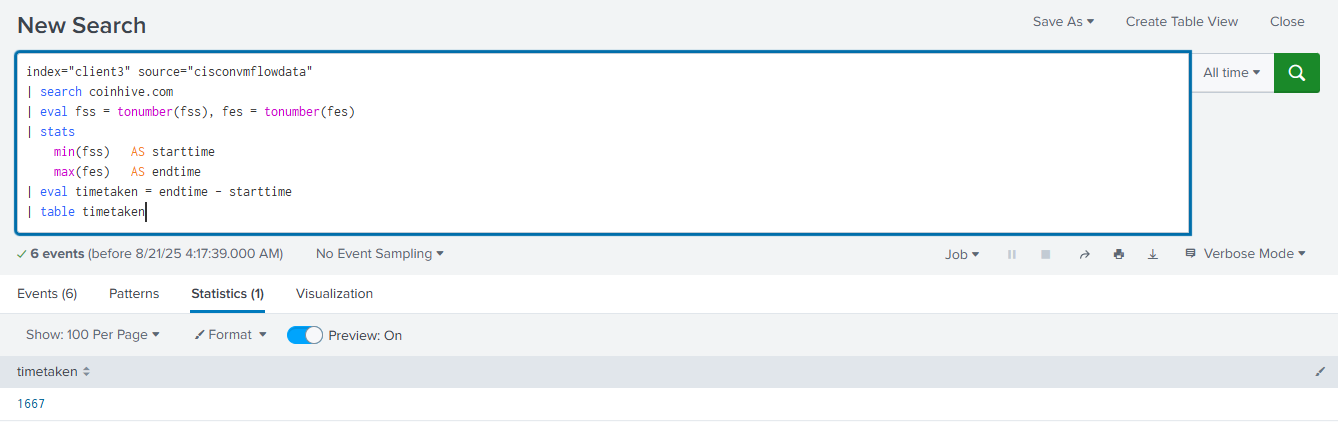
Identify it by its FQDN.

BSTOLL-L.froth.ly

14.2.9 Cryptomining duration via flow logs

14.2.9 Measuring duration of cryptomining from flow logs

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/11c31b70-77b5-4a7e-97cc-e28ce91232b0)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index="client3" source="cisconvmflowdata"

| search coinhive.com

| eval fss = tonumber(fss), fes = tonumber(fes)

| stats

min(fss) AS starttime

max(fes) AS endtime

| eval timetaken = endtime - starttime

| table timetaken

Question

What is the duration in seconds that the endpoint mined Monero according to the Cisco NVM flow logs?

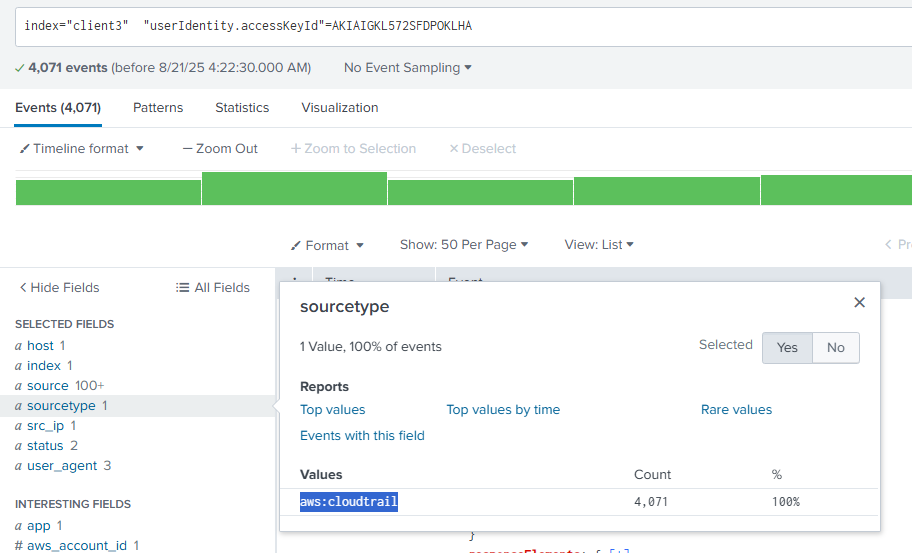
*Provide the number of seconds only.*

1667

14.2.10 Encoded email image

14.2.10 Safely examining encoded images in email attachments

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/679fd7ed-4cbc-46f4-8249-5464a8c40a18)**.** Use this worksheet to keep notes as you complete it. |
| --- |

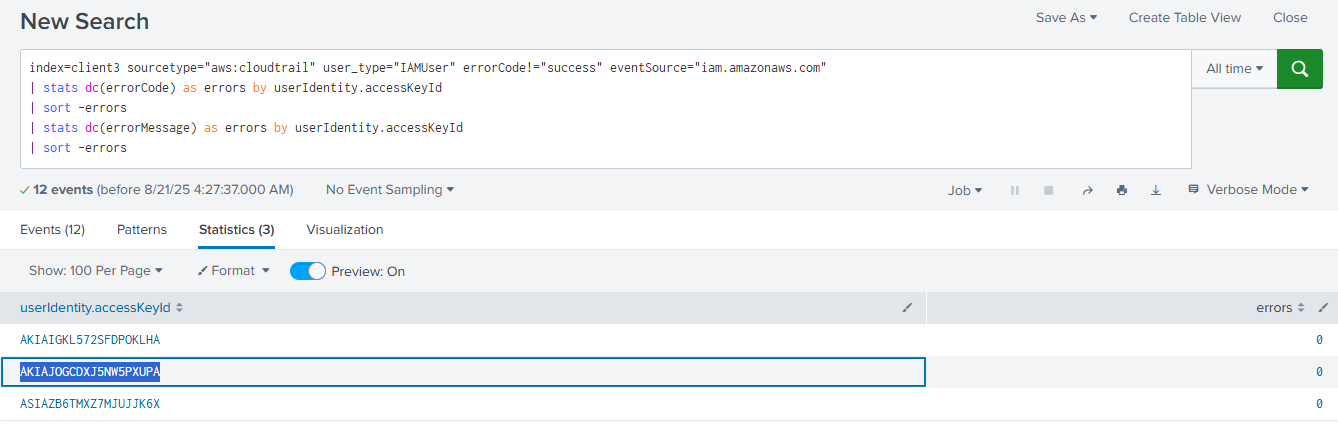


index="client3" "userIdentity.accessKeyId"=AKIAIGKL572SFDPOKLHA

Question

Which sourcetype contains the userIdentity.accessKeyId field?

Aws:cloudtrail



index=client3 sourcetype="aws:cloudtrail" user\_type="IAMUser" errorCode!="success" eventSource="iam.amazonaws.com"

| stats dc(errorCode) as errors by userIdentity.accessKeyId

| sort -errors

| stats dc(errorMessage) as errors by userIdentity.accessKeyId

| sort -errors

Question

Which IAM access key is responsible for the highest number of unique errors when trying to access IAM resources?

AKIAJOGCDXJ5NW5PXUPA

14.3 Leaked AWS keys

14.3.1 IAM access w most failures

14.3.1 Determining the IAM access key with the most distinct failures

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/3ef2e2ff-7a5e-404c-8e44-dd262b0697be)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index=client3 sourcetype=stream:smtp host=matar (AWS OR Amazon) (compromised OR notification OR "support case")

| spath content\_body

| spath sender\_email

| spath "receiver\_email{}"

| rex "New Support case: (?<case\_id>\\d+)"

| table \_time case\_id sender\_email receiver\_email{}

Question

Which sourcetype contains the userIdentity.accessKeyId field?

aws:cloudtrail

Question

After Bud’s AWS keys were leaked to a public repo, what support case ID did AWS assign when notifying him of the breach?

5244329601

14.3.2 Amazon support ID

14.3.2 Identifying the Amazon support ID associated with the compromised AWS access key

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/4e2a8d66-4353-4949-a6c0-ad7930bbdf76)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index=client3 sourcetype=stream:smtp host=matar (AWS OR Amazon) (compromised OR notification OR "support case")

| spath content\_body

| spath sender\_email

| spath "receiver\_email{}"

| rex "New Support case: (?<case\_id>\\d+)"

| table \_time case\_id sender\_email receiver\_email{}

Question

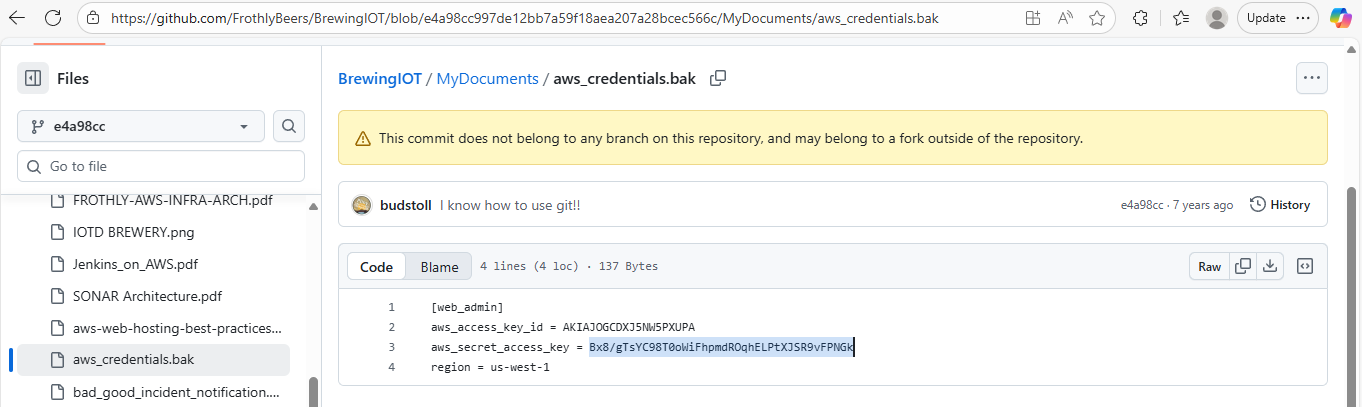
Which sourcetype contains the userIdentity.accessKeyId field?

aws:cloudtrail

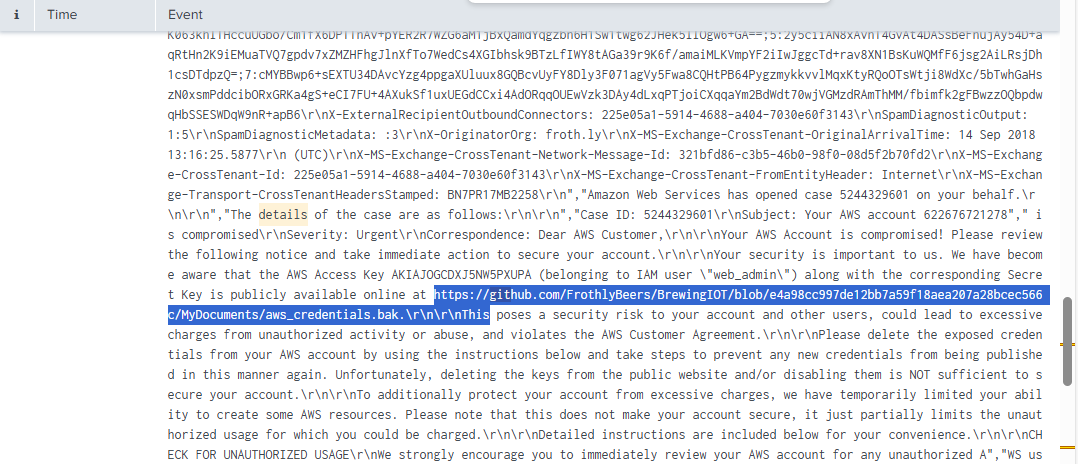
Question

After Bud’s AWS keys were leaked to a public repo, what support case ID did AWS assign when notifying him of the breach?

5244329601



[BrewingIOT/MyDocuments/aws\_credentials.bak at e4a98cc997de12bb7a59f18aea207a28bcec566c · FrothlyBeers/BrewingIOT · GitHub](https://github.com/FrothlyBeers/BrewingIOT/blob/e4a98cc997de12bb7a59f18aea207a28bcec566c/MyDocuments/aws_credentials.bak)



index=client3 sourcetype=stream:smtp host=matar

| spath "content\_body{}" | search "content\_body{}"="\*AWS Access Key AKIA\*"

| spath sender\_email

| spath "receiver\_email{}"

| spath subject

Question

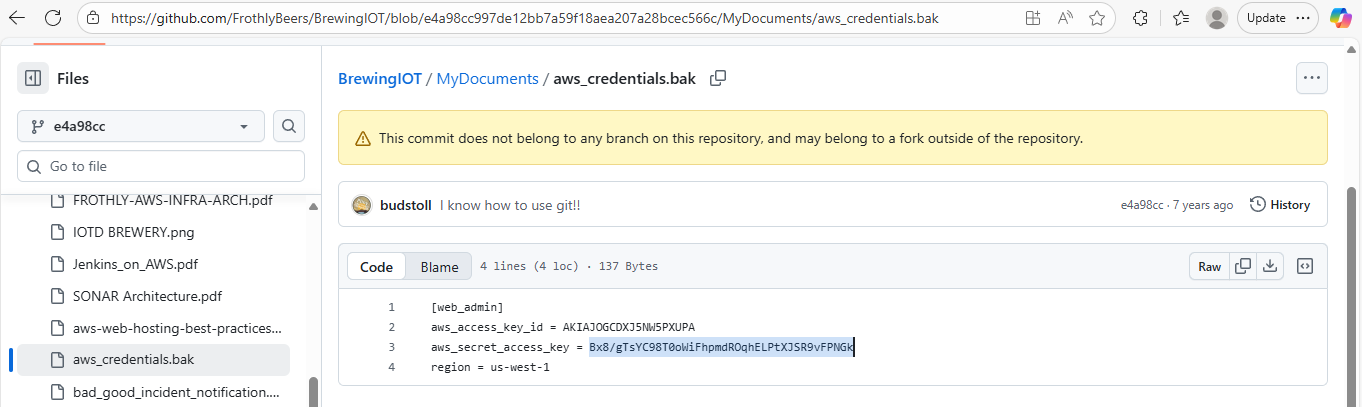
What is the secret access key associated with the AWS key that was exposed in the external repository?

Bx8/gTsYC98T0oWiFhpmdROqhELPtXJSR9vFPNGk

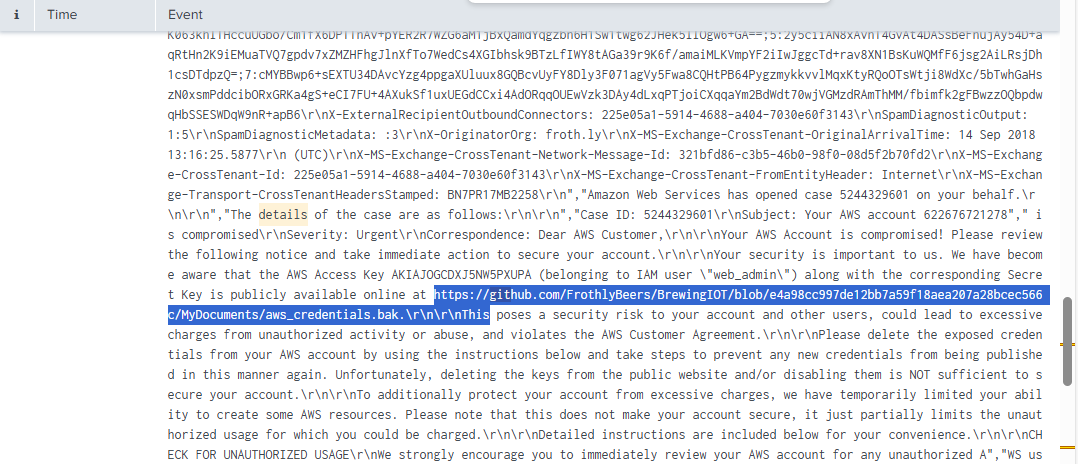
14.3.3 Leaked AWS key pair

14.3.3 Finding the leaked AWS key pair

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/21033c95-74ea-49c9-8472-b5837759e2e8)**.** Use this worksheet to keep notes as you complete it. |
| --- |



[BrewingIOT/MyDocuments/aws\_credentials.bak at e4a98cc997de12bb7a59f18aea207a28bcec566c · FrothlyBeers/BrewingIOT · GitHub](https://github.com/FrothlyBeers/BrewingIOT/blob/e4a98cc997de12bb7a59f18aea207a28bcec566c/MyDocuments/aws_credentials.bak)



index=client3 sourcetype=stream:smtp host=matar

| spath "content\_body{}" | search "content\_body{}"="\*AWS Access Key AKIA\*"

| spath sender\_email

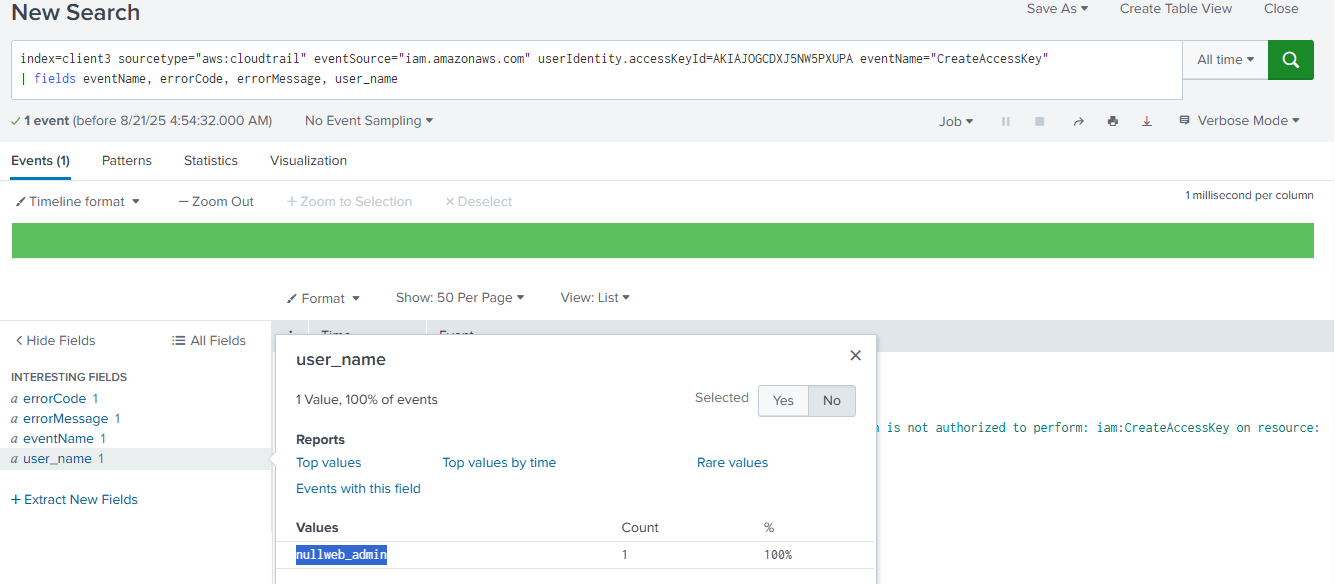
| spath "receiver\_email{}"

| spath subject

Question

What is the secret access key associated with the AWS key that was exposed in the external repository?

Bx8/gTsYC98T0oWiFhpmdROqhELPtXJSR9vFPNGk



index=client3 sourcetype="aws:cloudtrail" eventSource="iam.amazonaws.com" userIdentity.accessKeyId=AKIAJOGCDXJ5NW5PXUPA eventName="CreateAccessKey"

| fields eventName, errorCode, errorMessage, user\_name

Question

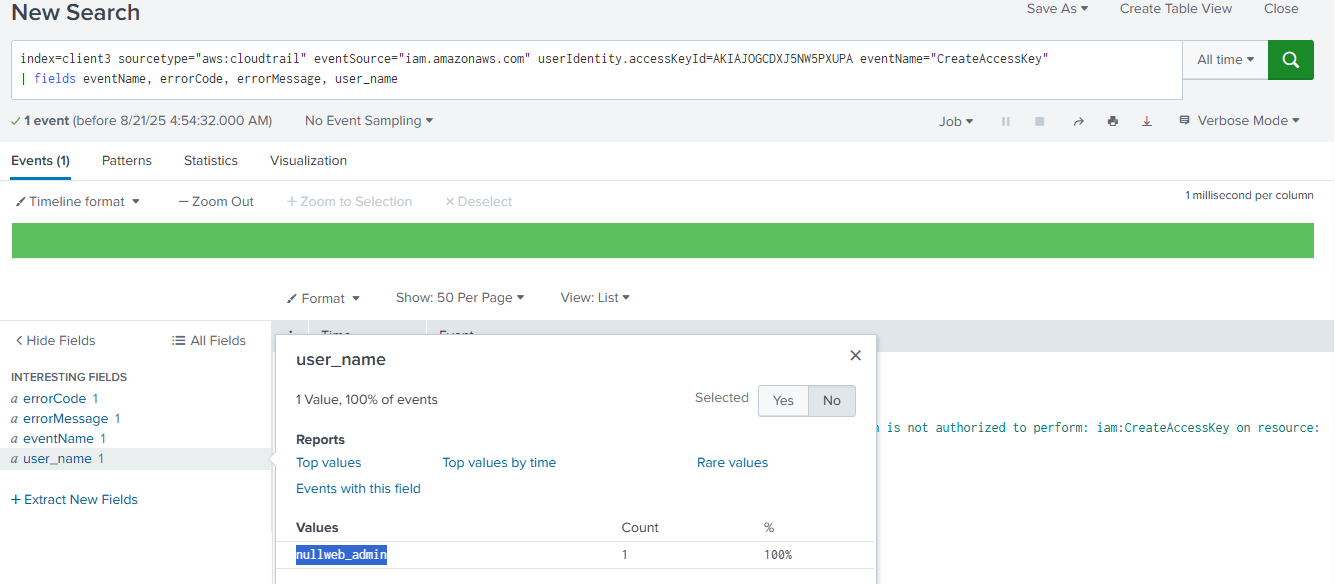
What is the name of the resource that the attacker tried to create a key for using the compromised access key?

nullweb\_admin

14.3.4 Resource launched by leaked key

14.3.4 Identifying the name of the resource launched using the leaked key

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/1cc7f316-8e56-456d-8e40-b8fce9eede72)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index=client3 sourcetype="aws:cloudtrail" eventSource="iam.amazonaws.com" userIdentity.accessKeyId=AKIAJOGCDXJ5NW5PXUPA eventName="CreateAccessKey"

| fields eventName, errorCode, errorMessage, user\_name

Question

What is the name of the resource that the attacker tried to create a key for using the compromised access key?

nullweb\_admin

| 8/20/18  9:27:06.000 AM |
| --- |



index=client3 sourcetype="aws:cloudtrail" AKIAJOGCDXJ5NW5PXUPA userIdentity eventName=DescribeAccountAttributes

Question

What is the complete user agent string from the application that attempted to describe an account using the leaked key?

ElasticWolf/5.1.6

14.3.5 Application used for unauthorized request

14.3.5 Determining the application responsible for the unauthorized request using the leaked key

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/54b44ec1-df6b-4ac6-b929-d49e675b6c28)**.** Use this worksheet to keep notes as you complete it. |
| --- |

| 8/20/18  9:27:06.000 AM |
| --- |

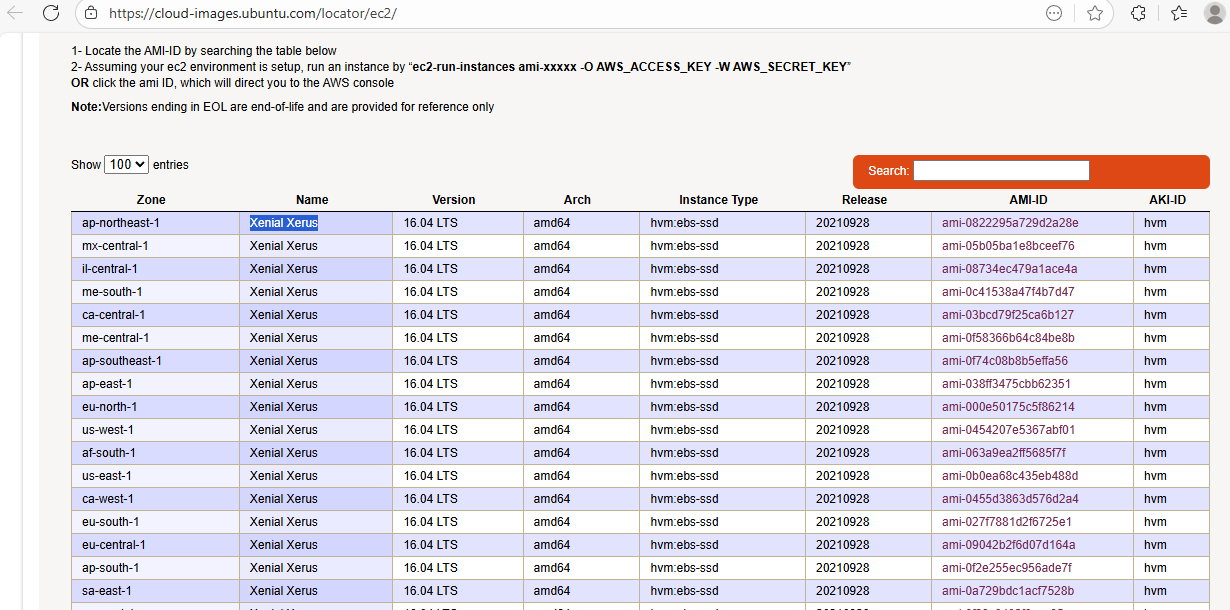


index=client3 sourcetype="aws:cloudtrail" AKIAJOGCDXJ5NW5PXUPA userIdentity eventName=DescribeAccountAttributes

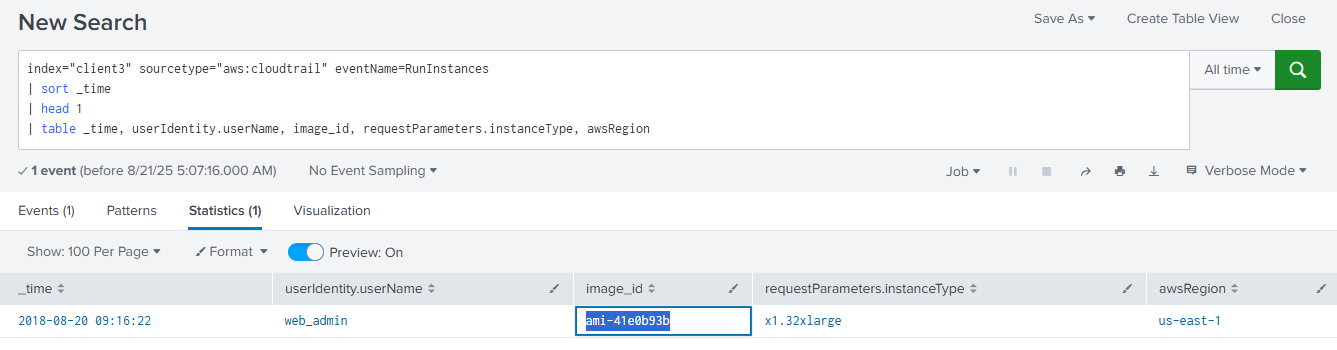
Question

What is the complete user agent string from the application that attempted to describe an account using the leaked key?

ElasticWolf/5.1.6



[Ubuntu Amazon EC2 AMI Finder](https://cloud-images.ubuntu.com/locator/ec2/)



index="client3" sourcetype="aws:cloudtrail" eventName=RunInstances

| sort \_time

| head 1

| table \_time, userIdentity.userName, image\_id, requestParameters.instanceType, awsRegion

Question

What is the Ubuntu version codename used in the adversary’s first launch attempt with the compromised IAM account?

*Your answer should be one word, no punctuation, all lowercase. It is the value in the Name column in the locator website.*

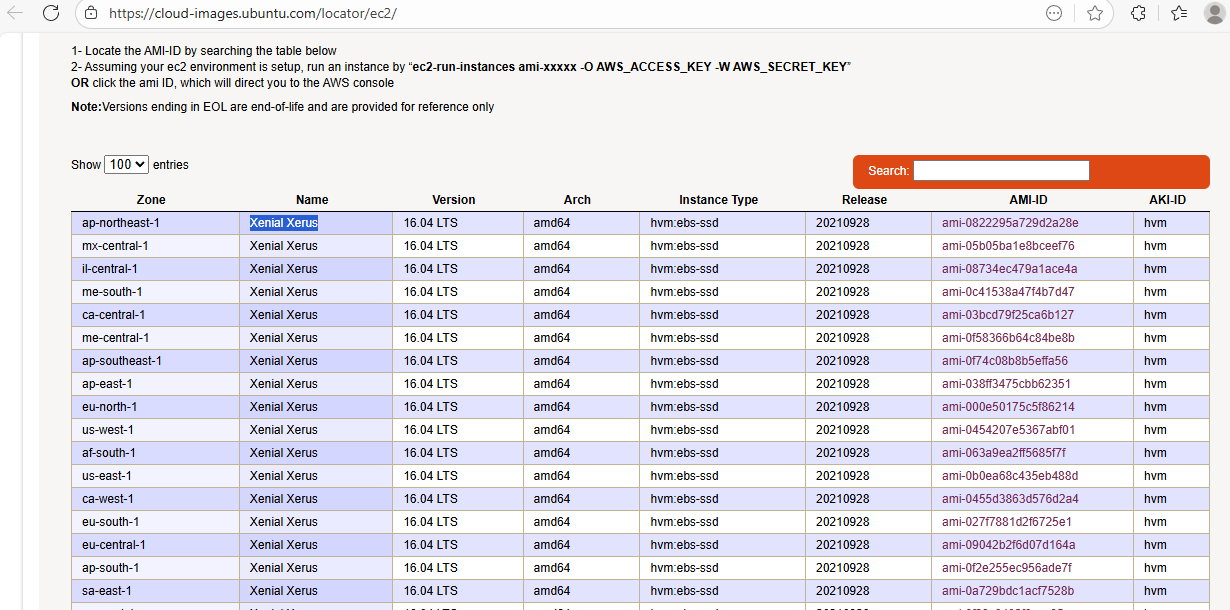
xenial

14.3.6 OS of Ubuntu instance

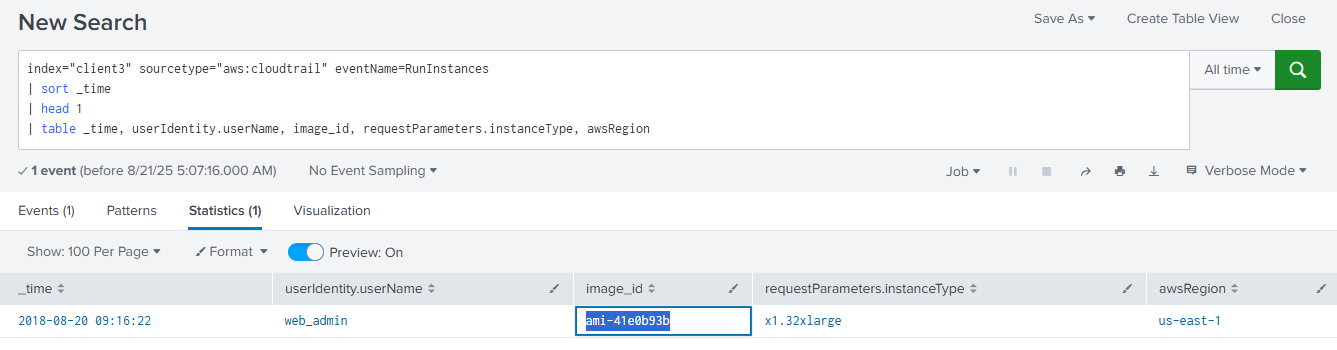
14.3.6 Classifying the OS version of a launched Ubuntu instance

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/ce1b6650-427f-45ce-b6f3-4dd4608c6e35)**.** Use this worksheet to keep notes as you complete it. |
| --- |

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/54b44ec1-df6b-4ac6-b929-d49e675b6c28)**.** Use this worksheet to keep notes as you complete it. |
| --- |



[Ubuntu Amazon EC2 AMI Finder](https://cloud-images.ubuntu.com/locator/ec2/)



index="client3" sourcetype="aws:cloudtrail" eventName=RunInstances

| sort \_time

| head 1

| table \_time, userIdentity.userName, image\_id, requestParameters.instanceType, awsRegion

Question

What is the Ubuntu version codename used in the adversary’s first launch attempt with the compromised IAM account?

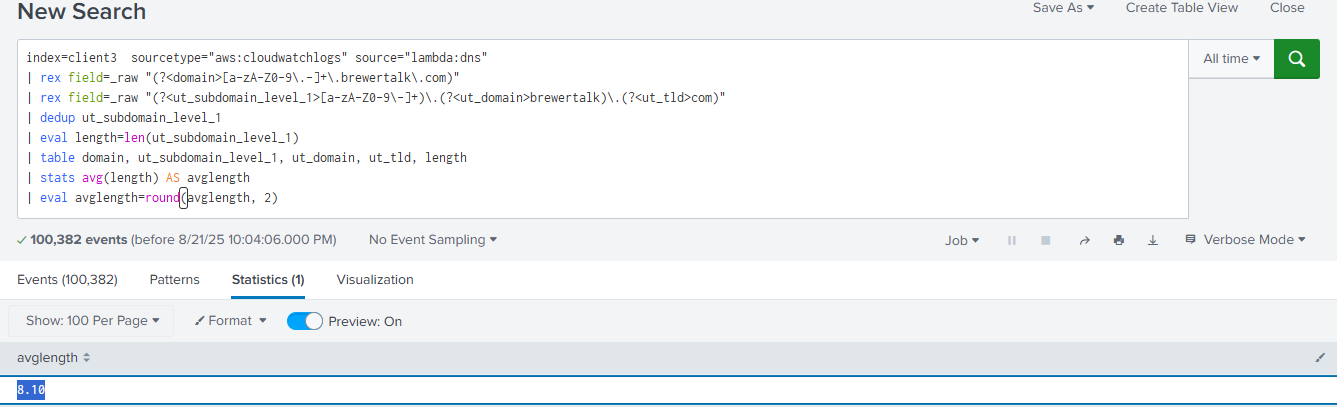
*Your answer should be one word, no punctuation, all lowercase. It is the value in the Name column in the locator website.*

xenial

14.3.7 Avg length of unique subdomains

14.3.7 Calculating the average length of unique subdomains

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/04f9bd5d-9e7f-4736-a971-a201819197b9)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index=client3 sourcetype="aws:cloudwatchlogs" source="lambda:dns"

| rex field=\_raw "(?<domain>[a-zA-Z0-9\.-]+\.brewertalk\.com)"

| rex field=\_raw "(?<ut\_subdomain\_level\_1>[a-zA-Z0-9\-]+)\.(?<ut\_domain>brewertalk)\.(?<ut\_tld>com)"

| dedup ut\_subdomain\_level\_1

| eval length=len(ut\_subdomain\_level\_1)

| table domain, ut\_subdomain\_level\_1, ut\_domain, ut\_tld, length

| stats avg(length) AS avglength

| eval avglength=round(avglength, 2)

Question

What is the average character length of unique third-level subdomains queried for brewertalk[.]com in Route 53?

*Round your answer to two decimal places.*

8.10

14.3.8 Defacement image filename

14.3.8 Finding the name of the image file used by the APT to deface the website

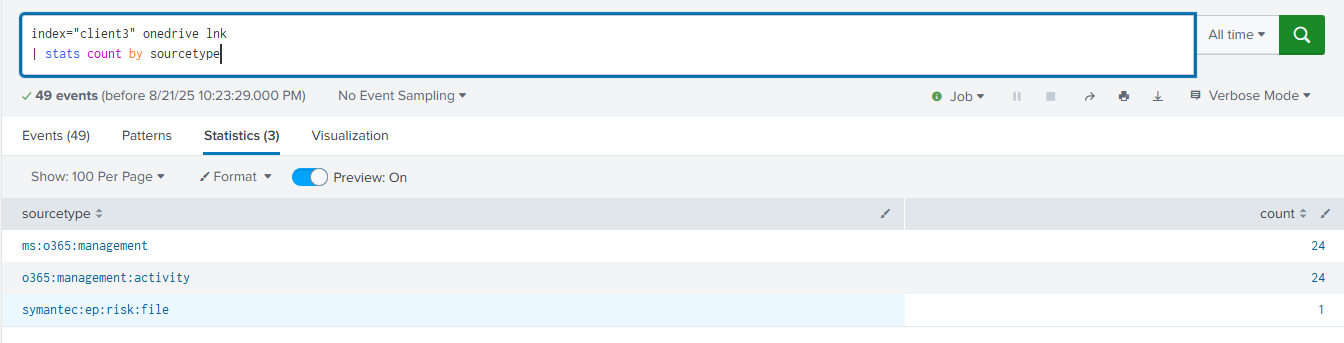
| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/7e50b7d1-ca99-4d37-94f4-b42dc27eb07e)**.** Use this worksheet to keep notes as you complete it. |
| --- |

14.4 A compromised endpoint

14.4.1 User agent string for malicious upload

14.4.1 Unveiling the user agent string associated with the malicious upload

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/9f1157eb-74a6-4c63-8cbb-ad4b11fabfda)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index="client3" onedrive lnk

| stats count by sourcetype

Question

Which sourcetype(s) look the most promising, in terms of hits?

*You may select more than one correct answer.*

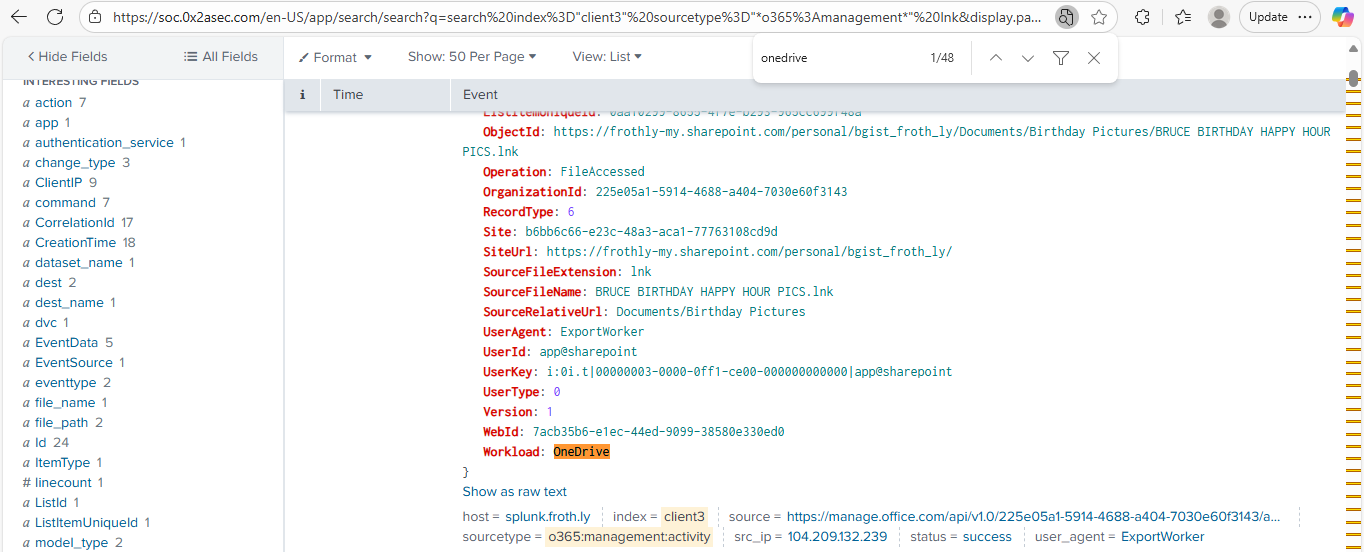
Choose as many as you like

ms:o365:management

Yep!

o365:management:activity

You got it!



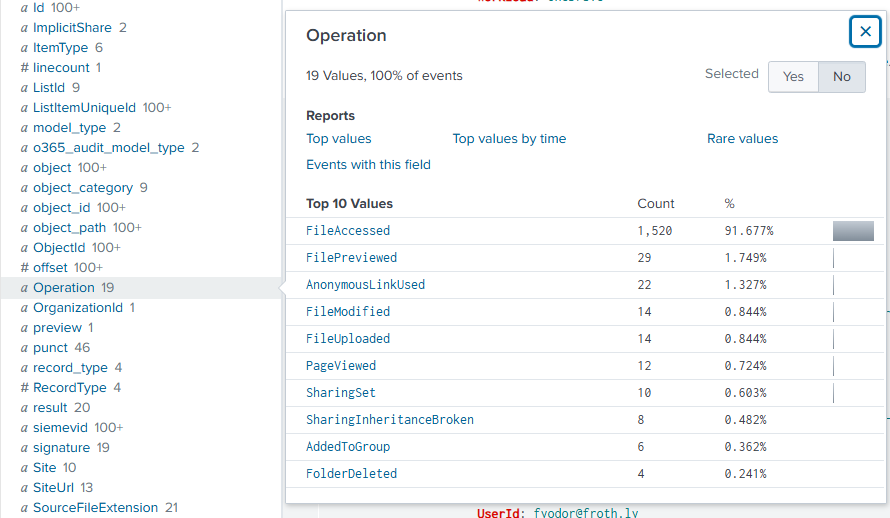
index="client3" sourcetype="\*o365:management\*" lnk

Question

Which field can you add to your search to limit results to OneDrive?

Workload

Yep! Other fields also duplicate this information, like app.

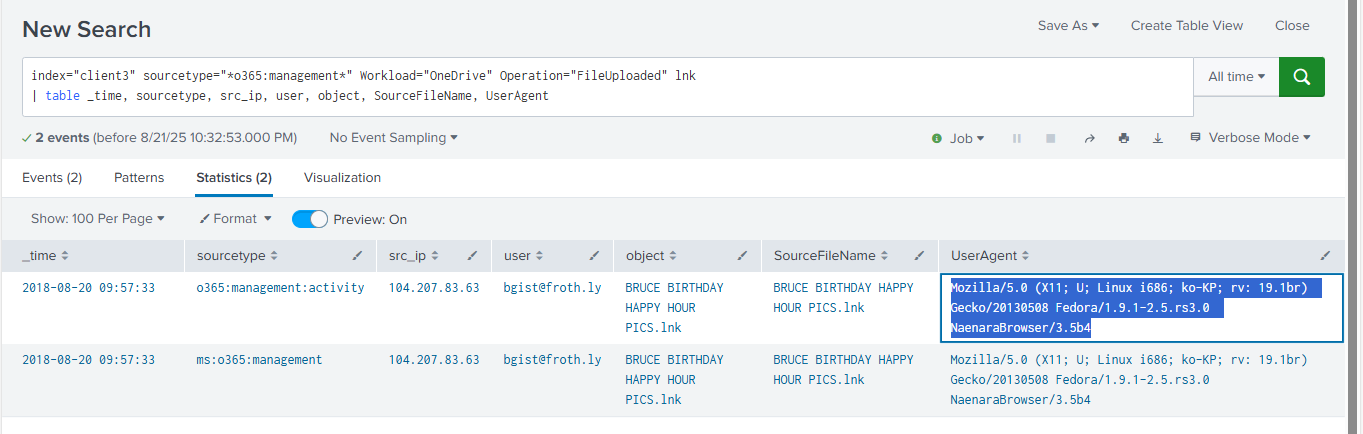


index="client3" sourcetype="\*o365:management\*" Workload="OneDrive"

Question

Which field can you add to your search to limit results to OneDrive?

Operation



index="client3" sourcetype="\*o365:management\*" Workload="OneDrive" Operation="FileUploaded" lnk

| table \_time, sourcetype, src\_ip, user, object, SourceFileName, UserAgent

Question

Which full user agent string identifies the client that uploaded the malicious shortcut file (.lnk) to OneDrive?

Mozilla/5.0 (X11; U; Linux i686; ko-KP; rv: 19.1br) Gecko/20130508 Fedora/1.9.1-2.5.rs3.0 NaenaraBrowser/3.5b4

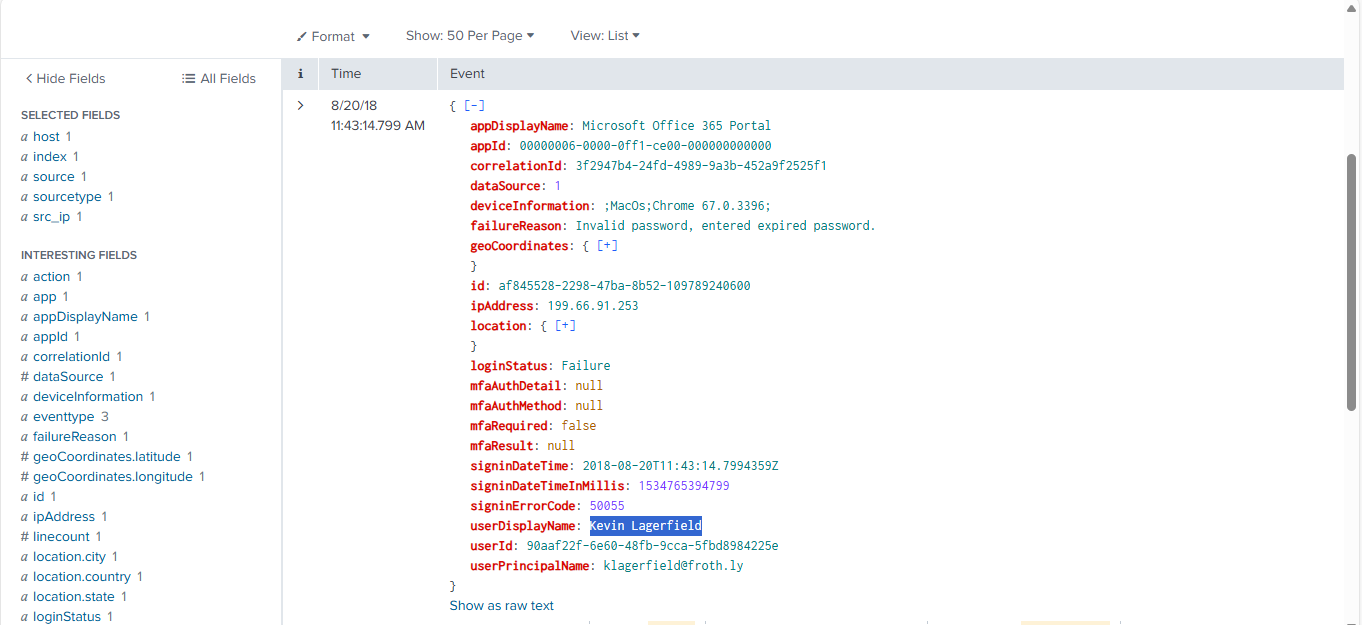
Well done!

14.4.2 IP of logged-in expired account

14.4.2 Revealing the IP associated with successful logins using an expired account

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/a3866797-5b99-4927-86fe-a284964bdaf0)**.** Use this worksheet to keep notes as you complete it. |
| --- |

| 8/20/18  11:43:14.799 AM |
| --- |



index="client3" sourcetype="ms:aad:signin" expired userDisplayName

Question

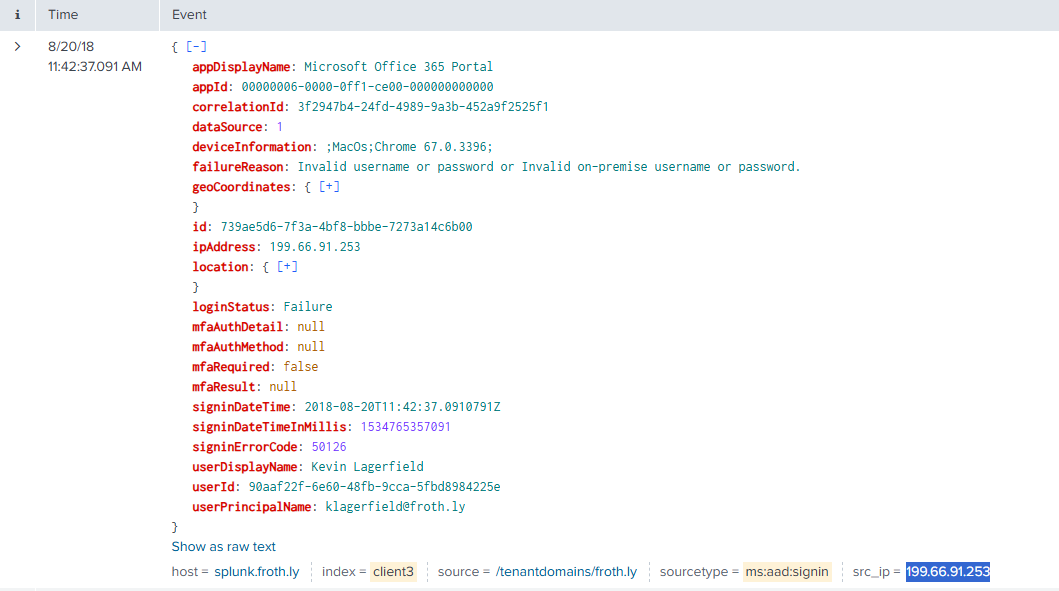
Which user display name can you use as a pivot in your next query?

Kevin Lagerfield

Perfect!

8/20/18

11:42:37.091 AM



index="client3" sourcetype="ms:aad:\*" (userDisplayName="Kevin Lagerfield" OR user\_id="kevin.lagerfield@froth.ly")

| sort \_time

Question

Which external client IP address successfully logged into Frothly using an expired account?

[199.66.91.253](https://soc.0x2asec.com/en-US/app/search/search?q=search%20index%3D%22client3%22%20sourcetype%3D%22ms%3Aaad%3A*%22%20(userDisplayName%3D%22Kevin%20Lagerfield%22%20OR%20user_id%3D%22kevin.lagerfield%40froth.ly%22)%20%0A%7C%20sort%20_time&display.page.search.mode=verbose&dispatch.sample_ratio=1&earliest=0&latest=&display.page.search.tab=events&display.general.type=events&sid=1755816064.22387#)

14.4.3 Discovery date of malicious macro

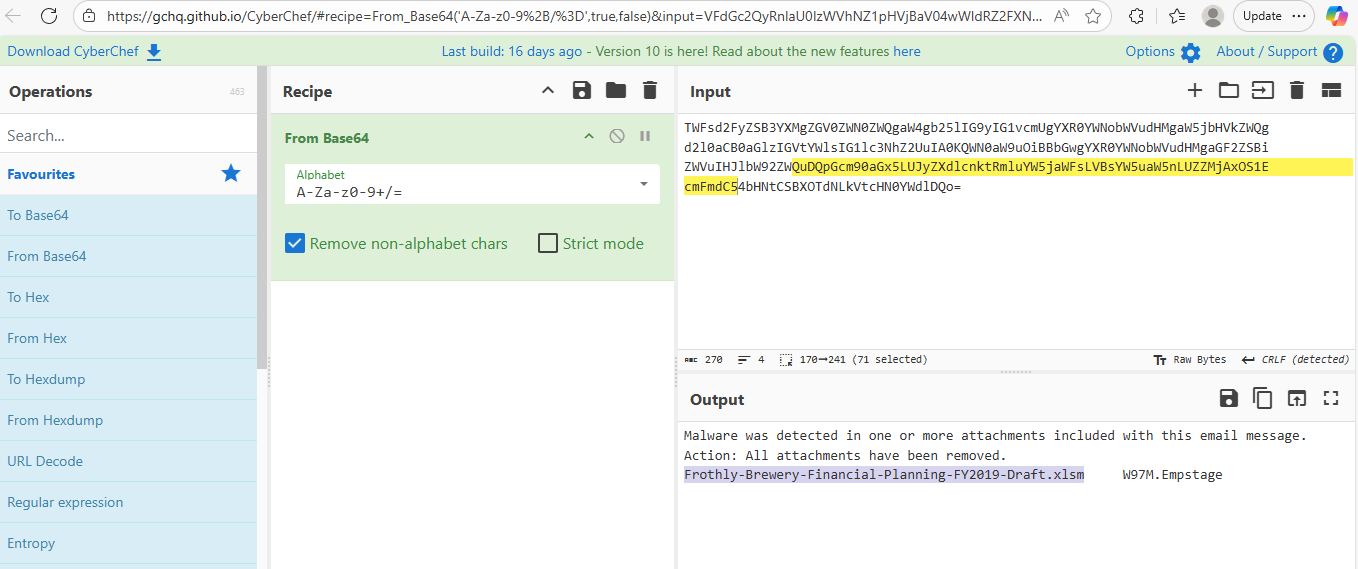
14.4.3 Using OSINT to establish the discovery date of the malicious macro

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/f1cb40c7-7524-4bf3-a0be-897897cae242)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index=client3 sourcetype=stream:smtp \*alert\* subject=\*

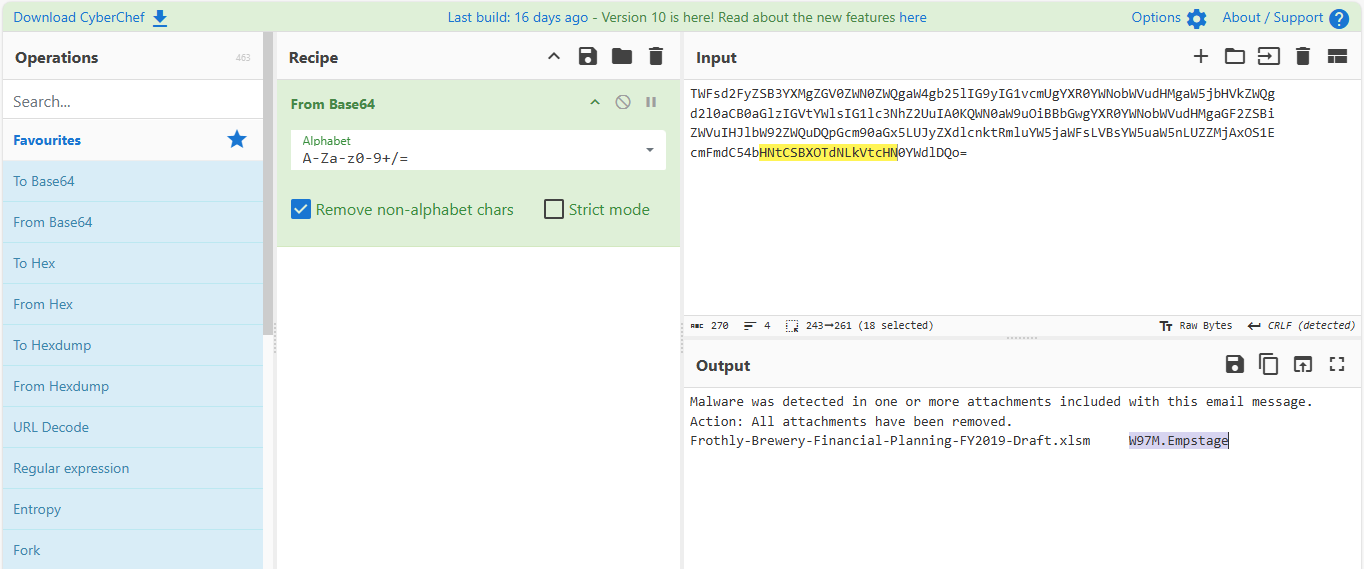
| table \_time subject attach\_transfer\_encoding{} content{} attach\_content\_decoded\_md5\_hash{}

<https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=VFdGc2QyRnlaU0IzWVhNZ1pHVjBaV04wWldRZ2FXNGdiMjVsSUc5eUlHMXZjbVVnWVhSMFlXTm9iV1Z1ZEhNZ2FXNWpiSFZrWldRZw0KZDJsMGFDQjBhR2x6SUdWdFlXbHNJRzFsYzNOaFoyVXVJQTBLUVdOMGFXOXVPaUJCYkd3Z1lYUjBZV05vYldWdWRITWdhR0YyWlNCaQ0KWldWdUlISmxiVzkyWldRdURRcEdjbTkwYUd4NUxVSnlaWGRsY25rdFJtbHVZVzVqYVdGc0xWQnNZVzV1YVc1bkxVWlpNakF4T1MxRQ>

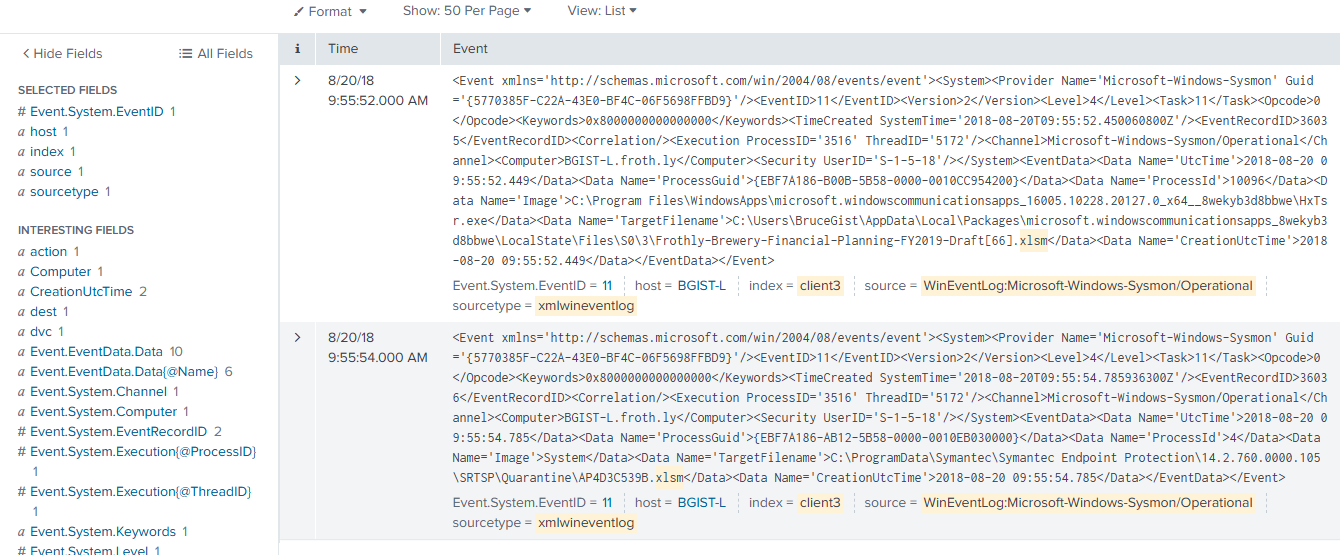
Question

What’s the XLSM filename you discovered in the decoded base64 blob?

Frothly-Brewery-Financial-Planning-FY2019-Draft.xlsm



<https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=VFdGc2QyRnlaU0IzWVhNZ1pHVjBaV04wWldRZ2FXNGdiMjVsSUc5eUlHMXZjbVVnWVhSMFlXTm9iV1Z1ZEhNZ2FXNWpiSFZrWldRZw0KZDJsMGFDQjBhR2x6SUdWdFlXbHNJRzFsYzNOaFoyVXVJQTBLUVdOMGFXOXVPaUJCYkd3Z1lYUjBZV05vYldWdWRITWdhR0YyWlNCaQ0KWldWdUlISmxiVzkyWldRdURRcEdjbTkwYUd4NUxVSnlaWGRsY25rdFJtbHVZVzVqYVdGc0xWQnNZVzV1YVc1bkxVWlpNakF4T1MxRQ>



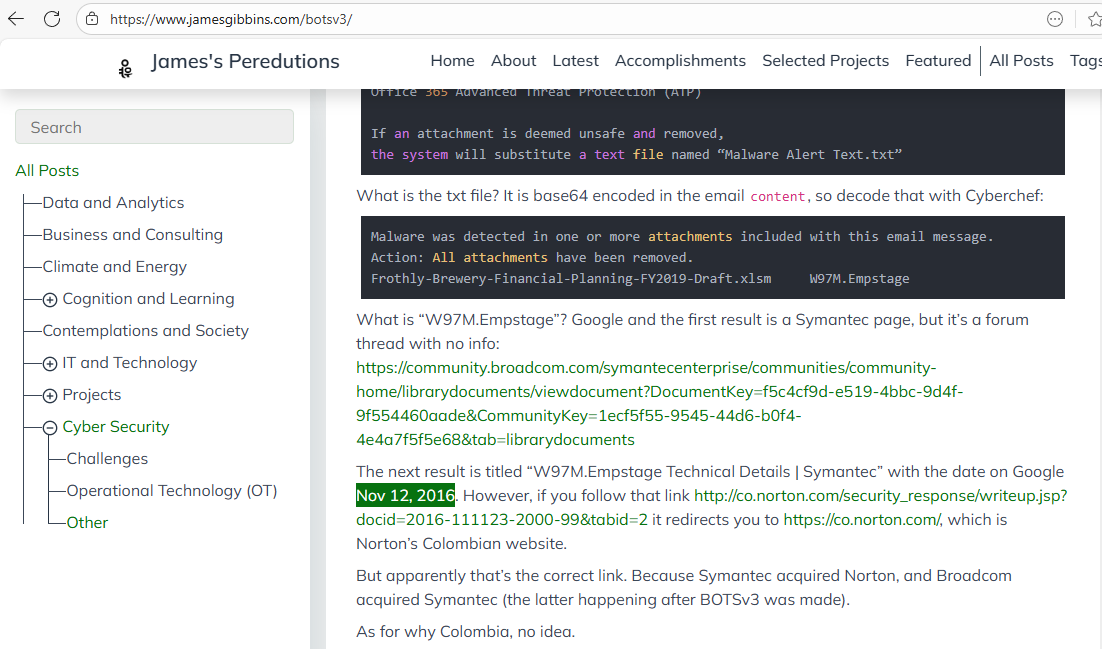
index=client3 sourcetype=xmlwineventlog source="WinEventLog:Microsoft-Windows-Sysmon/Operational" \*xlsm\*

| sort by +\_time

Question

What is the malware name you discovered in the decoded base64 blob and just confirmed the presence of using the SIEM’s logs?

W97M.Empstage



<https://www.jamesgibbins.com/botsv3/>

Question

What is the discovery date of the malware found in the macro-enabled document (according to Symantec)?

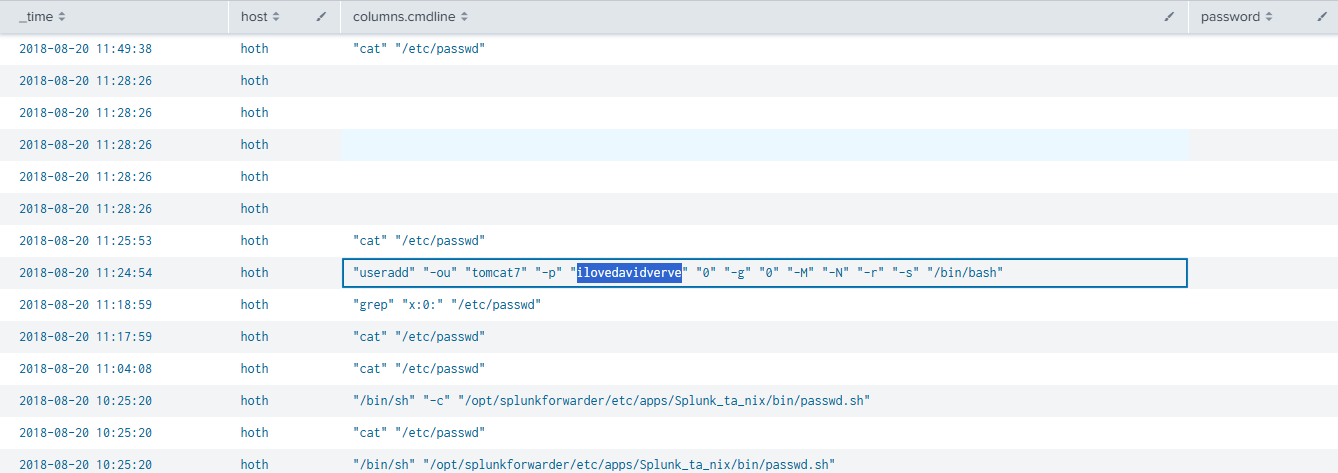
Use MM/DD/YY format (*e.g.,* [May 19, 1998](https://youtu.be/VVJldn_MmMY) would be 05/19/98).

11/12/16

14.4.4 User pw created post-pwning

14.4.4 Uncovering the password of the user created post-compromise

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/a3722ba7-8375-4098-bb04-e5408595805b)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index=client3 sourcetype=osquery:results host=hoth (useradd OR adduser OR passwd) columns.uid=0

| rex field=columns.cmdline "passwd\\s+[^\\s]+\\s+(?<password>[^\\s]+)"

| table \_time, host, columns.cmdline, password

Question

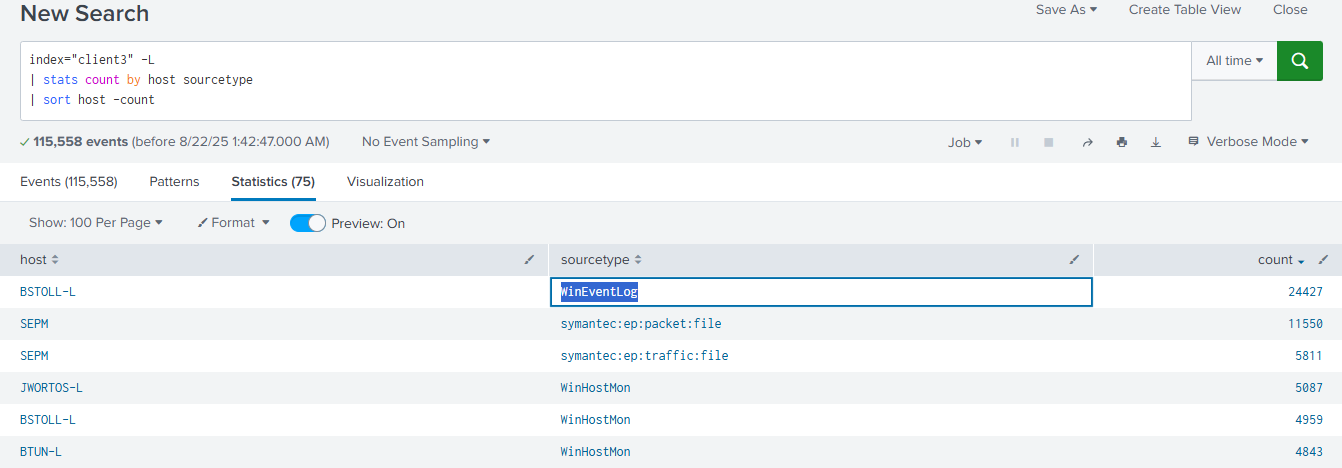
What password was assigned to the newly created user by root on Frothly’s local Linux machine?

ilovedavidverve

14.4.5 User created post-pwning

14.4.5 Retrieving the name of the user created post-compromise

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/49789a59-1441-4192-8119-b109414b009c)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index="client3" -L

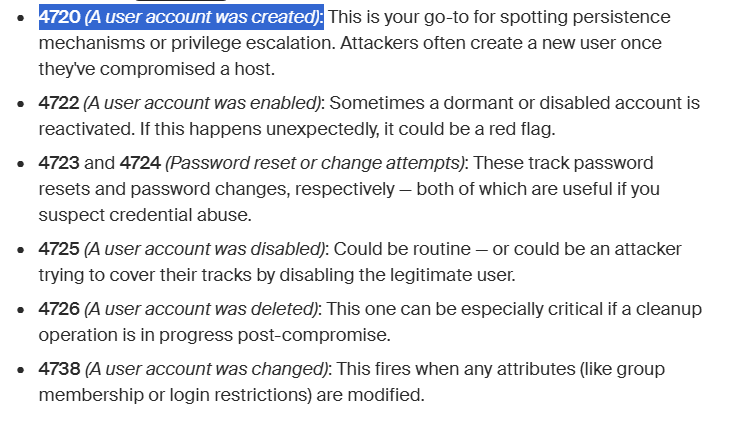
| stats count by host sourcetype

| sort host -count

Question

Which sourcetype is the most useful to go digging into?

WinEventLog



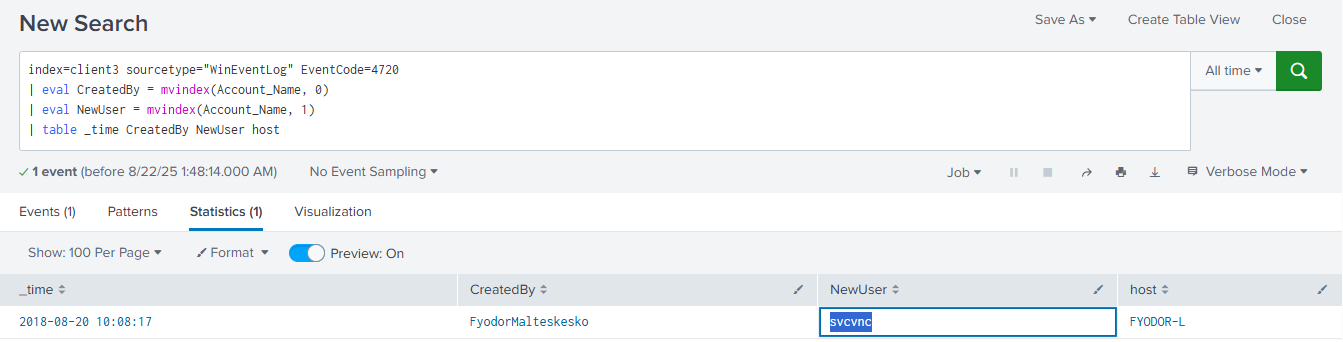
<https://tripleten.com/trainer/csa/lesson/49789a59-1441-4192-8119-b109414b009c/>

Question

Which EventCode is associated with user creation?

4720

2018-08-20 10:08:17



index=client3 sourcetype="WinEventLog" EventCode=4720

| eval CreatedBy = mvindex(Account\_Name, 0)

| eval NewUser = mvindex(Account\_Name, 1)

| table \_time CreatedBy NewUser host

Question

After the system was breached, what is the name of the new user account that was created?

svcvnc

14.4.6 1337-port process

14.4.6 Tracing the process responsible for listing on an elite port

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/6bbcb26f-2e8a-4026-aed9-3fb472af9001)**.** Use this worksheet to keep notes as you complete it. |
| --- |

| 8/20/18  11:55:34.000 AM |
| --- |



index=client3 sourcetype=osquery:results host=hoth name=\*port\* (1337 OR 31337)

Question

Which process ID corresponds to the process listening on a leet-numbered port?

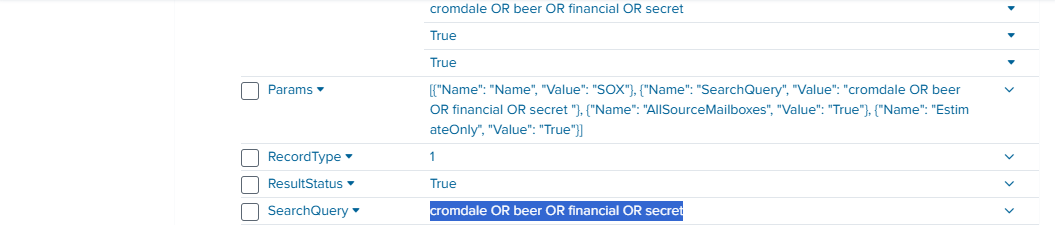
14356

14.4.7 Search query in URI

14.4.7 Decoding a search query from a URI

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/f6006427-9fe3-44c3-bb1f-c106cc542e3e)**.** Use this worksheet to keep notes as you complete it. |
| --- |

| 8/20/18  10:48:28.000 AM |
| --- |



index=client3 sourcetype=o365:management:activity Operation="New-MailboxSearch"

| table src\_ip, UserId, Params

Question

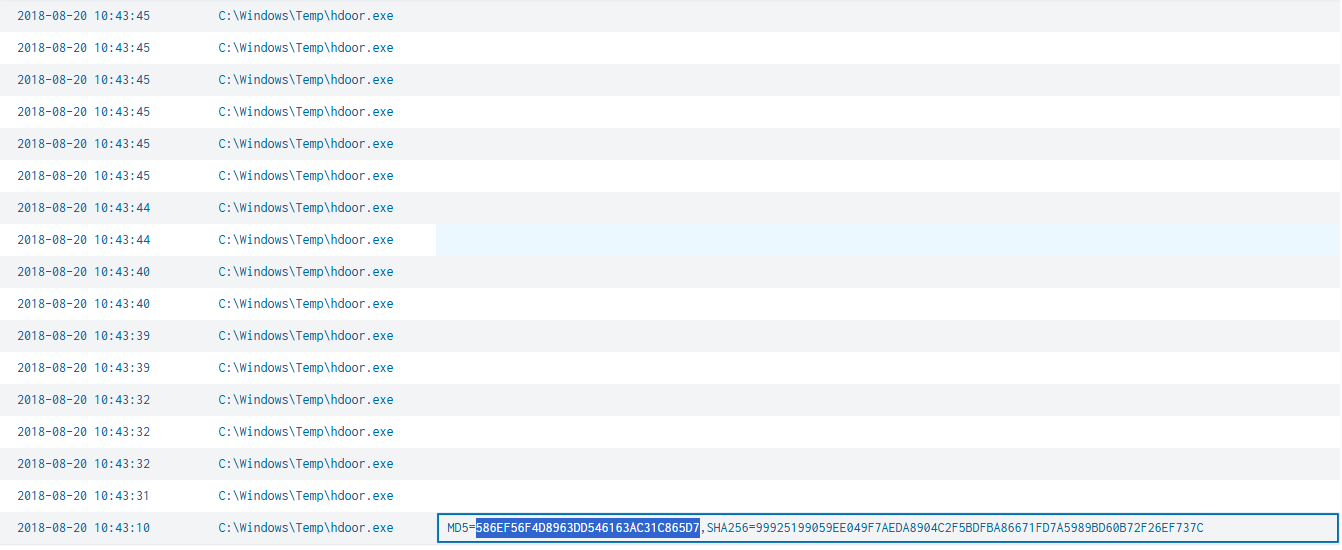
What was the search string used in the query that came from an external IP address associated with Frothly’s mail server?

cromdale OR beer OR financial OR secret

14.4.8 MD5 of scanning binary

14.4.8 Identifying the MD5 associated with the scanning binary

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/0f3856e8-77b7-43b1-b3d2-a1c90cdd1c6a)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index=client3 host="FYODOR-L" source="WinEventLog:Microsoft-Windows-Sysmon/Operational"

| rex field=\_raw "<Data Name='Image'>(?<Image>[^<]+)</Data>"

| search Image="\*hdoor.exe"

| rex field=\_raw "<Data Name='Hashes'>(?<Hashes>[^<]+)</Data>"

| table \_time Image Hashes

Question

What is the MD5 hash of the file that was downloaded to Fyodor’s system and used to perform a network scan at Frothly?

586EF56F4D8963DD546163AC31C865D7

14.4.9 Groups user added to post-pwning

14.4.9 Confirming the groups the user was added to post-compromise

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/bf51350b-3b2e-48ea-a0af-5e61a3a78f3b)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index=client3 source=WinEventLog:Security EventCode=4732 svcvnc

| table \_time, host, EventCode, Message, Group\_Name, member\_id

Question

Which user groups were assigned to this user [after the compromise of the endpoint](https://tripleten.com/trainer/csa/lesson/49789a59-1441-4192-8119-b109414b009c)?

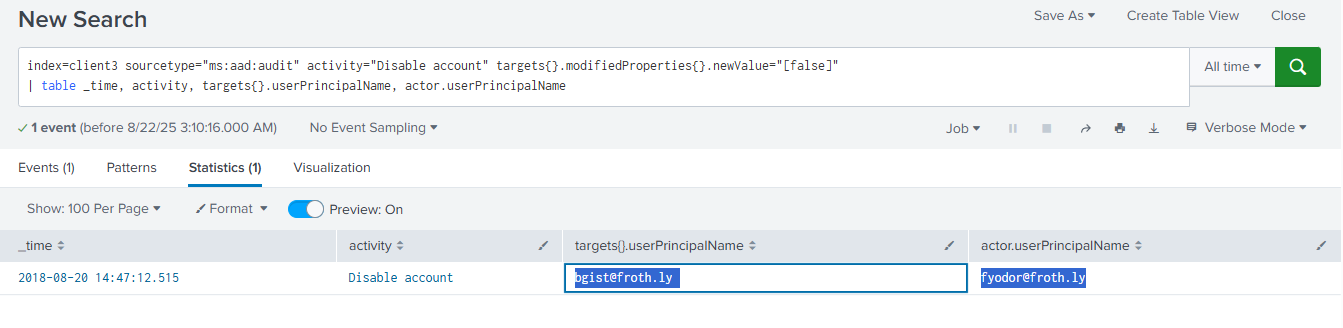
*Submit your answer in alphabetical order, comma-separated, with no spaces.*

Administrators,Users

14.4.10 Email address of disabled user

14.4.10 Extracting the disabled user’s email address

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/25bd39cb-b5cd-4181-a904-f7fe76b3d6d3)**.** Use this worksheet to keep notes as you complete it. |
| --- |

index=client3 sourcetype="ms:aad:audit" activity="Disable account" targets{}.modifiedProperties{}.newValue="[false]"

| table \_time, activity, targets{}.userPrincipalName, actor.userPrincipalName

Question

Which email address belonged to the disabled user during the attack?

[bgist@froth.ly](mailto:bgist@froth.ly)

Question

Which email address belonged to the user that performed the disabling during the attack?

[fyodor@froth.ly](mailto:fyodor@froth.ly)

14.5 A phishing attack

14.5.1 Artifact from removed malicious content

14.5.1 Pinpointing an artifact associated with removed malicious content

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/76934be3-97b5-4fdf-987e-b30f2bd26e3f)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/20/18

9:55:14.436 AM



index=client3 sourcetype="stream:smtp" "financial model" "FY2019" "macros" "enable macros"

Question

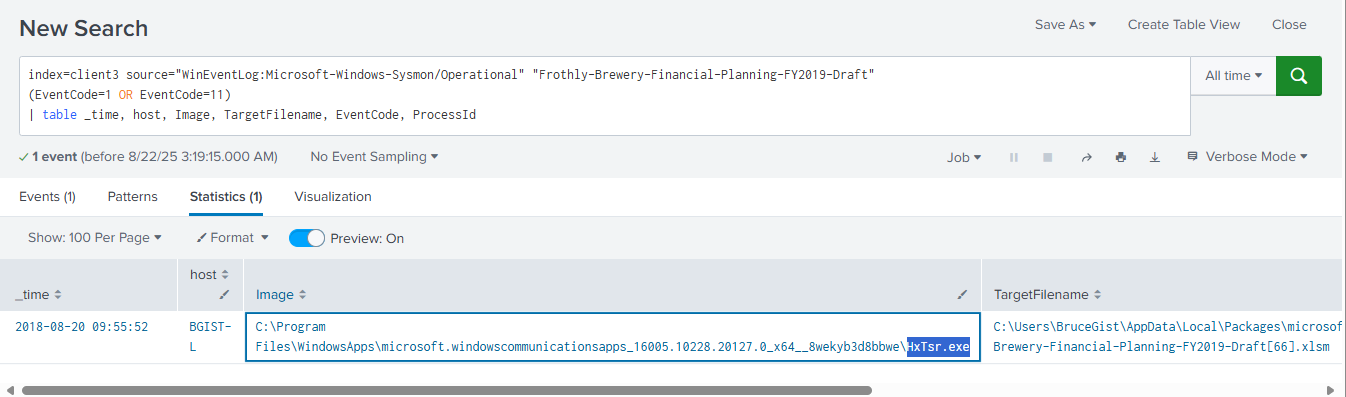
What is the filename (with extension) of the artifact left behind by the second phishing campaign sent to Frothly employees?

Frothly-Brewery-Financial-Planning-FY2019-Draft.xlsm

14.5.2 Executable embedded in malware

14.5.2 Unveiling the name of the executable embedded in the malware

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/8e499577-8842-4eca-96b8-8054ac16bd6c)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index=client3 source="WinEventLog:Microsoft-Windows-Sysmon/Operational" "Frothly-Brewery-Financial-Planning-FY2019-Draft"

(EventCode=1 OR EventCode=11)

| table \_time, host, Image, TargetFilename, EventCode, ProcessId

Question

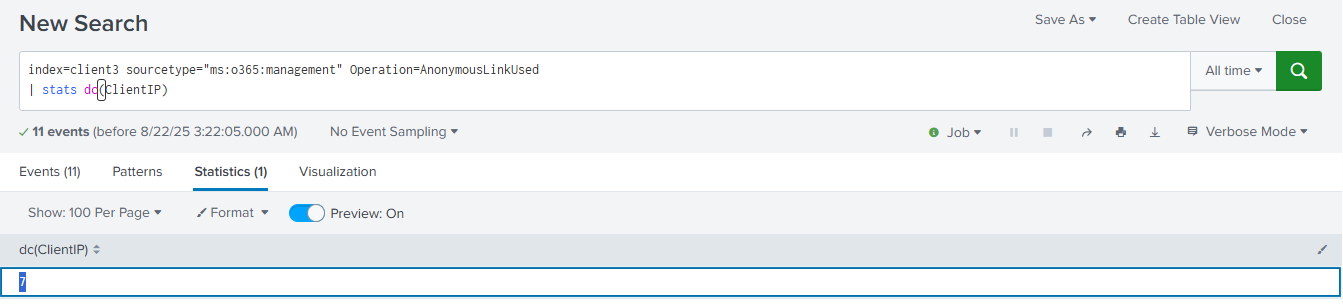
What is the name of the embedded executable (including file extension) found in the file you discovered in the [previous task](https://tripleten.com/trainer/csa/lesson/76934be3-97b5-4fdf-987e-b30f2bd26e3f)?

HxTsr.exe

14.5.3 Unique endpoints clicking the link

14.5.3 Calculating the number of unique endpoints that clicked the link

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/8b8c437d-6d48-4aaa-bd55-2cd83561f334)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index=client3 sourcetype="ms:o365:management" Operation=AnonymousLinkUsed

| stats dc(ClientIP)

Question

How many distinct IP addresses executed the malicious link file?

7

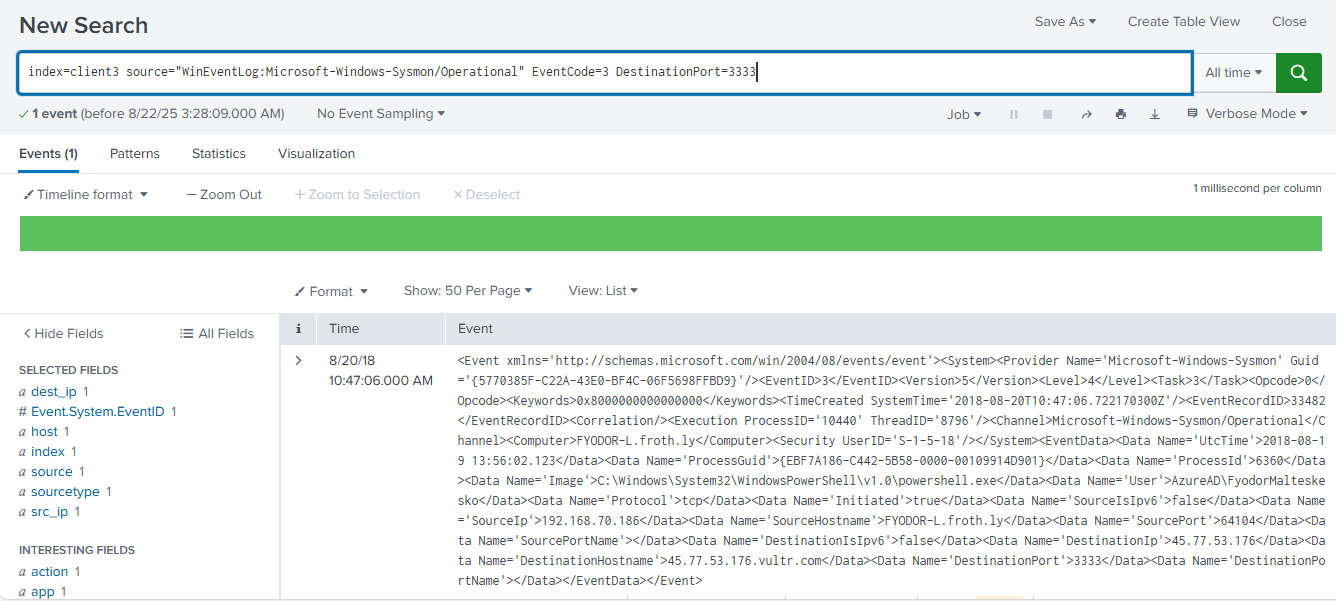
14.5.4 Port used to download pwntools

14.5.4 Confirming the port used to download malicious tools

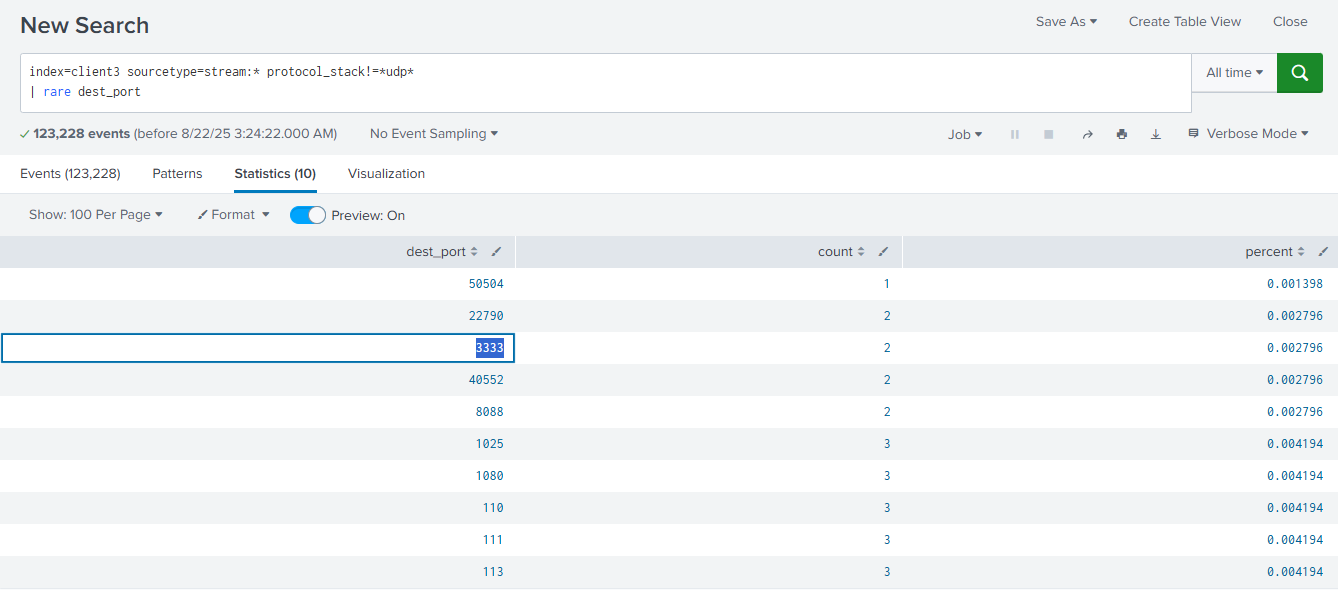
| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/176c78c1-6d82-470c-9f7a-518b355e6b6a)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/20/18

10:47:06.000 AM



index=client3 source="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=3 DestinationPort=3333



index=client3 sourcetype=stream:\* protocol\_stack!=\*udp\*

| rare dest\_port

Question

Which port was used by the attacker to retrieve their attack toolkit?

3333

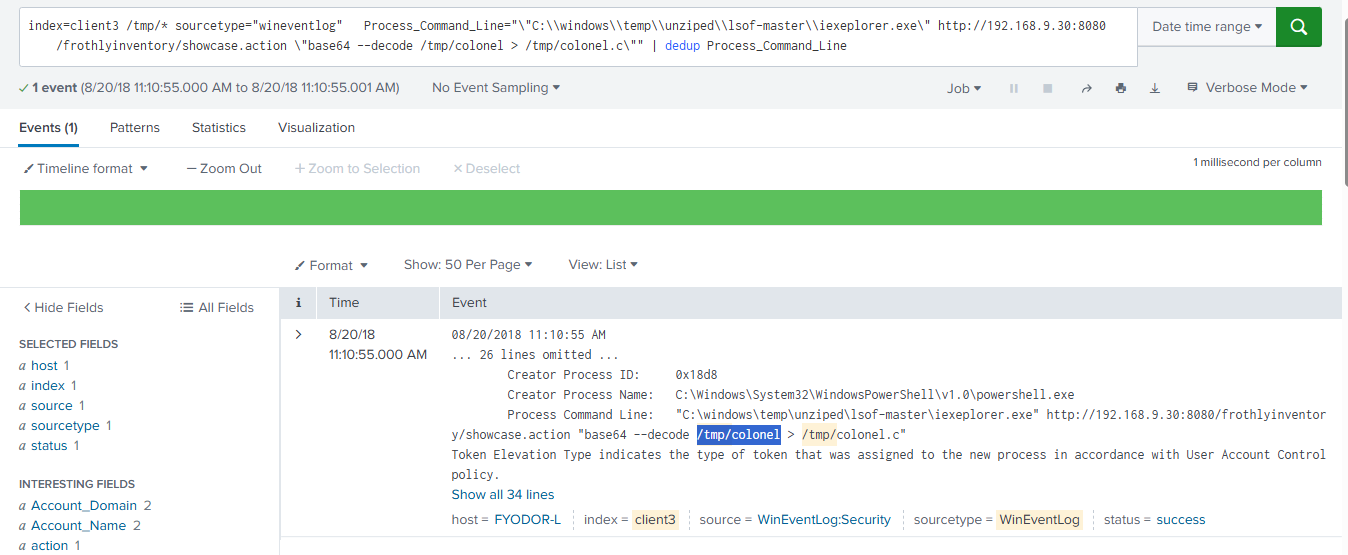
14.5.5 Remotely streamed files

14.5.5 Revealing remotely streamed files

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/dacbc503-89e1-454c-9481-e6bd2d36e738)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/20/18

11:10:55.000 AM

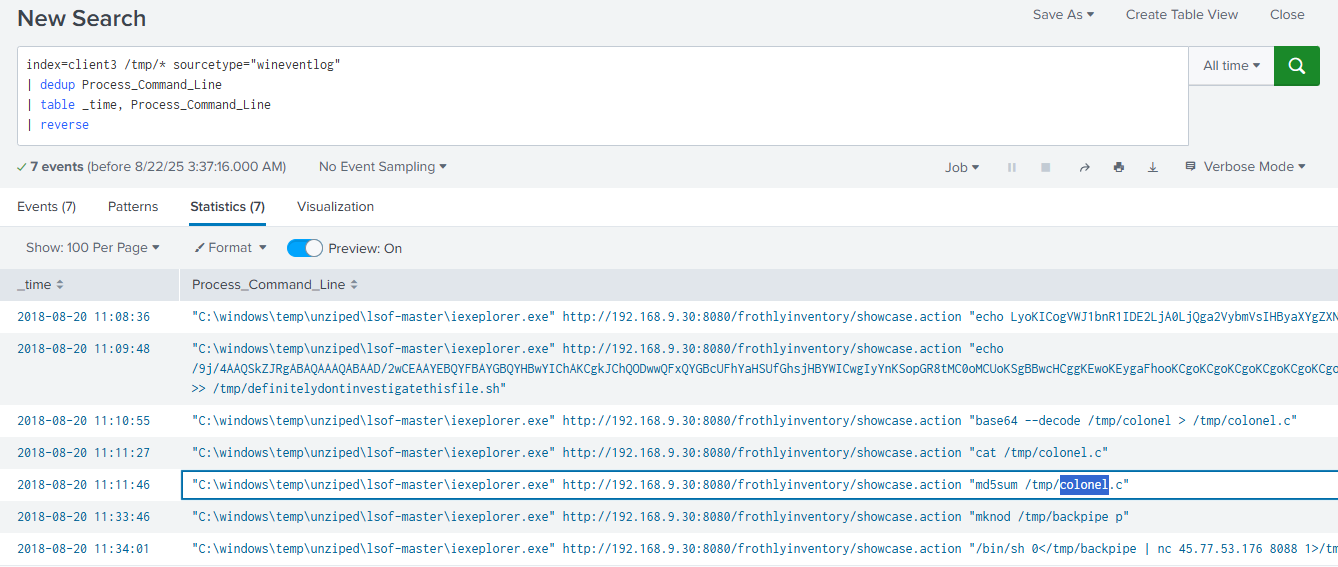


index=client3 /tmp/\* sourcetype="wineventlog" Process\_Command\_Line="\"C:\\windows\\temp\\unziped\\lsof-master\\iexeplorer.exe\" http://192.168.9.30:8080/frothlyinventory/showcase.action \"base64 --decode /tmp/colonel > /tmp/colonel.c\"" | dedup Process\_Command\_Line

Question

Select the new search pivot you could add to your query to zero in on the files created within the echo command.

(/tmp/colonel OR /tmp/\*.sh)



index=client3 /tmp/\* sourcetype="wineventlog"

| dedup Process\_Command\_Line

| table \_time, Process\_Command\_Line

| reverse

Question

What are the names of the two files (comma-separated, alphabetically) that were remotely streamed to /tmp during the intrusion?

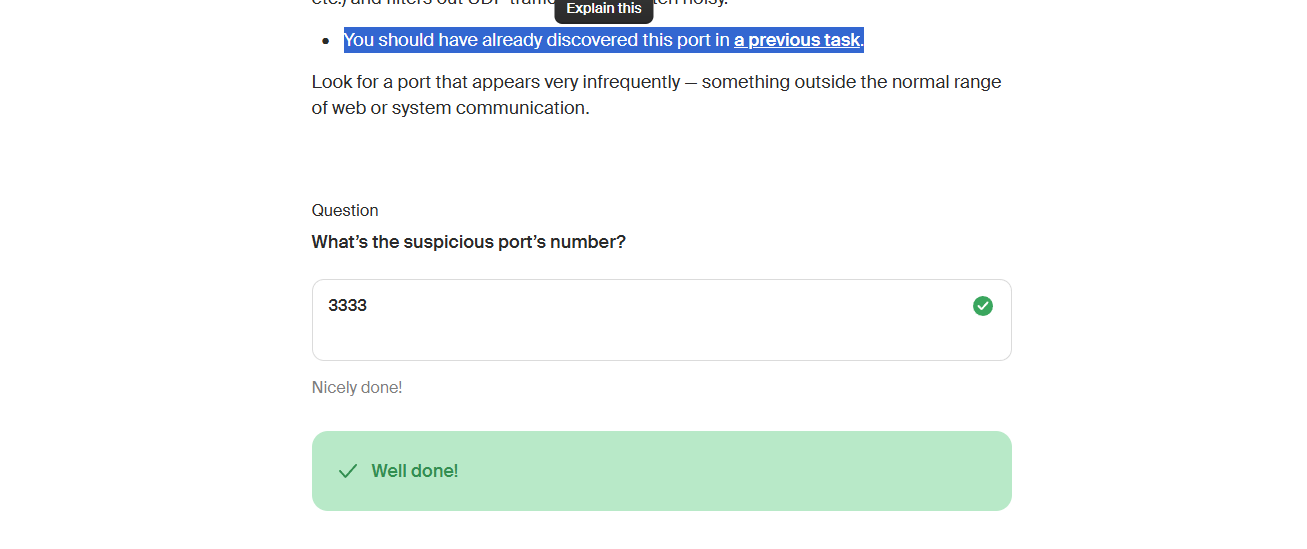
*(Submit answer listed alphabetically, comma-separated, no spaces.)*

colonel,definitelydontinvestigatethisfile.sh

14.5.6 File containing malicious tools

14.5.6 Inferring which file contains the malicious tools

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/461cd8a3-76ec-4ba8-b25e-ed0e84d51fa8)**.** Use this worksheet to keep notes as you complete it. |
| --- |

<https://tripleten.com/trainer/csa/lesson/461cd8a3-76ec-4ba8-b25e-ed0e84d51fa8/>

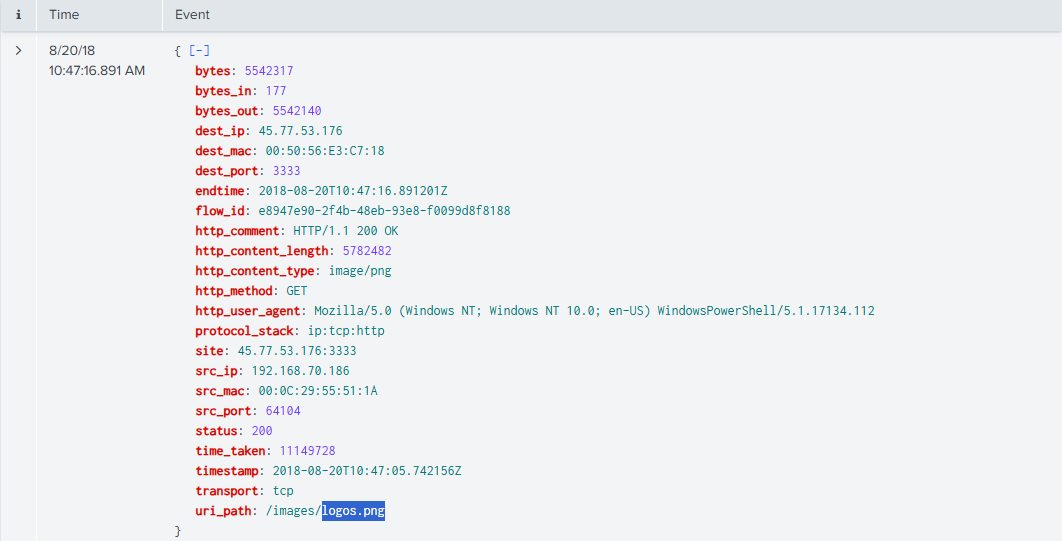
Question

What’s the suspicious port’s number?

3333

8/20/18

10:47:16.891 AM



index=client3 sourcetype=stream:\* protocol\_stack!=\*udp\* dest\_port=3333

Question

Which file likely contains the attacker’s toolkit (based on [earlier findings](https://tripleten.com/trainer/csa/lesson/176c78c1-6d82-470c-9f7a-518b355e6b6a))?

logos.png

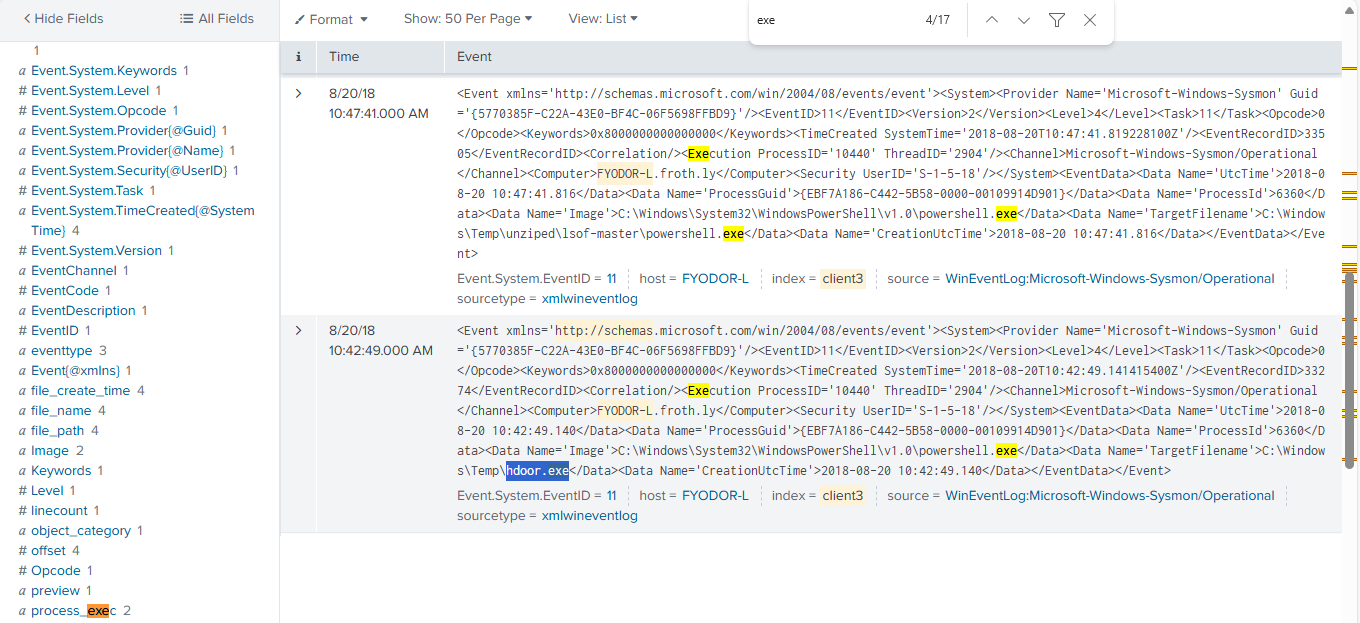
14.5.7 Malware uploaded to DA's endpoint

14.5.7 Figuring out the first malicious executable uploaded to the DA’s compromised endpoint

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/a413487b-46cf-466f-b7ed-17b7b64d1e69)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/20/18

10:42:49.000 AM



index=client3 FYODOR-L TargetFilename="\*.exe" EventCode=11

Question

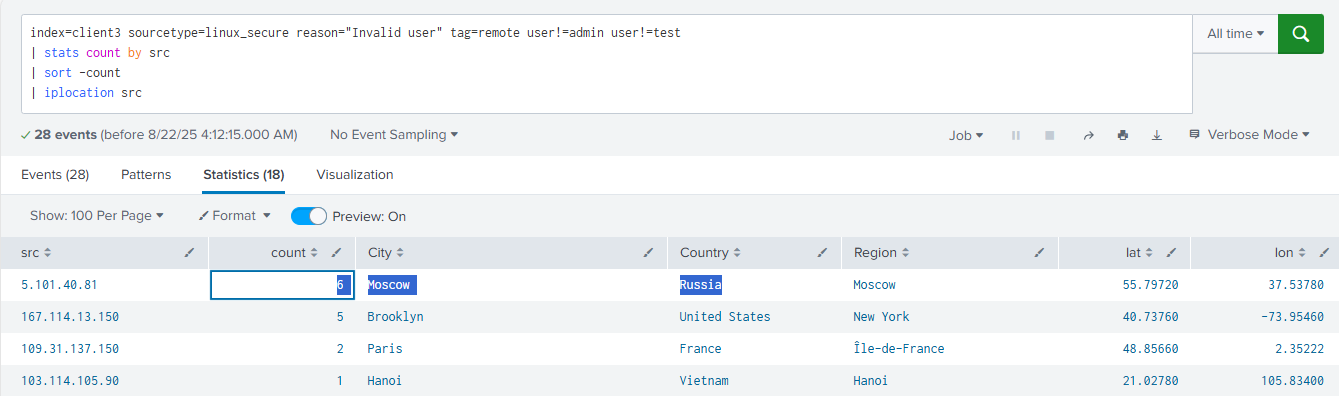
What is the name of the first executable file uploaded to the domain admin’s compromised machine?

hdoor.exe

14.5.8 Geolocating attack country

14.5.8 Geolocating the country from which an attack is originating

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/d11e3cd9-dac2-4957-9315-8f651f961681)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index=client3 sourcetype=linux\_secure reason="Invalid user" tag=remote user!=admin user!=test

| stats count by src

| sort -count

| iplocation src

Question

Which country is the origin of a minor brute-force or password spray attempt targeting Frothly's web servers?

Russia

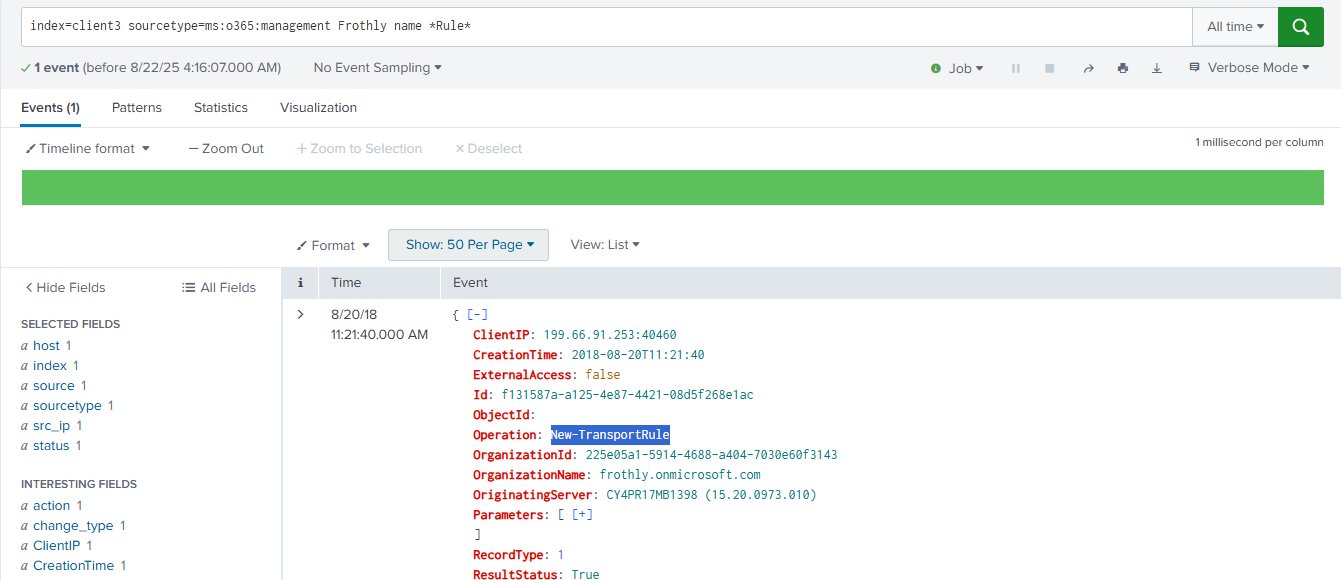
14.5.9 BBC rule created by attacker

14.5.9 Discovering details about a new BCC rule created by the adversary

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/d8a1eca6-41ab-49e1-8b7b-d5bf2d9326cc)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/20/18

11:21:40.000 AM

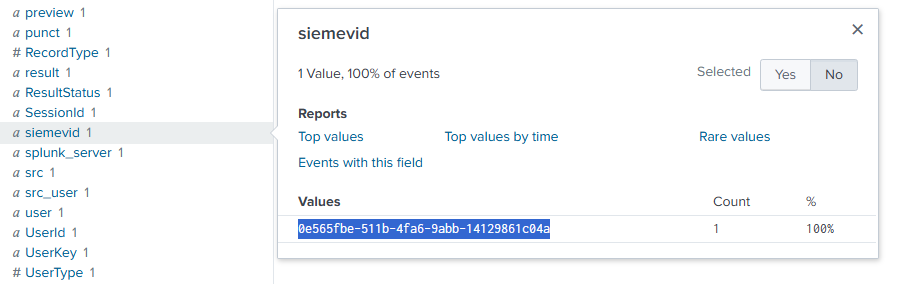


index=client3 sourcetype=ms:o365:management Frothly name \*Rule\*

Question

Which value in the Operation field for your search results looks the most promising for a rule creation event?

New-TransportRule



index=client3 sourcetype=ms:o365:management Frothly name \*Rule\* Operation="New-TransportRule"

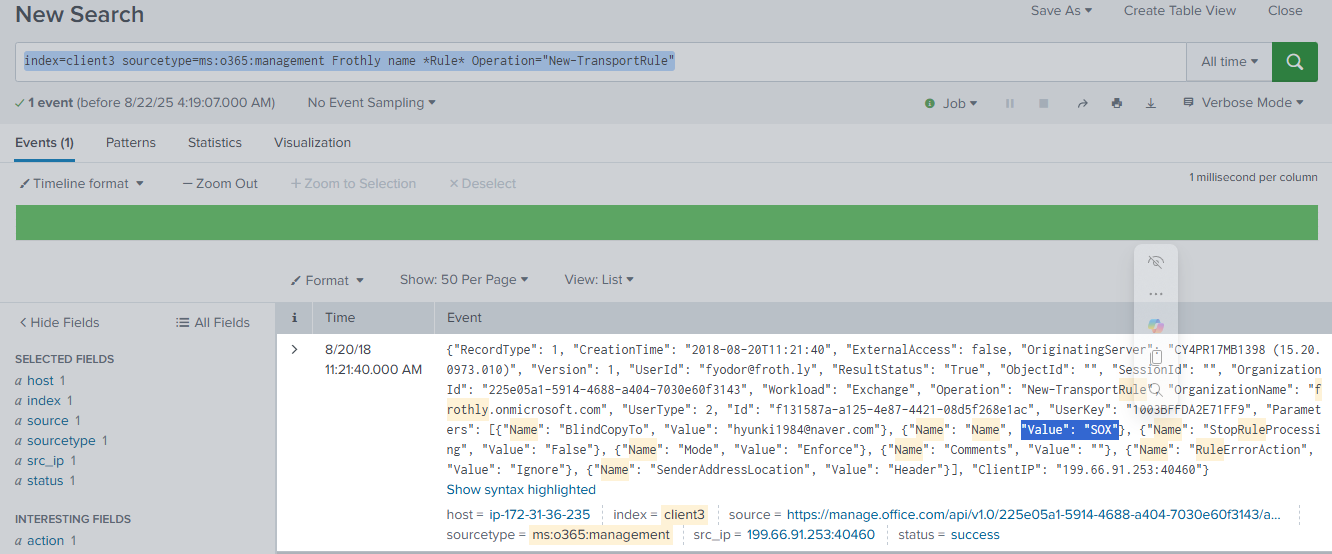
Question

What is the value assigned to the siemevid field within the single event log that appears with this new fine-tuned search query?

0e565fbe-511b-4fa6-9abb-14129861c04a

8/20/18

11:21:40.000 AM



index=client3 sourcetype=ms:o365:management Frothly name \*Rule\* Operation="New-TransportRule"

Question

What value was assigned to the Name parameter in the adversary’s BCC rule for exfiltrating Frothly’s email?

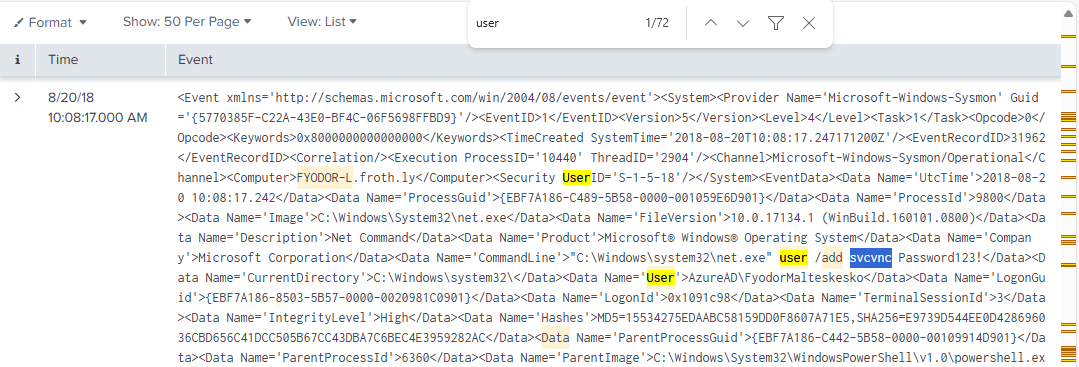
Sox

14.5.10 Post-pwn password creation

14.5.10 Determining the password of the user created post-compromise

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/de366159-279c-4fa3-8969-ff560903b91a)**.** Use this worksheet to keep notes as you complete it. |
| --- |

| 8/20/18  10:08:17.000 AM |
| --- |



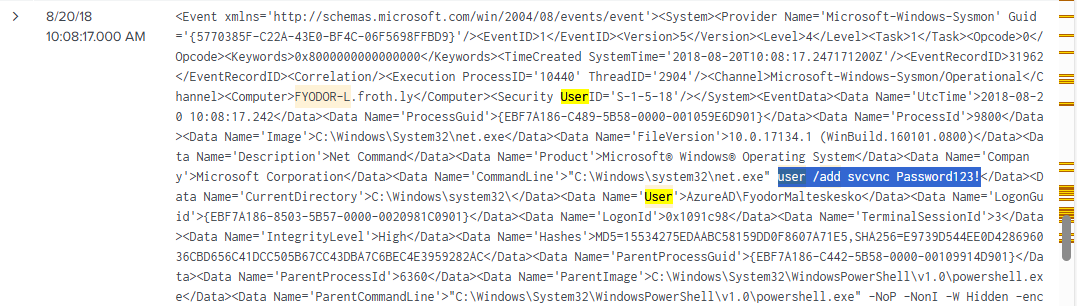
index=client3 FYODOR-L "add" "user" NOT "Network Connected Devices Auto-Setup" NOT ec2-user sourcetype!="stream:mysql"

Question

Which username was added to FYODOR-L?

svcvnc

| 8/20/18  10:08:17.000 AM |
| --- |



index=client3 FYODOR-L "add" "user" NOT "Network Connected Devices Auto-Setup" NOT ec2-user sourcetype!="stream:mysql"

Question

What password was set for the new user created on the compromised endpoint?

Password123!

14.5.11 Customer data exposed to attacker

14.5.11 Extracting the number of customers whose data was exposed to the adversary

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/bde820cf-3ce8-4bd6-b9a2-c5856c5317fb)**.** Use this worksheet to keep notes as you complete it. |
| --- |

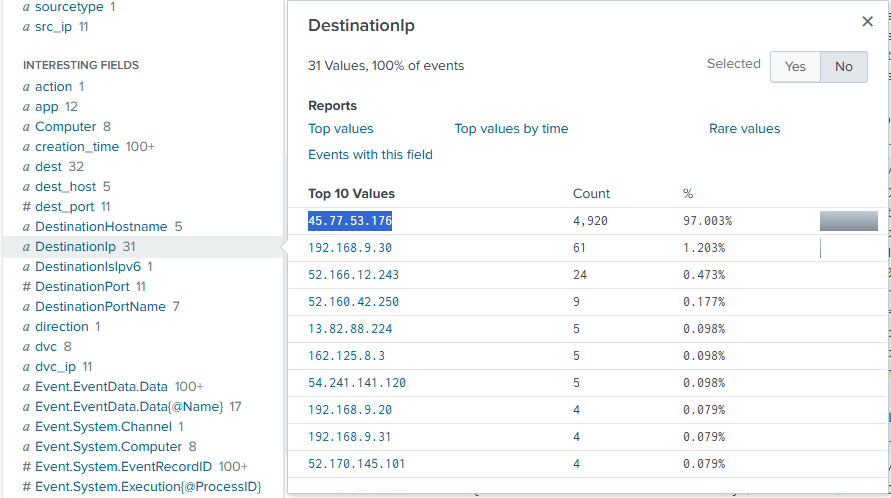
ADD YOUR NOTES HERE

14.6 Files, files, files

14.6.1 C2 server's URI

14.6.1 Retrieving the C2 server’s URI

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/adcda4e3-2c3a-4d98-960b-3776c9f2dcf4)**.** Use this worksheet to keep notes as you complete it. |
| --- |



index=client3 EventID=3 source="WinEventLog:Microsoft-Windows-Sysmon/Operational"

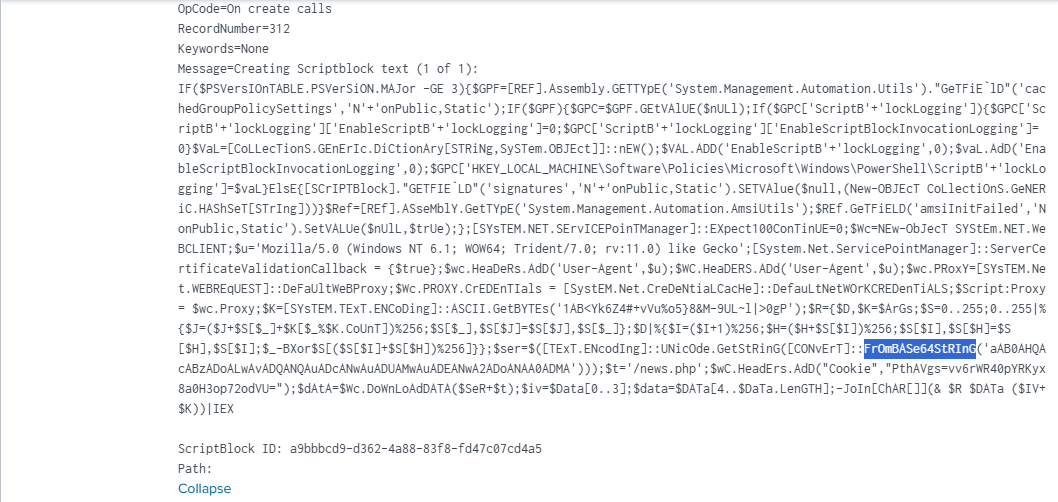
Question

What is the suspicious DestinationIp associated with a C2?

45.77.53.176

8/20/18

11:32:14.000 AM



index=client3 source=WinEventLog:Microsoft-Windows-PowerShell/Operational EventCode=4104 host=FYODOR-L

Question

What is the pivot contained in the Message field that likely contains a base64 blob?

FrOmBASe64StRInG



<https://chatgpt.com/c/68a802b1-8de4-8331-a6b2-46369393efde>

Question

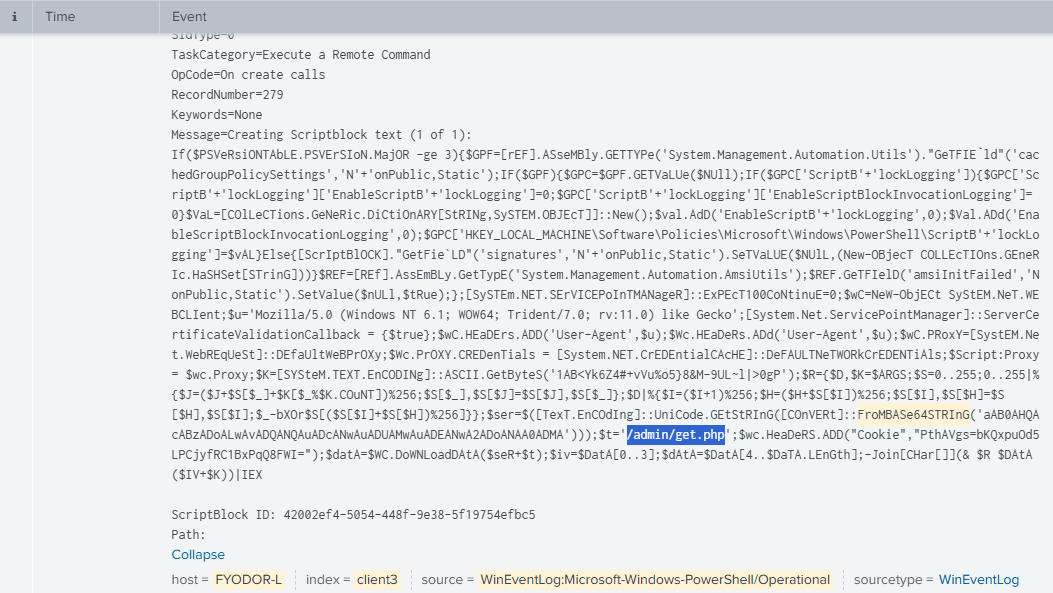
What is the decoded message?

<https://45.77.53.176:443>

aAB0AHQAcABzADoALwAvADQANQAuADcANwAuADUAMwAuADEANwA2ADoANAA0ADMA

8/20/18

10:07:07.000 AM



index=client3 source=WinEventLog:Microsoft-Windows-PowerShell/Operational host=FYODOR-L FromBase64String

Question

What is the full URI path that the C2 server accessed?

*e.g.,* if the complete URL is https://tripleten.com/usa-documents/outcomes/Outcomes\_Report\_2025.pdf, then the full URI path is /usa-documents/outcomes/Outcomes\_Report\_2025.pdf.

/admin/get.php

14.6.2 Hosts contacting C2 server

14.6.2 Identifying which hosts contacted the adversary’s C2 server

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/9c5c3d49-8fb6-4a07-abaf-73ef8981080c)**.** Use this worksheet to keep notes as you complete it. |
| --- |

| 8/20/18  10:01:00.000 AM |
| --- |



index=client3 /admin/get.php

Question

Which two short hostnames identify the Frothly endpoints that communicated with the adversary’s C2 servers?

*List in alphabetical order, separated with a comma; include no spaces.*

ABUNGST-L,FYODOR-L

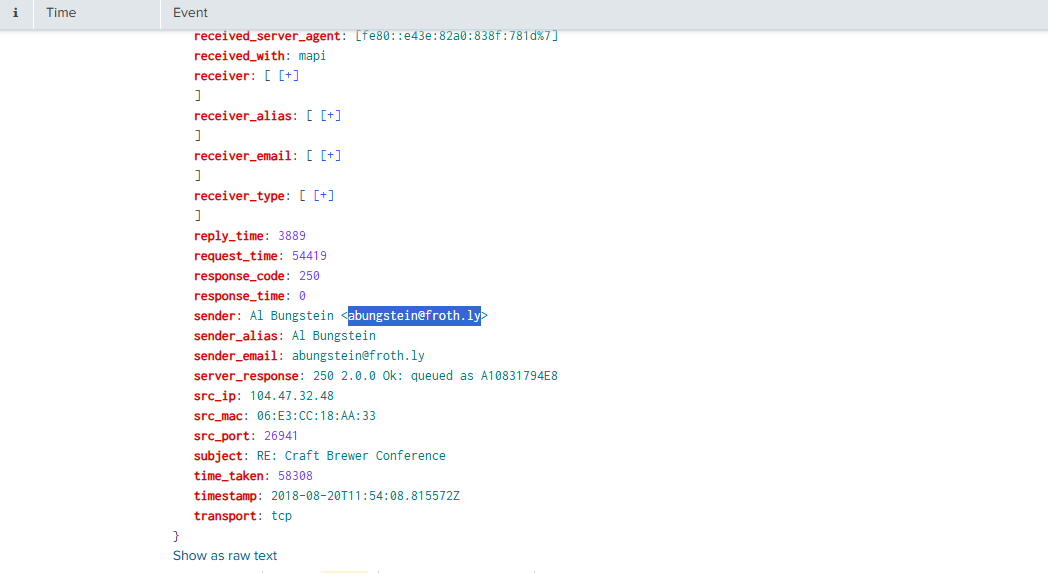
14.6.3 Contact info OSINT

14.6.3 Using OSINT to pivot off an indicator to find contact info

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/2f2877b8-ac7c-4a7b-a7d5-7d2121371402)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/20/18

11:54:08.872 AM

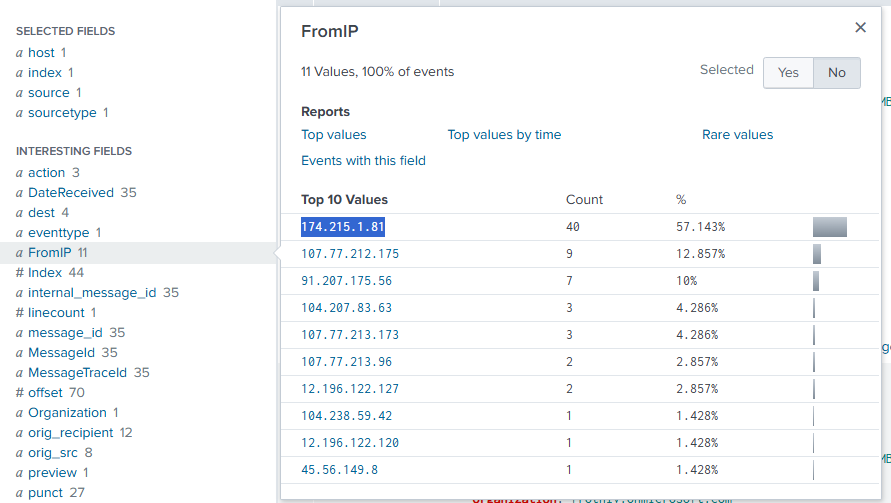


index=client3 Al Bungstein

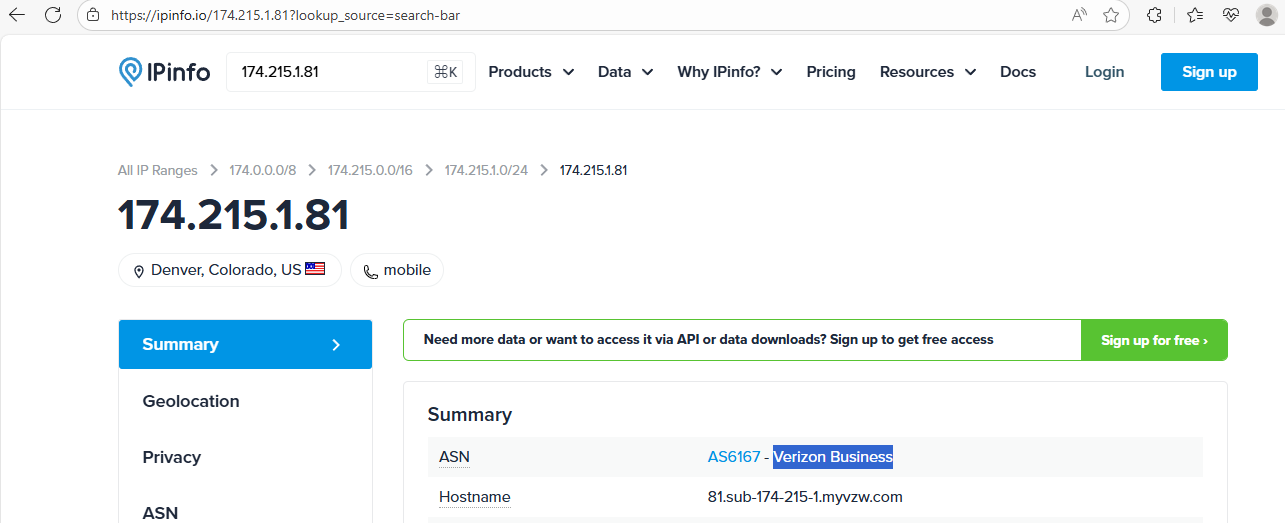
Question

What’s Al Bungstein’s email address?

[abungstein@froth.ly](mailto:abungstein@froth.ly)



index=client3 sourcetype=ms:o365:reporting:messagetrace [abungstein@froth.ly](mailto:abungstein@froth.ly)



<https://ipinfo.io/174.215.1.81?lookup_source=search-bar>

Question

What is the name of Al Bungstein’s mobile service provider?

*Two words separated by a space. Use Title Case.*

*Verizon Business*

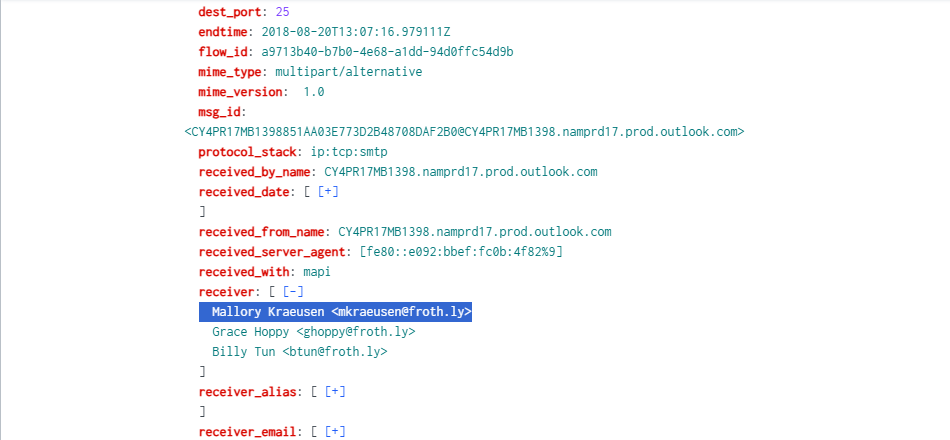
14.6.4 Max delta time

14.6.4 Calculating the max delta time between two timestamps

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/6e77bbfe-38a0-47c3-8378-0e9702a6f873)**.** Use this worksheet to keep notes as you complete it. |
| --- |

8/20/18

1:07:16.979 PM



index=client3 "Mallory Kraeusen"

Question

What is Mallory’s likely email address at Frothly?

[mkraeusen@froth.ly](mailto:mkraeusen@froth.ly)



index=client3 mkraeusen host="MKRAEUS-L"

Question

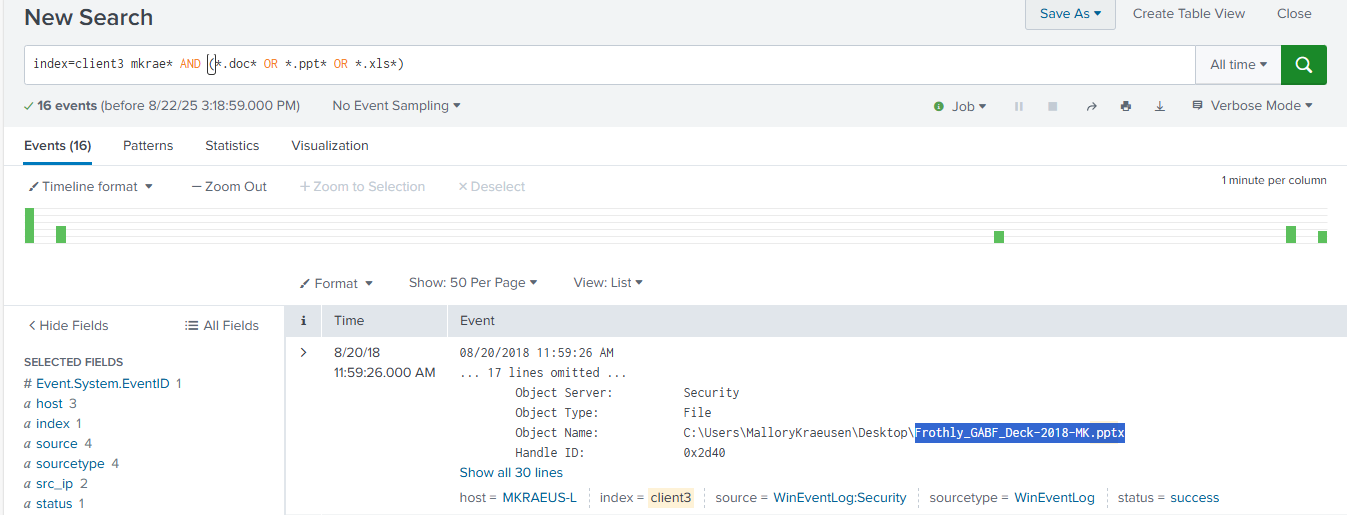
What is Mallory’s Windows device likely named?

*HINT: The hostnames are usually a max of 9 characters, meaning that it'll probably chop Mallory’s username off after 7 characters, leaving 2 characters for the* -L *naming convention.)*

MKRAEUS-L

8/20/18

11:59:26.000 AM



index=client3 mkrae\* AND (\*.doc\* OR \*.ppt\* OR \*.xls\*)

Question

What’s a likely useful file to pivot off of?

*HINT: It’s a PowerPoint!*

Frothly\_GABF\_Deck-2018-MK.pptx

8/20/18

10:31:14.000 AM



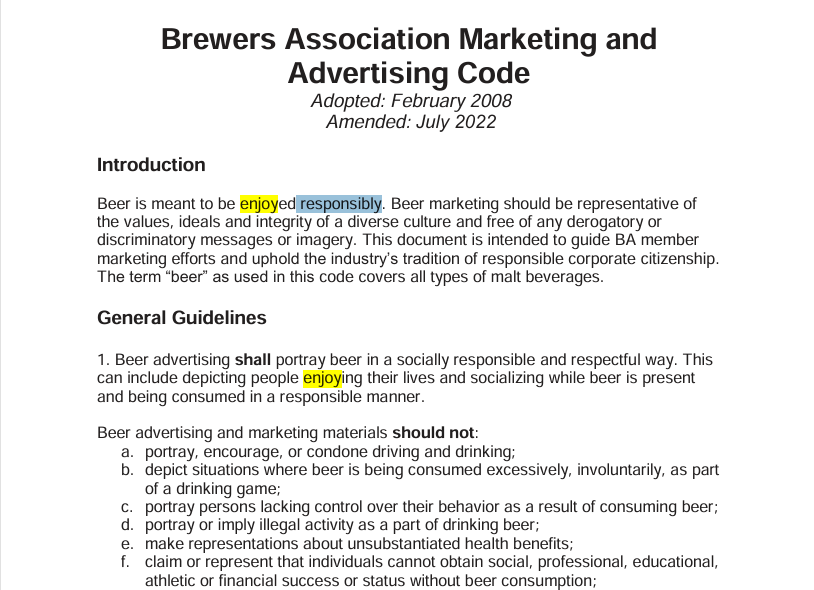
index=client3 Frothly\_GABF\_Deck-2018-MK.pptx sourcetype="code42:security"

Question

What’s the related document you managed to find?

*HINT: It’s a PDF!*

Ba\_advertising\_code\_overview.pdf

<https://www.brewersassociation.org/wp-content/uploads/2017/04/BA_Advertising_Code_Overview.pdf>

Question

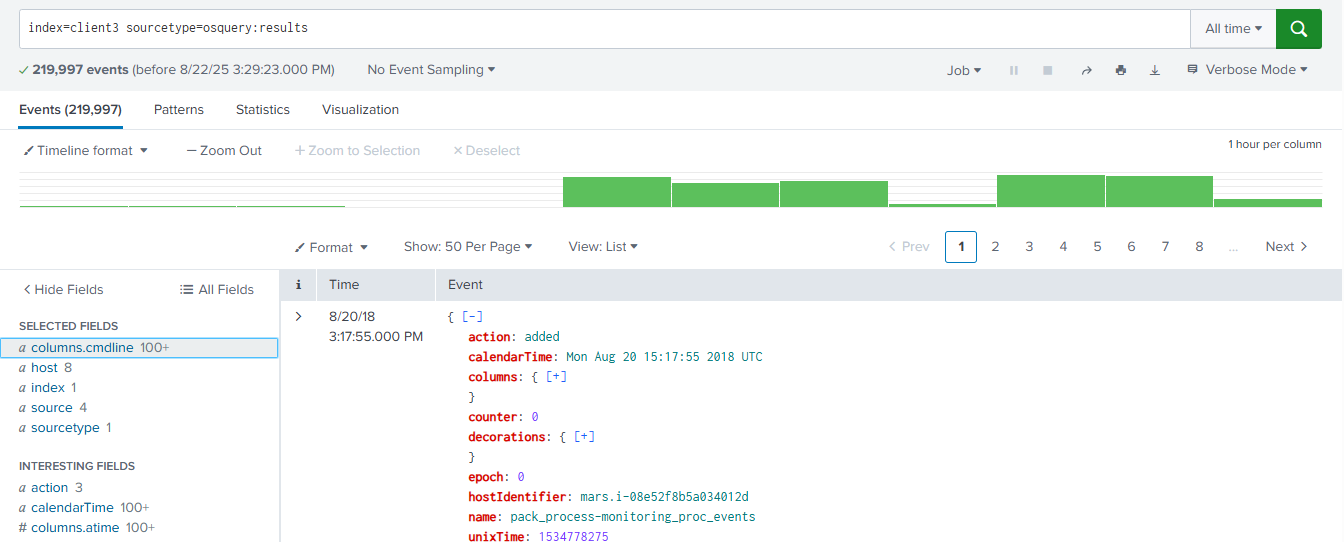
What single word best captures how Mallory’s research suggests beer should be enjoyed?

Responsibly

14.6.5 Contents of downloaded file

14.6.5 Revealing the contents of a downloaded file

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/c6fb0dea-29ff-4c1a-9e26-fb306239ddb9)**.** Use this worksheet to keep notes as you complete it. |
| --- |

index=client3 sourcetype=osquery:results

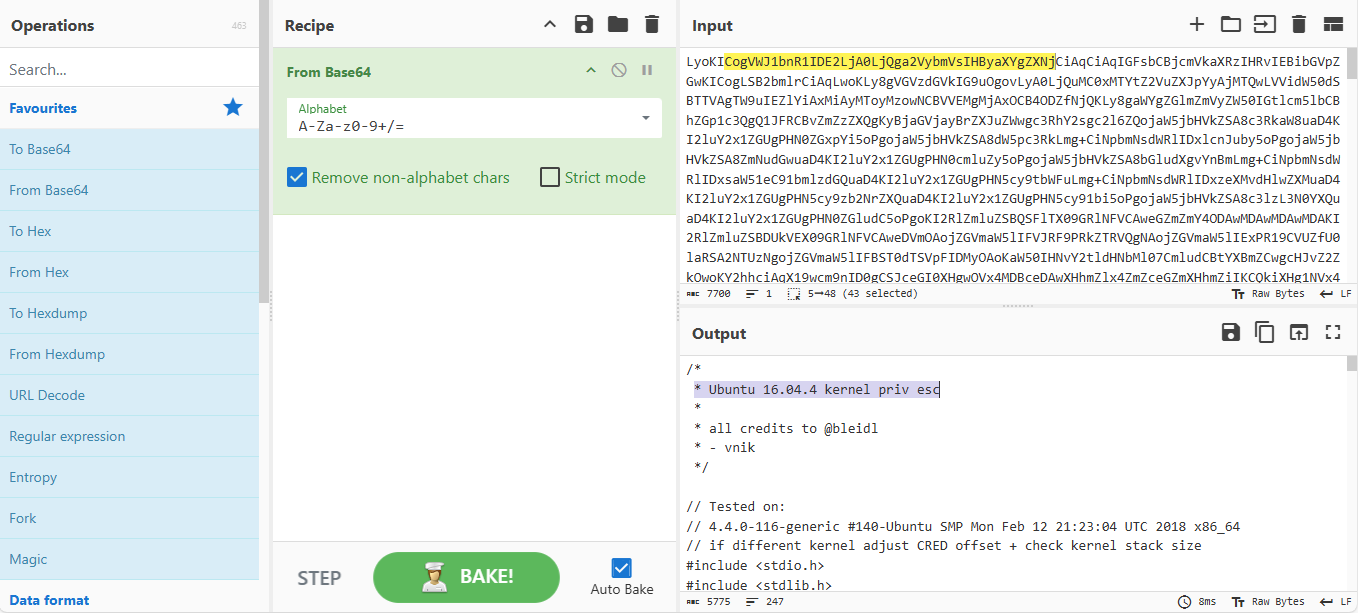
Question

Profile the osquery:results log source using the query index=client3 sourcetype=osquery:results and the All Fields button.

Which field appearing in this log source likely contains command-line arguments?

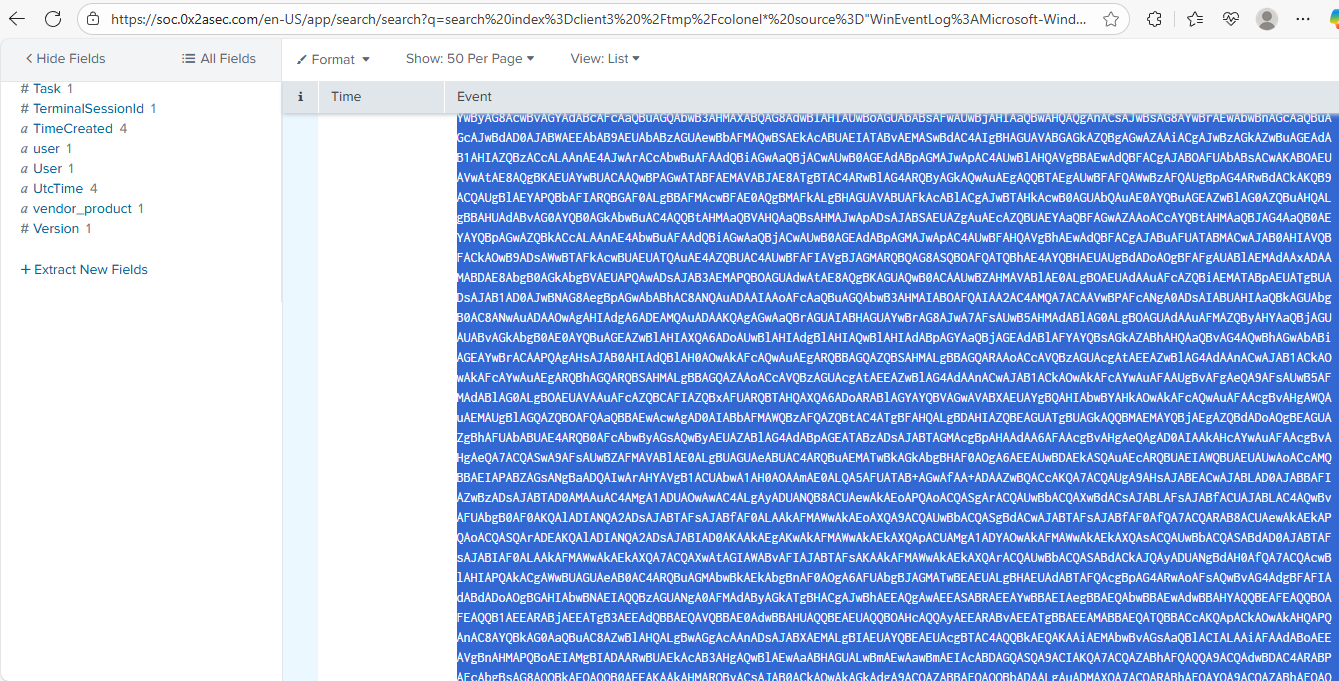
*If this information appears to be documented in multiple fields, opt for the one with a higher value in the # of Events and Event Coverage columns.*

Columns.cmdline



<https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=THlvS0lDb2dWV0oxYm5SMUlERTJMakEwTGpRZ2EyVnlibVZzSUhCeWFYWWdaWE5qQ2lBcUNpQXFJR0ZzYkNCamNtVmthWFJ6SUhSdklFQmliR1ZwWkd3S0lDb2dMU0IyYm1sckNpQXFMd29LTHk4Z1ZHVnpkR1ZrSUc5dU9nb3ZMeUEwTGpRdU1DMHhNVFl0WjJWdVpYSnBZeUFqTVRRd0xWVmlkVzUwZFNCVFRWQWdUVzl1SUVabFlpQXhNaUF5TVRveU16b3dOQ0JWVkVNZ01qQXhPQ0I0T0RaZk5qUUtMeThnYVdZZ1>

| 8/20/18  11:08:36.000 AM |
| --- |



index=client3 /tmp/colonel\* source="WinEventLog:Microsoft-Windows-Sysmon/Operational"

| dedup CommandLine

| reverse

Question

What is the full content of line 2 in the file that escalates tomcat8’s privileges to root?

\* Ubuntu 16.04.4 kernel priv esc

14.6.6 Privesc via process creation logs

14.6.6 Inspecting process creation logs for details about the adversary’s privesc method

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/8cf2c27e-7a11-4940-b393-65833967373e)**.** Use this worksheet to keep notes as you complete it. |
| --- |

ADD YOUR NOTES HERE

14.6.7 base64 image decoded

14.6.7 Using CyberChef to decode a base64 string to a viewable image

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/91f226e2-2fc8-482a-9974-cb477aa967c1)**.** Use this worksheet to keep notes as you complete it. |
| --- |

ADD YOUR NOTES HERE

14.6.8 VPN user traffic

14.6.8 Determining which VPN user generated the most traffic

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/10a264f6-cba3-40eb-8145-79c255fc5c98)**.** Use this worksheet to keep notes as you complete it. |
| --- |

ADD YOUR NOTES HERE

14.6.9 IQR outliers

14.6.9 Isolating outliers using IQR

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/2ebddf04-538d-4e29-8a9e-e0ddc40bacee)**.** Use this worksheet to keep notes as you complete it. |
| --- |

ADD YOUR NOTES HERE

14.6.10 Privesc vuln OSINT

14.6.10 Using OSINT to identify the vulnerability associated with a Linux privesc

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/18ccae17-d243-4438-a52b-5865b519cb54)**.** Use this worksheet to keep notes as you complete it. |
| --- |

ADD YOUR NOTES HERE

14.6.11 Command exec vulnerabilities

14.6.11 Using OSINT to establish the vulnerability used for command execution

| **Instructions for completing this task are located** [**here**](https://tripleten.com/trainer/csa/lesson/6876ec54-140d-46f4-8c1d-8cadc52498ab)**.** Use this worksheet to keep notes as you complete it. |
| --- |

ADD YOUR NOTES HERE