AWS Incident Response via CloudTrail

Description

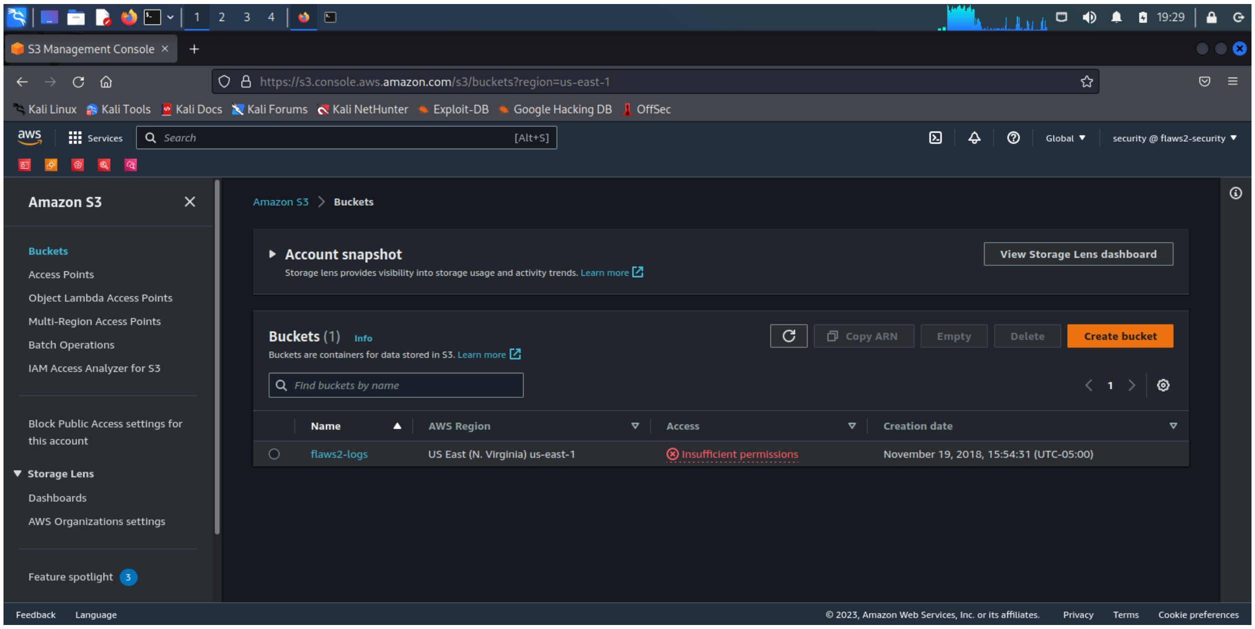
The purpose of this lab is to gain hands-on experience with conducting incident response on a compromised S3 bucket and IAM user within AWS. The lab involves identifying indicators of compromises on AWS via reading CloudTrail logs and creating Bash scripts for efficient analysis.

Programs and Environments Used

- Hypervisor: VirtualBox
- Environment: Kali Linux

Walkthrough

First, we want to log into the compromised IAM user AWS account to verify the compromised bucket is within the account. The compromised bucket along with the CloudTrail logs stored within the bucket can be seen below:



Account snapshot

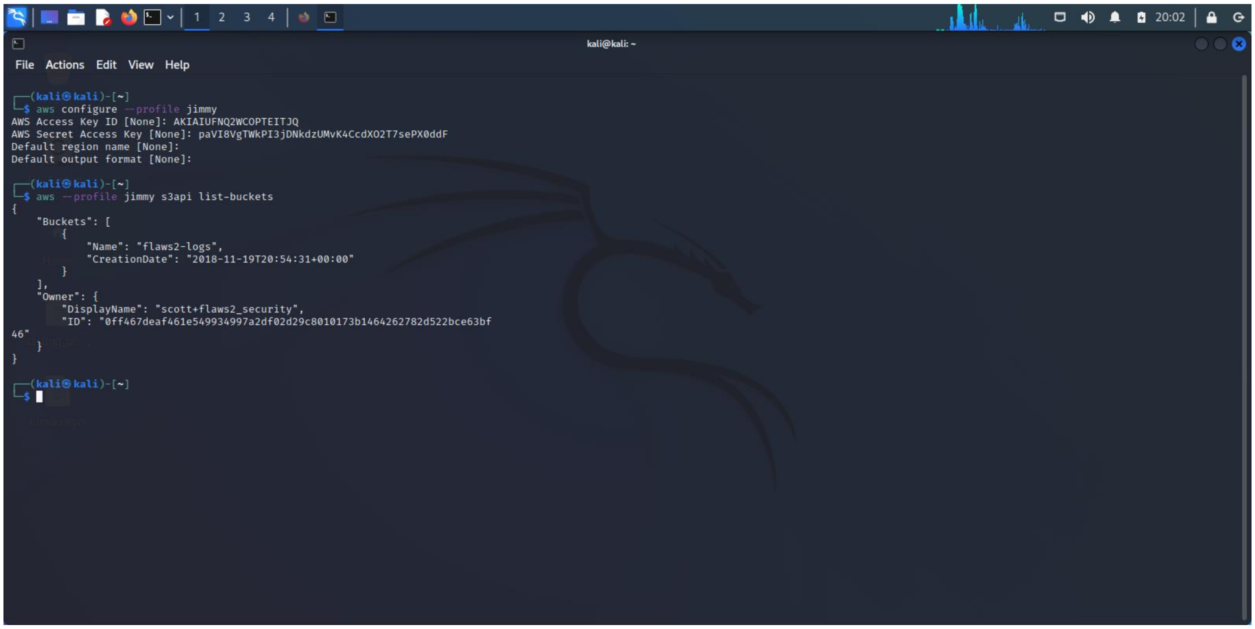
Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets (1) Info

Buckets are containers for data stored in S3. Learn more

Name	AWS Region	Access	Creation date
flaws2-logs	US East (N. Virginia) us-east-1	Insufficient permissions	November 19, 2018, 15:54:31 (UTC-05:00)

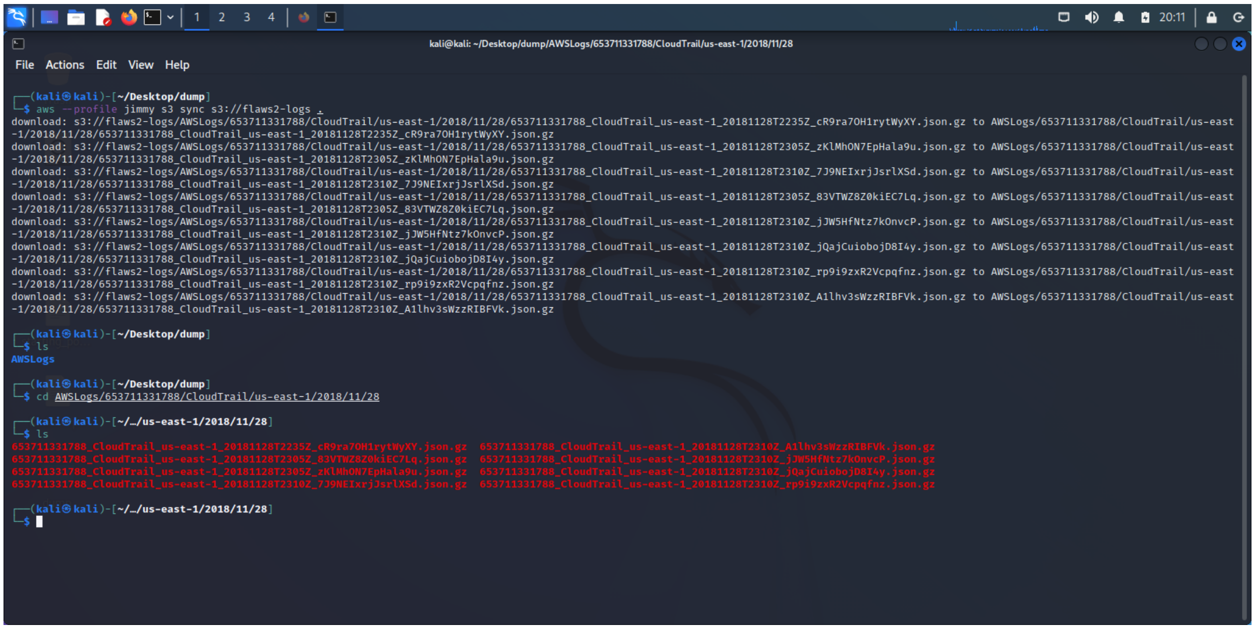
Once we verify the CloudTrail logs are present, we will then configure an AWS user profile via the Kali Linux command line named “jimmy” with the credentials of the compromised IAM user provided for this lab as seen below:



```
┌──(kali㉿kali)-[~]
└─$ aws configure --profile jimmy
AWS Access Key ID [None]: AKIAIUFNQ2WCOPTEITJQ
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]:

┌──(kali㉿kali)-[~]
└─$ aws --profile jimmy s3api list-buckets
{
    "Buckets": [
        {
            "Name": "flaws2-logs",
            "CreationDate": "2018-11-19T20:54:31+00:00"
        }
    ],
    "Owner": {
        "DisplayName": "scott+flaws2_security",
        "ID": "0ff467deaf461e549934997a2df02d29c8010173b1464262782d522bce63bf
46"
    }
}

┌──(kali㉿kali)-[~]
└─$ 
```

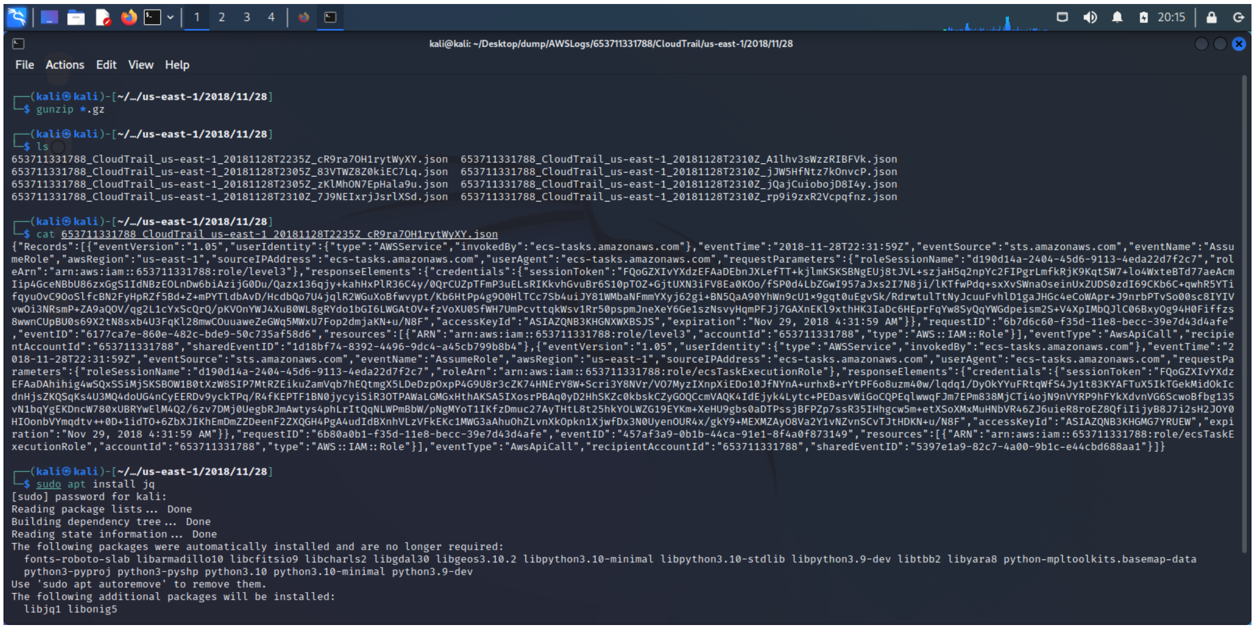
With the profile now created, we can use the “s3api list-buckets” command to verify that the same compromised bucket with the CloudTrail logs is present within the profile as seen above.

Afterwards, we would want to dump the contents of the buckets (which would be the CloudTrail logs) into a local directory of our Kali Linux machine for log analysis. To do that, we would sync the S3 bucket with our newly made profile into a directory. From there, we will enter into multiple directories until we can see all of the log files as .gz, which can be seen below:


1 2 3 4
20:11
kali@kali: ~/Desktop/dump/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28
File Actions Edit View Help

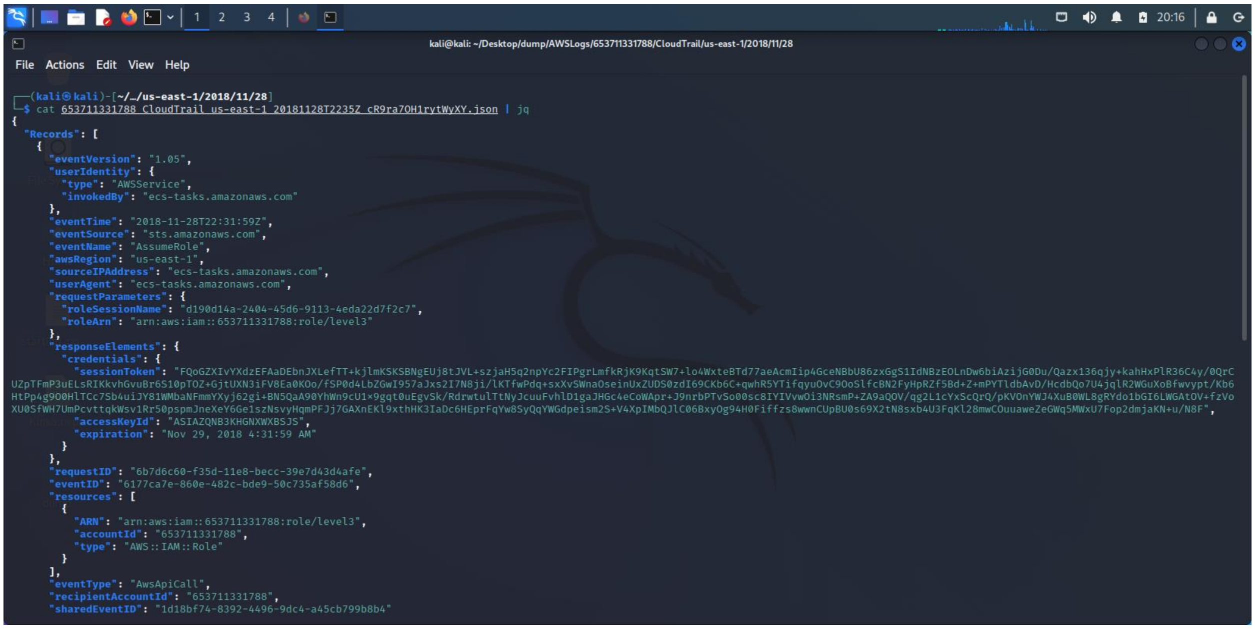
```
┌──(kali㉿kali)-[~/Desktop/dump]
└─$ aws --profile jimmy s3 sync s3://flaws2-logs .
download: s3://flaws2-logs/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28/653711331788_CloudTrail_us-east-1_20181128T2235Z_cR9ra7OH1rytWyXY.json.gz to AWSLogs/653711331788/CloudTrail/us-east
-1/2018/11/28/653711331788_CloudTrail_us-east-1_20181128T2235Z_cR9ra7OH1rytWyXY.json.gz
download: s3://flaws2-logs/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28/653711331788_CloudTrail_us-east-1_20181128T2305Z_zKlMhON7EpHala9u.json.gz to AWSLogs/653711331788/CloudTrail/us-east
-1/2018/11/28/653711331788_CloudTrail_us-east-1_20181128T2305Z_zKlMhON7EpHala9u.json.gz
download: s3://flaws2-logs/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28/653711331788_CloudTrail_us-east-1_20181128T2310Z_7J9NEIxrjJsrlXSd.json.gz to AWSLogs/653711331788/CloudTrail/us-east
-1/2018/11/28/653711331788_CloudTrail_us-east-1_20181128T2310Z_7J9NEIxrjJsrlXSd.json.gz
download: s3://flaws2-logs/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28/653711331788_CloudTrail_us-east-1_20181128T2305Z_83VTWZ8Z0kiEC7Lq.json.gz to AWSLogs/653711331788/CloudTrail/us-east
-1/2018/11/28/653711331788_CloudTrail_us-east-1_20181128T2305Z_83VTWZ8Z0kiEC7Lq.json.gz
download: s3://flaws2-logs/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28/653711331788_CloudTrail_us-east-1_20181128T2310Z_jJW5HfNtz7kOnvcP.json.gz to AWSLogs/653711331788/CloudTrail/us-east
-1/2018/11/28/653711331788_CloudTrail_us-east-1_20181128T2310Z_jJW5HfNtz7kOnvcP.json.gz
download: s3://flaws2-logs/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28/653711331788_CloudTrail_us-east-1_20181128T2310Z_jQajCuiobojD8I4y.json.gz to AWSLogs/653711331788/CloudTrail/us-east
-1/2018/11/28/653711331788_CloudTrail_us-east-1_20181128T2310Z_jQajCuiobojD8I4y.json.gz
download: s3://flaws2-logs/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28/653711331788_CloudTrail_us-east-1_20181128T2310Z_rp9i9zxR2Vcpqfnz.json.gz to AWSLogs/653711331788/CloudTrail/us-east
-1/2018/11/28/653711331788_CloudTrail_us-east-1_20181128T2310Z_rp9i9zxR2Vcpqfnz.json.gz
download: s3://flaws2-logs/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28/653711331788_CloudTrail_us-east-1_20181128T2310Z_A1lhv3sWzzRIBFVk.json.gz to AWSLogs/653711331788/CloudTrail/us-east
-1/2018/11/28/653711331788_CloudTrail_us-east-1_20181128T2310Z_A1lhv3sWzzRIBFVk.json.gz

┌──(kali㉿kali)-[~/Desktop/dump]
└─$ ls
AWSLogs

┌──(kali㉿kali)-[~/Desktop/dump]
└─$ cd AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28

┌──(kali㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ ls
653711331788_CloudTrail_us-east-1_20181128T2235Z_cR9ra7OH1rytWyXY.json.gz  653711331788_CloudTrail_us-east-1_20181128T2310Z_A1lhv3sWzzRIBFVk.json.gz
653711331788_CloudTrail_us-east-1_20181128T2305Z_83VTWZ8Z0kiEC7Lq.json.gz  653711331788_CloudTrail_us-east-1_20181128T2310Z_jJW5HfNtz7kOnvcP.json.gz
653711331788_CloudTrail_us-east-1_20181128T2305Z_zKlMhON7EpHala9u.json.gz  653711331788_CloudTrail_us-east-1_20181128T2310Z_jQajCuiobojD8I4y.json.gz
653711331788_CloudTrail_us-east-1_20181128T2310Z_7J9NEIxrjJsrlXSd.json.gz  653711331788_CloudTrail_us-east-1_20181128T2310Z_rp9i9zxR2Vcpqfnz.json.gz

┌──(kali㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ 
```

Since all of the logs are in .gz files, we will want to unzip them into .json files in order to read them. In addition, we will also install jq in which will let us be able to view .json files in a more readable format as seen below:



1
2
3
4
20:15
kali@kali: ~/Desktop/dump/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28
File
Actions
Edit
View
Help

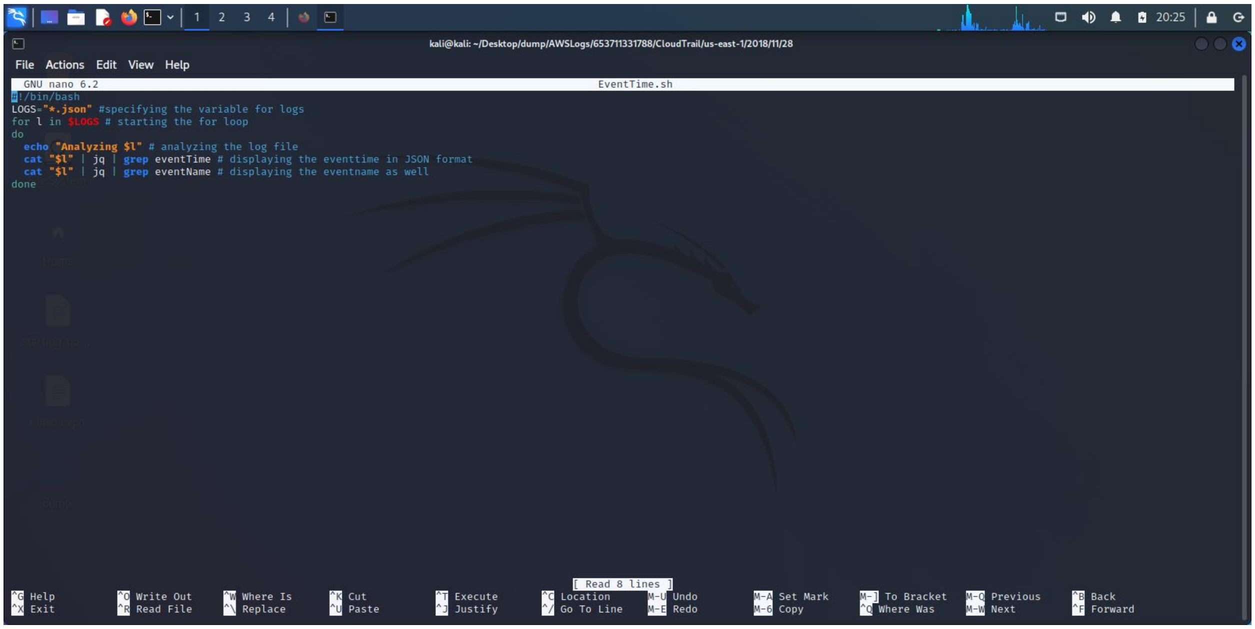
```
┌──(kali㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ gunzip *.gz

┌──(kali㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ ls
653711331788_CloudTrail_us-east-1_20181128T2235Z_cR9ra7OH1rytWyXY.json  653711331788_CloudTrail_us-east-1_20181128T2310Z_A1lhv3sWzzRIBFVk.json
653711331788_CloudTrail_us-east-1_20181128T2305Z_83VTWZ8Z0kiEC7Lq.json  653711331788_CloudTrail_us-east-1_20181128T2310Z_jJW5HfNtz7kOnvcP.json
653711331788_CloudTrail_us-east-1_20181128T2305Z_zKlMhON7EpHala9u.json  653711331788_CloudTrail_us-east-1_20181128T2310Z_jQajCuiobojD8I4y.json
653711331788_CloudTrail_us-east-1_20181128T2310Z_7J9NEIxrjJsrlXSd.json  653711331788_CloudTrail_us-east-1_20181128T2310Z_rp9i9zxR2Vcpqfnz.json

┌──(kali㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ cat 653711331788_CloudTrail_us-east-1_20181128T2235Z_cR9ra7OH1rytWyXY.json
{"Records":[{"eventVersion":"1.05","userIdentity":{"type":"AWSService","invokedBy":"ecs-tasks.amazonaws.com"},"eventTime":"2018-11-28T22:31:59Z","eventSource":"sts.amazonaws.com","eventName":"Assu
meRole","awsRegion":"us-east-1","sourceIPAddress":"ecs-tasks.amazonaws.com","userAgent":"ecs-tasks.amazonaws.com","requestParameters":{"roleSessionName":"d190d14a-2404-45d6-9113-4eda22d7f2c7","rol
eArn":"arn:aws:iam::653711331788:role/level3"},"responseElements":{"credentials":{"sessionToken":"FQoGZXIvYXdzEFAaDEbnJXLefTT+kjlmKSKSBNgEUj8tJVL+szjaH5q2npYc2FIPgrLmfkRjK9KqtSW7+lo4WxteBTd77aeAcm
Iip4GceNBbU86zxGgS1IdNBzEOLnDw6biAzijG0Du/Qazx136qjy+kahHxPlR36C4y/0QrCUZpTFmP3uELsRIKkvhGvuBr6S10pTOZ+GjtUXN3iFV8Ea0KOo/fSP0d4LbZGwI957aJxs2I7N8ji/lKTfwPdq+sxXvSWnaOseinUxZUDS0zdI69CKb6C+qwhR5YTi
fqyuOvC9OoSlfcBN2FyHpRZf5Bd+Z+mPYTldbAvD/HcdbQo7U4jqlR2WGuXoBfwvypt/Kb6HtPp4g9O0HlTCc7Sb4uiJY81WMbaNFmmYXyj62gi+BN5QaA90YhWn9cU1x9gqt0uEgvSk/RdrwtulTtNyJcuuFvhlD1gaJHGc4eCoWApr+J9nrbPTvSo00sc8IYIV
vwOi3NRsmP+ZA9aQOV/qg2L1cYxScQrQ/pKVOnYWJ4XuB0WL8gRYdo1bGI6LWGAtOV+fzVoXU0SfWH7UmPcvttqkWsv1Rr50pspmJneXeY6Ge1szNsvyHqmPFJj7GAXnEKl9xthHK3IaDc6HEprFqYw8SyQqYWGdpeism2S+V4XpIMbQJlC06BxyOg94H0Fiffzs
8wwnCUpBU0s69X2tN8sxb4U3FqKl28mwCOuuaweZeGWq5MWxU7Fop2dmjaKN+u/N8F","accessKeyId":"ASIAZQNB3KHGNXWXBSJS","expiration":"Nov 29, 2018 4:31:59 AM"}},"requestID":"6b7d6c60-f35d-11e8-becc-39e7d43d4afe"
,"eventID":"6177ca7e-860e-482c-bde9-50c735af58d6","resources":[{"ARN":"arn:aws:iam::653711331788:role/level3","accountId":"653711331788","type":"AWS::IAM::Role"}],"eventType":"AwsApiCall","recipie
ntAccountId":"653711331788","sharedEventID":"1d18bf74-8392-4496-9dc4-a45cb799b8b4"},{"eventVersion":"1.05","userIdentity":{"type":"AWSService","invokedBy":"ecs-tasks.amazonaws.com"},"eventTime":"2
018-11-28T22:31:59Z","eventSource":"sts.amazonaws.com","eventName":"AssumeRole","awsRegion":"us-east-1","sourceIPAddress":"ecs-tasks.amazonaws.com","userAgent":"ecs-tasks.amazonaws.com","requestPa
rameters":{"roleSessionName":"d190d14a-2404-45d6-9113-4eda22d7f2c7","roleArn":"arn:aws:iam::653711331788:role/ecsTaskExecutionRole"},"responseElements":{"credentials":{"sessionToken":"FQoGZXIvYXdz
EFAaDAhihig4wSQxSSiMjSKSBOW1B0tXzW8SIP7MtRZEikuZamVqb7hEQtmgX5LDeDzpOxpP4G9U8r3cZK74HNErY8W+Scri3Y8NVr/VO7MyzIXnpXiEDo10JfNYnA+urhxB+rYtPF6o8uzm40w/lqdq1/DyOkYYuFRtqWfS4Jy1t83KYAFTuX5IkTGekMidOkIc
dnHjsZKQSqKs4U3MQ4doUG4nCyEERDv9yckTPq/R4fKEPTF1BN0jycyiSiR3OTPAWaLGMGxHthAKSA5IXosrPBAq0yD2HhSKZc0kbskCZyGOQCcmVAQK4IdEjyk4Lytc+PEDasvWiGoCQPEqlwwqFJm7EPm838MjCTi4ojN9nVYRP9hFYkXdvnVG6ScwoBfbg135
vN1bqYgEKDncW780xUBRYwElM4Q2/6zv7DMj0UegbRJmAwtys4phLrItQqNLWPmBbW/pNgMYoT1IKfzDmuc27AyTHtL8t25hkYOLWZG19EYKm+XeHU9gbs0aDTPssjBFPZp7ssR35IHhgcw5m+etXSoXMxMuHNbVR46ZJ6uieR8roEZ8QfiIijyB8J7i2sH2JOY0
HIOonbVYmqdtv++0D+1idTO+6ZbXJIKhEmDmZZDeenF2ZXQGH4PgA4udIdBXnhVLzVFkEKc1MWG3aAhuOhZLvnXkOpkn1XjwfDx3N0UyenOUR4x/gkY9+MEXMZAyO8Va2Y1vNZvnSCvTJtHDKN+u/N8F","accessKeyId":"ASIAZQNB3KHGMG7YRUEW","expi
ration":"Nov 29, 2018 4:31:59 AM"}},"requestID":"6b80a0b1-f35d-11e8-becc-39e7d43d4afe","eventID":"457af3a9-0b1b-44ca-91e1-8f4a0f873149","resources":[{"ARN":"arn:aws:iam::653711331788:role/ecsTaskE
xecutionRole","accountId":"653711331788","type":"AWS::IAM::Role"}],"eventType":"AwsApiCall","recipientAccountId":"653711331788","sharedEventID":"5397e1a9-82c7-4a00-9b1c-e44cbd688aa1"}]}

┌──(kali㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ sudo apt install jq
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  fonts-roboto-slab libarmadillo10 libcfitsio9 libcharls2 libgdal30 libgeos3.10.2 libpython3.10-minimal libpython3.10-stdlib libpython3.9-dev libtbb2 libyara8 python-mpltoolkits.basemap-data
  python3-pyproj python3-pyshp python3.10 python3.10-minimal python3.9-dev
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libjq1 libonig5
```



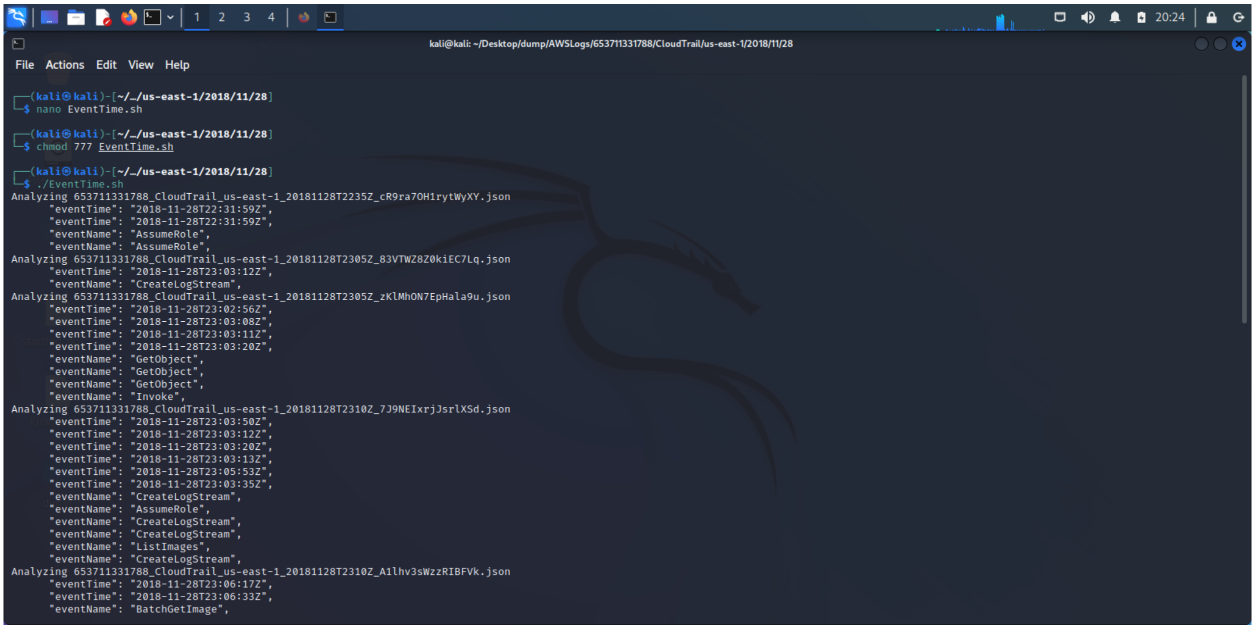
1
2
3
4
20:16
kali@kali: ~/Desktop/dump/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28
File
Actions
Edit
View
Help

```
┌──(kali㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ cat 653711331788_CloudTrail_us-east-1_20181128T2235Z_cR9ra7OH1rytWyXY.json | jq
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "AWSService",
        "invokedBy": "ecs-tasks.amazonaws.com"
      },
      "eventTime": "2018-11-28T22:31:59Z",
      "eventSource": "sts.amazonaws.com",
      "eventName": "AssumeRole",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "ecs-tasks.amazonaws.com",
      "userAgent": "ecs-tasks.amazonaws.com",
      "requestParameters": {
        "roleSessionName": "d190d14a-2404-45d6-9113-4eda22d7f2c7",
        "roleArn": "arn:aws:iam::653711331788:role/level3"
      },
      "responseElements": {
        "credentials": {
          "sessionToken": "FQoGZXIvYXdzEFAaDEbnJXLefTT+kjlmKSKSBNgEUj8tJVL+szjaH5q2npYc2FIPgrLmfkRjK9KqtSW7+lo4WxteBTd77aeAcmIip4GceNBbU86zxGgS1IdNBzEOLnDw6biAzijG0Du/Qazx136qjy+kahHxPlR36C4y/0QrC
UZpTFmP3uELsRIKkvhGvuBr6S10pTOZ+GjtUXN3iFV8Ea0KOo/fSP0d4LbZGwI957aJxs2I7N8ji/lKTfwPdq+sxXvSWnaOseinUxZUDS0zdI69CKb6C+qwhR5YTifqyuOvC9OoSlfcBN2FyHpRZf5Bd+Z+mPYTldbAvD/HcdbQo7U4jqlR2WGuXoBfwvypt/Kb6
HtPp4g9O0HlTCc7Sb4uiJY81WMbaNFmmYXyj62gi+BN5QaA90YhWn9cU1x9gqt0uEgvSk/RdrwtulTtNyJcuuFvhlD1gaJHGc4eCoWApr+J9nrbPTvSo00sc8IYIVvwOi3NRsmP+ZA9aQOV/qg2L1cYxScQrQ/pKVOnYWJ4XuB0WL8gRYdo1bGI6LWGAtOV+fzVo
XU0SfWH7UmPcvttqkWsv1Rr50pspmJneXeY6Ge1szNsvyHqmPFJj7GAXnEKl9xthHK3IaDc6HEprFqYw8SyQqYWGdpeism2S+V4XpIMbQJlC06BxyOg94H0Fiffzs8wwnCUpBU0s69X2tN8sxb4U3FqKl28mwCOuuaweZeGWq5MWxU7Fop2dmjaKN+u/N8F",
          "accessKeyId": "ASIAZQNB3KHGNXWXBSJS",
          "expiration": "Nov 29, 2018 4:31:59 AM"
        }
      },
      "requestID": "6b7d6c60-f35d-11e8-becc-39e7d43d4afe",
      "eventID": "6177ca7e-860e-482c-bde9-50c735af58d6",
      "resources": [
        {
          "ARN": "arn:aws:iam::653711331788:role/level3",
          "accountId": "653711331788",
          "type": "AWS::IAM::Role"
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "653711331788",
      "sharedEventID": "1d18bf74-8392-4496-9dc4-a45cb799b8b4"
```

With the CloudTrail logs now readable, we can conduct incident response by searching for indicators of compromise within these log files. For instance, we can create a simple Bash script to search for all events filtered by their name and time as seen below:



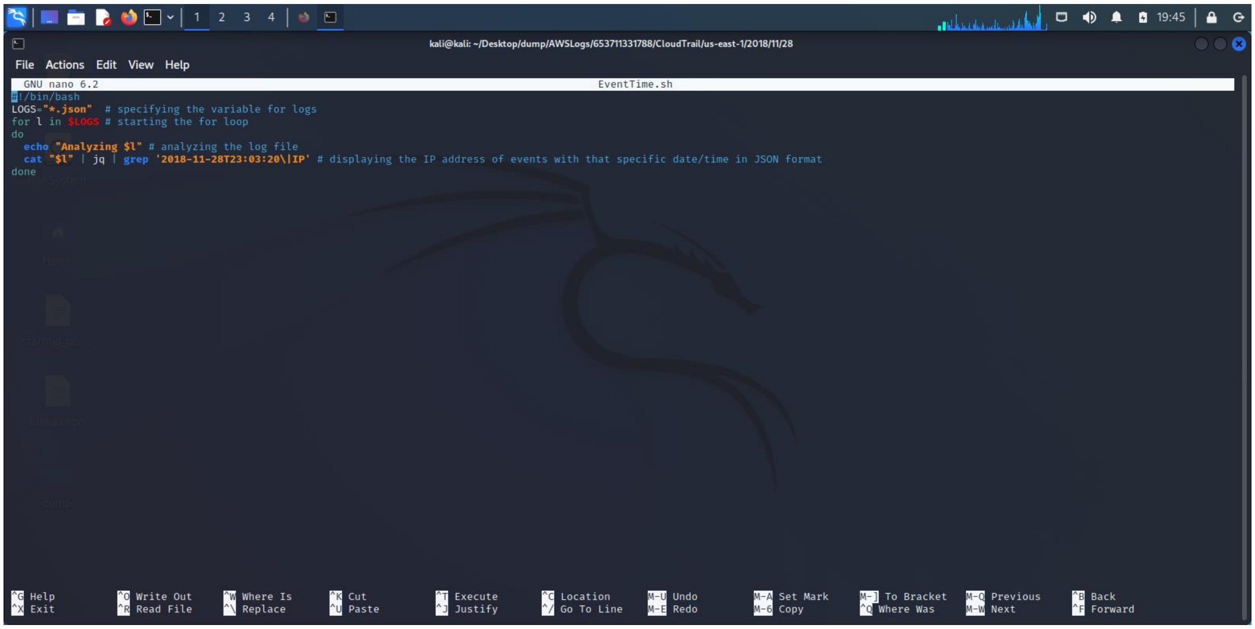
```
#!/bin/bash
LOGS="*.json" #specifying the variable for logs
for l in $LOGS # starting the for loop
do
  echo "Analyzing $l" # analyzing the log file
  cat "$l" | jq | grep eventTime # displaying the eventtime in JSON format
  cat "$l" | jq | grep eventName # displaying the eventname as well
done
```



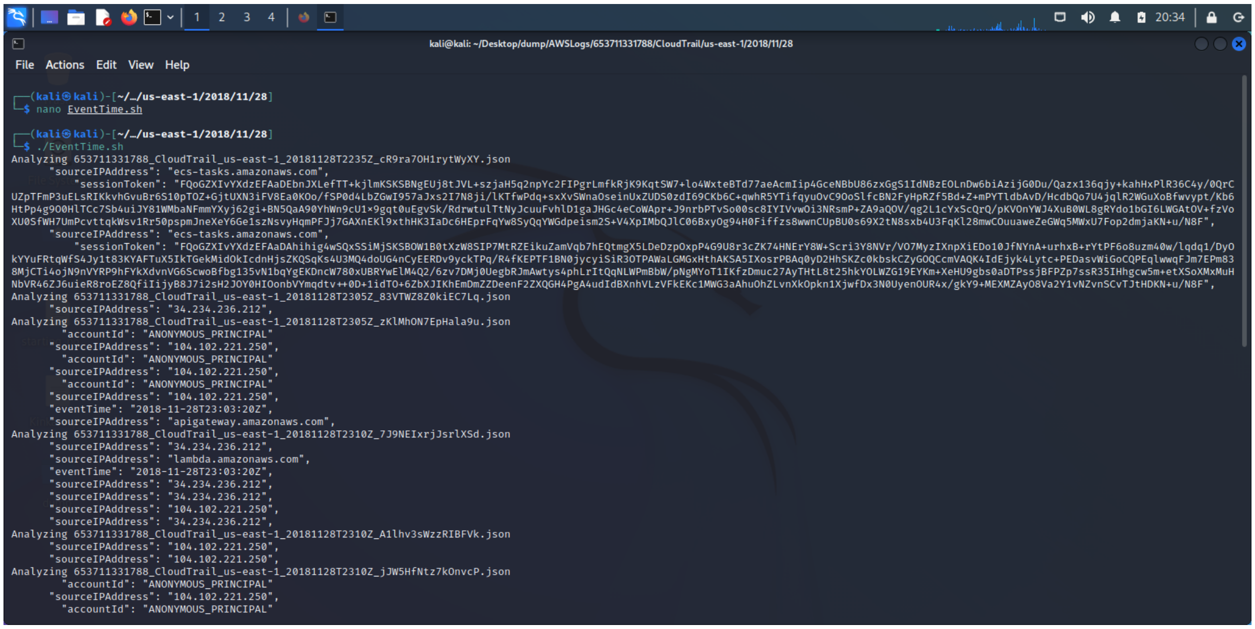
1 2 3 4
20:24
kali@kali: ~/Desktop/dump/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ nano EventTime.sh

┌──(kali㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ chmod 777 EventTime.sh

┌──(kali㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ ./EventTime.sh
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2235Z_cR9ra7OH1rytWyXY.json
      "eventTime": "2018-11-28T22:31:59Z",
      "eventTime": "2018-11-28T22:31:59Z",
      "eventName": "AssumeRole",
      "eventName": "AssumeRole",
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2305Z_83VTWZ8Z0kiEC7Lq.json
      "eventTime": "2018-11-28T23:03:12Z",
      "eventName": "CreateLogStream",
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2305Z_zKlMhON7EpHala9u.json
      "eventTime": "2018-11-28T23:02:56Z",
      "eventTime": "2018-11-28T23:03:08Z",
      "eventTime": "2018-11-28T23:03:11Z",
      "eventTime": "2018-11-28T23:03:20Z",
      "eventName": "GetObject",
      "eventName": "GetObject",
      "eventName": "GetObject",
      "eventName": "Invoke",
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2310Z_7J9NEIxrjJsrlXSd.json
      "eventTime": "2018-11-28T23:03:50Z",
      "eventTime": "2018-11-28T23:03:12Z",
      "eventTime": "2018-11-28T23:03:20Z",
      "eventTime": "2018-11-28T23:03:13Z",
      "eventTime": "2018-11-28T23:05:53Z",
      "eventTime": "2018-11-28T23:03:35Z",
      "eventName": "CreateLogStream",
      "eventName": "AssumeRole",
      "eventName": "CreateLogStream",
      "eventName": "CreateLogStream",
      "eventName": "ListImages",
      "eventName": "CreateLogStream",
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2310Z_A1lhv3sWzzRIBFVk.json
      "eventTime": "2018-11-28T23:06:17Z",
      "eventTime": "2018-11-28T23:06:33Z",
      "eventName": "BatchGetImage",
```

As we see in the second image above, there seems to be a bunch of events being logged at that specific date and time. To conduct further analysis, we can then modify our Bash script to search for any IP addresses associated with those event times as seen below:

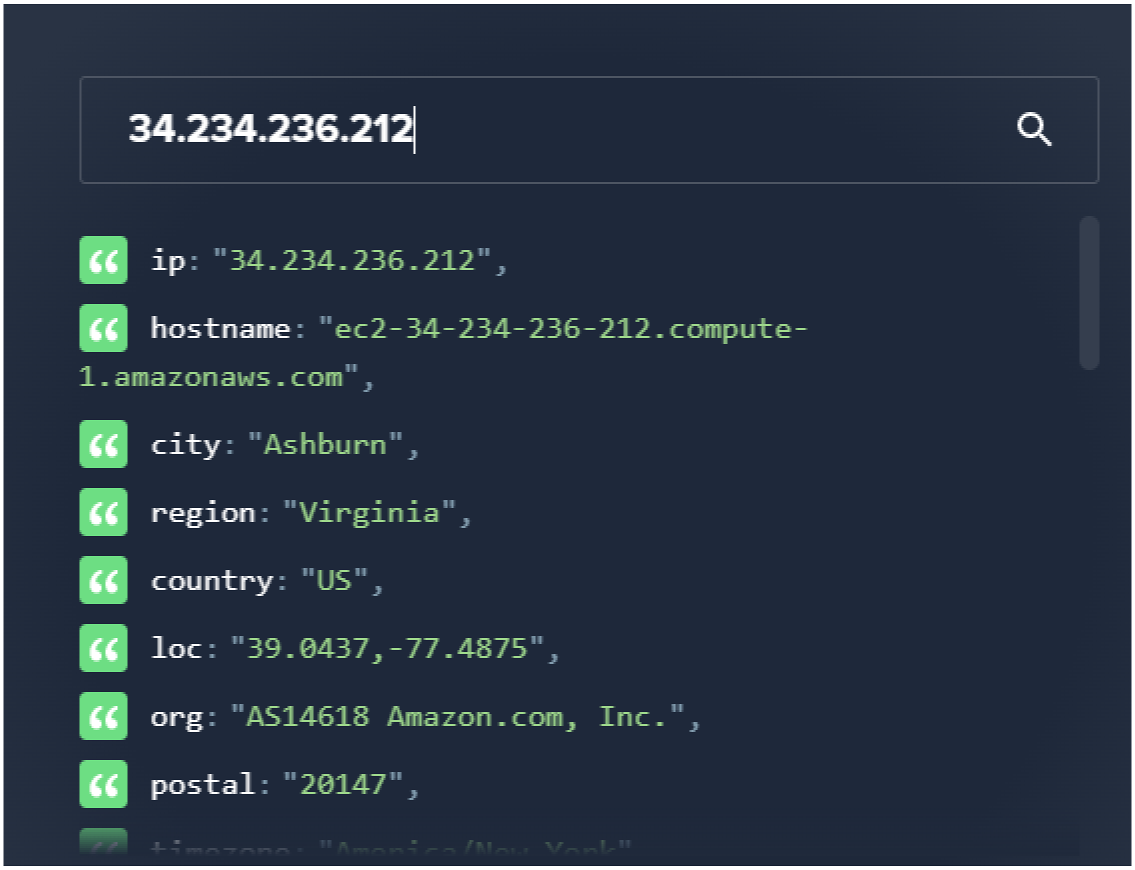

kali@kali: ~/Desktop/dump/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28
File Actions Edit View Help
GNU nano 6.2
EventTime.sh
^G Help ^X Exit
^O Write Out ^R Read File
^W Where Is ^\ Replace
^K Cut ^U Paste
^T Execute ^J Justify
^C Location ^/ Go To Line
M-U Undo M-E Redo
M-A Set Mark M-6 Copy
M-] To Bracket ^Q Where Was
M-Q Previous M-W Next
^B Back ^F Forward

```
#!/bin/bash
LOGS="*.json"  # specifying the variable for logs
for l in $LOGS # starting the for loop
do
  echo "Analyzing $l" # analyzing the log file
  cat "$l" | jq | grep '2018-11-28T23:03:20\|IP' # displaying the IP address of events with that specific date/time in JSON format
done
```


kali@kali: ~/Desktop/dump/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28
File Actions Edit View Help

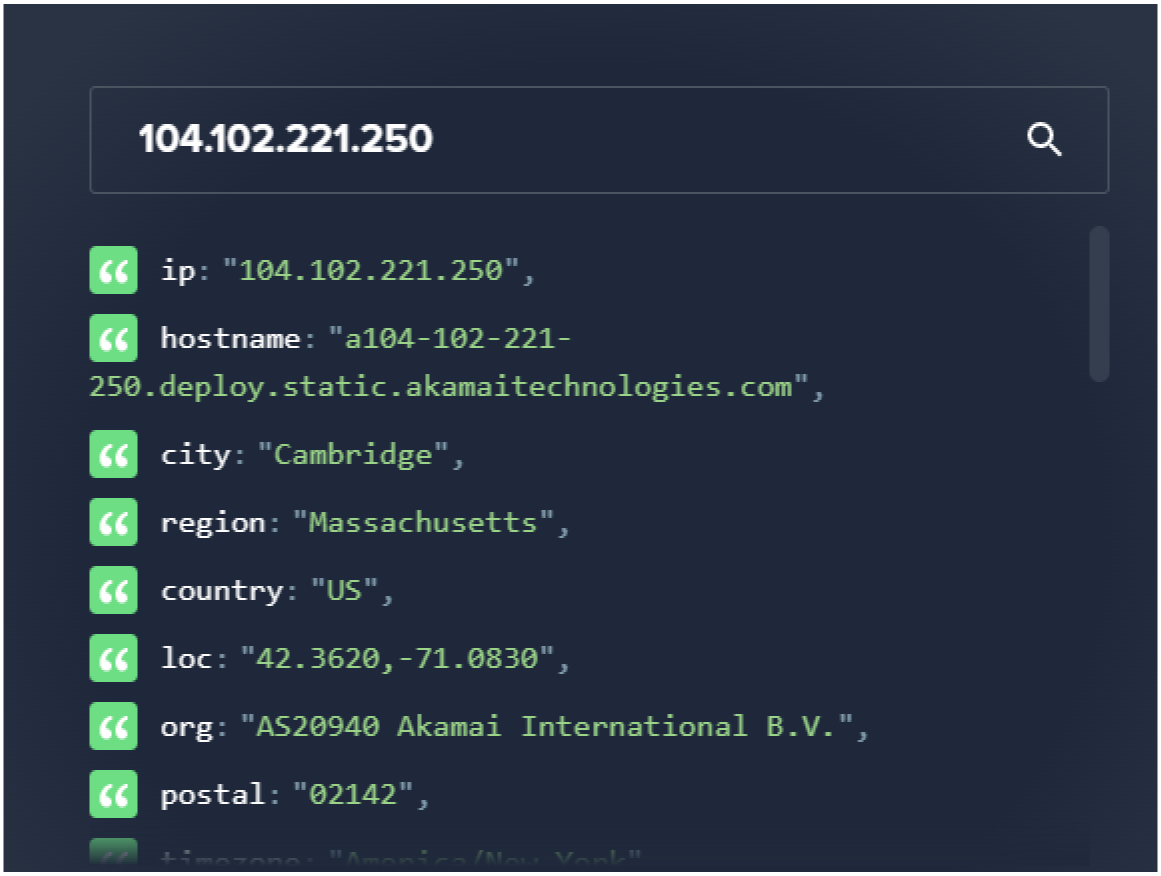
```
┌──(kali㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ nano EventTime.sh

┌──(kali㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ ./EventTime.sh
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2235Z_cR9ra7OH1rytWyXY.json
      "sourceIPAddress": "ecs-tasks.amazonaws.com",
          "sessionToken": "FQoGZXIvYXdzEFAaDEbnJXLefTT+kjlmKSKSBNgEUj8tJVL+szjaH5q2npYc2FIPgrLmfkRjK9KqtSW7+lo4WxteBTd77aeAcmIip4GceNBbU86zxGgS1IdNBzEOLnDw6biAzijG0Du/Qazx136qjy+kahHxPlR36C4y/0QrC
UZpTFmP3uELsRIKkvhGvuBr6S10pTOZ+GjtUXN3iFV8Ea0KOo/fSP0d4LbZGwI957aJxs2I7N8ji/lKTfwPdq+sxXvSWnaOseinUxZUDS0zdI69CKb6C+qwhR5YTifqyuOvC9OoSlfcBN2FyHpRZf5Bd+Z+mPYTldbAvD/HcdbQo7U4jqlR2WGuXoBfwvypt/Kb6
HtPp4g9O0HlTCc7Sb4uiJY81WMbaNFmmYXyj62gi+BN5QaA90YhWn9cU1x9gqt0uEgvSk/RdrwtulTtNyJcuuFvhlD1gaJHGc4eCoWApr+J9nrbPTvSo00sc8IYIVvwOi3NRsmP+ZA9aQOV/qg2L1cYxScQrQ/pKVOnYWJ4XuB0WL8gRYdo1bGI6LWGAtOV+fzVo
XU0SfWH7UmPcvttqkWsv1Rr50pspmJneXeY6Ge1szNsvyHqmPFJj7GAXnEKl9xthHK3IaDc6HEprFqYw8SyQqYWGdpeism2S+V4XpIMbQJlC06BxyOg94H0Fiffzs8wwnCUpBU0s69X2tN8sxb4U3FqKl28mwCOuuaweZeGWq5MWxU7Fop2dmjaKN+u/N8F",
      "sourceIPAddress": "ecs-tasks.amazonaws.com",
          "sessionToken": "FQoGZXIvYXdzEFAaDAhihig4wSQxSSiMjSKSBOW1B0tXzW8SIP7MtRZEikuZamVqb7hEQtmgX5LDeDzpOxpP4G9U8r3cZK74HNErY8W+Scri3Y8NVr/VO7MyzIXnpXiEDo10JfNYnA+urhxB+rYtPF6o8uzm40w/lqdq1/DyO
kYYuFRtqWfS4Jy1t83KYAFTuX5IkTGekMidOkIcdnHjsZKQSqKs4U3MQ4doUG4nCyEERDv9ycktTPq/R4fKEPTF1BN0jycyiSiR3OTPAWaLGMGxHthAKSA5IXosrPBAq0yD2HhSKZc0kbskCZyGOQCcmVAQK4IdEjyk4Lytc+PEDasvWiGoCQPEqlwwqFJm7EPm83
8MjCTi4ojN9nVYRP9hFYkXdvnVG6ScwoBfbg135vN1bqYgEKDncW780xUBRYwElM4Q2/6zv7DMj0UegbRJmAwtys4phLrItQqNLWPmBbW/pNgMYoT1IKfzDmuc27AyTHtL8t25hkYOLWZG19EYKm+XeHU9gbs0aDTPssjBFPZp7ssR35IHhgcw5m+etXSoXMxMuH
NbVR46ZJ6uieR8roEZ8QfiIijyB8J7i2sH2JOY0HIOonbVYmqdtv++0D+1idTO+6ZbXJIKhEmDmZZDeenF2ZXQGH4PgA4udIdBXnhVLzVFkEKc1MWG3aAhuOhZLvnXkOpkn1XjwfDx3N0UyenOUR4x/gkY9+MEXMZAyO8Va2Y1vNZvnSCvTJtHDKN+u/N8F",
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2305Z_83VTWZ8Z0kiEC7Lq.json
      "sourceIPAddress": "34.234.236.212",
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2305Z_zKlMhON7EpHala9u.json
        "accountId": "ANONYMOUS_PRINCIPAL"
      "sourceIPAddress": "104.102.221.250",
        "accountId": "ANONYMOUS_PRINCIPAL"
      "sourceIPAddress": "104.102.221.250",
        "accountId": "ANONYMOUS_PRINCIPAL"
      "sourceIPAddress": "104.102.221.250",
      "eventTime": "2018-11-28T23:03:20Z",
      "sourceIPAddress": "apigateway.amazonaws.com",
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2310Z_7J9NEIxrjJsrlXSd.json
      "sourceIPAddress": "34.234.236.212",
      "sourceIPAddress": "lambda.amazonaws.com",
      "eventTime": "2018-11-28T23:03:20Z",
      "sourceIPAddress": "34.234.236.212",
      "sourceIPAddress": "34.234.236.212",
      "sourceIPAddress": "104.102.221.250",
      "sourceIPAddress": "34.234.236.212",
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2310Z_A1lhv3sWzzRIBFVk.json
      "sourceIPAddress": "104.102.221.250",
      "sourceIPAddress": "104.102.221.250",
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2310Z_jJW5HfNtz7kOnvcP.json
        "accountId": "ANONYMOUS_PRINCIPAL"
      "sourceIPAddress": "104.102.221.250",
        "accountId": "ANONYMOUS_PRINCIPAL"
```

From the results in the second image above, it looks like there are two different IP addresses associated with these events occurring relatively close to each other. Using a domain lookup website, we can see that one of the source IP addresses is not from Amazon, but from Akamai instead, which would be considered as an indicator of compromised given it is not associated with Amazon's AWS as seen below:



34.234.236.212

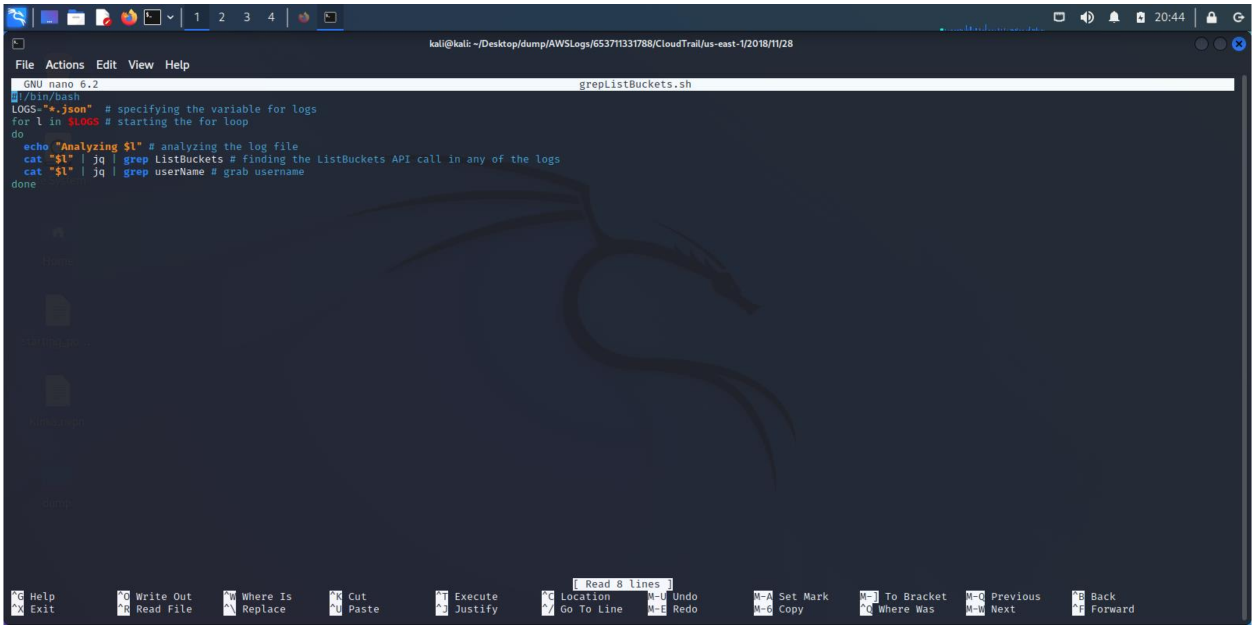
```
ip: "34.234.236.212",
hostname: "ec2-34-234-236-212.compute-
1.amazonaws.com",
city: "Ashburn",
region: "Virginia",
country: "US",
loc: "39.0437,-77.4875",
org: "AS14618 Amazon.com, Inc.",
postal: "20147",
timezone: "America/New_York"
```



104.102.221.250

```
ip: "104.102.221.250",
hostname: "a104-102-221-250.deploy.static.akamaitechnologies.com",
city: "Cambridge",
region: "Massachusetts",
country: "US",
loc: "42.3620,-71.0830",
org: "AS20940 Akamai International B.V.",
postal: "02142",
timezone: "America/New_York"
```

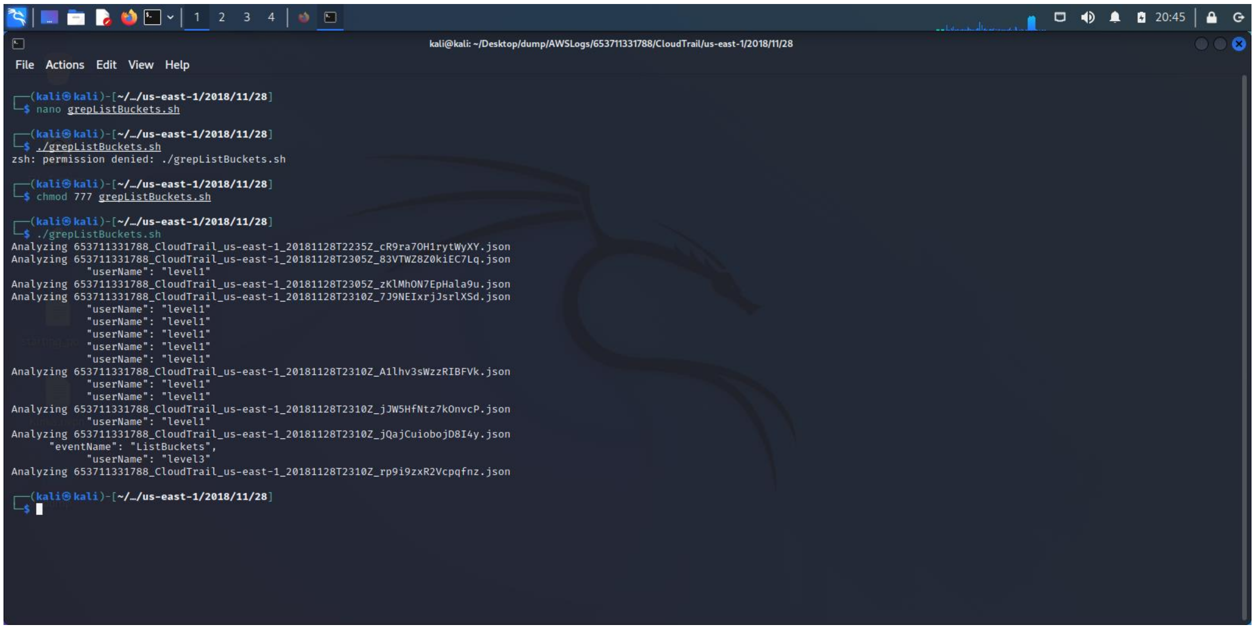
Continuing with conducting incident response, we can create a new Bash script that can search through the logs for any users who invoke the listBuckets API call, which can be seen as suspicious and a potential indicator of compromise. The Bash script and the user identified can be seen below:



kali@kali: ~/Desktop/dump/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28

```
#!/bin/bash
LOGS="*.json"  # specifying the variable for logs
for l in $LOGS # starting the for loop
do
  echo "Analyzing $l" # analyzing the log file
  cat "$l" | jq | grep ListBuckets # finding the ListBuckets API call in any of the logs
  cat "$l" | jq | grep userName # grab username
done
```

[Read 8 lines]



1
2
3
4
20:45
kali@kali: ~/Desktop/dump/AWSLogs/653711331788/CloudTrail/us-east-1/2018/11/28
File
Actions
Edit
View
Help

```
┌──(kali㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ nano grepListBuckets.sh

┌──(kali㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ ./grepListBuckets.sh
zsh: permission denied: ./grepListBuckets.sh

┌──(kali㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ chmod 777 grepListBuckets.sh

┌──(kali㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ ./grepListBuckets.sh
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2235Z_cR9ra7OH1rytWyXY.json
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2305Z_83VTWZ8Z0kiEC7Lq.json
            "userName": "level1"
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2305Z_zKlMhON7EpHala9u.json
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2310Z_7J9NEIxrjJsrlXSd.json
            "userName": "level1"
            "userName": "level1"
            "userName": "level1"
            "userName": "level1"
            "userName": "level1"
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2310Z_A1lhv3sWzzRIBFVk.json
            "userName": "level1"
            "userName": "level1"
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2310Z_jJW5HfNtz7kOnvcP.json
            "userName": "level1"
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2310Z_jQajCuiobojD8I4y.json
      "eventName": "ListBuckets",
            "userName": "level3"
Analyzing 653711331788_CloudTrail_us-east-1_20181128T2310Z_rp9i9zxR2Vcpqfnz.json

┌──(kali㉿kali)-[~/…/us-east-1/2018/11/28]
└─$ 
```

The user “level3” is the only user that invoked the listBuckets API call as seen in the second image above.

Next Steps

With this lab introducing how to conduct incident response within a cloud environment, I plan on looking around and analyzing more aspects of the CloudTrail logs while learning more about AWS and their services in general. In addition, this lab has introduced the usage of Bash scripts for me, which I will consider learning on improving my scripting skills in Bash for the future.