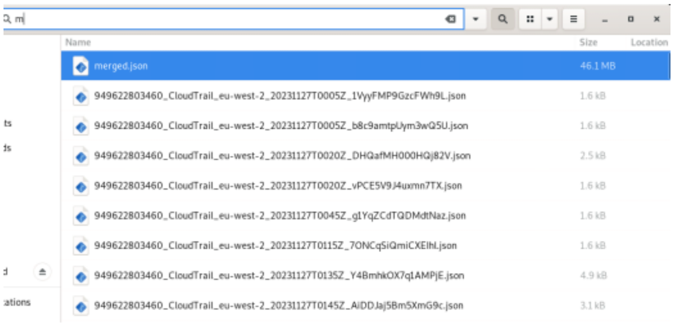
OpTinselTrace-2 Challenge

Sherlock Scenario

It seems our precious technology has been leaked to the threat actor. Our head Elf, PixelPepermint, seems to think that there were some hard-coded sensitive URLs within the technology sent. Please audit our Sparky Cloud logs and confirm if anything was stolen! PS - Santa likes his answers in UTC... Please note - these Sherlocks are built to be completed sequentially and in order!

***After downloading the files I copied and pasted all the json files together in one folder and used the commmand**
find . -name "*.json" -exec cat {} + | jq -s '.' > merged.json
To parsed all the files together*

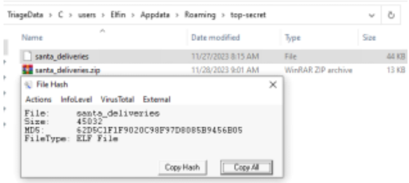


```
Name                                                                      Size
merged.json                                                               46.1 MB
949622803460_CloudTrail_eu-west-2_20231127T0005Z_1VyyFMP9GzcFWh9L.json    1.6 kB
949622803460_CloudTrail_eu-west-2_20231127T0005Z_b8c9amtpUym3wQ5U.json    1.6 kB
949622803460_CloudTrail_eu-west-2_20231127T0020Z_DHQafMH000HQj82V.json    2.5 kB
949622803460_CloudTrail_eu-west-2_20231127T0020Z_vPCE5V9J4uxmn7TX.json    1.6 kB
949622803460_CloudTrail_eu-west-2_20231127T0045Z_g1YqZCdTQDMdtNaz.json    1.6 kB
949622803460_CloudTrail_eu-west-2_20231127T0115Z_7ONCqSiQmiCXElhl.json    1.6 kB
949622803460_CloudTrail_eu-west-2_20231127T0135Z_Y4BmhkOX7q1AMPjE.json    4.9 kB
949622803460_CloudTrail_eu-west-2_20231127T0145Z_AiDDJaj5Bm5XmG9c.json    3.1 kB
```

Task 1:
What is the MD5 sum of the binary the Threat Actor found the S3 bucket location in?

In the first challenge the exfiltrated file the user sent to the attacker is located at "elfidence_collection \TriageData\C\users\Elfin\Appdata\Roaming\top-secret"

I checked the MD5 of the santa_deliveries



TriageData › C › users › Elfin › Appdata › Roaming › top-secret

Name	Date modified	Type	Size
santa_deliveries	11/27/2023 8:15 AM	File	44 KB
santa_deliveries.zip	11/28/2023 9:01 AM	WinRAR ZIP archive	13 KB

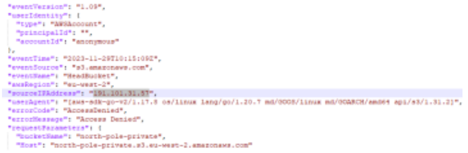
```
File:     santa_deliveries
Size:     45032
MD5:      62D5C1F1F9020C98F97D8085B9456B05
FileType: ELF File
```

Answer: 62d5c1f1f9020c98f97d8085b9456b05

Task 2:
What time did the Threat Actor begin their automated retrieval of the contents of our exposed S3 bucket?

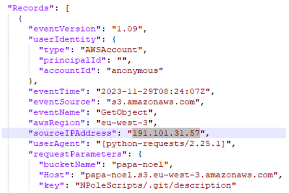
This task and task 3 are the last ones I completed so I used my other answers to complete this tasks

I searched for the source attacker IP 191.101.31.57 and found some logs with AccessDenied



```
"eventVersion": "1.09",
"userIdentity": {
  "type": "AWSAccount",
  "principalId": "",
  "accountId": "anonymous"
},
"eventTime": "2023-11-29T10:15:09Z",
"eventSource": "s3.amazonaws.com",
"eventName": "HeadBucket",
"awsRegion": "eu-west-2",
"sourceIPAddress": "191.101.31.57",
"userAgent": "[aws-sdk-go-v2/1.17.8 os/linux lang/go/1.20.7 md/GOOS/linux md/GOARCH/amd64 api/s3/1.31.2]",
"errorCode": "AccessDenied",
"errorMessage": "Access Denied",
"requestParameters": {
  "bucketName": "north-pole-private",
  "Host": "north-pole-private.s3.eu-west-2.amazonaws.com"
```

Then I scrolled down to other logs and found a log with the S3 bucket name papa-noel which was the last answer of the challenge with eventName "GetObject" so I assumed this Is the first retrieval of the contents.

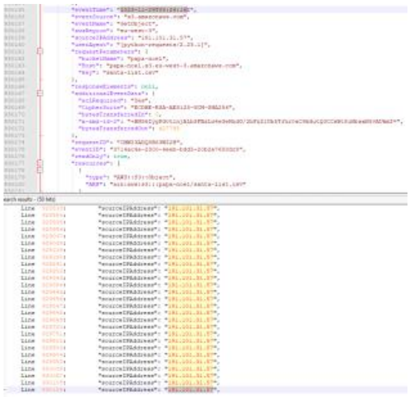


```
"Records": [
  {
    "eventVersion": "1.09",
    "userIdentity": {
      "type": "AWSAccount",
      "principalId": "",
      "accountId": "anonymous"
    },
    "eventTime": "2023-11-29T08:24:07Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "GetObject",
    "awsRegion": "eu-west-3",
    "sourceIPAddress": "191.101.31.57",
    "userAgent": "[python-requests/2.25.1]",
    "requestParameters": {
      "bucketName": "papa-noel",
      "Host": "papa-noel.s3.eu-west-3.amazonaws.com",
      "key": "NPoleScripts/.git/description"
```

Answer: 2023-11-29 08:24:07

Task 3:
What time did the Threat Actor complete their automated retrieval of the contents of our exposed S3 bucket?

Just like task 2, I kept scrolling down the logs and found all the files the attacker retrieved and also found the file answer for task 5 which I didn't answered.
I kept scrolling until the last log and found the complete automated timestamp



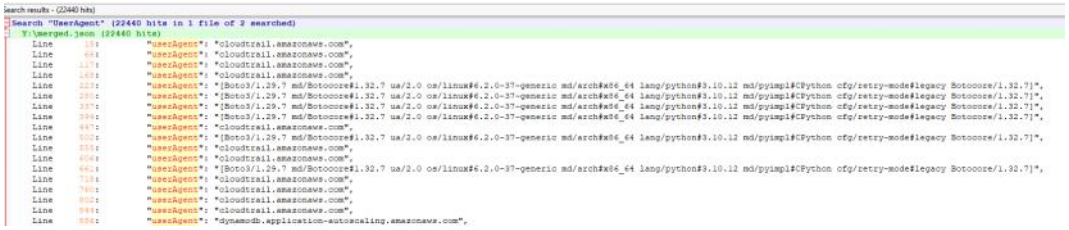
```
"eventTime": "2023-11-29T08:24:16Z",
"eventSource": "s3.amazonaws.com",
"eventName": "GetObject",
"awsRegion": "eu-west-3",
"sourceIPAddress": "191.101.31.57",
"userAgent": "[python-requests/2.25.1]",
"requestParameters": {
  "bucketName": "papa-noel",
  "Host": "papa-noel.s3.eu-west-3.amazonaws.com",
  "key": "santa-list.csv"
},
"responseElements": null,
"additionalEventData": {
  "aclRequired": "Yes",
  "CipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "bytesTransferredIn": 0,
  "x-amz-id-2": "[illegible]",
  "bytesTransferredOut": [illegible]
},
"requestID": "[illegible]",
"eventID": "[illegible]",
"readOnly": true,
"resources": [
  {
    "type": "AWS::S3::Object",
    "ARN": "arn:aws:s3:::papa-noel/santa-list.csv"
```

```
earch results - (50 hits)
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
    Line [illegible]:        "sourceIPAddress": "191.101.31.57",
```

Answer: 2023-11-29 08:24:16

Task 4:
Based on the Threat Actor's user agent - what scripting language did the TA likely utilise to retrieve the files?

I opened the merged.json file with Notepad++ and searched for UserAgent and found the unusual user agent

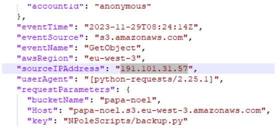


```
Search results - (22440 hits)
Search "UserAgent" (22440 hits in 1 file of 2 searched)
  Y:\merged.json (22440 hits)
    Line    15:        "userAgent": "cloudtrail.amazonaws.com",
    Line    68:        "userAgent": "cloudtrail.amazonaws.com",
    Line   117:        "userAgent": "cloudtrail.amazonaws.com",
    Line   162:        "userAgent": "cloudtrail.amazonaws.com",
    Line   223:        "userAgent": "[Boto3/1.29.7 md/Botocore#1.32.7 ua/2.0 os/linux#6.2.0-37-generic md/arch#x86_64 lang/python#3.10.12 md/pyimpl#CPython cfg/retry-mode#legacy Botocore/1.32.7]",
    Line   280:        "userAgent": "[Boto3/1.29.7 md/Botocore#1.32.7 ua/2.0 os/linux#6.2.0-37-generic md/arch#x86_64 lang/python#3.10.12 md/pyimpl#CPython cfg/retry-mode#legacy Botocore/1.32.7]",
    Line   337:        "userAgent": "[Boto3/1.29.7 md/Botocore#1.32.7 ua/2.0 os/linux#6.2.0-37-generic md/arch#x86_64 lang/python#3.10.12 md/pyimpl#CPython cfg/retry-mode#legacy Botocore/1.32.7]",
    Line   394:        "userAgent": "[Boto3/1.29.7 md/Botocore#1.32.7 ua/2.0 os/linux#6.2.0-37-generic md/arch#x86_64 lang/python#3.10.12 md/pyimpl#CPython cfg/retry-mode#legacy Botocore/1.32.7]",
    Line   447:        "userAgent": "cloudtrail.amazonaws.com",
    Line   502:        "userAgent": "[Boto3/1.29.7 md/Botocore#1.32.7 ua/2.0 os/linux#6.2.0-37-generic md/arch#x86_64 lang/python#3.10.12 md/pyimpl#CPython cfg/retry-mode#legacy Botocore/1.32.7]",
    Line   555:        "userAgent": "cloudtrail.amazonaws.com",
    Line   606:        "userAgent": "cloudtrail.amazonaws.com",
    Line   661:        "userAgent": "[Boto3/1.29.7 md/Botocore#1.32.7 ua/2.0 os/linux#6.2.0-37-generic md/arch#x86_64 lang/python#3.10.12 md/pyimpl#CPython cfg/retry-mode#legacy Botocore/1.32.7]",
    Line   718:        "userAgent": "cloudtrail.amazonaws.com",
    Line   760:        "userAgent": "cloudtrail.amazonaws.com",
    Line   802:        "userAgent": "cloudtrail.amazonaws.com",
    Line   844:        "userAgent": "cloudtrail.amazonaws.com",
    Line   886:        "userAgent": "dynamodb.application-autoscaling.amazonaws.com",
```

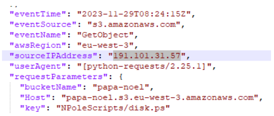
Answer: python

Task 5:
Which file did the Threat Actor locate some hard coded credentials within?

I found this answer while searching for the answer in task 3.
While scrolling down looking at the files that the attacker was retrieving I found several files which was suspicious like disk.ps, backup.py, claus.py

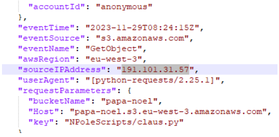


```
    "accountId": "anonymous"
  },
  "eventTime": "2023-11-29T08:24:14Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "GetObject",
  "awsRegion": "eu-west-3",
  "sourceIPAddress": "191.101.31.57",
  "userAgent": "[python-requests/2.25.1]",
  "requestParameters": {
    "bucketName": "papa-noel",
    "Host": "papa-noel.s3.eu-west-3.amazonaws.com",
    "key": "NPoleScripts/backup.py"
```



```
"eventTime": "2023-11-29T08:24:15Z",
"eventSource": "s3.amazonaws.com",
"eventName": "GetObject",
"awsRegion": "eu-west-3",
"sourceIPAddress": "191.101.31.57",
"userAgent": "[python-requests/2.25.1]",
"requestParameters": {
  "bucketName": "papa-noel",
  "Host": "papa-noel.s3.eu-west-3.amazonaws.com",
  "key": "NPoleScripts/disk.ps"
```

I tried both files but the correct one was claus.py



```
    "accountId": "anonymous"
  },
  "eventTime": "2023-11-29T08:24:15Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "GetObject",
  "awsRegion": "eu-west-3",
  "sourceIPAddress": "191.101.31.57",
  "userAgent": "[python-requests/2.25.1]",
  "requestParameters": {
    "bucketName": "papa-noel",
    "Host": "papa-noel.s3.eu-west-3.amazonaws.com",
    "key": "NPoleScripts/claus.py"
```

Answer: claus.py

Task 6:

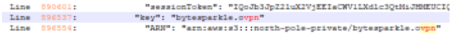
The first malicious IP I found was 191.101.31.57 when I searched for the UserAgent so I also checked if it was malicious.
The second malicious IP I found is after I completed task 7.

Answer: 45.133.193.41, 191.101.31.57

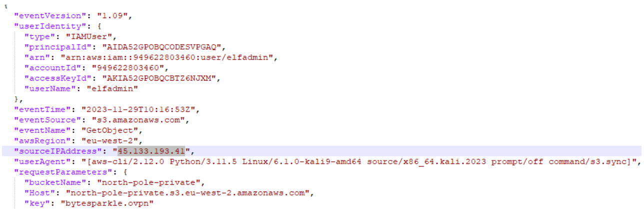
Task 7:
We are extremely concerned the TA managed to compromise our private S3 bucket, which contains an important VPN file. Please confirm the name of this VPN file and the time it was retrieved by the TA.

I completed this task before completing task 6 so I also found the malicious IP

I searched the word VPN in the logs and checked the source IP and found that this IP is malicious and also a file name with the extension of .ovpn



```
 Line  590601:              "sessionToken": "IQoJb3JpZ2luX2VjEEIaCWV1LXdlc3QtMiJHMEUCI(
 Line  596537:            "key": "bytesparkle.ovpn"
 Line  596554:              "ARN": "arn:aws:s3:::north-pole-private/bytesparkle.ovpn"
```

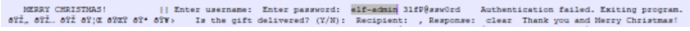


```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDA52GPOBQCODESVPGAQ",
    "arn": "arn:aws:iam::949622803460:user/elfadmin",
    "accountId": "949622803460",
    "accessKeyId": "AKIA52GPOBQCBTZ6NJXM",
    "userName": "elfadmin"
  },
  "eventTime": "2023-11-29T10:16:53Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "GetObject",
  "awsRegion": "eu-west-2",
  "sourceIPAddress": "45.133.193.41",
  "userAgent": "[aws-cli/2.12.0 Python/3.11.5 Linux/6.1.0-kali9-amd64 source/x86_64.kali.2023 prompt/off command/s3.sync]",
  "requestParameters": {
    "bucketName": "north-pole-private",
    "Host": "north-pole-private.s3.eu-west-2.amazonaws.com",
    "key": "bytesparkle.ovpn"
```

Answer: bytesparkle.ovpn, 2023-11-29 10:16:53

Task 8:
Please confirm the username of the compromised AWS account?

I searched the exfiltrated file santa_deliveries and found a username and password

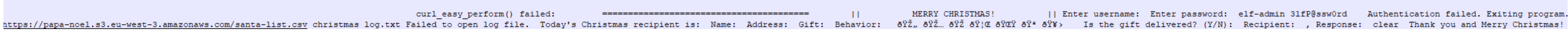


```
    MERRY CHRISTMAS!          || Enter username:  Enter password:  elf-admin 31fP@ssw0rd    Authentication failed. Exiting program.
 ðŸŽ„ ðŸŽ… ðŸŽ ðŸ¦Œ ðŸŒŸ ðŸª ðŸ¥›    Is the gift delivered? (Y/N):  Recipient:  , Response:  clear  Thank you and Merry Christmas!
```

Answer: elfadmin

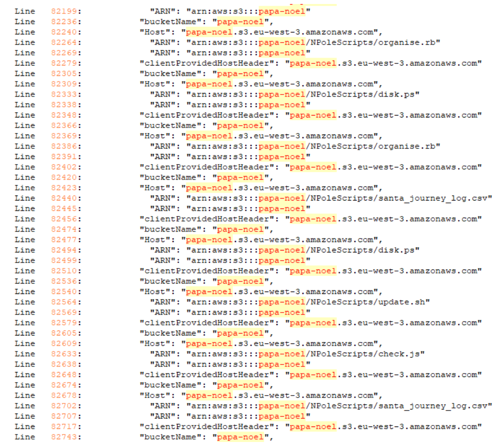
Task 9:
Based on the analysis completed Santa Claus has asked for some advice. What is the ARN of the S3
Bucket that requires locking down?

I checked the santa_deliveries file once again near the username and password and I noticed a link with
s3.amazonaws.com named papa-noel



```
                                                                                  curl_easy_perform() failed:         ========================================        ||          MERRY CHRISTMAS!          || Enter username:  Enter password:  elf-admin 31fP@ssw0rd    Authentication failed. Exiting program.
https://papa-noel.s3.eu-west-3.amazonaws.com/santa-list.csv christmas log.txt Failed to open log file.  Today's Christmas recipient is:  Name:  Address:  Gift:  Behavior:   ðŸŽ„ ðŸŽ… ðŸŽ ðŸ¦Œ ðŸŒŸ ðŸª ðŸ¥›    Is the gift delivered? (Y/N):  Recipient:  , Response:  clear  Thank you and Merry Christmas!
```

Then I searched papa-noel in the merged.json and found several file names with this S3 so I copied the
ARN name



```
   Line   82199:              "ARN": "arn:aws:s3:::papa-noel"
   Line   82236:            "bucketName": "papa-noel",
   Line   82240:            "Host": "papa-noel.s3.eu-west-3.amazonaws.com",
   Line   82264:              "ARN": "arn:aws:s3:::papa-noel/NPoleScripts/organise.rb"
   Line   82269:              "ARN": "arn:aws:s3:::papa-noel"
   Line   82279:            "clientProvidedHostHeader": "papa-noel.s3.eu-west-3.amazonaws.com"
   Line   82305:            "bucketName": "papa-noel",
   Line   82309:            "Host": "papa-noel.s3.eu-west-3.amazonaws.com",
   Line   82333:              "ARN": "arn:aws:s3:::papa-noel/NPoleScripts/disk.ps"
   Line   82338:              "ARN": "arn:aws:s3:::papa-noel"
   Line   82348:            "clientProvidedHostHeader": "papa-noel.s3.eu-west-3.amazonaws.com"
   Line   82366:            "bucketName": "papa-noel",
   Line   82369:            "Host": "papa-noel.s3.eu-west-3.amazonaws.com",
   Line   82386:              "ARN": "arn:aws:s3:::papa-noel/NPoleScripts/organise.rb"
   Line   82391:              "ARN": "arn:aws:s3:::papa-noel"
   Line   82402:            "clientProvidedHostHeader": "papa-noel.s3.eu-west-3.amazonaws.com"
   Line   82420:            "bucketName": "papa-noel",
   Line   82423:            "Host": "papa-noel.s3.eu-west-3.amazonaws.com",
   Line   82440:              "ARN": "arn:aws:s3:::papa-noel/NPoleScripts/santa_journey_log.csv"
   Line   82445:              "ARN": "arn:aws:s3:::papa-noel"
   Line   82456:            "clientProvidedHostHeader": "papa-noel.s3.eu-west-3.amazonaws.com"
   Line   82474:            "bucketName": "papa-noel",
   Line   82477:            "Host": "papa-noel.s3.eu-west-3.amazonaws.com",
   Line   82494:              "ARN": "arn:aws:s3:::papa-noel/NPoleScripts/disk.ps"
   Line   82499:              "ARN": "arn:aws:s3:::papa-noel"
   Line   82510:            "clientProvidedHostHeader": "papa-noel.s3.eu-west-3.amazonaws.com"
   Line   82536:            "bucketName": "papa-noel",
   Line   82540:            "Host": "papa-noel.s3.eu-west-3.amazonaws.com",
   Line   82564:              "ARN": "arn:aws:s3:::papa-noel/NPoleScripts/update.sh"
   Line   82569:              "ARN": "arn:aws:s3:::papa-noel"
   Line   82579:            "clientProvidedHostHeader": "papa-noel.s3.eu-west-3.amazonaws.com"
   Line   82605:            "bucketName": "papa-noel",
   Line   82609:            "Host": "papa-noel.s3.eu-west-3.amazonaws.com",
   Line   82633:              "ARN": "arn:aws:s3:::papa-noel/NPoleScripts/check.js"
   Line   82638:              "ARN": "arn:aws:s3:::papa-noel"
   Line   82648:            "clientProvidedHostHeader": "papa-noel.s3.eu-west-3.amazonaws.com"
   Line   82674:            "bucketName": "papa-noel",
   Line   82678:            "Host": "papa-noel.s3.eu-west-3.amazonaws.com",
   Line   82702:              "ARN": "arn:aws:s3:::papa-noel/NPoleScripts/santa_journey_log.csv"
   Line   82707:              "ARN": "arn:aws:s3:::papa-noel"
   Line   82717:            "clientProvidedHostHeader": "papa-noel.s3.eu-west-3.amazonaws.com"
   Line   82743:            "bucketName": "papa-noel",
```

Answer: arn:aws:s3:::papa-noel